híradástechnika

VOLUME L.

1999/10

50th ANNIVERSARY

journal on
C5
communications
computers
convergence
contents
companies

JOURNAL ON C^5

A PUBLICATION OF THE SCIENTIFIC SOCIETY FOR TELECOMMUNICATIONS, HUNGARY

Szerkesztőség / Editorial office
HÍRADÁSTECHNIKA
1061 Budapest, Paulay E. u. 56. II.14/A.
Telefon:(361) 341-6421, (361) 470-0713
Fax: (361) 341-6421, (361) 470-0713

Előfizetés / Orders to
Híradástechnikai Tudományos Egyesület
1055 Budapest, Kossuth tér 6-8.
Tel./Fax: (361) 353-1027

*** 2000. január 30-ig 50% kedvezmény.**

2000-es ELŐFIZETÉSI DÍJAK (12 szám + 1 CD)
Hazai közületi előfizetők részére
1 évre 20000 Ft +12% ÁFA = Btto 22400 Ft
Hazai egyéni előfizetők részére*
1 évre 4000 Ft +12% ÁFA = Btto 4480 Ft
HTE tag előfizetők részére
1 évre 2000 Ft +12% ÁFA = Btto 2240 Ft

Subscription rates for foreign subscribers in 2000
(12 issues + 1 CD) 100 USD, single copies 10 USD
Transfer should be made to the Scientific Society for Telecommunications
H-1055 Budapest, Kossuth tér 6-8.

HÍRADÁSTECHNIKA, JOURNAL ON C^5 is published monthly, in English and in Hungarian by Regiszter Kft.
H-1164 Budapest, Csókakő u. 27. Phone: (361) 400-2166, 400-2167, Fax: 400-2168.
Type-setting by HTE. Printed by Regiszter Kft.

HU ISSN 0018-2028

HÍRADÁSTECHNIKA

JOURNAL ON C5

Vol. L. No. 10, OCTOBER, 1999
HU ISSN 0018-2028

50 years

from the Telecommunications Scientific Society

e-commerce@special.issue

Abstract: In this issue 5 papers are presented. The first 4 tutorial in-depth papers on E-commerce are written in English. The last paper of this issue is a critical review of our technical environment with special outlook to the mixing problems of English and Hungarian languages.

E-COMMERCE TRENDS

TAMÁS SZABAD

DEPARTMENT OF ELECTROMAGNETIC THEORY, TECHNICAL UNIVERSITY OF BUDAPEST
H-1111 BUDAPEST, EGRY J. U. 18.
E-MAIL: SZABADT@SCH.BME.HU

In this article the emphasis is made on the future trends of electronic commerce. The current market of electronic commerce in Europe will be presented, and then a comprehensive overview of E-commerce is given. Analysing the different aspects of the key trends, the issues and concepts that need to be addressed in the millennium are highlighted.

1. INTRODUCTION

There was a remarkable growth in E-commerce infrastructure and services between 1996 and 1999. Today, as the number of Internet users increases there is a worldwide change in doing business. A lot of potential consumers and business partners are trading over the Internet with a new form of commerce, the electronic commerce or E-commerce.

However, E-commerce is just the part of a much greater conception, the E-business. The E-business is the transformation of key business processes through the use of Internet technologies [5]. Companies do not have to create new business procedures and start again everything from the very beginning. In fact, they can merge their existing infrastructure and business processes into the Internet technologies with accurate solutions. And taking advantage of E-business, they can develop interactive, transaction-based, flexible, reliable and scalable applications, which can give them the competitiveness due to reducing operational costs and growing revenue.

This article focuses only on E-commerce activity and future trends. At first, an overview of the European E-commerce market is given. Note that the acceptance and application of E-commerce is growing exponentionally. After a brief introduction to the terms of E-commerce, its impacts and issues will be presented, which are essential to companies that are planning or already carrying out E-commerce. It will also be looked at the technological background, which is necessary to realize E-commerce. At the end, a will survey will be given for the possible future trends of E-commerce with drawing the conclusions.

2. THE E-COMMERCE MARKET IN EUROPE

This status of E-commerce in Europe is based on a survey made by Romtec in June 1998. The survey was conducted with 570 companies across the EU and Norway and eight industry sectors. Some little modifications were made according to the current situation [1].

Nowadays there is an explosion in the number of E-commerce applications being put in place. As of the end of 1998, 29 % of European businesses used Internet-based E-commerce applications and, by the end of 1999, approximately 47 % of European businesses are using Internet-based E-commerce applications (see *Fig. 1*). From an end-user perspective, critical mass (defined as 50 % penetration) occurs when an E-commerce application becomes the norm. This is expected to be the case for the majority of businesses before the end of 2001 for each of marketing, sales, post-sales and purchasing applications.

At a country and sector level, there are significant differences in E-commerce application usage. Scandinavia leads, and is expected to lead E-commerce application take-up. Germany is set to overtake the UK, which is falling back in its adoption rate, while the Mediterranean countries, Spain, Portugal and Italy, are fast catching up with the leaders and will have a similar adoption profile by the beginning of the millennium. Adoption in France is slower. Across industries, business services and utilities are the most dynamic in terms of E-commerce adoption, with the finance sector lagging the trend.

At the moment most organizations are responding defensively, rather than strategically to E-commerce. Competition is a substantial motivating factor, particularly for "second-wave" companies with plans to implement E-commerce.

E-commerce is seen as an add-on, rather than as a replacement for other market channels or business processes. Low expectations of hard benefits from E-commerce mean that companies are not yet re-engineering business processes and models to meet the new opportunities and challenges that E-commerce brings. Most organizations are adopting E-commerce without demanding a strong business case for it; indeed, 65 % of businesses require a 10 % or less increase on sales revenue to feel that E-commerce adoption is justified.

Early adopters, particularly in industry sectors serving customer markets, indicate that their E-commerce experience to date has not yet lived up to their expectations. While bottom line benefits, such as reduced costs, were rated as less important than enhancing Quality of Service to customers, and greater flexibility, the lack of a quantifiable return on investment is of concern to businesses.

Rapid infrastructure and E-commerce applications growth are inadequate indicators of real E-commerce capability in the market. The survey found that indifference ("wait and see") is the biggest barrier to further uptake of E-commerce. This may only be dispelled by hard evidence that E-commerce is effective and delivers real business benefit.

IDC (International Data Corporation) forecasts that Western European revenue from Internet/E-commerce will rise from ECU 900 million in 1997 to ECU 26 billion in 2001. Security is another area, which needs to be addressed, in terms of changing business and consumer perceptions about the security of E-commerce transactions. Failure to do so will hold back adoption of transactional applications, such as sales, purchasing and post-sales.

Also, it is critical from a business point of view that the network, over which E-commerce taking place is reliable enough. Nowadays, as regards the infrastructure of the Intranet, network errors such as a cable break or switch fail could stop transactions accidentally. There is not enough redundancy built in to overcome these situations. Beside security it is also an area of great concern, if we consider that in several years a company could gain its revenues mainly from E-commerce. It follows from this that it should be emphasized over the whole network to make the connections as reliable as possible.

It is clear from the survey that E-commerce over Internet is rapidly being accepted as a significant way in which most organizations will conduct business within the next two to five years. The key challenge stays to persuade organizations to act strategically rather than defensively in response to E-commerce to maximize the business benefits of this revolutionary opportunity.

Note that E-commerce applications do not necessarily involve the execution of financial transactions (transfer of funds) across electronic networks.

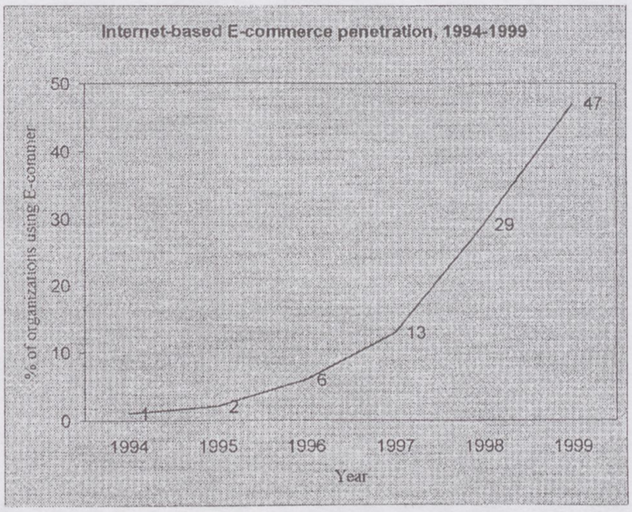


Fig. 1. Internet-based E-commerce penetration, 1994-1999

3. WHAT E-COMMERCE IS ALL ABOUT?

3.1. Definition of terms

E-commerce is a commercial activity conducted over electronic networks, often over the Internet, which lead to the purchase or sale of goods or services [1].

E-commerce activities are carried out by three main communities: business, consumer and government. The two relationships most often considered are *business to business* and *business to consumer*.

3.1.1. Business-to-business E-commerce

At present, most business-to-business E-commerce is carried out by business partners who are known for one another, across electronic networks known as Extranets. For example, a customer may order product electronically from a regular supplier with the supplier sending invoices electronically in return.

The term Extranet may be used to describe networks of business partners regardless of the underlying network technology in use. However, Extranets are increasingly associated with business-to-business E-commerce over the Internet. At present, most Extranets support continuous relationships between known trading partners, particularly over private networks using established Electronic Data Interchange (EDI) technology.

3.1.2. Business-to-consumer E-commerce

Business-to-consumer E-commerce is carried out over the public Internet. This type of E-commerce allows individual consumers to purchase, pay for and, depending of the form of the purchase, receive goods or services over electronic networks. For example, a consumer may use the Internet to order flowers or a flight, sending their credit card details over the Internet in payment. The Internet also provides an effective way of supporting, monitoring, and building relationships with customers.

3.2. E-commerce applications

The Romtec survey confirms that the adoption process for E-commerce applications is common for all countries, industry sectors, and sizes of site, but the rate of adoption will vary depending on country, sector and site size.

The four types of E-commerce applications currently being established across the Internet are:

- marketing (use of the Web for advertising or promotion);
- sales (receiving orders from customers; customer invoicing, collection or payment);
- post-sales (online supply to customers; customer support; customer monitoring and relationship development);
- purchasing (use of the Web to seek suppliers; receiving purchase orders and after-sales support; payment of suppliers).

E-commerce applications have been in place for some 20 years over private EDI networks. Such applications facilitated back-office functions such as ordering, invoicing and settlement. However, E-commerce applications over the Internet are demonstrating a different pattern of adoption, with greater emphasis on front-office function and interaction with customers. In 1998, the Internet was treated primarily as a marketing channel, and significantly less as a medium for completing transactions.

As Romtec survey shows, marketing applications are typically established first, through web sites which are set up to promote an organization's products and services. Organizations may pilot the site for several months or years before adding transactional capabilities. In a minority of cases, usually when the Internet is the only sales channel for the organization, or the channel through which it expects to receive a significant portion of its revenue, the site will be set up from the start to support transactions. These transactions include purchase ordering and/or payment, and post-sales applications such as electronic delivery and/or electronic delivery tracking.

Other European surveys are also confirming these adoption trends. In 1998, the majority of European web sites were dedicated to marketing applications. A 1998 survey of major CGP web sites in the European consumer packaged goods sector, carried out by IBM, looked at 65 sites representing over 160 companies and found that only six of these sites supported online sales, of which four were addressed to US consumers only. A Global Survey of Chief Information Executives carried out by Deloitte & Touche Consulting in late 1997 shows that 43 % of western European companies carry out marketing over the Internet, compared to 18 % who support transactions with consumers. This picture changes, however, in the business-to-business sector, where 43 % of the sample claim to be carrying out EDI transactions over the Internet with their business partners.

The situation will also change significantly again within the next two years, according to the Deloitte & Touche and Romtec surveys. *Fig. 2* shows the growth anticipated by Deloitte & Touche in marketing, transactional (sales and post-sales) and supply chain (purchasing) applications. The figures for Western Europe suggest slower growth in each application area than for the survey as a whole, although they are in line with the survey's growth predictions for the world's other two major markets, North America and Asia Pacific.

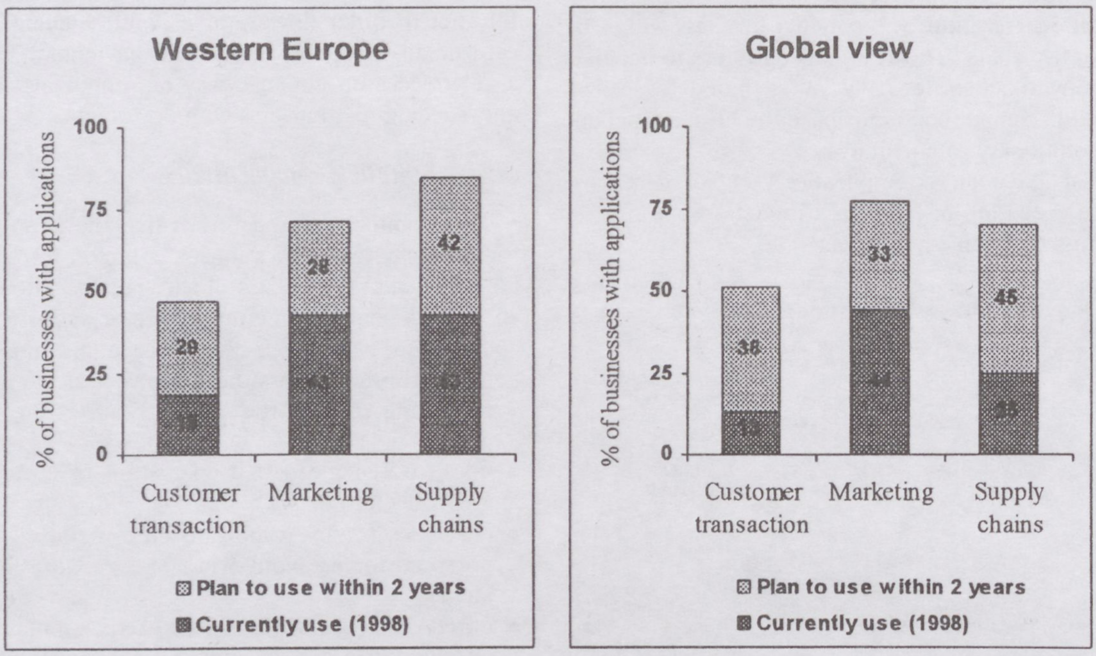


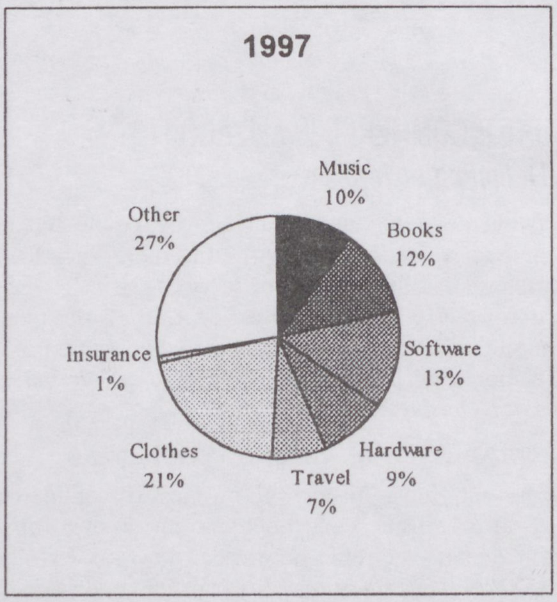
Fig. 2. Growth of Internet applications, 1998-2000

3.3. *Staying competitive*

The E-commerce market is becoming more competitive in two ways:

- An increasing amount of business is being carried out through online channels in certain sectors (books, computer software and hardware, music and travel), in competition with traditional channels.
- Within the E-commerce channel, Internet-only companies are beginning to face severe competition from rivals in a marketplace with no physical constraints to expansion.

Datamonitor estimates that online shopping at European web sites will rise from ECU 95 million in 1997 to ECU 4.3 billion by 2002. *Fig. 3* shows the proportion of that spends by consumer goods category. Increasingly, sophisticated sites that allow consumers quickly and easily to compare prices and find the best deal are encouraging greater shopping online rather than through conventional channels, particularly in the case of books, music and travel.



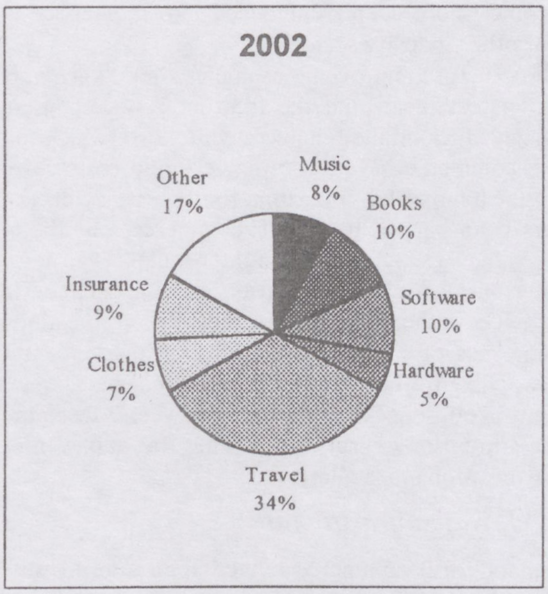


Fig. 3. Product mix for online shopping, 1997 and 2002

In this environment, the received wisdom is that companies should adopt two competitive strategies:

- re-engineering their business processes onto electronic networks to reduce costs;
- provide value-added services on top of commodity products.

Survey results show that most European companies are not motivated onto the Internet by the opportunity to reduce costs. In the Romtec survey (see *Fig. 4*), reduced costs was listed fifth in a ranking of benefits, after much more important motivators such as improving quality of customer service, and access to new customers and markets. Reduced costs are a by-product of E-commerce for many companies, with the exception of Internet-only businesses, such as Swedish software distributor Buyonet. Where an E-commerce market segment is maturing and therefore becoming highly competitive, for example in the global financial sector, reducing the costs does rank more highly.

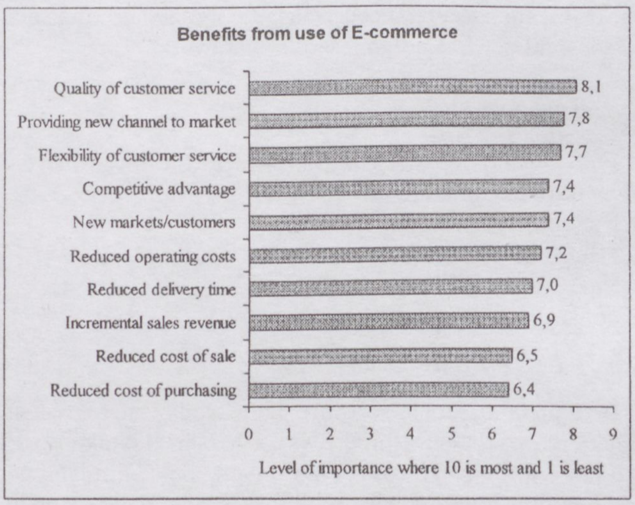


Fig. 4. Importance placed on benefits from use of E-commerce

Quality and flexibility of customer service rated highly as E-commerce benefits among the European companies surveyed by Romtec. This suggests that businesses expect competitive advantage to come through adding value, rather than through price competition.

Competition on the Internet is currently greater than competition between the Internet and existing channels to market and is intensified by there being relatively few customers and a lack of global boundaries. 40 % of organizations in the Romtec survey were motivated to take up E-commerce by peer pressure from existing competitors. Once on the Internet, competition can be strong: the Internet music company, Cerberus, finds that any innovative moves it makes are very quickly copied by competitors, and this has an impact on its customer base.

3.4. Changing organisations

Optimism over E-commerce application growth is registered by both the Romtec and Deloitte & Touche surveys, yet it is currently having very little impact on existing organizations in Europe. While there are examples of software distributors turning themselves from physical to Internet-only companies, there are few, if any in other European industry sectors. In the majority of cases, Internet-only companies are new start-ups, and many of them are intermediaries in new market areas, that is, "middlemen", providing Internet-based services that enable buyers to find sellers, and vice-versa, in particular markets.

Intermediaries will play an increasingly vital economic role over the next two to five years in matching suppliers and customers, potentially creating a competitive environment in favour of the smaller, more "agile" and niche supplier over larger businesses. At this point, E-commerce will begin to have an impact on many more organizations [1].

Today, when businesses, large and small, open up a new channel to market through the Internet, they are typically doing so without significantly changing their existing business, or taking on new staff. Cedlerts Fisk, for example, services orders to customers, which are taken via the Internet, in the quiet moments when its staff are not fulfilling orders for business customers. Surgicon, a small UK distributor of surgical products, has redeployed staff as a result of putting an online order and fulfillment capability in place.

Organizational "shrinkage" is being enabled by E-commerce in the more advanced North American E-commerce market. British Airways has decided to close its physical sales outlets in the USA because of the success it has had selling tickets over the Internet. As the propensity for buying online increases in Europe, Datamonitor predicts that such moves will be replicated here, too.

However, organizational change will generally be slow in enterprises serving traditional consumer markets. In the financial services sector, Ernst & Young found that more than 21 % of its businesses did not intend to make changes in other channels because of investments in E-commerce. The number of businesses indicating that they would provide incentives for customers to use lower-cost E-commerce delivery channels fell from 85 % in 1996 to 72 % in 1997, while the number of businesses with no plans to do so rose. Romtec's survey findings in the finance, retail/wholesale and transport/travel sectors confirm that these sectors are proceeding cautiously, with significant impact on their existing organizations unlikely before 2001.

3.5. E-commerce issues

3.5.1. Public infrastructure

In July 1998 Network Wizards estimated that there were more than 36 million hosts world-wide (www.nw.com), and Nua Ltd estimated that in August 1998, there were 147 million adults with access to the Internet (www.nua.ie). The continuing expansion of the Internet, as illustrated by the facts suggests there will be increasing E-commerce opportunities as an ever-greater potential customer base comes online. Nua estimates that Europe account for 22 % of the world-wide Internet population (with the USA/Canada holding 58 %, Asia Pacific 15 %, South America 3 %, Africa 1 % and the Middle East 1 %).

Schema estimates (The Market for IP-based Services in Europe, 1998) that by the end of 1997 the total number of companies using Internet Protocol (IP) services in Europe reached 2.6 million, representing a 4.1 million sites. On the basis of a survey conducted between January and June 1998, Schema has derived figures for the number of business Internet subscriptions by country (see *Fig. 5*). It forecasts that the number of connected business sites will grow to 10.6 million by the end of 2003. Within the same timeframe, residential subscriptions are predicted to grow from 6.3 million to 30 million in Europe [1].

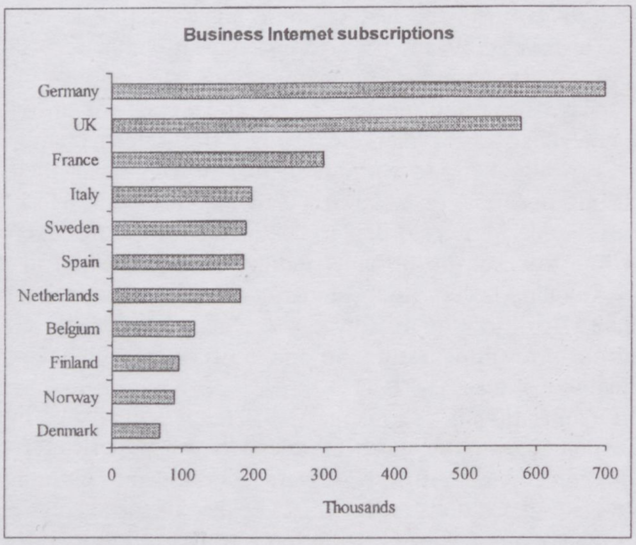


Fig. 5. Business Internet subscriptions in Europe

This growth will have an impact on Internet infrastructure, including access, bandwidth and governance issues. The increase in Internet Service Providers is facilitating access to the Internet, although as there are now an estimated 20,000 to 30,000 ISPs world-wide, most of which are very small, it is likely that there will be a market shakeout over the next few years. This is likely to consolidate service provision in the hands of far fewer companies. At the same time, the face of Internet service provision may change as it becomes more deeply embedded into the service offerings of other industry sectors.

Infrastructure improvements and greater choice of bandwidth services mean that the Internet is becoming an increasingly efficient and reliable medium over which to conduct E-commerce. Major bottlenecks and costs currently in the local loop and in customer support may deter consumers from participating in E-commerce, but the backbone traffic has a fairly constant profile at present, attracting business-to-business users to use cheaper Internet services rather than private network connections for certain types of E-commerce traffic. However, capacity and switching/routing in the international backbone may become a bottleneck in the coming years, discouraging business-to-business users from using the public Internet, unless this problem is addressed.

3.5.2. Private infrastructure

Demand for E-commerce-related applications is shaping organizations' private infrastructures. The use of the web and private EDI networks to bind customers and suppliers into transactional business processes, videoconferencing in support of collaborative working, marketing and distance learning, and the use of multicast push technology to deliver electronic products and services, are all having an impact on corporate networks.

It is costly and complex to implement in-house private network infrastructure that: delivers high bandwidth end-to-end; supports multimedia communications – voice, video and data; and supports a quality of service capability that will commit bandwidth to real-time applications, such ass voice, video, and business-critical transactions. Companies are beginning to turn to third parties, such as ISPs, to provide the private infrastructure they need to support Internet and E-commerce applications.

The blurring of boundaries between public and private infrastructure, which has made E-commerce possible, will gain momentum as E-commerce applications themselves become more widespread and sophisticated. Trends for the future include companies making private network infrastructures available to trading partners as Extranets and the increasing extension of E-commerce across wireless networks, such as enhanced GSM, its third generation successor, and newly-emerging satellite networks.

3.6. Technology

Four technology blocks are critical to the future development of E-commerce:

- E-commerce servers;
- electronic payment;
- smart cards;
- network access devices.

3.6.1. E-commerce servers

E-commerce server software has steadily increased in function over the past three years. 1996 saw the take-up of the first sophisticated commerce servers aimed at high-end transactional environments in Europe and also the launch of the first low cost solutions for individual merchants. By 1998, the market was less well-defined, with highly customizable E-commerce "framework" products making an entrance.

E-commerce servers increasingly incorporate middleware and support for standards such as EDI to enable integration with back-office operational systems, including enterprise resource planning (ERP) and logistics systems. At same time, the developers of such systems are extending them to support Internet E-commerce. In two years' time, an organization's key operational systems may well contain many of the applications currently separated out into E-commerce server today. The Internet will merely be one of many channels to market, with a consistent set of back-office processes operating across all channels.

The full set of functions needed to carry out secure E-commerce is still too expensive for small and medium-sized organizations. A number of commercial E-commerce application services are beginning to appear which serve this business-to-business market; in many cases, they are adaptations of successful business-to-customer E-commerce implementations.

3.6.2. Electronic payment

The three main forms of payment supported by E-commerce sales applications are:

- credit card;
- electronic cheque;
- electronic cash.

Credit card is still the most popular form of payment on the Internet.

A 1998 survey carried out for ICL by MORI to determine attitudes towards technology and its impact on lifestyles in four European countries (Sweden, Germany, France, UK) and the USA, found that around 40 % of the 3,500 businesses were favourable towards the idea of electronic cash. In Europe, the Swedes were most in favour (50 %) followed by the French (44 %) and Britons (39 %), just ahead of the Germans (37 %).

Though a technology important to underpinning business-to-consumer E-commerce, E-cash has been slow to make an impact on the market. In 1998, issues of competing smart card technology and interoperability between payment mechanisms began to be addressed. This will help to accelerate acceptance of E-cash, as will clarification over the role of, and regulatory environment for, E-cash issuing organizations, which is now emerging in Europe.

3.6.3. Smart cards

Multi-application smart cards, which underpin other key E-commerce technologies, including E-cash and E-commerce-enabled mobile phones, have now emerged from the concept stage and started to ship in 1998. France is in the best position to make the transition to multi-application smart cards; over 20 million customers of French banks possess smart card-based credit cards. Scandinavia is also ahead in the rollout of such cards. At the end of 1997, Sweden Post launched a smart card-based secure E-mail service (@Post). By the millennium, it expects four million Swedes to be carrying smart cards that give them access to @Post and other Internet-based services.

Smart card technology for E-commerce faces cultural barriers. In the MORI survey, UK businesses (60 %) were most interested in a single smart card that would allow them to reduce the number of other cards to just one, compared to 42 % in Sweden, 43 % in Germany and 45 % in France. The ability to pay electronically was not seen as a perceived benefit of smart cards.

Multi-application smart card issues include security, rival operating system technology, the lack of mature development tools, interoperability with different types of reading device, and the definition of a cardlet loading protocol. Industry fore is gradually resolving these issues.

3.6.4. Internet access devices

An expanding range of devices able to access the Internet will accelerate its penetration within Europe and increase the potential consumer base for E-commerce. Until 1998, the only means of connecting to the Internet has been via a computer and modem. From 1999, this will change, as other Internet-enabled devices become available.

Web-enabled mobile phones, due in 1999, will become one segment of a larger category of handheld mobile information devices. Information-centric devices, with built-in modems or PC cards, support for Internet access protocols and native browsers, began shipping in 1998. By the end of 1999, the first information-centric products are scheduled to appear, supporting wireless technology known as Bluetooth. This will enable sophisticated mobile E-commerce applications, such as mobile electronic dealing rooms and mobile travel applications, to be developed. The low cost of such units compared to PCs will help push Internet-based E-commerce to a broad customer base.

Multimedia kiosks providing pay-as-you-go access to the Internet have already been successfully installed in pilot locations, such as the city of Tampere in Finland. Although they have the potential to increase access to the Internet, they face similar infrastructure and cost-of-investment barriers to smart cards and are unlikely to be in widespread use across Europe until after the millennium.

The first trial combining digital television with access to the web began in Europe in the second half of 1998 and manufacturers of set-top boxes and televisions for the European market are producing early equipment that supports Internet access. This equipment is expected to appear in volume from 1999 onwards.

Digital television has the potential to deliver mass-market access to the Internet, but subsequent E-commerce opportunities may take several years to realize. Among the countries in Europe, Belgium is in a unique position to capitalize early on such an opportunity: 95 % of Belgian homes are connected to cable television, the infrastructure for which is being upgraded over the next four years into a high-speed bi-directional digital information highway.

3.7. Standardization

E-commerce could not be carried out without certain standards. As we saw in previous sections, business partners cannot communicate in the lack of a common protocol or language [3]. We need standards for electronic payment, smart cards and Internet-enabled devices, and for information interchange. Companies expect the integration of established systems as well as the growing interchange of information in such a way that they need to invest as less as possible to do business with any potential partners. This is only realizable if they adopt standard solutions in the ever-changing E-commerce field.

The key for managing business over the Internet or private networks is that the participants of businesses understand one another's business data and processes, that is one another's language. The recently developed XML (Extensible Markup Language) could be one of those common languages. It is a W3C recommendation, a standard owned by W3C and not by any vendors [4]. It is also open and free, and XML parsers are available for all platforms. Such common languages could greatly facilitate the penetration of E-commerce in the world.

However, standards for devices and hardware are much less unambiguous, because the objective of hardware manufacturers is generally opposite. Their intention is that business partners and consumers use their product and not one of another hardware manufacturer's. Hence, it is important to work out common interfaces over which the different types of hardware elements could interchange information.

3.8. Security

Security is still a barrier to electronic commerce, although increasingly security risks are being weighted against the commercial risks of delaying exploitation of the Internet. The Romtec survey found that uncertainty over business benefits, resulting in a "wait and see" attitude (mentioned by 24 % of businesses) was a stronger disincentive to adopt E-commerce than security (mentioned by 15 %). In its 1998 Global Survey of Chief Information Executives, Deloitte & Touche Consulting found that security came top of CIO's list of barriers to the development of all types of Internet E-commerce applications. Nevertheless, the same businesses expected a dramatic rise in the number of such applications over the next two years.

The security technologies needed are particularly expensive for small and medium-sized companies. Many such organizations setting up Extranets, currently do so with very low levels of security, basing proof of identity (authentication) on easily-hacked passwords, rather than on encrypted keys, certificates and digital signatures.

Larger organizations are beginning to put in place certificate-based security infrastructures. The investment bank Soundview Financial Group forecasts that this market for certification authority products and services will reach ECU 940 million world-wide in 2001.

4. KEY TRENDS FOR THE FUTURE

This section considers E-commerce trends in six areas:

- country trends;
- sectoral trends;
- application trends;
- business model change trends;
- technology trends;
- regulatory trends.

4.1. Country trends

The Mediterranean countries, Spain/Portugal and Italy, will continue in catch-up mode with Northern Europe and their aggressive investment in, and exploitation of E-commerce will bring them up to comparable levels of capability by 2002. France is also in catch-up mode, but is currently showing less enthusiasm for E-commerce than its southern neighbours. The rate of development in the more advanced Northern European markets will begin to slow after 2000, with the UK already showing signs of dropping back behind Germany and Scandinavia.

4.2. Sectoral trends

Finance appears one of the most conservative sectors in its approach to E-commerce: however, it also emerges as the only sector taking a strategic view. The implementation of a strategic approach to E-commerce will inevitably mean business model change, a longer process than merely bolting support for the Internet onto the existing business.

Utilities are the most demanding of a strong financial business case for investment in E-commerce. However, they are also begin driven into early adoption by the threat of competition in increasingly deregulated markets. E-commerce within this sector will reach critical mass early in the new millennium.

The transport/travel sector, although showing clear signs of how the Internet and disinter-mediation are increasing competition, is not rushing to put Internet E-commerce applications in place to counter this threat. In fact, transport/travel will be one of the later sectors to achieve critical mass in marketing, sales, purchasing and post-sales applications. This may reflect the effect of existing private electronic infrastructure that is locking transport/travel companies into a specific business model from which it will be difficult to break free until the volume of Internet transactions and sales rises.

Many government organizations are planning to lead best practice in the E-commerce arena by carrying out more of their informational, transactional and procurement services online, and many services will be rolling out by the end of 1999. Such a public sector lead will considerably advantage the commercial sectors within these counties.

4.3. Application trends

In the year 2001, critical mass point will be reached for E-commerce marketing applications in Europe, when the 1998 ratio of web-marketeers to non-web-marketeers will be reversed.

The trend towards putting customer-focussed E-commerce applications in place first will continue, with only the most advanced organizations installing Internet-based supply chain applications that support interaction with suppliers before 2002. By 2001, however, critical mass point will be reached for E-commerce purchasing and sales applications, supporting growing numbers of supply chains end-to-end.

"Killer" applications will be those that promote transparency between buyer and seller, making it easy and attractive for customers to do business with a particular company. By 2001, critical mass point will be reached for E-commerce post-sales applications. These will begin to be customers' first choice when seeking support, pushing the telephone into second place.

The trend towards more ad-hoc relationships with customers will continue. This has implications for the selling organization's competitiveness and cost structures, and also for the quality of its marketing and sales applications. However, transparency and support for a high percentage of ad-hoc transactions require innovation and business change. Most organizatons will not be ready to face the upheaval required to make such changes until after the millennium [1].

In the near future E-commerce applications will be developed particularly in the business-to-business sector. This is because in this sector the business partners are known for each other, so their identification is easy. In addition, they have the necessary infrastructure to carry out the authentication processes, and the new solutions can adopt the established EDI or other Extranet systems shortening the time of new developments.

4.4. Business model change trends

The top five benefits of E-commerce identified by the survey sampled overall, are:

- improved Quality of Service to customers;
- new channel to market;
- flexibility of customer service;
- competitive advantage;
- new markets/customers.

To achieve the benefits of competitive advantage and access to new markets/customers, organizations do need to change existing business processes and support structures more radically. In sectors such as retail/wholesale, transport/travel and other services, which rank competitive advantage highly, there are emerging examples of innovative exploitation of the Internet, including highly targeted cybermalls such as Buckingham Gate, and marketplaces (EMB), and the creation of Internet-based value-added service offerings. Organizations competing in these areas often create new Internet companies with different business models to handle this area of the business, however, rather than attempting the more difficult task of re-engineering their existing business to integrate the Internet channel [2].

It is likely that the majority of companies will be using the Internet to trade with their partners, and particularly their customers, by 2002. By 2005, most supply chains will trade electronically. Leading-edge organizations by this time will have re-engineered themselves as virtual companies, keeping control of brand and marketing functions and using electronic networks to produce the support services they need, monitor service level agreements with provider organizations, manage distributed processes across provider organizations and enter into new partnerships for marketing and support purposes.

4.5. Infrastructure and technology investment trends

The basic infrastructure for E-commerce – modem and Internet-enabled devices of all types, public infrastructure and private networking technology – will continue to expand rapidly. The rollout of Web-enabled mobile phones, digital broadcasting services and smart card-enabled PCs in 1999 will increase the choice of electronic ways in which businesses can interact with their customers. A number of service providers, including retailers and banks, will also provide basic access to the Internet, increasing the numbers of potential customers online.

A significant number of European organizations, particularly those with plans for E-commerce and those in large companies, will exploit this infrastructure in defensive mode. They will adopt Internet E-commerce because their competitors do, rather than because they have a clear strategy and business case. In these circumstances, their investment in E-commerce technology and applications may be limited and potentially ineffective within two to three years. Those organizations investing in technology that changes external relationships with and processes between business partners and customers are likely to be more successful in the long-term. However, their short-term positions may be precarious due to the lack of critical mass in E-commerce activity before 2000. Such companies are already showing themselves as E-commerce pioneers and are likely to be small to medium-sized, with an entrepreneurial, expansion-oriented culture [1]. The trends show that E-commerce solution providers will try to evolve standard infrastructures and applications to simplify for their business partners the adoption of E-commerce. This can give hope for the previously mentioned companies and shorten the time necessary to achieve critical mass in E-commerce activity.

By 2002, it is possible that the public network infrastructure will begin to fail to keep up with the increasing demands of Internet users and delays will become unacceptable. New multichannel services provided by digital broadcasting will replace the Internet as the focus for business-to-consumer E-commerce, while an increasing proportion of business-to-business E-commerce will be conducted over private IP-based Extranets. By 2005, smart cards will become key to all aspects of E-commerce.

4.6. Regulatory trends

By 2000, consumer protection regulation should be clarified and contract law and domain names/trademarks issues resolved through agreement on practical guidelines. A new Internet global taxation regime will begin to emerge after 2002, while favourable national legislation will fuel the growth of secure "trust" infrastructure (certification, digital signatures) for E-commerce. By 2005, a workable framework for a global trust infrastructure will be laid down, as a result of international harmonisation of laws governing the licensing of certification authorities and data protection [6].

5. CONCLUSIONS

E-commerce is currently in the stage of constant transformation. There are few mellowed systems and adoptations carrying out E-commerce, however, the companies have to join in the electronic business world, because trends show a tremendous growth, and those who does not change their business processes in time, fall behind.

In the near future E-commerce will be primarily carried out in the business-to-business sector. In Europe, the businesses are now adopting a "wait and see" attitude, which is the bigger retentiveness to the propagation of E-commerce. If they really want to take full advantage of the new opportunities of the E-commerce, they have to re-engineer, and incorporate Internet technology into their core business processes. The companies mainly intend to improve the quality of service on top of commodity products and provide value-added services. However, at present, the small and medium-sized companies cannot afford the infrastructure and applications to carry out E-commerce.

The number of businesses and consumers increases radically, which makes E-commerce more and more cheap and the business more payable. The underlying technology that permit to govern E-commerce over the Internet will probably be the E-cash and E-commerce-enabled mobile phones in the business-to-consumer sector. Meanwhile an increasing proportion of the business-to-business E-commerce are conducted over private IP-based Extranets.

Because the Internet has no boundaries (in the sense that it is not bounded by country borders), it needs international regulation of laws to provide a global security and the protection of personal and other rights. It relates tightly to security solutions and together they can elevate the confidence in E-commerce which is a very important issue.

As it can be seen, there are a lot of open questions, but the evolution will not stop and there is hope that E-commerce will be a standard way to do business.

REFERENCES

[1] European Information Technology Observatory 1999, European Information Technology Observatory (EITO) – European Economic Interest Grouping (EEIG), 1999

[2] Tibor Kiss: The E-business changes everything, Byte, December 1998 – January 1999

[3] Taimur Aslam: Protocols for E-commerce, Dr. Dobb's Journal, December 1998

[4] http://www.w3.org/

[5] http://www.ibm.com/

[6] János Verebics: Internet on the verge on law, Journal on C5, June 1999

AZ ELEKTRONIKUS KERESKEDELEM FEJLŐDÉSI IRÁNYAI

SZABAD TAMÁS

ELMÉLETI VILLAMOSSÁGTAN TANSZÉK, BUDAPESTI MŰSZAKI EGYETEM
E-MAIL: SZABADT@SCH.BME.HU

Az elektronikus kereskedelem infrastruktúrája és szolgáltatásai hatalmas fejlődésen mentek át az 1996 és 1999 között eltelt időszakban. Az Internet felhasználók száma napról napra emelkedik, és ez világszerte megváltoztatja az üzleti élet menetét. Nagyon sok potenciális fogyasztó és üzleti partner kereskedik már az Internet igénybe vételével a kereskedelem új formájával, az elektronikus kereskedelemmel.

A cikk áttekitést ad az elektronikus kereskedelem helyzetéről és az erőviszonyokról Európában. Láthatjuk, hogy jelenleg kevés kiforrott rendszer és alkalmazás van. Mégis a cégeknek, vállalatoknak be kell kapcsolódniuk az elektronikus üzletvitel világába, különben a versenytársaik megelőzik őket, és ez könnyen az ő bevételeik csökkenését okozhatja.

Az elektronikus kereskedelem fejlődése azt mutatja, hogy a jövőben a kereskedés új formája elsősorban az üzletfelek között (a business-to-business szektorban) fog zajlani. Európában a vállalatok hozzáállása a "várjunk, és nézzük meg mi lesz" elvet követi, ami nagyon megnehezíti az elektronikus keresedelem elterjedését.

A megvalósításhoz szükséges technológia és infrastruktúra már jelenleg is rendelkezésre áll, sőt ezen a területen is további fejlődés várható. Mivel a kereskedés főleg az Interneten történik, a nemzetközi jogharmonizáció meghozhatja a várva várt áttörést, és ez új lendületet adhat mind az üzletfelek, mind a fogyasztók vásárlási kedvének. A rengeteg nyitott kérdés ellenére az elektronikus kereskedelem a kereskedés általánosan elfogadott megoldásává válhat – néhány éven belül.

Tamás Szabad received his M.Sc. in Computer Science from the Technical University of Budapest in 1999. He wrote his thesis with the title of Application of the Wavelet Transform in the Processing of Sounds (in Hungarian). He was given a prize at the Scientific Conference of University Students, and participated in the Conference of Graduate Students in 1998 and 1999, respectively. Tamás Szabad has published two referenced papers in the Journal on C5 as a co-author during the last two years. From September 1999 he pursues Ph.D. studies at the Department of Electromagnetic Theory in the field of electronic commerce. He investigates the applications of telecommunications and informatics of electronic commerce and authorization centers.

ELECTRONIC PAYMENT SYSTEMS: ELECTRONIC CASH

ANDRÁS BODOR

DEPARTMENT OF ELECTROMAGNETIC THEORY
TECHNICAL UNIVERSITY OF BUDAPEST
H-1111 BUDAPEST, EGRY J. U. 18.

This paper examines the current state of electronic money systems. First the current trends in ecommerce systems and the benefits it offers to the sellers and buyers are outlined. Then opportunities of the banks in this new market: electronic payment systems are introduced. In the section 'Electronic Money' of this paper the basics of digital coin based money, as a type of Internet payment mechanisms and it's general characteristics will be sketched. Then four real electronic money system: NetCash, Mondex, Millicent, Ecash will be examined. The third and fourth proposals will be in a more detailed manner discussed. The final part of the paper compares the money systems and outlines the way how financial institutions should use this opportunity.

1. COMMERCE ON THE INTERNET

The growth of the Internet and the advent of electronic commerce are bringing about enormous changes around the world in society, politics and government, and in business. The ways in which trading partners communicate, conduct commerce are governed have been enriched and changed forever.

The delivery of value-added content and services over the Internet's World Wide Web holds great promise for both businesses and consumers. Web-based businesses can offer a greater selection of products and services to a larger, global customer base. And because distributing products over the Web eliminates the high costs of product packaging and distribution, businesses can pass along some of their cost savings to customers.

Fundamental changes are taking place in the way consumers and merchants trade. Characteristics of trading that have changed markedly include:

- Presence: Face-to-face transactions become the exception, not the rule. Already with the rise of mail order and telephone order placement this change has been felt in western commerce. Electronic commerce over the Internet will further expand the scope and volume of transactions conducted without ever seeing the people who are a part of the enterprise with whom one does business.
- Authentication: An important part of personal presence is the ability of the parties to use familiar objects and dialogue to confirm they are who they claim to be. The seller displays one or several well-known financial logos that declaim his ability to accept widely used credit and debit instruments in the payment part of a purchase. The buyer brings government or financial institution identification that assures the seller she will be paid. People use intangibles such as personal appearance and conduct, location of the store, apparent quality and familiarity with brands of merchandise, and a good clear look in the eye to reinforce formal means of authentication.
- Payment instruments: Despite the enormous size of bank card financial payments associations and their members, most of the world's trade still takes place using the coin of the realm or barter. The present infrastructure of the payments business cannot economically support low value transactions and could not survive under the consequent volumes of transactions if it did accept low value transactions.
- Transaction values: New meaning for low value transactions arises in the Internet where sellers may wish to offer for example, pages of information for fractions of currency that do not exist in the real world.
- Delivery: New modes of delivery must be accommodated such as direct electronic delivery. The means by which receipt is confirmed and the execution of payment change dramatically where the goods or services have extremely low delivery cost but may in fact have very high value. Or, maybe the value is not high, but once delivery occurs the value is irretrievably delivered so payment must be final and non-refundable but delivery nonetheless must still be confirmed before payment. Incremental delivery such as listening or viewing time or playing time are other models that operate somewhat differently in the virtual world [1].

2. BENEFITS OF ELECTRONIC COMMERCE

The cost of doing business changes dramatically when content providers move from distributing physical items to distributing bits moved by electronic means. It is estimated that 75 percent of the purchase price of physical goods goes to support the underlying costs of manufacturing, packaging, distributing, and wholesaling and retailing the products. On the World Wide Web, content providers can avoid most manufacturing costs and all physical packaging costs for information goods. They can also bypass traditional physical distribution and sales channels and directly deliver goods online to customers.

Electronic commerce has a number of potential benefits to both the buyers and the sellers. The categories and benefits are described here:

2.1. Benefits to sellers

- Cheap global marketing for products using the means of multimedia.
- The potential for virtual corporations without real stores.
- Relatively small investments make the markets easily penetrable by so called microcorporations.
- Catalogs and other available information can be kept up to date.
- Customer service can be enhanced with email. Easy and responsive communication won't require as many clerks.
- Commerce can be fast and easy and will not be tied to time or place.

2.2. Benefits to buyers

All of the advantages the seller has are also advantages to the buyer. A lighter sales channel can lower prices at the same time it raises the quality of customer service.

Purchases can be made anywhere with a computer and a network connection.

The sellers can modify their supply faster to real demand due to easier feedback from the customers through email.

The roles of the manufacturers and sellers can be redistributed. Support will come from a party that is most capable of doing it. A network-savvy manufacturer will probably support customers directly. An advanced retailer might on the other hand purchase the support from a third party.

Communication through Usenet News and mailing lists has already created an independent source of information on products from other users.

2.3. Benefits to other parties

Manufacturers want to have their goods on sale at as many points of sale as possible.

Distributors may think of the new marketplace as a way to differentiate their services from those of their competitors.

Banks feel that the new methods will increase the amount of financial transactions and the need for financing.

Computer and software industry will have another field to sell their products and services [2].

3. OVERVIEW OF INTERNET BANKING

As mentioned before, considering that banks are in the payment business, banks now have a golden opportunity for additional service revenue laid at their feet. Banks, of all parties involved, have the most arrows in their quiver when it comes to being successful payment merchants. They have large operation center environments and big iron in the back office, which can handle not only large volumes but hosting of server-side wallets and public key infrastructure as well. They also need new sources of service revenues as lucrative assets bleed off to mutual funds, insurers, etc. Lastly, but most importantly, they remain the most trusted link in the chain.

Opportunities for banks to increase their presence in this space are multiplying quickly. Internet user numbers already reached the critical mass needed to justify the medium as a stable channel. Likewise, the big merchants that banks love to serve are now moving online and high-traffic points are becoming clear [3].

This means that financial institutions may enlarge their market area without building new offices or field services, respectively. Because of its image as an innovative corporation, better interacting possibilities, the usage of rationalization potentials, promotion of self-service ideas, the improvement of its competitive situation by development of core competencies together with the construction of market entry barriers, it may be possible to increase profits and market shares.

One way of exploiting rationalization potentials is the implementation of the entire transaction (from purchase to payment) under a common user interface. Information collected in operative databases of financial institutions allows them to act as information brokers. Offering special information in closed user groups may result in more intense customer commitment, as well as customer bonding. Know-how that is built up by Internet presence may be used to facilitate Internet presence of smaller companies. The use of digital coin-based money to completely settle transactions in the Internet is a new service provided by financial institutions [4].

4. OVERVIEW OF INTERNET PAYMENT SYSTEMS

Important characteristics for an Internet payment system include security, reliability, scalability, anonymity, acceptability, customer base, flexibility, convertibility, efficiency, ease of integration with applications, and ease of use. Some of these characteristics, like anonymity, are more important in some communities, or for certain kinds of transactions, than they are in other communities. These characteristics are presented for discussion and comparison.

Security

Since payments involve actual money, payment systems will be a prime target for criminals. Since Internet services are provided today on networks that are relatively open, the infrastructure supporting electronic commerce must be usable and resistant to attack in an environment where eavesdropping and modification of messages is easy.

Reliability

As more commerce is conducted over the Internet, the smooth running of the economy will come to depend on the availability of the payment infrastructure, making it a target of attack for vandals. Whether the result of an attack by vandals or simply poor design, an interruption in the availability of the infrastructure would be catastrophic. For this reason, the infrastructure must be highly available and should avoid presenting a single point of failure.

Scalability

As commercial use of the Internet grows, the demands placed on payment servers will grow too. The payment infrastructure as a whole must be able to handle the addition of users and merchants without suffering a noticeable loss of performance. The existence of central servers through which all transactions must be processed will limit the scale of the system. The payment infrastructure must support multiple servers, distributed across the network.

Anonymity

For some transactions, the identity of the parties to the transaction should be protected; it should not be possible to monitor an individual's spending patterns, nor determine one's source of income. An individual is traceable in traditional payment systems such as checks and credit cards. Where anonymity is important, the cost of tracking a transaction should outweigh the value of the information that can be obtained by doing so.

Acceptability

The usefulness of a payment mechanism is dependent upon what one can buy with it. Thus, a payment instrument must be accepted widely. Where payment mechanism are supported by multiple servers, users of one server must be able to transact business with users of other servers.

Customer base

The acceptability of a payment mechanism is affected by the size of the customer base, i.e. the number of users able to make payments using the mechanism. Merchants want to sell products, and without a large enough base of customers using a payment mechanism, it is often not worth the extra effort for a merchant to accept the mechanism.

Flexibility

Alternative forms of payment are needed, depending on the guarantees needed by the parties to a transaction, the timing of the payment itself, requirements for auditability, performance requirements, and the amount of the payment. The payment infrastructure should support several payment methods including instruments analogous to credit cards, personal checks, cashier's checks, and even anonymous electronic cash

Convertibility

Users of the Internet will select financial instruments that best suit their needs for a given transaction. It is likely that several forms of payment will emerge, providing different tradeoffs with respect to the characteristics just described. In such an environment it is important that funds represented by one mechanism be easily convertible into funds represented by others.

Efficiency

Royalties for access to information may generate frequent payments for small amounts. Applications must be able to make these "micropayments" without noticeable performance degradation. The cost per transaction of using the infrastructure must be small enough that it is insignificant even for transaction amounts on the order of pennies.

Ease of integration

Applications must be modified to use the payment infrastructure in order to make a payment service available to users. Ideally, a common API should be used so that the integration is not specific to one kind of payment instrument. Support for payment should be integrated into request-response protocols on which applications are built so that a basic level of service is available to higher level applications without significant modification.

Ease of use

Users should not be constantly interrupted to provide payment information and most payments should occur automatically. However, users should be able to limit their losses. Payments beyond a certain threshold should require approval. Users should be able to monitor their spending without going out of their way to do so.

Most recently proposed, announced, and implemented Internet payment mechanisms can be grouped into three broad classes: electronic currency systems, credit-debit systems, and systems supporting secure presentation of credit card numbers. In less common use are forms of payment that can be described as direct transfer or use of a collection agent [5]. In the next sections this paper concentrates on electronic cash systems.

5. ELECTRONIC MONEY SYSTEMS

5.1. The Basics

The term 'money' is used in this paper loosely, following a notion of John Kenneth Galbraith, who stated that "money is nothing more or less than what he or she always thought it was – what is commonly offered or received for the purchase or sale of goods, services or other things" (Galbraith, 1995, p. 3). The term 'electronic money' is used to encompass both chip-based stored-value cards and net-based payment mechanisms that store and convey value in and of themselves rather than merely representing value residing elsewhere, such as a deposit account.

Electronic money is currently a very nascent setting, neither its technical, legal, economic nor cultural components are fully formulated. Consequently, a great number of competing proposals are in different stages of development and being used. This section aims to outline the general characteristics that inform all proposals and to provide a brief overview of the different groups that are actively shaping the current development [8].

5.2. Basic Principles of Electronic Coin-based Payment Systems

Due to the increasing importance of electronic commerce via the Internet the importance of digital money increases. Representing "real" money in an electronic world means that properties and functionalities like anonymity, authenticity, as well as availability of pico-payments are considered. Like "real" money, digital coins have an inherent value [4].

Despite the somewhat confusing diversity of proposals that seem to offer quite different solutions, all electronic money schemes share a common basis of issues that they somehow have to address. Based on Lynch; Lundquist (1996), Matonis (1995) and Okamoto; Ohta (1991) six (structural) problem areas can be defined that have to be addressed by any system:

Independence

Is the electronic money independent of any physical condition? It has to be transferable though open networks and storable on different devices and in different locations inside and outside these networks. Cash, evidently, is dependent on its physical condition in so far as it equates the unit-value of money with the storage medium (paper, coins) in which it resides. It can not be transferred onto any other medium without ceasing to be cash. On the other hand, the cash economy is a truly open network, which all forms of physical money can enter and exit quite freely. Even though the limits of the acceptance of specific cash clearly define different segments within the network Changing from one segment into the other is not only unproblematic, but an essential, institutionalized feature of the network itself (currency exchange).

Security

Can it be copied (reused) and forged? This, obviously, must be prevented. Not only must the electronic money software be secure but also all the communication between the partners of a transaction must not be interceptible. Cash solves this problem based on its physical properties. A bill can be in only one place at any given time, therefore the question whether is has been duplicated can be decided locally, based on the thing. The transfer of cash is done normally in the presence of both parties and therefore unproblematic.

Privacy

What kinds of transactional information are generated and who has access to them? All levels of privacy are technically possible. Privacy is related to the encryption technology used in the security features of the system, however, there is no correlation between the two. Anonymous transactions are not per se more or less secure than fully traceable ones. Cash is fully anonymous while a credit card has limited anonymity, because all usage information is gathered in the central database of the processing institution such as VISA or MasterCard as well as in the database of the bank that holds the account to which a credit card must be tied. These databases are private properties and their use is subject to changing corporate policies. All electronic money systems have to define a range of privacy between the two poles: total anonymity and full auditability

Transferability

Who can pay and who can receive money? The cash must be transferable between users in all forms of "peer-to-peer payment". With cash this is no problem while with traditional credit cards this is impossible unless the payee has the privileged merchant status that is not intended to be available for everyone.

Divisibility

What are the payment units? The size of the units and the number of different units has to be defined. In contrast to cash, where the physical properties limit not only the size but also the number of units due to reasons of practicality, these constraints do not apply to electronic money. All sizes of units are, technically speaking, equal. The limits arise due to specific design properties.

Ease of use

What hardware, software and expertise is required? Electronic money has to be easy to use since the systems aim, at least theoretically, at the totality of the population addressing all kinds of individual expertise.

There are two different types of approaches to electronic money: on-line and off-line electronic money.

On-line means there is a need to interact with a bank or another "trusted third party" (via modem or network) to conduct a transaction. On-line systems prevent fraud by requiring merchants to contact the bank's computer with every sale. The bank's computer maintains a database that can indicate to the merchant if a given piece of electronic money is still valid. This is similar to the way merchants currently verify credit cards at the point of sale.

Off-line means that a transaction can be conducted without having to involve a bank directly. Off-line electronic money systems prevent fraud in basically two different ways. There is a hardware and a software approach. The hardware approach relies on some kind of a tamper-proof chip in a smart card that keeps a mini database. The software approach is to structure the electronic money and cryptographic protocols to reveal the identity of the double spender by the time the piece of e-money makes it back to the bank. If users of the off-line electronic money know they will get caught, the incidence of double spending will be minimized, at least in the theory.[8]

On-line or off-line, those six characteristics (independence, security, privacy, transferability, divisibility, and ease of use) define the problem space that each electronic money system promoter attempts to solve for one goal: public acceptance wide enough to make the system profitable for those who run it.

Depending on the way digital money is implemented there exist different cryptographic methods and organizational precautions to avoid the usage of forged money. Basically, there are two different types of digital coin-based money:

- Using specific cryptographic methods the anonymity of digital money may be achieved. Then, neither the financial institution nor the dealer may build up a connection between the customer and coins used by him. The financial institution only knows to which customer the coins are transferred initially[6]
- Coins with customer identifying characteristics allow the financial institution to identify the customer and to follow up on payments where the coin has been used in.

Also, the payment process may be classified into online and offline transactions. Table 1 summarises the different approaches.

Table 1. Security approaches to avoid copying digital coins [7]

	Offline payments by storing information	Online payments with check
Anonymous digital coins	Secret sharing on the coin	Blinding by financial institution
Coins with identifying characteristics	Transaction on the coin	Information by financial institution

- If an online payment takes place the coins will be checked immediately for authenticity. This implies that a digital coin is used only once. The financial institution needs to check the authenticity by using a list of all coins that have been issued or a list of all coins that have been sent in for credit.
- In case of offline payments the coins may be used more than once. To avoid double spending it is necessary to store information about the user or the users on the coin in order to be able to perform checks later. Anonymity may be guaranteed by so-called secret sharing. Then, the financial institution only gets information in case of double spending [4].

5.3. The Actors

Three different groups can be identified that ultimately influence which system(s) will be accepted. One is the industry, comprising two subgroups: the one that processes the financial information (large multi-national banking corporations and the major credit card firms), and the one that develops the hard- and software (ranging from encryption specialists to manufacturers of chips and readers for smart cards). These two subgroups are highly interlinked [7] in complex structures of competing alliances.

The second important group is the government defining the legal framework in which the electronic money systems will have to operate. The global nature of the network environment puts certain limits on the reach of individual governments and their power to regulate. As with all problems related to transactions over global networks, the governments have to operate in the dichotomy of international standardisation of legal systems and national implementation of these standards.

While a national government in such an environment is no longer completely autonomous in setting the legal framework, it remains the only actor that can ultimately enforce any kind of international legal system. Of specific concerns from the governmental point of view are two related problems: tax evasion and money laundering. On all levels of national and international governmental organizations proposals on how to regulate electronic commerce and money are currently being worked on.

The third group are the users, both the customers and the merchants. However, their role is different. While the first two groups have the ability to influence the definition of the system itself, the users have mainly the possibility of choice only from among potions presented by others to them. They can favour one system over the other or not accept any of them. However, it is difficult to assess how extensively this will influence the specifics of any given system and how much these specifics influence the customer decision once the industry's standards are defined. Very influential in terms of user acceptance will also be the conditions under which the industry's favoured system(s) will be offered [8].

The three groups—industry, government, and users—are highly related and their decisions are influenced not only by their own preferences but also by their assessment of the preferences of the other two groups. The industry has to develop a system that is not only optimal to them, but also conform with existing laws and not likely to be outlawed in the future. Furthermore it has to assess what might be accepted by the users and how to influence the acceptance of their competing solutions. The governments while consolidating its own (tax) base have to relate their decisions on the industry's development and balance it with their own responsibility to the public good. The users are likely to base their decisions on the anticipated future of the industry. Once a standard seems to be defined it is likely that acceptance will concentrate there, not because it is necessarily the "best" but because it seems to be the standard. The economist W. Brian Arthur calls this phenomenon of self-perpetuating dynamics the "law of increasing returns and path dependence" which are "mechanisms of positive feedback that operate – within markets, businesses and industries – to reinforce that which gains success or aggravate that which suffers loss." However, the single most influential group is clearly the industry, not only because the nature of the technological development (high pace, capital intensity, complexity, and global scope) structurally favours the industry over the slower national governments and the generally uninformed public, but also because the US administration, as the single most important government, shows great reluctance in seeking an active role for the government. A (December 1996) government proposal called "A Framework for Global Electronic Commerce" is based on four principles:

1. The private sector should lead.
2. Governments should avoid undue restrictions on electronic commerce.
3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.
4. Governments should recognize the unique qualities of the Internet [8].

5.4. Netcash

Introduction

NetCash [9], [10] is a framework for electronic cash developed at the Information Sciences Institute of the University of Southern California. It uses identified online electronic cash. Although the cash is identified there are mechanisms whereby coins can be exchanged to allow some anonymity. The system is based on distributed currency servers where electronic checks, such as NetCheque can be exchanged for electronic cash. The use of multiple currency servers allows the system to scale well [11].

NetCash is designed to support realtime electronic payments with varying transaction anonymity characteristics to geographically dispersed clients in multiple administrative domains. The primary contribution of NetCash is as a framework for integrating anonymous electronic currency into the global banking and accounting infrastructure. This Section defines a practical electronic currency protocol that provides weaker anonymity than the unconditional anonymity provided by Chaum [6] (see later). The framework is useful even where unconditional anonymity is required since the protocols implementing Chaum's currency can replace the basic building blocks of the protocol described in [13] while leaving the basic framework intact. The NetCash infrastructure is based on independently managed, distributed currency servers that provide a point of exchange between anonymous electronic currency and nonð anonymous instruments such as electronic checks. In the framework, checks based on the global accounting infrastructure tie together currency servers in different administrative domains, into a financial federation where currency minted by different servers is accepted [7].

The Communication Structure

The NetCash system consists of buyers, merchants, and currency servers. An organisation wishing to set up and manage a currency server obtains insurance for the new currency from a central certification authority. The currency server generates a public/private key pair. The public key is then certified by being signed by the central authority. This certificate contains a certificate ID, name of the currency server, currency server's public key, issue date and an expiry date, all signed by the central authority:
{Certif_id,CS_name,K[public,CS],issue_date,exp_date}
K[private,Auth]

The currency server mints electronic coins, which consist of:

1. *Currency Server Name:* Identifies a currency server.
2. *Currency Server Network Address:* Where the currency server can be found. If this address is no longer in use, a name server can be queried to find the current address.
3. *Expiry Date:* Limits the state that must be maintained by each currency server.
4. *Serial Number:* Uniquely identifies the coin.
5. *Coin Value:* Amount coin is worth.

The coin is signed with the currency server's private key:
{CS_name,CS_addr,exp_date,serial_num,coin_val}K[private,CS]

The currency server keeps track of the serial numbers of all outstanding coins. In this way double spending can be prevented by checking a coin's serial number with the currency server at the time of purchase (or exchange). If the coin's serial number is in the database it has not been spent already and is valid. When the coin is checked the serial number is then removed from the database. The coin is then replaced with a new coin (coin exchange).

An electronic cheque can be exchanged with a currency server for electronic coins. The currency server is trusted not to record to whom the coins are issued. To further aid anonymity a holder of coins can go to any currency server and exchange valid coins for new ones. The currency server does not know who is exchanging coins, only the network address of where they are coming from. By performing the exchange and by choosing any currency server to do this with, it becomes difficult to track the path of the coins. If a currency server receives coins that were not minted by it, it will contact the minting currency server to validate those coins.

Fig. 1 shows how a buyer uses NetCash coins to purchase an item from a merchant. In this transaction the buyer remains anonymous since the merchant will only know the network address of where the buyer is coming from. NetCash assumes that the buyer has or can obtain the public key of the merchant, and that the merchant has the public key of the currency server.

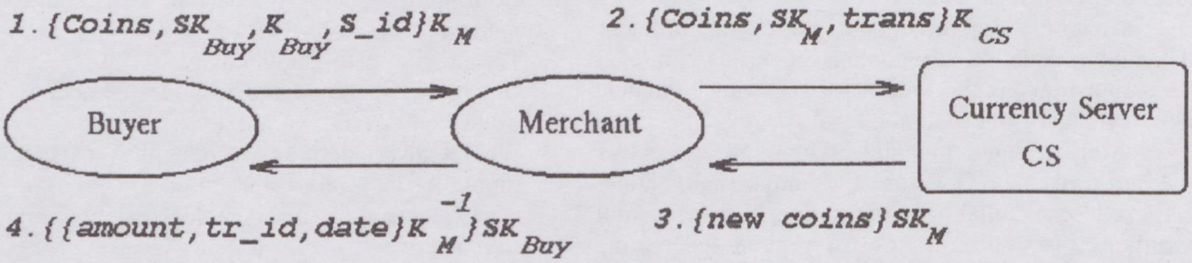


Fig. 1. Purchasing from a merchant using NetCash

Implementation details of how the NetCash protocols might be linked with applications such as the Web are not available, but it could be done in a similar fashion to Ecash using an out-of-band communications channel. The transaction consists of the following four steps, starting from when the buyer attempts to pay the merchant:

1. The buyer sends the electronic coins in payment, the identifier of the purchased service(S_id), a freshly generated secret key (SK[Buyer]), and a public session key (K[public,Buyer]), all encrypted with the Merchant's public key, to the merchant.
{Coins,SK[Buyer],K[public,Buyer],S_id}K[public,Merchant]
The message can't be eavesdropped or tampered with. The secret key is used by the merchant to establish a secure channel with the buyer later. The public session key is later used to verify that subsequent requests

originate from the buyer who paid for the service.

2. The Merchant needs to check that the received coins are valid. To do this he sends them to the currency server to be exchanged for new coins or for a cheque. The merchant generates a new symmetric session key SK[Merchant] and sends this along with the coins and the chosen transaction type to the currency server. The whole message is encrypted with the server's public key so that only it can see the contents:
{Coins,SK[Merchant],transaction_type}K[public,CS]
3. The Currency Server checks that the coins are valid by checking its database. A valid coin is one whose serial number appears in the database. The server will then return new coins or a cheque to the merchant, encrypted with the merchant's session key:
{New_coins}SK[Merchant]
4. Having received new coins (or a cheque) the merchant knows that he has been properly paid by the buyer. He now returns a receipt, signed with his private key and encrypted with the buyer's secret key:
{{Amount,transaction_id,date}K[private,Merchant]}SK[Buyer]
The buyer can then use the transaction identifier and the public session key to obtain the service purchased.

Discussion

This is the basic purchase protocol used in NetCash. While it prevents double spending it does not protect the buyer from fraud. There is nothing to stop the merchant spending the buyer's coins without providing a receipt.

Extensions to the protocol are detailed in [10]. These are more complex and give protection against fraud for both the merchant and buyer. There are also mechanisms to allow the merchant to be fully anonymous to the buyer. Partially off-line protocols where the bank does not need to be contacted during a purchase are also described. These however rely on the buyer contacting the currency server beforehand, and knowing who the merchant is at that time. They use a time window in which the coins are only valid for certain short lengths of time. Full technical details are given in [10].

The advantages of NetCash are that it is scalable and secure. It is scalable since multiple currency servers are present and security is provided by the cryptographic protocols used. Possible disadvantages of the system are that it uses many session keys and in particular public key session keys. To generate a public key of suitable length to be secure takes a very large amount of time compared with that involved in generating a symmetric session key. This could compromise the performance of the system as a whole.

NetCash provides scalability and acceptability with weaker anonymity and only a limited form of offline-operation. For many transactions this is sufficient. Where unconditional anonymity or completely offline operation is required, this framework can be extended to integrate exchanges from other protocols. Protocols have been proposed that support scalable distributed accounting without anonymity. These protocols provide an accounting infrastructure within which funds can be transferred between clients and servers [11].

5.5. Mondex

Introduction

Multifunctionality is one of the most exceptional features of Mondex, a system that intends become "an electronic equivalent of cash". It is based on a smart card that can hold money and transfer it in both ways. The Mondex card is a debit card in the sense that is can only be used to spend as long as it holds previously loaded money. The Mondex technology, in development since 1990, is exclusively owned by Mondex International, a London-based firm .

The Communication Structure

At the core of the Mondex system is a smart card that is able to accept, store and distribute money. Moreover, the card does not only store the current total amount of money, it is also stores its recent payment history. At the moment, there are two different types of cards, the consumer card that stores the last 10 transactions and the merchant card that stores the last 300 transactions. This number of transactions stored is limited by the present state of suitable micro-chips, however, Mondex announces in the FAQ section of their webpage that "with more powerful chips this trail capacity is likely to increase".

The Mondex card issued by banks and connected to a bank account. Each card has an unique 16 digit number that identifies the person to whom the card is issued. This number is transferred with every transaction from one Mondex chip to another and displayed in the payment trail.

The transfer money both Mondex cards (the sending and the receiving one) have to be inserted in some kind of reader where the start to communicate to authenticate each other. Mondex is a closed system in the sense that cash can only be transferred from one Mondex card to another. Based on non-disclosed identifying features the cards establish a secure communication using digital signatures for transaction and receipt.

Encryption plays a central role in the Mondex scheme. It has to guarantee that only authenticated, untampered Mondex cards are used in the system and that the communication between the two cards can not be intercepted. Therefore the receipt that ends each transaction is crucial to proof the uninterrupted transfers of the cash.

As a stored value card with strong encryption Mondex does not need a central clearing institution as, for example, the DigiCash system. The transfer is direct between the two sides. However, this increases the security risks substantially. If a card could be forged and new money inserted into the system it would be impossible to differentiate forged from legitimate money. Therefore the constant update and the secrecy of the details of the communication protocol is an essential feature of the Mondex system.

Since all communication between the readers is encrypted Mondex can use open communication networks such as the telephone system or the Internet. Card readers can be attached to computers or phones – similar to the existing phone card readers – they can also be used, for example, in stores, buses or parking meters.

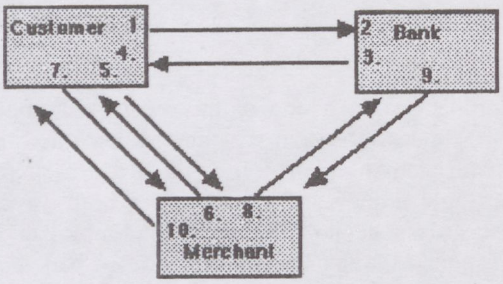


Fig. 2. The Mondex Structure

Mondex allows uncleared, reciprocal transfers between all groups within the system. Between the bank and the customer, among customers (peer-to-peer) and between the merchants and the customers.

Discussion

Mondex has an extensive industry support. Besides the majority holder MasterCard, the shareholders of Mondex International Limited include NatWest Bank, Midland Bank, Royal Bank of Canada, Canadian Imperial Bank of Commerce, Hongkong Shanghai Banking Corporation, Wells Fargo, AT&T, Chase Manhattan, First Chicago NBD and 10 major banks in Australia (Business Wire, 24.2.1997). With such a support Mondex has resources to pursue its implementation that are by far greater than any other electronic money systems.

However, what differentiates Mondex is not only that is one of the industry's most favourite solutions, but also that is, once the hardware is in place, fairly easy to use in quite conventional ways, superficially mimicking the conventional ideas about cash being money that resides in the user's wallet until it is taken out or additional money is deposited.

What might be the single most important feature is its multi-functionality: it can be used in a number of different situations, such as traditional, physical payment situations, in store or peer-to-peer, but also as a means of electronic payment over all kinds of networks and it can be used for large payments and also for micropayment. A card can store several hundred $ while the lowest threshold for Mondex is somewhere around a few cents. At the current stage is optimized to be used for medium sized payments. Functions as the storing capability of the last 300 (or 10) transactions make no sense if the payment size is very small. However, Mondex is adaptable in this regard.

Mondex has been developed primarily for the direct substitution of traditional cash in physical situations, therefore the first large public test sites have been localities: the two mid-sized towns Swindon UK and Guelph, Ont.. However, Mondex is developing applications and partnerships to use its smart cards also over the Internet in partnership with AT&T, HP and Open Market Inc [8].

5.6. Millicent

Introduction

The goal for MilliCent is to allow for transactions that are inexpensive yet secure. This is achieved by using accounts based on scrip and brokers to sell scrip.

A piece of scrip represents an account the customer has established with a vendor. At any given time, a vendor has outstanding scrip (open accounts) with the recently active customers. The balance of the account is kept as the value of the scrip. When the customer makes a purchase with scrip, the cost of the purchase is deducted from the scrip's value and new scrip (with the new value/account balance) is returned as change. When the customer has completed a series of transactions, he can "cash in" the remaining value of the scrip (close the account).

Brokers serve as accounting intermediaries between customers and vendors. Customers enter into long-term relationships with brokers, in much the same way as they would enter into an agreement with a bank, credit card company, or Internet service provider. Brokers buy and sell vendor scrip as a service to customers and vendors. Broker scrip serves as a common currency for customers to use when buying vendor scrip, and for vendors to give as a refund for unspent scrip.

Security and Trust

The security model for MilliCent is based on the assumption that scrip is used for small amounts. People and businesses treat coins differently than they treat bills, and treat small bills differently than large bills. In MilliCent people treat scrip as they would treat change in their pocket.

Since people don't need a receipt when buying candy from a vending machine, they don't need a receipt when buying an item using scrip. If they don't get what they paid for, they complain and get a refund. If they lose a coin every now and then, they aren't too upset.

It is expected, that users to have a few dollars of scrip at a time. We don't expect them to have hundreds, or even tens, of dollars of scrip. As a result, scrip is not worth stealing unless you can steal lots of it; and if you steal lots, you will get caught.

Trust Modell

MilliCent assumes asymmetric trust relationships among the three entities – customers, brokers, and vendors. Brokers are assumed to be the most trustworthy, then vendors, and, finally, customers. The only time customers need to be trusted is when they complain about service problems.

Brokers will tend to be large, well-known, and reputable financial institutions (like Visa, MasterCard, and banks) or major Internet or online service providers (like CompuServe, NETCOM, or AOL). Finally, there will be large numbers of customers who are as trustworthy as people are in general.

Three factors make broker fraud unprofitable. First, customer and vendor software can independently check the scrip and maintain account balances, so any fraud by the broker can be detected. Second, customers do not hold much scrip at any one time, so a broker would have to commit many fraudulent transactions to make much of a gain and this makes them likelier to be caught. Finally, the reputation of a broker is important for attracting customers and a broker would quickly lose its reputation if customers have troubles with the broker. The repeat business of active customers is more valuable to a broker than the scrip that it could steal.

Vendor fraud consists of not providing goods for valid scrip. If this happens, customers will complain to their broker, and brokers will drop vendors who cause too many complaints. This acts as an effective policing mechanism, because vendors need a broker to easily conduct business in MilliCent.

As a result, the MilliCent protocol is skewed to prevent customer fraud (forgery and double spending) while providing indirect detection of broker and vendor fraud.

Security

The security of MilliCent transactions comes from several aspects.

- All transactions are protected.
  Every MilliCent transaction requires that the customer knows the secret associated with the scrip. The protocol never sends the secret in the clear, so there is no risk due to eavesdropping. No piece of scrip can be reused, so a replay attack will fail. Each request is signed with the secret, so there is no way to intercept scrip and use the scrip to make a different request.
- Inexpensive transactions limit the value of fraud.
  Inexpensive transactions can rely on inexpensive security: it's not worth using expensive computer resources to steal inexpensive scrip. In addition, it would take many illegal uses of scrip to acquire much money, and that raises the probability of getting caught.
- Fraud is detectable and eventually traceable.
  Fraud is detected when the customer doesn't obtain the desired goods from the vendor, or when the balance returned to the customer doesn't match the balance due. If the customer is cheating, then the vendor's only loss is the cost of detecting the bad scrip and denying service. If the vendor is cheating, the customer will report a problem to the broker. When a broker notices a pattern of complaints from many customers against a vendor, it can pinpoint the fraud and cut off all dealings with the vendor. If a broker is cheating, the vendor will notice bad scrip coming from many customers, all originating from a single broker. The vendor can then publicize its complaint in an appropriate venue.

Scrip

The main properties of scrip are:

- It has value at a specific vendor.
- It can be spent only once.
- It is tamper resistant and hard to counterfeit.
- It can be spent only by its rightful owner.
- It can be efficiently produced and validated.

The next sections give more detail about scrip and its use, but the basic techniques to achieve these properties are outlined here:

- The text of the scrip gives its value and identifies the vendor.
- The scrip has a serial number to prevent double spending.
- There is a digital signature to prevent tampering and counterfeiting.
- The customer signs each use of scrip with a secret that is associated with the scrip.
- The signatures can be efficiently created and checked using a fast one-way hash function (like MD5 or SHA).

Scrip Structure

There are three secrets involved in producing, validating, and spending scrip. The customer is sent one secret, the customer_secret, to prove ownership of the scrip. The vendor uses one secret, the master_customer_secret, to derive the customer_secret from customer information in the scrip. The third secret, the master_scrip_secret, is used by the vendor to prevent tampering and counterfeiting.

The secrets are all used in a way that shows knowledge of the secret without revealing the secret. To attest to a message, the secret is appended to the message, and the result is hashed to produce a signature. The message (without the secret) and the signature prove – due to the one-way nature of the hash function – knowledge of the secret, because the correct signature can only be derived if you know the secret.

Scrip has the following fields (Fig. 3):

- Vendor identifies the vendor for the scrip.
- Value gives the value of the scrip.
- ID# is the unique identifier of the scrip. Some portion of it is used to select the master_scrip_secret used for the certificate.
- Cust_ID# is used to produce the customer secret. A portion of Cust_ID# is used to select the master_customer_secret which is also used in producing the customer secret.
- Expires is the expiration time for the scrip.
- Props are extra data describing customer properties (age, state of residence, etc.) to the vendor.
- Certificate is the signature of the scrip.

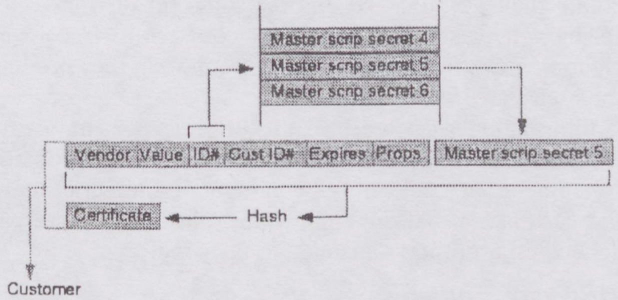


Fig. 3. The certificate of a piece of scrip is generated by hashing the body of the scrip with a secret. The secret is selected using a portion of the scrip's ID#.

Validation and expiration

Scrip is validated in two steps. First (Fig. 4), the certificate is recomputed and checked against the certificate sent with the scrip. If the scrip has been tampered with, then the two certificates will not match. Second, there is a unique identifier (ID#) included in the scrip body and the vendor can check for double spending by seeing if it has recorded that identifier as already spent. Generating and validating scrip each require a little text manipulation and one hash operation. Unless the secret is known, scrip cannot be counterfeited or altered.

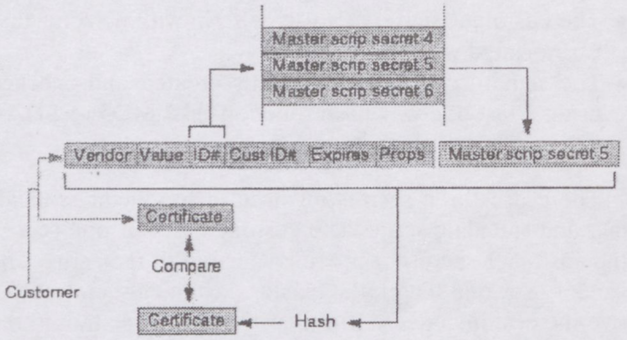


Fig. 4. The received scrip is validated by regenerating the certificate and comparing it to the transmitted one. If they are identical, the scrip is valid.

The vendor records the unique identifier of every piece of scrip that is spent, so that is cannot be fraudulently re-spent. To save the vendor from maintaining this record forever, each each piece of scrip is given an expiration time. Once the scrip expires, the vendor no longer has to worry about it being re-spent and can erase its record of the scrip.

Customers are responsible for renewing or cashing in scrip before it expires. The old scrip is submitted to the vendor, who returns new scrip with a later expiration time (and a new serial number). Vendors may choose to charge a small fee for this service, discouraging users from obtaining more scrip than they will need in the near future.

Properties

Scrip also has fields for storing properties, which are inserted by the vendor or broker when the scrip is produced. The exact property fields and their values will depend on an agreement between the brokers and vendors. The brokers will get the information from customers when they create their account and enforce some set of rules when selling vendor scrip. Vendors, of course, are free to include whatever properties they desire in scrip they produce themselves.

Information such as the state of residence, or age of the consumer assists the vendor in making sales decisions. Adult material could only be bought if the scrip shows the customer is old enough. State sales tax charges can depend on a property included in the scrip.

Millicent Protocols

Scrip is the basis of a family of MilliCent protocols. Three of them will be compared in their simplicity, secrecy, and security.

The first, "scrip in the clear", is the simplest and most efficient protocol. It is the basis for the other two protocols, but it may not be useful in practice because it is too insecure. The second, "private and secure", is secure and offers good privacy, but it is more expensive. The third, "secure without encryption", is also secure, but trades privacy for greater efficiency.

Scrip in the clear

In the simplest possible MilliCent protocol, the customer just sends an unspent piece of scrip in the clear (i.e., not encrypted or protected in any way) along with each request to the vendor. The vendor returns the desired result along with a new piece of scrip (also in the clear) as change.

This protocol offers almost no security: an eavesdropping third party can intercept the scrip being returned as change and use it himself. When the rightful owner later attempted to spend the scrip, the vendor would have a record of it being previously spent, and would refuse the request.

Private and Secure

To add security and privacy to the MilliCent protocol, a shared secret can be established between the two parties and then use the secret to set up a secure communications channel using an efficient, symmetric encryption method (such as DES, RC4, or IDEA).

In MilliCent, scrip can be used to establish this shared key. When a customer buys an initial piece of scrip for a vendor, a secret is generated based on the customer identifier, and returned securely with the scrip (Fig. 5). This requires either that the transaction be performed using some secure non-MilliCent protocol, or that the scrip be purchased using a secure MilliCent transaction.

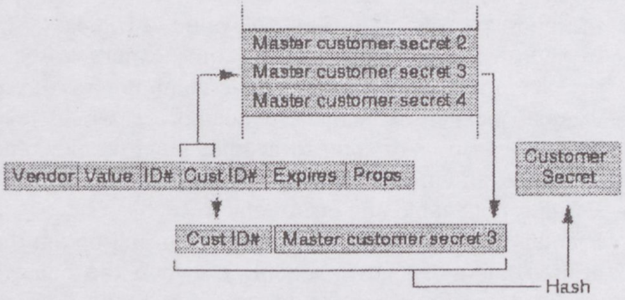


Fig. 5. The customer secret is generated by hashing the customer identifier with a secret. The secret is selected using a portion of the customer identifier.

The vendor does not directly record the secret associated with the piece of scrip. Instead, the customer identifier (Cust_ID#) field of the scrip allows rapid recalculation of the secret. The customer identifier must be unique whenever scrip is transmitted to a new customer, but it need not have any connection to the identity of the customer.

When the vendor receives the request, he derives the customer secret from the customer identifier in the scrip, derives the message key from the customer secret, and uses the message key to decrypt the request. The change scrip can be returned in the clear, while the response and any new secrets are returned to the customer encrypted by the message key.

In this protocol the request and the response are kept totally private; unless an eavesdropper knows the customer secret, he can't decrypt the messages. In addition, an eavesdropper can't steal the scrip because it can't be spent without knowing the customer secret.

Secure without encryption

The previous section describes how the secret shared by the customer and vendor can be exploited to achieve security and privacy. But a full-blown encrypted channel may be overkill for some MilliCent applications. In this, third variant of the protocol, the privacy of the request and response is given up to eliminate the use of encryption.

As in the previous protocol, the customer securely gets an initial piece of scrip and customer secret. To make a purchase, the customer sends the request, scrip, and a "signature" of the request to the vendor. The signature is produced in the same way that the certificate of the scrip is produced. The scrip and request are concatenated with the customer secret. The customer runs an efficient cryptographic one-way hash function over this string and sends the resulting hash as the signature.

When the vendor receives the request, he derives the customer secret from the scrip and regenerates the signature for the request. If the scrip or request have been tampered with in any way, the signature will not match (Fig. 6).

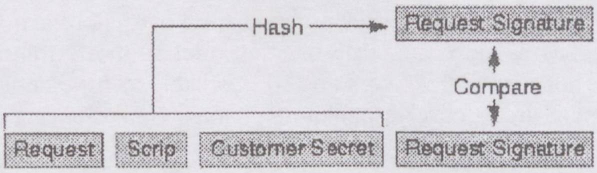


Fig. 6. The request is validated by re-generating the request signature and comparing to the transmitted signature. If they match, the request is valid.

The vendor now handles the request and returns a fresh piece of scrip as change. The change scrip shares the same customer identifier as the scrip submitted with the request, so that the original customer secret can be used to spend the change. There is no need to encrypt any of the response; an eavesdropper can't steal the scrip because the signature of the request can't be made without knowing the customer secret. The vendor may sign the response with the customer secret in order to prove authenticity to the customer.

Thus, with only a few hashes, MilliCent provides a lightweight and secure protocol.

Brokers

Brokers maintain the accounts of customers and vendors, and they handle all real-money transactions. The customer establishes an account with a broker by using some other method (like a credit card, or a higher-security electronic commerce system) to buy some broker scrip. The customer then uses the broker scrip to buy vendor scrip.

The vendor and the broker have a long-term business relationship. The broker sells vendor scrip to customers and pays the vendor. There can be different business models for the way the broker gets vendor scrip, for example, pay in advance, consignment sale, or licensed production. In all models, the broker can make a profit selling scrip because he pays the vendor (at a discount) for scrip in bulk and sells individual pieces to customers.

When a customer wants to make a purchase, the customer contacts the broker to obtain the necessary vendor scrip. The customer uses his broker scrip to pay for the vendor scrip using the MilliCent protocol. The broker returns the new vendor scrip along with change in broker scrip.

We will examine three ways in which the broker gets the vendor scrip. The "scrip warehouse" model assumes a casual relationship between the broker and vendor. The "licensed scrip producer" model assumes a substantial and long-lasting relationship between the broker and vendor. The "multiple broker" model assumes a relationship between brokers, but requires no relationship between the vendor and broker.

Scrip warehouse

When the broker is acting as a scrip warehouse, the broker buys multiple pieces of scrip from a vendor. The broker stores the scrip and sells the pieces one at a time to customers.

This model assumes no special relationship between the vendor and broker. It works best when the broker's customers have a light to moderate demand for that vendor's scrip. The broker uses the MilliCent protocol to buy the scrip from the vendor in the same way a customer would. Selling scrip in large blocks is more efficient for the vendor since the communication and financial transaction costs are amortized over all the pieces of scrip. The broker makes a profit when it resells the scrip to customers at full price. The vendor depends on the broker to ensure any customer properties encoded in the scrip.

Licensed scrip production

If a broker's customers buy a lot of scrip for a specific vendor, it may be desirable for a vendor to "license" the broker to produce vendor scrip. This means that the broker generates scrip that the vendor can validate and accept. The vendor sells the the broker the right to generate scrip using a given master_scrip_secret, series of scrip ID#'s, master_customer_secret, and series of customer identifiers. The vendor can validate the licensed scrip because the master_scrip_secret is known from the series of the scrip ID# and the master_customer_secret is known from the series of the customer identifier.

Brokers produce the scrip and collect money from customers; vendors record the total value of scrip originating from a particular broker. When all the scrip produced under a particular contract has expired, brokers and vendors can settle up. The broker presumably takes some commission for producing the scrip.

A license covers a specific series (unique range of identifiers (ID#'s)) of scrip for a given period of time, and the secrets shared between the broker and vendor only apply to that series. A vendor can issue licenses to different brokers by giving out different series and secrets to each one. Of course, a vendor can produce its own scrip using its own private series and secrets.

Licensing scrip production is more efficient for the vendor and broker than the scrip warehouse model. There is less communication because the license is smaller to transmit than a few pieces of scrip. The vendor does less computation since it does not have to generate the scrip itself. The broker does not have to store large blocks of scrip, since it can generate the scrip on demand. Additionally, it allows the broker to encode specific user properties into each piece of scrip it generates.

Multiple Broker

In an environment where there are multiple brokers, a customer of one broker may want to make a purchase from a vendor associated with another broker. If the vendor only wants to have an account with its own broker (perhaps to simplify accounting), the customer will have to go through the vendor's broker to buy vendor scrip.

The entire transaction will go like this:

- The customer asks his broker for vendor scrip.
- The customer's broker tries to set up account with the vendor.
- The vendor tells the customer's broker his broker's name.
- The customer's broker buys broker scrip from the vendor's broker.
- The customer's broker returns the vendor's broker's scrip to the customer.
- The customer buys vendor scrip from the vendor's broker.
- The customer uses the vendor scrip at the vendor.

The idea of licensed scrip production can be extended so that brokers can generate broker scrip for other brokers [12].

Discussion

The range of potential applications for MilliCent is quite broad. With current technology, MilliCent is appropriate for transactions from a few dollars to as little as one-tenth of a cent. The upper bound comes from the trust model for brokers and the availability of alternative protocols appropriate for transactions above a few dollars, while the lower bound comes from a conservative estimate based on the computational costs of a broker. This price range covers most print and information services that will be available in an online format – magazines, newspapers, encyclopedias, indices, newsletters, and databases.

MilliCent reduces the overhead of accounts in a number of ways:

- Communication costs are reduced by verifying the scrip locally at the vendor's site; there are almost no MilliCent-specific communication costs during a normal transaction. There is also no need for a centralized server or an expensive transaction-processing protocol. In a centralized scheme, the central site is a bottleneck; the provider must have sufficient computing power to handle the peak transaction rate. In MilliCent, there is no central server; there can be many brokers, a broker is only involved in a fraction of the transactions between a customer and a vendor, and the transactions involving a broker are lightweight.
- Cryptographic costs are reduced to keep them in line with the scale of transactions; there's no need for strong or expensive cryptographic schemes because the value of the scrip is relatively low. The cost of breaking the protocol must be only greater than the value of the scrip itself.
- Accounting costs are reduced by using brokers to handle accounts and billing. The customer establishes an account with a broker; the broker establishes its own accounts with the vendors. Using brokers allows us to split a customer-vendor account into two accounts: one between the customer and broker, and another between the broker and the vendor. This reduces the total number of accounts. Instead of many separate accounts for every customer-vendor combination, each customer has only one account with a broker (or, at most, a couple of brokers); and each vendor has long-standing accounts with just a few brokers.

  In most account-based schemes, the vendor maintains the account balance. In MilliCent, the customer maintains the account balance – it is encoded in the scrip held by the customer. There is no risk for the vendor because a digital signature prevents the customer from modifying the scrip's value. Since the scrip contains the account balance and a proof of correctness for that value, the vendor does not need to look up the customer's balance, saving disk activity.
- The minimum monthly charges are not as much of a problem because they are amortized over more activity. The single customer-broker account supports transactions with all vendors and so it is likely to have enough activity to cover a minimum charge. By pre-paying the broker, even the monthly accumulation of charges can be avoided [12].

MacKie-Mason and Varian [13] argue that as the Internet develops there will be increasing pressure for usage-based charges. Current free Internet services like e-mail, file transfers, the Internet telephone, and teleconferencing will have to be paid for. At the lowest level, they estimate that the cost of transmitting one packet on the Internet backbone is one six-hundredth of a cent. MilliCent is quite efficient enough for such packet-level charges; for these there are proposals like the non-cryptographic Digital Silk Road [14]. MilliCent can be used for per-connection charges for these services.

5.7. Ecash – Digicash

Introduction

DigiCash, founded 1990, is the company of David Chaum, a internationally acknowledged expert in the field of cryptography who has worked on related projects for more than a decade. The main concern of his Ecash is "unconditional untraceability" of all financial transactions. To achieve this, the system relies extensively on cryptographic public-key solutions developed by Chaum (Chaum 1985, 1992, 1996) [8].

Like banknotes, eCash can be withdrawn from and deposited to transaction demand deposit accounts. And like banknotes, one person can transfer possession of a given amount of eCash to another person. But unlike cash, when a customer pays another customer an electronic bank will play an unobtrusive but essential role [15].

The customer and the merchant need a bank account with a bank issuing Ecash as well as they need to register with DigiCash to obtain a special software, the "cyberwallet". This software allows to generate randomly 100 digit numbers. These numbers represents the "raw material" of a coin. The numbers are blinded (multiplied with a factor only known to the sender) and sent to the bank. They become "real" coins when they are digitally validated by the issuing bank. The bank validates the coins by adding a string of numbers to them. The new sequence of numbers (consisting of the blinded number of the customer and the validation string of the bank) now represents a coin, a fixed amount of money, hence the slogan of DigiCash: "Numbers that are money". Before sending it back to the customer the bank subtracts the amount from his account. Since the coins are blinded the bank does not know which coins it has validated, it only knows the amount validated and the recipient of the Ecash. This is similar to cash and enough to do information all accounting but not enough to connect a specific coin to the customer. The customer receives the validated coins and unblinds them [8].

Advantage of Blinded Coins

This extension of digital signatures, called blind signatures, can restore privacy. Before sending a note number to the bank for signing, the customer in essence multiplies it by a random factor. Consequently, the bank knows nothing about what it is signing except that it carries the customer's digital signature. After receiving the blinded note signed by the bank, the customer divides out the blinding factor and uses the note as before.

The blinded note numbers are "unconditionally untraceable" that is, even if the shop and the bank collude, they cannot determine who spent which notes. Because the bank has no idea of the blinding factor, it has no way of linking the note numbers that the merchant deposits with the customer's withdrawals. Whereas the security of digital signatures is dependent on the difficulty of particular computations, the anonymity of blinded notes is limited only by the unpredictability of the customer's random numbers. If someone wishes, however, the customer can reveal these numbers and permit the notes to be stopped or traced.

Blinded electronic bank notes protect an individual's privacy, but because each note is simply a number, it can be copied easily. To prevent double spending, each note must be checked on-line against a central list when it is spent. Such a verification procedure might be acceptable when large amounts of money are at stake, but it is far too expensive to use when someone is just buying a newspaper. To solve this problem David Chaum, Amos Fiat and Moni Naor have proposed a method for generating blinded notes that requires the payer to answer a random numeric query about each note when making a payment. Spending such a note once does not compromise unconditional untraceability, but spending it twice reveals enough information to make the payer's account easily traceable. In fact, it can yield a digitally signed confession that cannot be forged even by the bank [6].

The Communication Structure

To make a purchase, the customer contacts the merchant and the two cyberwallets connect to prepare the transfer of the appropriate amount of coins. The transfer is conducted after the customer has confirmed it. The customer can specify certain transfers (for instance, to a specific address and up to a certain amount) to be conducted automatically in the background without requiring an extra confirmation.

The merchant sends the coins to the bank that has originally validated those coins. The bank proves whether the coins have been spent already by checking the number which it had added to the blinded coins against database of spent coins. If the coins are valid, then the bank transfers the money to the merchant's account: in effect, the coins have to be (de)centrally cleared.

All communication in the DigiCash system is digitally signed and encrypted, based on a public-key structure. For instance, the merchant encrypts the received coins with her private key (signature) and additionally with the bank's public key (communication security). This guarantees that only the bank can decrypt the message (and use the coins). The merchant has therefore the certainty that only the bank can get her coins and the bank knows the authenticated sender of the coins.

The whole communication process can be conducted in a couple of seconds.

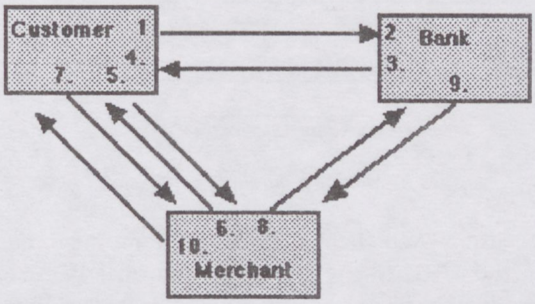


Fig. 7. Using the DigiCash Payment Scheme

Part I Making Money

1. The customer's cyberwallet software generates random serial numbers for the Ecash coins. The serial numbers are then blinded. The blinded coins are sent to the bank.
2. The bank checks the signature and debits the signature owner's account.
3. The bank validates the coins and returns them to the customer.
4. The customer unblinds the coins.

Part II Spending Money

5. The customer sends a buying request to the merchant.
6. The merchant send a request back to the cyberwallet software to send the money.
7. The customer confirms the transaction, the software transfers the exact number of coins.

Part III Redeeming Money

8. The merchant has to check the validity of the coins. She sends them to the bank that issued the coins.
9. The banks checks the serial number for double spending. If the coins are valid, the bank destroys the coins, adds the number to the database of spent coins and transfers the amount to the merchant's account.

Part IV Finishing the Transaction

10. After the coins have been validated, the merchants sends a receipt to the customer and the financial transaction is finished [8].

The Protocol of Spending Ecash coins

To spend Ecash coins, the user starts up their cyberwallet software and a normal Web client and then browses the Web till they find a merchant shop selling goods. The Ecash software can be used with any existing Web client and Web server software. A merchant shop is simply a HTML document with URLs representing the items for sale. To buy an item the user selects the URL representing that item. The following steps then occur as shown in Fig. 8.

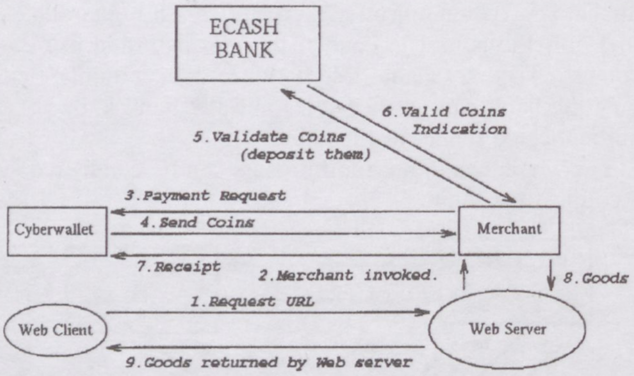


Fig. 8. Making a purchase with Ecash

1. The user's Web client sends a HTTP message requesting the URL to the Merchant's normal Web server. This URL will invoke a Common Gateway Interface (CGI) program.
2. The CGI program invoked will be the merchant Ecash software, and it will be passed details of the item selected encoded in the URL. The location of the buyer's host machine will also be passed in an environment variable from the server to the merchant Ecash software.
3. The merchant software, now contacts the buyer's wallet using a TCP/IP connection, asking it for payment.
4. When the cyberwallet receives this request, it will prompt the user, asking them if they wish to make the payment. If they agree, the cyberwallet will gather together the exact amount of coins and send this as payment to the merchant. The coins will be encrypted with the merchant's public key so that only the merchant can decrypt them:

   {Coins}K[public,Merchant]

   If they disagree or do not have the exact denominations necessary to make a correct payment, the merchant is sent a payment refusal message.
5. When the merchant receives the coins in payment, he must verify that they are valid coins, and have not been double spent. To do this he must contact the bank, as only the minting bank can tell whether coins have been spent before or not. Thus the merchant packages the coins, signs the message with his private key, encrypts the message with the bank's public key, and sends it to the bank:

   {{Coins}K[private,Merchant]}K[public,Bank]
6. The bank validates the coins by checking the serial numbers with the large on-line database of all the serial numbers ever spent and returned to the bank. If the numbers appear in the database then they are not valid, since they have been spent before. If the serial numbers don't appear in the database, and have the bank's signature on them, then they are valid. The value of the coins are credited to the merchant's account. The coins are destroyed, and the serial numbers added to the the database of spent coins. Thus coins are good for one transaction only. The bank notifies the merchant of the successful deposit.
7. Since the deposit was successful, the merchant was paid, and a signed receipt is returned to the buyer's cyberwallet.
8. The purchased item, or an indication of successful purchase of hard goods, is then sent from the merchant Ecash software to the Web Server.
9. The Web server forwards this information to the buyer's Web client [11].

Discussion

DigiCash is a full-fledged electronic money system. It's most unique feature is the user's anonymity intended by Chaum to "return control of personal information to the individual" ([6] p. 96). This means the customer and the merchant do not have to know each other (except for delivering purposes) and the bank can not connect the coins to a customer. The merchant only knows that the coins are valid and the bank only knows it issued the coins (and they haven't been spent yet) but does not know to whom. The user's control is strong because the anonymity features of the system are built into the client software (blinding the coins before sending them to the bank for validation) and are independent of the intentions or the policies of any company involved in the transaction process: the untraceability of the user is indeed unconditional, unless the user tries to spend it twice, which guarantees the security of the system

The system is primarily oriented towards PCs that are connected to a network. On the PC the special software must be installed and the network connection must not be interrupted during the transaction process since the merchant verifies the validity online before sending the requested product or service.

The system, however, is very flexible and can also be used offline for peer-to-peer payment. The coin, if duplicated, reveals the sender's identity and DigiCash claims that its Ecash is less likely to be forged than any traditional paper-based cash.

Furthermore, the DigiCash software does not necessarily need to reside on a PC it can also be applied for smart cards or other electronic devices. In this sense is independent of any specific physical device.

Technically, the main problem with Ecash may be the size of the database of spent coins. If a large number of people start using the system, the size of this database will become very large and unmanageable. Keeping a database of the serial number of every coin ever spent in the system is not a scaleable solution. DigiCash plans to use multiple banks each minting and managing their own currency with interbank clearing to handle the problems of scaleability.

Another problem could be the coin-based structure of

Ecash. The system has no change-return capability. As consequence, the customer must always provide the exact number of coins required for the purchase. The number of coins must be determined when the customer requests the money from the issuing bank. The low costs of transaction, supposedly less than US$ 0.01, allow to use Ecash for very small payments. However, this means that the user needs a considerable amount of coins. This inflexibility combined with the use of strong cryptography makes the system not very easy to use for multi-purpose situations like general spending over the Internet.

Paired with the reluctance of the financial industry and the government agencies against the unconditional untraceability this led to the situation that DigiCash despite of being one of the best known and most advanced projects in the field of electronic money has still not been able to build major industry alliances with banks that would actually issue Ecash

Ecash might find more acceptance in situations where anonymity is less contested and the value of each transfer more standardized, for example in systems to collect tolls for highways for which it has been tested extensively.

However, DigiCash is potentially a very powerful and versatile system. The transaction costs of possibly less than a tenth of a cent that could allow purchases of as little a one cent worth. From the user's point of view the unconditional anonymity might be very welcome, especially if the payment mechanism is so fine-grained that it is able to measure user behaviour down to very small units, in this case cent by cent.[8]

6. COMPARISON

The payment systems outlined each have their strengths and weaknesses. Ecash is a fully secure system that provides for very strong anonymity. The use of banks within the system reflects current practice in non-electronic payment systems. Successful operation of the Ecash system depends on the maintenance of a central database of all coins ever issued within the system. If it were to become accepted as a global payment system, this would quickly become a major problem.

MilliCent is best suited for a series of inexpensive, casual transactions. It relies on other protocols for initial account establishment between brokers and customers, and brokers and vendors. Other higher-value protocols are also used for the funds transfers that occur when accounts are periodically settled.

NetCash uses identified coins with multiple currency servers, and thus, while anonymity is maintained, there is only a requirement to keep track of all currency currently in circulation. This makes for a much more scaleable solution to the payment problem. NetCash is also fully secure, and achieves this using protocols that are quite complex in nature.

Mondex can be used for simple, everyday cash transactions. The Mondex electronic cash system operates on a smart card which stores information on a microchip, so it requires a hardware and a software too. But it offers a strong encrypton for the transaction.

As the search for a successful Internet business model continues, people are beginning to realize that no single business model is right for every content provider and multiple business models can be used in parallel. The next table compares the electronic cash systems:introduced in this paper.

7. CONCLUSIONS

Currently most financial institutions use the Internet as a presentation medium. Often there is a possibility to request additional information or to perform individual calculations. Business transactions are rather rare at least in most European countries. On the other hand, a lot of effort is devoted to construct solutions to manage financial routine transactions like money transfers, opening and closing of accounts, implementation and deletion of standing orders and much more. Payment systems are developed to facilitate electronic commerce. In order to realize significant rationalization potentials no isolated but integrated solutions that support existing business processes are required. Collaboration between competing financial institutions may be necessary to cut down development costs.

In general, financial institutions have to decide on their Internet presence. Is it worth to invest significant sums? It can be shown that there are not necessarily first mover advantages. On the other hand, fast reactions to actions of competitors are difficult since significant know-how is required to quickly build up an Internet presence. This implies that waiting too long may be extremely harmful and expensive. Consequently, a good strategy should be built up for know-how by means of small or medium pilot projects. Actions of competitors,as well as the development of the Internet should be monitored closely [4].

It is expected, that some banks will soon take up the challenge and see the obvious (and now stable) connections between marketing, payments, and the Internet – as is occurring in the smart card and bill payment markets. Some large partnerships are emerging, spurring activity among banks to grab the branding opportunities that have been present for several years. This is thought to be a marketing land-grab at first, as smart cards, SET, and bill payment are backed up behind Y2K and Internet banking in the technology queue [3]. Nonetheless, opportunities inherent in the integration of the Internet and its related opportunities will be a key differentiator between banks that will fully realize the value of their technology investments in the next decade and those that won't.

Table 2.

E-cash System/ Characteristic[8]	Netcash	DigiCash	Millicent	Mondex
Independence	No, PC only solution	Yes, mainly PC applicable based, but also for other storage devices	No, PC only solution	No, based on Proprietary smart card technology
Security	High, based on public key encryption	High, based on strong public key encryption and third party validation	Medium, based on light encryption issuerspecification. Small values make it light encryption secure enough to prevent infringement	High, based on unrevealed encryption technology
Privacy	Weak anonmity, but with extensions are available to give more protection against fraud	Very high, Guarantees unconditional untraceability of the user	Medium, the broker Knows who and where, but not what. The vendors knows what but not who.	Contested, most likely medium. The issuer controls the flows into and out of the circulation but not within
Transferability	Low, only an electronic cheque can be exchanged for electronic coins	High, user to user payment possible	Medium, scrip can be transferred freely but only used at specific sites.	High, user to user Payment possible
Divisibility	Medium, coin based	Medium, coin based from one cent upwards, low transaction costs	High, micropayment from a fraction of a cent to 5 $, very low transaction costs	High, from one cent to several hundred $, low transaction costs
Ease of use	Medium, complicated to set up (independent currency servers)	Medium, complicated to set-up and understand but easy to use	Medium, complicated to set up, easy to usc	High, easy to set up, easy to use, but needs hardware
On-line/ off-line	Needs clearing, can be used partially off-line	Needs clearing, can be used off-line	On-line only	Can be used off-line

REFERENCES

[1] Internet Open Trading Protocol, Part 2: Specification, Version: 0. 9, Date: 12 January 1998, Status: Draft for Public Comment

[2] Models of Electronic Commerce, Petra Aukia, Nixy Oy, Proceedings of Helsinki University of Technology Seminar on Network Security, 1995

[3] Internet Payments: Momentum or Muddle, Scott Smith, Journal of Internet Baninkg and Commerce: 1998. 11. 12, http://www. arraydev.com/commerce/JIIBC/current. html

[4] Internet Banking – An Overview, Juergen Seitz and Eberhard Stickel, Journal of Internet Baninkg and Commerce: 1998. 01. 8, http://www.arraydev.com/commerce/JIIBC/current. html

[5] NetCheque, Netcash, and the characteristics of Internet Payment Services, B. Clifford Neuman and Gennady Medvinsky, presented at MIT Workshop on Internet Economics, March, 1995

[6] Chaum, D. (1992): Achieving Electronic Privacy. In: Scientific American, August, pp. 96-101.

[7] Schuster, R., Färber, J., Eberl, M. (1997): Digital Cash: Zahlungssysteme im Internet. Berlin u.a.

[8] Electronic Money: Preparing the Stage, Felix Stalder, University of Toronto, June, 1997

[9] Gennady Medvinsky and B. Clifford Neuman. Electronic Currency for the Internet. Electronic Markets, Vol. 3. No. 9/10, October, 1993

[10] Gennady Medvinsky and B. Clifford Neuman. NetCash: A design for practical electronic currency on the Internet. In Proceedings of the First ACM Conference on Computer and Communications Security, November, 1993

[11] Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, Michael Peirce, Donal O'Mahony, Computer Science Department, Trinity College, Dublin 2, Ireland

[12] The MilliCent Protocol for Inexpensive Electronic Commerce, Steve Glassman, Mark Manasse, Martín Abadi, Paul Gauthier, Patrick Sobalvarro

[13] Jeffrey K. MacKie-Mason, Hal R. Varian. Some FAQs about usage based pricing. University of Michigan, September, 1994, URL: ftp://gopher.econ. lsa. umich. edu/pub/Papers/useFAQs. html

[14] Norman Hardy and Eric Dean Tribble, The Digital Silk Road URL: ftp://ftp.netcom.com/pub/jo/joule/DSR/DSR1.txt.gz or http: //web.gmu.edu:80/bcox/Bionomics/Extropians /HardyTribbleSilkRoad.htm

[15] DigiCash Inc., http://www.digicash.com/

ELEKTRONIKUS FIZETÉSI RENDSZEREK: ELEKTRONIKUS PÉNZ

BODOR ANDRÁS

ELMÉLETI VILLAMOSSÁGTAN TANSZÉK
BUDAPESTI MŰSZAKI EGYETEM
1111 BUDAPEST, EGRY J. U. 18.
E-MAIL: SZABADT@SCH.BME.HU

Ez a cikk az elektronikus fizetőeszközöket mutatta be általánosságban, illetve 4 konkrét elektronikus pénzrendszer bemutatásával.

Az első részben bevezetésképpen azokról a változásokról volt szó, amelyek az internetes kereskedelem megjelenésével mentek végbe, különös tekintettel a kereskedők és a vásárlók közötti viszonyra. Az elektronikus kereskedelem számos előnnyel jár az eladók a vásárlók és több más szektor számára is. Egy ilyen szektort képeznek a bankok, pénzügyi intézetek, melyek számára egy új szolgáltatás nyújtásának a lehetősége kínálkozik.

Az internetes fizetési rendszerek áttekintésével azok lényegesebb jellemzőit soroltuk fel, melyeknek segítségével az új rendszerek összehasonlíthatóak. A fizetési módszerek közül az elektronikus pénzzel foglalkozott részletesebben e cikk.

Egy rövid bevezetés után az elektronikus pénz világába annak legfőbb 6 problémakörébe kapott az olvasó betekintést, majd összehasonlításra kerültek az on-line és off-line rendszerek a titkosítás tekintetében is. Hogy később mely elektronikus pénzrendszer lesz általánosan elfogadott, ezt 3 főbb különböző csoport határozza meg: az ipar, melyet a software és hardware fejlesztő cégek alkotják, a kormányzat mely a működés jogi kereteit határozza meg, valamint a felhasználók, mely csoport alatt a vásárlók és kereskedők értendőek.

Ezen csoportok bemutatása után az egyes fizetőeszközökkel foglalkozott részletesen a cikk. A NetCash, melyet a dél Kaliforniai Information Sciences Institute Egyetemen fejlesztettek ki egy keretrendszert biztosít az elektronikus pénzhez. Ennek segítségével valósidejű fizetéseket változó tranzakció anonymitással lehet lebonyolítani. E rendszer fő előnye a skálázhatósága és biztonsága. A Mondex egy smart kártyán alapuló pénzhelyettesítő rendszer melyhez szükséges egy kártyaolvasó hardver. Ipari támogatottsága és sokoldalúsága miatt valószínűsíthető elterjedése. A kis értékű, de biztonságos tranzakciók lebonyolítására lett kifejleszve a Millicent rendszer, melynek biztonsági modelljét, struktúráját, protokolljait részletesen mutattuk be.

Végül a David Chaum által alapított cég – DigiCash – terméke az Ecash került a nagyító alá. A titkosított érmék felhasználásával az elektronikus pénz felhasználója maximálisan anonim maradhat, ez a fő előnye ennek a rendszernek.

Legvégül a bemutatott rendszereket egy táblázatban a már megismert fő szempontok szerint hasonlítottuk össze, így nyilvánvalóvá vált az egyes rendszerek erőssége és gyengesége.

András Bodor is a PhD student of the Technical University of Budapest. He graduated in this year, 1999 on the TUB as computer scientist. In the first two years he studied in German language, then spent a half year on the Technical University of Karlsruhe. In 1997, after he became back from Germany he hold a lecture on the Frühlingsakademie in Balatonfüred, then in 1998 in Münich in German language on the area of internet security and electronic cash. He took part on the Scientific Conference of University students with the lecture and essay of WWW based information system and have been awarded a reward price. He also participated on the Conference of Graduating Student '99, TUB with the lecture: Design and development of Internet based Information systems. For a half year he went back to Germany, to the Technical University of Kralsruhe to complete his Diploma work where he designed and implemented a Web Wrapper Generator. In the 1999/6 issue of this Journal on C5 he published the article WWW based information system with Tamás Szabad. His research area is e-commerce systems, Internet security.

SECURITY ASPECTS OF INTERNET USAGE

RICHÁRD GÁL

DEPARTMENT OF ELECTROMAGNETIC THEORY
TECHNICAL UNIVERSITY OF BUDAPEST
H-1111 BUDAPEST, EGRY J. U. 18.

Nowadays there is a trend when companies are taking advantage of the Internet in ever-increasing rate, despite the fact that the underlying architecture cannot be considered secure. Additionally, vendors, standards bodies, security organizations, and practitioners cannot agree on a standard, compliant, and technically available approach. Internet technologies offer great potential for cost savings over existing technologies. Internet-based applications provide a standard communications interface and protocol suite ensuring interoperability and access to heterogeneous data and information resources. Most WWW browsers run on all systems and provide a common user interface and ease of use to a wide range of people. All of these make the access to information ubiquitous and fairly straightforward. Using the Internet involves more people than ever before, emphasizing the need to communicate both strategic and tactical security plans broadly and effectively. The security challenges and the resultant problems become larger and more complex in such an environment. In this article I would like to make a brief overview of Internet communications from security viewpoint with special attention to existing secure WWW technologies and strategies using firewalls. At the outset, however, I consider important to understand the basic protocols used by the Internet. In the first section TCP/IP protocols are reviewed. First, the TCP/IP protocol stack is described in terms of the OSI model. Then, the network- and application level protocols are examined. Ideas in the above mentioned topics are necessary to understand the rest of the article. The second section looks into the problem of what contributes to system corruptions and how to avoid them. In the third section the focus is entirely on WWW security technologies like SSL (Secure Sockets Layer), S-HTTP (Secure-HTTP), some architectural questions and audit tools and capabilities. The last section concentrates on firewalls. Packet-filters, application-gateways and circuit-gateways are examined and some overview of the virtual private networks is made.

1. INTRODUCTION

Companies continue to flock to the Internet in ever-increasing numbers, despite the fact that the overall and underlying environment is not secure. To further complicate the matter, vendors, standards bodies, security organizations, and practitioners cannot agree on a standard, compliant, and technically available approach.

Having the tools and solutions available within the marketplace is a beginning, but also strategies and migration paths are needed to accommodate and integrate Internet, intranet, and World Wide Web (WWW) technologies into our existing IT infrastructure. Security solutions are slowly emerging, but interoperability, universally accepted security standards, application programming interfaces (APIs) for security, vendor support and cooperation, and multiplatform security products are still problematic. Where there are products and solutions, they tend to be vendor-centric or only address one of a larger set of security problems and requirements.

As for the Internet, which is a distributed environment, there are more players, and it is more difficult to find or interpret the overall requirements. More people are involved than ever before, emphasizing the need to communicate both strategic and tactical security plans broadly and effectively throughout the entire enterprise. The security challenges and the resultant problems become larger and more complex in this environment. Management must be kept up-to-date and thoroughly understand overall risk to the corporation's information assets with the implementation or decisions to implement new technologies.

For most of us, the WWW will be one of the most universal and influential trends impacting our internal enterprise and its computing and networking support structure. It will widely influence our decisions to extend our internal business processes out to the Internet and beyond. It will enable us to use the same user interface, the same critical systems and applications, work towards one single original source of data.

Everyone is aware of the statistics on the growth of the Internet over the last decade. The use of the WWW can even top that growth, causing the traffic on the Internet to double every six months.

Companies are predominately using the Web technologies on the intranet to share information and documents. Future application possibilities are basically any enterprise-wide application such as education and training; corporate policies and procedures; human resources applications such as a resume, job posting, etc.; and company information. External Web applications include marketing and sales.

Quite frequently companies continue to select one of two choices when considering the implementation of WWW and Internet technologies. Some companies, who are more technically astute and competitive, have jumped in totally and are exploiting Internet technologies, electronic commerce, and the use of the Web. Others, of a more conservative nature and more technically inexperienced, continue to maintain a hard-line policy on external connectivity, which basically continues to say "NO."

Internet technologies offer great potential for cost savings over existing technologies, representing huge investments over the years in terms of revenue and resources now supporting corporate information infrastructures and contributing to the business imperatives of those enterprises. Internet-based applications provide a standard communications interface and protocol suite ensuring interoperability and access to the organization's heterogeneous data and information resources. Most WWW browsers run on all systems and provide a common user interface and ease of use to a wide range of corporate employees.

Typically, the browser software is free, bundled in vendor product suites, or very affordable. Access to information, as previously stated, is ubiquitous and fairly straightforward.

Use of internal WWW applications can change the very way organizations interact and share information. When established and maintained properly, an internal WWW application can enable everyone on the internal network to share information resources, update common use applications, receive education and training, and keep in touch with colleagues at their home base, from remote locations, or on the road.

2. A BRIEF OVERVIEW OF TCP/IP

TCP/IP refers to two network protocols (or methods of data transport) used on the Internet. They are Transmission Control Protocol and Internet Protocol, respectively. These network protocols belong to a larger collection of protocols, or a protocol suite. These are collectively referred to as the TCP/IP suite.

Protocols within the TCP/IP suite work together to provide data transport on the Internet. In other words, these protocols provide nearly all services available to today's Net surfer. Some of those services include:

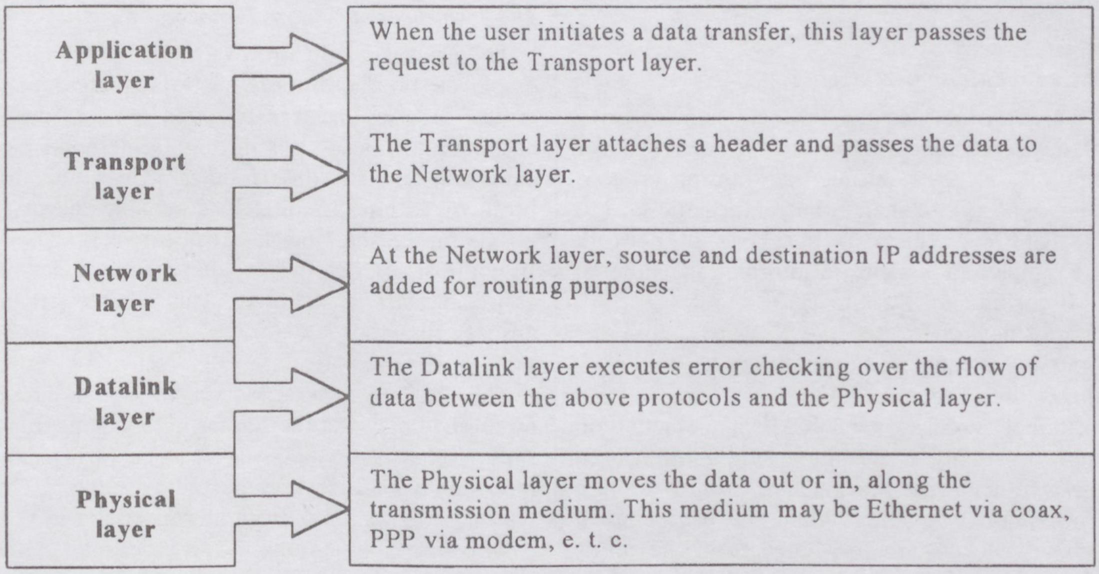
- Transmission of electronic mail,
- File transfers,
- Usenet news delivery,
- Access to the World Wide Web.

There are two classes of protocol within the TCP/IP suite:

- The network-level protocol,
- The application-level protocol.

2.1. Looking into TCP/IP

TCP/IP operates through the use of a protocol stack. This stack is the sum total of all protocols necessary to complete a single transfer of data between two machines. (It is also the path that data takes to get out of one machine and into another.) The stack is broken into layers, five of which are of concern here. To grasp this layer concept, examine Fig. 1.



Application layer

When the user initiates a data transfer, this layer passes the request to the Transport layer.

Transport layer

The Transport layer attaches a header and passes the data to the Network layer.

Network layer

At the Network layer, source and destination IP addresses are added for routing purposes.

Datalink layer

The Datalink layer executes error checking over the flow of data between the above protocols and the Physical layer.

Physical layer

The Physical layer moves the data out or in, along the transmission medium. This medium may be Ethernet via coax, PPP via modem, e. t. c.

Fig. 1. The TCP/IP stack

After data has passed through the process illustrated in Fig. 1, it travels to its destination on another machine or network. There, the process is executed in reverse (the data first meets the physical layer and subsequently travels its way up the stack). Throughout this process, a complex system of error checking is employed both on the originating and destination machine.

Each layer of the stack can send data to and receive data from its adjoining layer. Each layer is also associated with multiple protocols. At each tier of the stack, these protocols are hard at work, providing the user with various services.

2.2. Network-Level Protocols

Network protocols are those protocols that engage in (or facilitate) the transport process transparently. These are invisible to the user unless that user employs utilities to monitor system processes.

Sniffers are devices that can monitor such processes. A sniffer is a device – either hardware or software – that can read every packet sent across a network. Sniffers are commonly used to isolate network problems that, while invisible to the user, are degrading network performance. As such, sniffers can read all activity occurring between network-level protocols. Moreover, as it might be guessed, sniffers can pose a tremendous security threat.

Important network-level protocols include:

- The Address Resolution Protocol (ARP),
- The Internet Control Message Protocol (ICMP),
- The Internet Protocol (IP),
- The Transmission Control Protocol (TCP).

I will briefly examine each, offering only an overview.

The Address Resolution Protocol

The Address Resolution Protocol (ARP) serves the critical purpose of mapping Internet addresses into physical addresses. This is vital in routing information across the Internet. Before a message (or other data) is sent, it is packaged into IP packets, or blocks of information suitably formatted for Internet transport. These contain the numeric Internet (IP) address of both the originating and destination machines. Before this package can leave the originating computer, however, the hardware address of the recipient (destination) must be discovered. This is where ARP makes its debut.

An ARP request message is broadcast on the subnet. This request is received by a router that replies with the requested hardware address. This reply is caught by the originating machine and the transfer process can begin.

ARP's design includes a cache. In this manner, hardware addresses of remote machines or networks are remembered, and this memory obviates the need to conduct subsequent ARP queries on them. This saves time and network resources.

However, address caching (not only in ARP but in all instances) does indeed pose a unique security risk. If such address-location entries are stored, it makes it easier for a cracker to forge a connection from a remote machine, claiming to hail from one of the cached addresses.

The Internet Control Message Protocol

The Internet Control Message Protocol handles error and control messages that are passed between two (or more) computers or hosts during the transfer process. It allows those hosts to share that information. In this respect, ICMP is critical for diagnosis of network problems. Examples of diagnostic information gathered through ICMP include

- When a host is down,
- When a gateway is congested or inoperable,
- Other failures on a network.

Perhaps the most widely known ICMP implementation involves a network utility called ping. Ping is often used to determine whether a remote machine is alive. Ping's method of operation is simple: When the user pings a remote machine, packets are forwarded from the user's machine to the remote host. These packets are then echoed back to the user's machine. If no echoed packets are received at the user's end, the ping program usually generates an error message indicating that the remote host is down.

The Internet Protocol

IP belongs to the network layer. The Internet Protocol provides packet delivery for all protocols within the TCP/IP suite. Thus, IP is the heart of the incredible process by which data traverses the Internet. To explore this process, I have drafted a small model of an IP datagram (see Fig. 2).

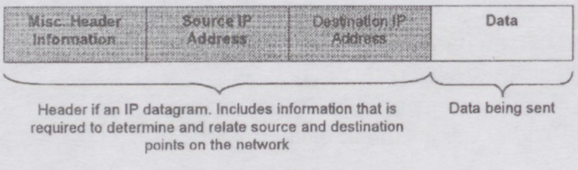

Misc. Header Information
Source IP Address
Destination IP Address
Data
Header if an IP datagram. Includes information that is required to determine and relate source and destination points on the network
Data being sent

Fig. 2. The IP datagram

As illustrated, an IP datagram is composed of several parts. The first part, the header, is composed of miscellaneous information, including originating and destination IP address. Together, these elements form a complete header. The remaining portion of a datagram contains whatever data is then being sent.

The amazing thing about IP is this: if IP datagrams encounter networks that require smaller packages, the datagrams bust apart to accommodate the recipient network. Thus, these datagrams can fragment during a journey and later be reassembled properly (even if they do not arrive in the same sequence in which they were sent) at their destination.

Even further information is contained within an IP datagram. Some of that information may include identification of the protocol being used, a header checksum, and a time-to-live specification. This specification is a numeric value. While the datagram is traveling the void, this numeric value is constantly being decremented. When that value finally reaches a zero state, the datagram dies. Many types of packets have time-to-live limitations. Some network utilities (such as Traceroute) utilize the time-to-live field as a marker in diagnostic routines.

The Transmission Control Protocol

The Transmission Control Protocol is the chief protocol employed on the Internet. It facilitates such mission-critical tasks as file transfers and remote sessions. TCP accomplishes these tasks through a method called reliable data transfer. In this respect, TCP differs from other protocols within the suite. In unreliable delivery, you have no guarantee that the data will arrive in a perfect state. In contrast, TCP provides what is sometimes referred to as reliable stream delivery. This reliable stream delivery ensures that the data arrives in the same sequence and state in which it was sent.

The TCP system relies on a virtual circuit that is established between the requesting machine and its target. This circuit is opened via a three-part process, often referred to as the three-part handshake. The process typically follows the pattern illustrated in Fig. 3.

After the circuit is open, data can simultaneously travel in both directions. This results in what is sometimes called a full-duplex transmission path. Full-duplex transmission allows data to travel to both machines at the same time. In this way, while a file transfer (or other remote session) is underway, any errors that arise can be forwarded to the requesting machine.

TCP also provides extensive error-checking capabilities. For each block of data sent, a numeric value is generated. The two machines identify each transferred block using this numeric value. For each block successfully transferred, the receiving host sends a message to the sender that the transfer was clean. Conversely, if the transfer is unsuccessful, two things may occur:

- The requesting machine receives error information,
- The requesting machine receives nothing.

When an error is received, the data is retransmitted unless the error is fatal, in which case the transmission is usually halted. A typical example of a fatal error would be if the connection is dropped. Thus, the transfer is halted for no packets.

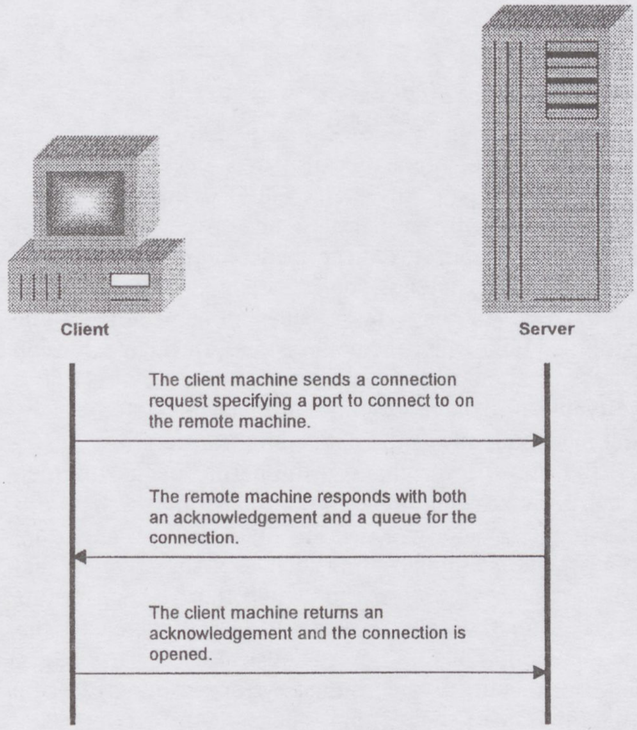

Client
Server
The client machine sends a connection request specifying a port to connect to on the remote machine.
The remote machine responds with both an acknowledgement and a queue for the connection.
The client machine returns an acknowledgement and the connection is opened.

Fig. 3. The TCP/IP three-way handshake

Similarly, if no confirmation is received within a specified time period, the information is also retransmitted. This process is repeated as many times as necessary to complete the transfer or remote session.

Each time one machine requests a connection to another, it specifies a particular destination. In the general sense, this destination is expressed as the Internet (IP) address and the hardware address of the target machine. However, even more detailed than this, the requesting machine specifies the application it is trying to reach at the destination. This involves two elements:

- A program called inetd,
- A system based on ports.

inetd

Daemons are programs on UNIX platforms that continuously listen for other processes (in this case, the process listened for is a connection request). Daemons loosely resemble terminate and stay resident (TSR) programs in the Microsoft platform. These programs remain alive at all times, constantly listening for a particular event. When that event finally occurs, the TSR undertakes some action.

inetd is a very special daemon. This is because inetd is the main daemon running on a UNIX machine. It listens for connection requests from the void. When it receives such a request, it evaluates it. This evaluation seeks to determine one thing only: What service does the requesting machine want? For example, does it want FTP? If so, inetd starts the FTP server process. The FTP server can then process the request from the void. At that point, a file transfer can begin. This all happens within the space of a second or so.

In general, inetd is started at boot time and remains resident (in a listening state) until the machine is turned off or until the root operator expressly terminates that process.

Ports

Many TCP/IP programs can be initiated over the Internet. Most of these are client/server oriented. As each connection request is received, inetd starts a server program, which then communicates with the requesting client machine.

To facilitate this process, each application (FTP or Telnet, for example) is assigned a unique address. This address is called a port. The application in question is bound to that particular port and, when any connection request is made to that port, the corresponding application is launched (inetd is the program that launches it).

There are thousands of ports on the average Internet server. For purposes of convenience and efficiency, a standard framework has been developed for port assignment. In other words, although a system administrator can bind services to the ports of his or her choice, services are generally bound to recognized ports. These are commonly referred to as well-known ports.

Please peruse Talbe 1 for some commonly recognized ports and the applications typically bound to them.

Table 1. Common ports and their corresponding services or applications

Service or Application	*Port*
File Transfer Protocol (FTP)	21
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Finger	79
Hypertext Transfer Protocol (HTTP)	80

All services in the table are application-level protocols or services (that is, they are visible to user and the user can interact with them at the console).

2.3. Application level protocols

Application-level protocols are visible to the user in some measure. For example, File Transfer Protocol (FTP) is visible to the user. The user requests a connection to another machine to transfer a file, the connection is established, and the transfer begins. During the transfer, a portion of the exchange between the user's machine and the remote machine is visible (primarily error messages and status reports on the transfer itself, for example, how many bytes of the file have been transferred at any given moment).

Telnet

The purpose of the Telnet protocol is to provide a fairly general, bi-directional, eight-bit byte-oriented communications facility. Its primary goal is to allow a standard method of interfacing terminal devices and terminal-oriented processes to each other. Telnet not only allows the user to log in to a remote host, it allows that user to execute commands on that host.

Even though GUI applications have taken the world by storm, Telnet – which is essentially a text-based application – is still incredibly popular. There are many reasons for this. First, Telnet allows you to perform a variety of functions (retrieving mail, for example) at a minimal cost in network resources. Second, implementing secure Telnet is quite a simple task. There are several programs to implement this, the most popular of which is Secure Shell.

File Transfer Protocol

File Transfer Protocol is the standard method of transferring files from one system to another.

The objectives of FTP are:

1. to promote sharing of files (computer programs and/or data),
2. to encourage indirect or implicit (via programs) use of remote computers,
3. to shield a user from variations in file storage systems among Hosts, and
4. to transfer data reliably and efficiently. FTP, though usable directly by a user at a terminal, is designed mainly for use by programs.

For over two decades, researchers have investigated a wide variety of file-transfer methods. The development of FTP has undergone many changes in that time.

FTP file transfers occur in a client/server environment. The requesting machine starts one of the clients. This generates a request that is forwarded to the targeted file server (usually a host on another network). Typically, the request is sent by inetd to port 21. For a connection to be established, the targeted file server must be running an FTP server or FTP daemon.

FTPD is the standard FTP server daemon. Its function is simple: to reply to connect requests received by inetd and to satisfy those requests for file transfers. This daemon comes standard on most distributions of UNIX .

FTPD waits for a connection request. When such a request is received, FTPD requests the user login. The user must either provide his or her valid user login and password or may log in anonymously.

Once logged in, the user may download files. In certain instances and if security on the server allows, the user may also upload files.

Simple Mail Transfer Protocol

The objective of Simple Mail Transfer protocol (SMTP) is to transfer mail reliably and efficiently. SMTP is an extremely lightweight and efficient protocol. The user (utilizing any SMTP- compliant client) sends a request to an SMTP server. A two-way connection is subsequently established. The client forwards a MAIL instruction, indicating that it wants to send mail to a recipient somewhere on the Internet. If the SMTP allows this operation, an affirmative acknowledgment is sent back to the client machine. At that point, the session begins. The client may then forward the recipient's identity, his or her IP address, and the message (in text) to be sent.

Despite the simple character of SMTP, mail service has been the source of countless security holes. (This may be due in part to the number of options involved. Misconfiguration is a common reason for holes.)

SMTP servers are native in UNIX. Most other networked operating systems now have some form of SMTP.

Hypertext Transfer Protocol

Hypertext Transfer Protocol is perhaps the most renowned protocol of all because it is this protocol that allows users to surf the Net. HTTP is an application-level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information systems. It is a generic, stateless, object-oriented protocol which can be used for many tasks, such as name servers and distributed object management systems, through extension of its request methods (commands). A feature of HTTP is the typing of data representation, allowing systems to be built independently of the data being transferred.

HTTP has forever changed the nature of the Internet, primarily by bringing the Internet to the masses. It works via a request/response scenario. And this is an important point. Whereas applications such as Telnet require that a user remain logged on (and while they are logged on, they consume system resources), HTTP eliminate this phenomenon. Thus, the user is pushed back a few paces. The user (client) only consumes system resources for the instant that he or she is either requesting or receiving data.

2.4. Conclusion on TCP/IP

Today it is fairly clear that TCP/IP basically comprises the Internet itself. It is a complex collection of protocols, many of which remain invisible to the user. There are actually hundreds of them. Better than half of the primary protocols have had one or more security holes.

In essence, the point is that there are hundreds of ways to move data across the Net. Until recently, utilizing these protocols called for accessing them one at a time. That is, to arrest a Gopher session and start a Telnet session, the user had to physically terminate the Gopher connection. The HTTP browser changed all that and granted the average user much greater power and functionality. Indeed, FTP, Telnet, NTTP, and HTTP are all available at the click of a button.

3. SECURITY CONCEPTS AND MEASURES

The intensive use of the internet, the growing motivation of companies to appear on the Web and the underlying protocols address the problem of maintaining sufficient level of security in an organization's intranet especially when the internal electronic infrastructure is exposed to the outside world by means of the Internet. It is however not only malicious hacker type of attacks that impose a threat to the computer system but also other human related threats, computer viruses and physical threats. In the following I intend to make an overview of the threats that may threaten a computer system.

3.1. Threats to Computer Networks

The greatest threat posed to LANs and WANs are people – and this threat is primarily from insiders. These are employees who make errors and omissions and employees who are disgruntled or dishonest. People threats are costly. Employee errors, accidents, and omissions cause some 50 to 60Disgruntled employees and dishonest employees add another 20threats are estimated to account for over 75organizations each year. Outsider threats such as hackers and viruses add another 5should be noted that these figures were published in 1988, and since that time there has been a dramatic increase in virus incidents, which may significantly enlarge the dollar loss from outsider threats, particularly in the LAN/WAN environment [7].

3.1.1. Human Related Threats

System Administration Error

This area includes all human errors occurring in the setup, administration, and operation of LAN systems, ranging from the failure to properly enable access controls and other security features to the lack of adequate backups. The possible consequences include loss of data confidentiality, integrity, and system availability, as well as possible embarrassment to the company or the individual.

PC Operator Error

This includes all human errors occurring in the operation of PC/LAN systems, including improper use of logon/passwords, inadvertent deletion of files, and inadequate backups. Possible consequences include data privacy violations and loss of capabilities, such as the accidental erasure of critical programs or data.

Software/Programming Error

These errors include all the "bugs," incompatibility issues, and related problems that occur in developing, installing, and maintaining software on a LAN. Possible consequences include degradation, interruption, or loss of LAN capabilities.

Unauthorized Disclosure

This is defined as any release of sensitive information on the LAN that is not sanctioned by proper authority, including those caused by carelessness and accidental release. Possible consequences are violations of law and policy, abridgement of rights of individuals, embarrassment to individuals and the company, and loss of shareholder confidence in the company.

Unauthorized Use

Unauthorized use is the employment of company resources for purposes not authorized by the corporation and the use of non-company resources on the network, such as using personally owned software at the office. Possible consequences include the introduction of viruses, and copyright violations for use of unlicensed software.

Fraud/Embezzlement

This is the unlawful deletion of company recorded assets through the deceitful manipulation of internal controls, files, and data, often through the use of a LAN. Possible consequences include monetary loss and illegal payments to outside parties.

Modification of Data

This is any unauthorized changing of data, which can be motivated by such things as personal gain, favoritism, a misguided sense of duty, or a malicious intent to sabotage. Possible consequences include the loss of data integrity and potentially flawed decision making. A high risk is the disgruntled employee.

Alteration of Software

This is defined as any unauthorized changing of software, which can be motivated by such things as disgruntlement, personal gain, or a misguided sense of duty. Possible consequences include all kinds of processing errors and loss of quality in output products.

Theft of Computer Assets

Theft includes the unauthorized/unlawful removal of data, hardware, or software from company facilities. Possible consequences for the loss of hardware can include the loss of important data and programs resident on the hard disk or on diskettes stored in the immediate vicinity.

3.1.2. Viruses and Related Threats

Computer viruses are the most widely recognized example of a class of programs written to cause some form of intentional disruption or damage to computer systems or networks. A computer virus performs two basic functions: it copies itself to other programs, thereby infecting them, and it executes the instructions the author included in it. Depending on the author's motives, a program infected with a virus may cause damage immediately upon its execution, or it may wait until a certain event has occurred, such as a particular time or date. The damage can vary widely, and can be so extensive as to require the complete rebuilding of all system software and data. Because viruses can spread rapidly to other programs and systems, the damage can multiply geometrically.

Related threats include other forms of destructive programs such as Trojan horses and network worms. Collectively, they are known as malicious software. These programs are often written to masquerade as useful programs, so that users are induced into copying them and sharing them with their friends. The malicious software phenomenon is fundamentally a people problem, as it is frequently authored and often initially spread by individuals who use systems in an unauthorized manner. Thus, the threat of unauthorized use, by both unauthorized and authorized users, must be addressed as a part of virus prevention [7].

3.1.3. Physical Threats

Electrical power problems are the most frequent physical threat to LANs, but fire or water damage is the most serious. Physical threats generally include the following [7]:

Electrical Power Failures/Disturbances

This is any break or disturbance in LAN power continuity that is sufficient to cause operational interruption, ranging from high-voltage spikes to area "brownouts." Possible consequences range from minor loss of input data to temporary shutdown of systems.

Hardware Failure

Hardware failures include any failure of LAN components (particularly disk crashes in PCs). Possible consequences include loss of data or data integrity, loss of processing time, and interruption of services, and may also include degradation or loss of software capabilities.

Fire/water Damage

This could include a major catastrophic destruction of an entire building, partial destruction within an office area, LAN room fire, water damage from sprinkler system, and/or smoke damage. The possible consequences include loss of the entire system for extended periods of time.

Other Physical Threats

These include environmental failures/mishaps involving air conditioning, humidity, heating, liquid leakage, explosion, and contamination. Physical access threats include sabotage/terrorism, riot/civil disorders, bomb threats, and vandalism. Natural disasters include flood, earthquake, hurricane, snow/ice storm, windstorm, tornado, and lightning [7].

3.2. Widely Used Hacker Techniques

In today's electronic environment, the threat of being hacked is no longer an unlikely incident, occurring in a few unfortunate organizations. New reports of hacker incidents and compromised systems appear almost daily. As organizations continue to link their internal networks to the Internet, system managers and administrators are becoming increasingly aware of the need to secure their systems. Implementing basic password controls is no longer adequate to guard against unauthorized access to data. Organizations are now looking for more up-to-date techniques to assess and secure their systems. To be able to keep the preventive measures up-to-date security managers and system administrators must be aware of the hacking techniques by which their internal system can be compromised. For example a popular method to identify and eliminate security weaknesses in a network involves an approach that uses hacker methods and is called "self hack audit" (SHA) [5]. In the following section a brief introduction to popular hacker techniques tries to raise the attention to what attacks an internal network may encounter.

3.2.1. Accessing the Log-In Prompt

One method of gaining illegal access to a computer system is through the log-in prompt. This situation may occur when the hacker is physically within the facility or is attempting to access the system through a dial-in connection.

Physical Access

An important step in securing corporate information systems is to ensure that physical access to computer resources is adequately restricted. Any internal or external person who gains physical access to a terminal is given the opportunity to attempt to sign on at the log-in prompt.

To reduce the potential for unauthorized system access by way of a terminal within the organization's facility, it is advised to ensure that:

- Terminals are located in physically secure environments,
- Appropriate access control devices are installed on all doors and windows that may be used to access areas where computer hardware is located,
- Personal computers that are connected to networks are password-protected if they are located in unrestricted areas. A hacker trying to access the system would be required to guess a legitimate password before gaining access through the log-in prompt,
- Users do not write their passwords on or near their work areas.

Dial-in Access

A PC dial-in connection can be made directly to a LAN server. This connection can occur when a server has been fitted with a dial-in port capability. The remote PC requires communications software, a modem, a telephone line, and the LAN dial-in number to complete the connection. This access procedure invokes the LAN access control measures such as log-on/password requirements. LANs usually have specific controls for remote dial-in procedures. The remote unit used to dial-in may be any computer, including a laptop PC.

A PC can remotely control a second PC via modems and commercially purchased software products such as PC Anywhere and Carbon Copy. When this second PC is cabled to a LAN, a remote connection can be made from the first PC through the second PC into the LAN. The result is access to the LAN within the limits of the user's access controls. One example of this remote control access is when an individual uses a home computer to dial in to their office PC and remotely control the office PC to access the LAN. The office PC is left running to facilitate this connection. It should be noted that the LAN may not have the capability to detect that a remote-control session is taking place.

Many "daemon dialers" are readily available on the Internet. These programs, when given a range of numbers to dial, can identify valid modem numbers. Once a hacker discovers an organization's modem number, he or she can dial in and, in most cases, immediately gain access to the log-in prompt. Dial-in capabilities dramatically increase the risk of unauthorized access to the system, thereby requiring strong password protection and other safeguards, such as call-back devices. To minimize the potential for security violations by way of dial-in network access, the network administrator should ensure that:

- Adequate controls are in place for dial-in sessions, such as switching off the modem when not in use, using a call-back facility, or requiring an extra level of authentication, such as a one-time password, for dial-in sessions,
- The organization's logo and name are removed from the log-in screen so that the hacker does not know which system has been accessed.

A warning message alerts unauthorized persons that access to the system is an offense and that their activities may be logged. This is a legal requirement in some countries.

3.2.2. Obtaining Passwords

Once the hacker has gained access to an organization's log-in prompt, he or she can attempt to sign on to the system. In most cases this procedure requires a valid user ID and password combination.

Brute Force Attacks

Brute force attacks involve manual or automated attempts to guess valid passwords. Many password guessing programs are available on the Internet. Most hackers have a "password hit list," which is a collection of default passwords automatically assigned to various system accounts whenever they are installed. For example, the default password for the guest account in most UNIX systems is "guest".

To protect the network from unauthorized access, it should be ensured that:

- All user accounts are password protected,
- Password values are appropriately selected to avoid guessing,
- Default passwords are changed once the system is installed,
- Failed log-in attempts are logged and followed up appropriately,
- User accounts are locked out after a predefined number of sign-on failures,
- Users are forced to select passwords that are difficult to guess,
- Users are forced to change their passwords periodically throughout the year,
- Unused user accounts are disabled.

Password Cracking

Most UNIX sites store encrypted passwords together with corresponding user accounts in a file called /etc/passwd. Should a hacker gain access to this file, he or she can simply run a password cracking program (like Crack). These programs usually work by encrypting a standard dictionary with the same encryption algorithm used by UNIX systems (called crypt). It then compares each encrypted dictionary word against the entries in the password file until it finds a match.

Suggestions to combat the hacker's use of password-cracking software:

- Encrypted passwords are stored in a shadow password file and that the file is adequately protected,
- All "weak" passwords are identified by running Crack against the password file,
- Software such as Npasswd or Passwd+ is used to force users to select passwords that are difficult to guess,
- Users do not write their passwords on or near their work environments,
- Only the minimum number of users have access to the command line to minimize the risk of copying the /etc/passwd file.

Keystroke Logging

It is fairly easy to type in a short script to capture sign-on sessions. A hacker can use a diskette to install a keystroke-logging program onto a workstation. Once this Trojan horse is installed, it works in the background and captures every sign-on session, based on trigger key words. The hacker can read the captured keystrokes from a remote location and gain access to the system. This technique is very simple and almost always goes unnoticed.

To prevent a hacker's access to the system by way of a keystroke-logging program, the network administrator should ensure that:

- Privileged accounts (e.g., root) require one-time passwords,
- The host file system and individual users' workstations are periodically scanned for Trojan horses that could include keystroke-logging programs,
- Adequate physical access restrictions to computer hardware are in place to prevent persons from loading Trojan horses.

Packet Sniffing

The Internet offers a wide range of network monitoring tools, including network analyzers and "packet sniffers." These tools work by capturing packets of data as they are transmitted along a communications segment. Once a hacker gains physical access to a PC connected to a LAN and loads this software, he or she is able to monitor data as it is transferred between locations. Alternatively, the hacker can attach a laptop to a network port in the office and capture data packets.

Remembering that network traffic often is not encrypted, there is a high chance that the hacker will capture valid user account and password combinations.

We can reduce the possibility of account and password leaks through packet sniffers by ensuring that:

- Communications lines are segmented as much as practical,
- Sign-on sessions and other sensitive data are transmitted in an encrypted format,
- Privileged accounts (e.g., root) sign on using one-time passwords,
- Physical access to communications lines and computer hardware is restricted.

Social Engineering

Hackers often select a user account that has not been used for a period of time (typically about two weeks) and ensure that it belongs to a user whom the administrator is not likely to recognize by voice. Hackers typically target accounts that belong to interstate users or users in another building. Once they have chosen a target, they assume a user's identity and call the administrator or the help desk, explaining that they have forgotten their passwords. In most cases, the administrator or help desk will reset passwords for the hackers over the telephone.

3.2.3. General Access Methods

Hackers use a variety of methods to gain access to a host system from another system.

Internet Protocol Address Spoofing

In a typical network, a host allows other "trusted" hosts to communicate with it without requiring authentication (i.e., without requiring a user account and password combination). Hosts are identified as trusted by configuring files such as the .rhost and /etc/hosts.equiv files. Any host other than those defined as trusted must provide authentication before being allowed to establish communication links.

Internet protocol (IP) spoofing involves an untrusted host connecting to the network and pretending to be a trusted host. This access is achieved by the hacker changing his IP number to that of a trusted host. In other words, the intruding host fools the host on the local network into not challenging it for authentication.

The following measures help to avoid this type of security violation:

- Firewalls and routers are appropriately configured so that they reject IP spoofing attacks,
- Only appropriate hosts are defined as trusted within /etc/hosts.equiv, and file permissions over this file are adequate,
- Only appropriate hosts are defined within users' /.rhost files. If practical, these files should be removed.

Session Hijacking

Session hijacking is still another Internet security threat. The major tasks for the attacker who wants to hijack an ongoing session between remote hosts are to locate an existing connection between two hosts, then fabricate packets that bear the address of these hosts. Now by sending these packets to the other host and sending packets to the spoofed host to instruct it to terminate the session, the attacker can pick up the connection.

Unattended Terminals

It is quite common to find user terminals left signed on and unattended for extended periods of time, such as during lunch time. Assuming that the hacker can gain physical access to users' work areas (or assuming that the hacker is an insider), this situation is a perfect opportunity for a hacker to compromise the system's security. A hacker may use an unattended terminal to process unauthorized transactions, insert a Trojan horse, download a destructive virus, modify the user's .rhost file, or change the user's password so that the hacker can sign on later.

The network administrator can minimize the threat from access through unattended terminals by ensuring that:

- User sessions are automatically timed out after a predefined period of inactivity, or password-protected screen savers are invoked,
- Users are regularly educated and reminded about the importance of signing off their sessions whenever they expect to leave their work areas unattended,
- Adequate controls are in place to prevent unauthorized persons from gaining physical access to users' work areas.

Writeable Set User ID Files

UNIX allows executable files to be granted root privileges by making file permissions set user ID (SUID) root. Hackers often search through the file system to identify all SUID files and to determine whether they are writeable. Should they be writeable, the hacker can insert a simple line of code within the SUID program so that the next time it is executed it will write to the /etc/passwd file and this will enable the hacker to gain root privileges. The network administrator can reduce the possibility of illegal access through SUID files by ensuring that:

- Only a minimum number of programs are assigned SUID file permissions,
- Programs that are SUID are not writeable by users other than root,
- Executables defined within the system cron tables (especially the root cron table) are not writeable by users other than root because they are effectively SUID root.

Until recently, most intruders have attempted to carefully cover up the indications of their activity, often by installing programs that have selectively eliminated data from system logs. In addition, for the same reason they have avoided causing system crashes or causing massive slowdowns or disruption. Recently, however, a significant proportion of the perpetrator community has apparently shifted its strategy by increasingly perpetrating denial of service attacks. Many types of hosts, for example, crash or perform a core dump when they are sent a ping packet that exceeds a specified size limit or when they are flooded with SYN (Synchronize) packets that initiate host-to-host connections. These denial of service attacks comprise an increasing proportion of observed Internet attacks; they constitute a particularly serious threat because many organizations, above all else, require continuity of computing and networking operations.

3.3. Risks and possible damages

An examination of the potential problems that can arise on a poorly secured system will help in understanding the need for security. Three basic kinds of malicious behavior are

- Denial of service,
- Compromising the integrity of the information,
- Disclosure of information.

3.3.1. Denial of Service

Denial of service occurs when a hostile entity uses a critical service of the computer system in such a way that no service or severely degraded service is available to others. Denial of service is a difficult attack to detect and protect against, because it is difficult to distinguish when a program is being malicious or is simply greedy.

3.3.2. Compromising the Integrity of the Information

Most people take for granted that the information stored on the computer system is accurate, or at least has not been modified with a malicious intent. If the information loses its accuracy, the consequences can be extreme. For example, if competitors hacked into a company's database and deleted customer records, a significant loss of revenues could result. Users must be able to trust that data are accurate and complete.

3.3.3. Disclosure of Information

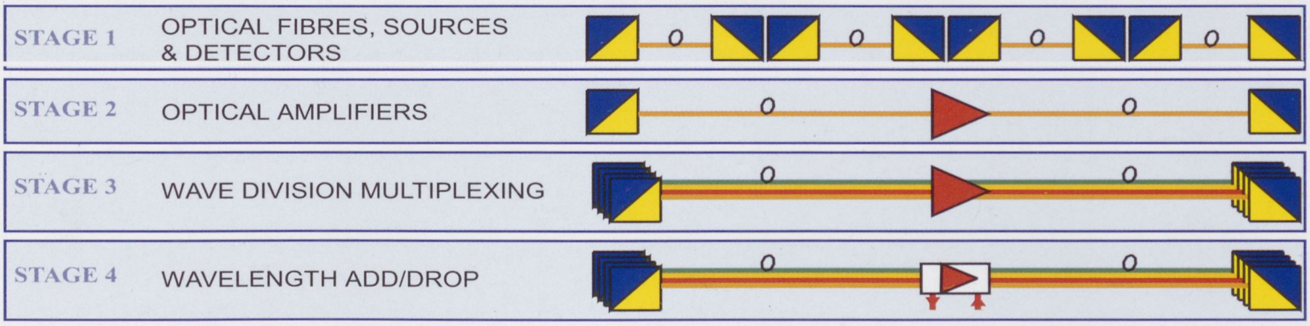
Probably the most serious attack is disclosure of information. If the information taken off a system is important to the success of an organization, it has considerable value to a competitor. Limiting user access to the information needed to perform specific jobs increases data security dramatically.

C64

COMING SOON:2000/1-5

PIRELLI

Key Stages in Photonics Road Map: Stage 4



STAGE 1 OPTICAL FIBRES, SOURCES & DETECTORS

STAGE 2 OPTICAL AMPLIFIERS

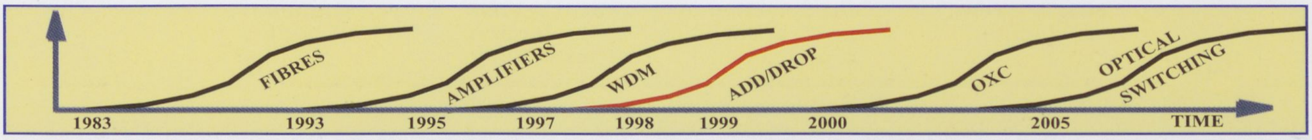
STAGE 3 WAVE DIVISION MULTIPLEXING

STAGE 4 WAVELENGTH ADD/DROP

OADM capability

•33%-50% of total number of wavelength at each amplifier site

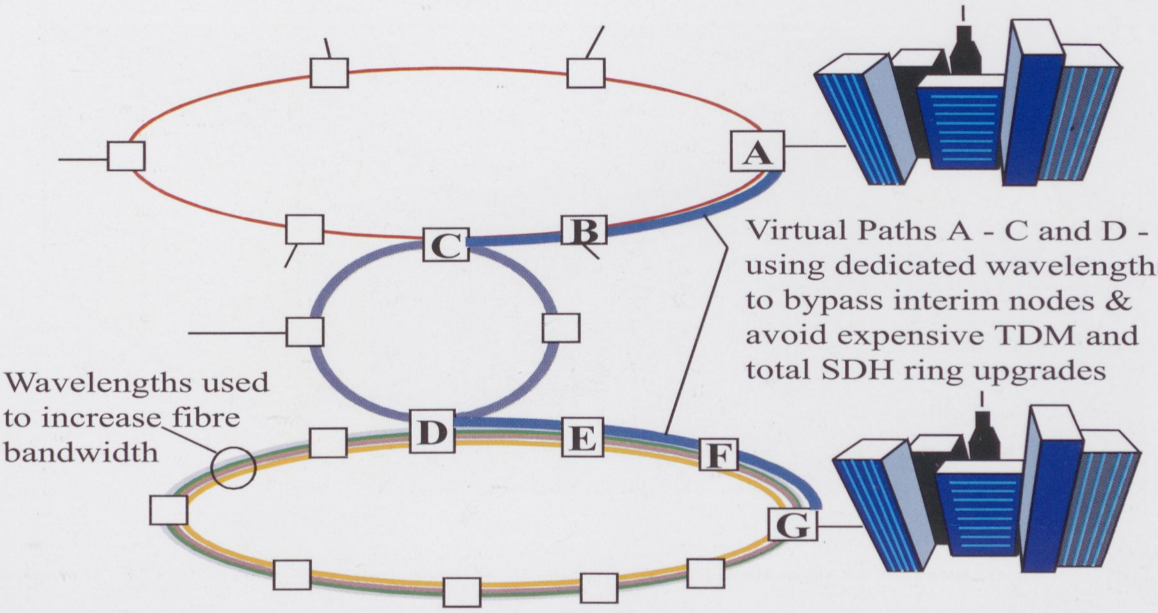
•Reduced cost and footprint compared with a terminal site



Key Stages in Photonics Road Map: Stage2 C64

PIRELLI

Key Stages in Photonics Road Map: Stage 4



Virtual Paths A - C and D - G using dedicated wavelengths to bypass interim nodes & avoid expensive TDM and total SDH ring upgrades

Wavelengths used to increase fibre bandwidth

Pirelli proprietary 1999

THE FIRST WDM WORKSHOP IN HUNGARY

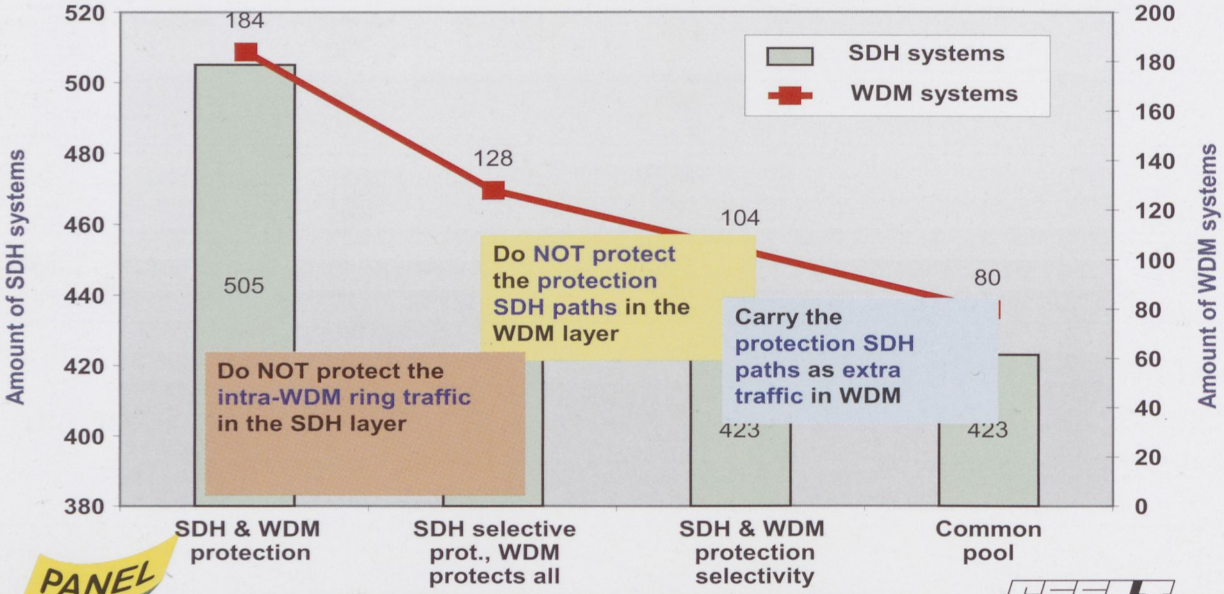
C48

COMING SOON:2000/1-5

SDH
over
WDM

Results for SDH protected over WDM protected

8 WDM nodes scenario



Do NOT protect the intra-WDM ring traffic in the SDH layer

Do NOT protect the protection SDH paths in the WDM layer

Carry the protection SDH paths as extra traffic in WDM

PANEL

AC205

Mauro RAVERA

First Hungarian WDM Workshop - March 23rd 1999

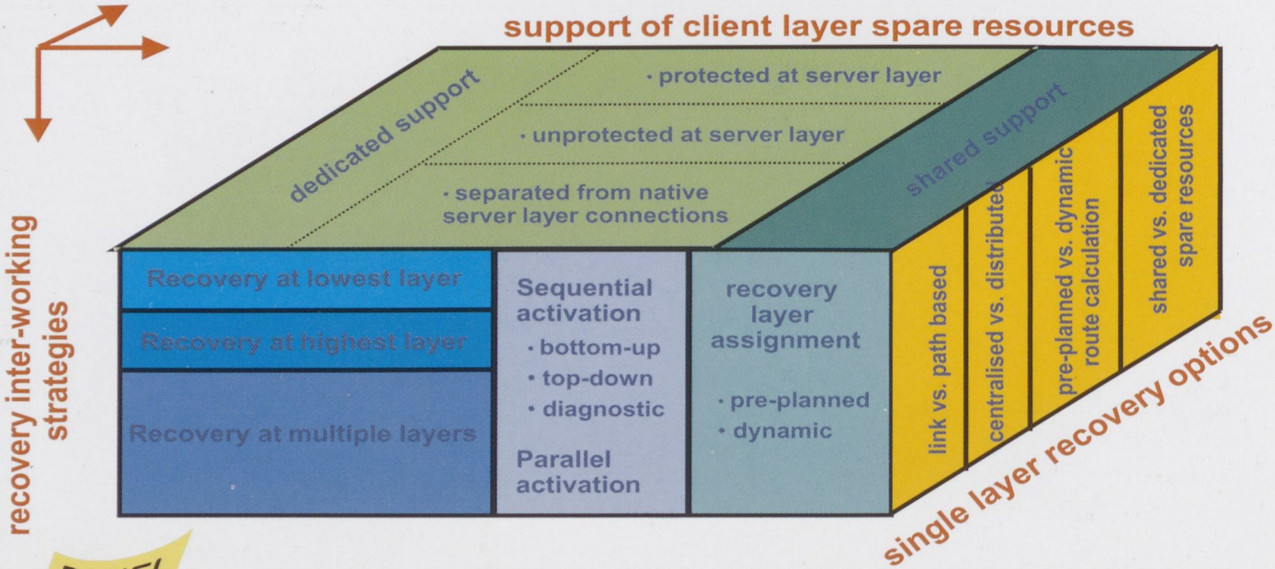
CSELT

page 52

Results for SDH protected over WDM protected C48

CONCLUSIONS

Framework for multi-layer survivability



support of client layer spare resources
dedicated support
· protected at server layer
· unprotected at server layer
· separated from native server layer connections
shared support
recovery inter-working strategies
Recovery at lowest layer
Recovery at highest layer
Recovery at multiple layers
Sequential activation
· bottom-up
· top-down
· diagnostic
Parallel activation
recovery layer assignment
· pre-planned
· dynamic
link vs. path based
centralised vs. distributed
pre-planned vs. dynamic route calculation
shared vs. dedicated spare resources
single layer recovery options

PANEL

AC205

Mauro RAVERA

First Hungarian WDM Workshop - March 23rd 1999

CSELT

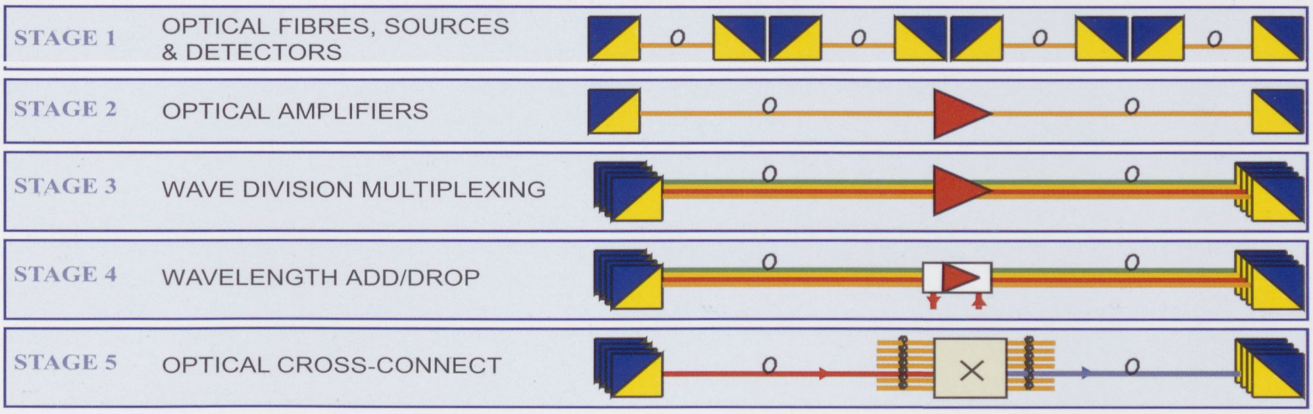
THE FIRST WDM WORKSHOP IN HUNGARY

C65

COMING SOON:2000/1-5

PIRELLI

Key Stages in Photonics Road Map: Stage 5



STAGE 1 OPTICAL FIBRES, SOURCES & DETECTORS

STAGE 2 OPTICAL AMPLIFIERS

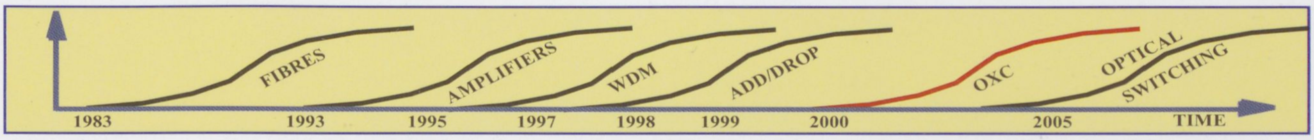
STAGE 3 WAVE DIVISION MULTIPLEXING

STAGE 4 WAVELENGTH ADD/DROP

STAGE 5 OPTICAL CROSS-CONNECT

Anticipated OXC capability

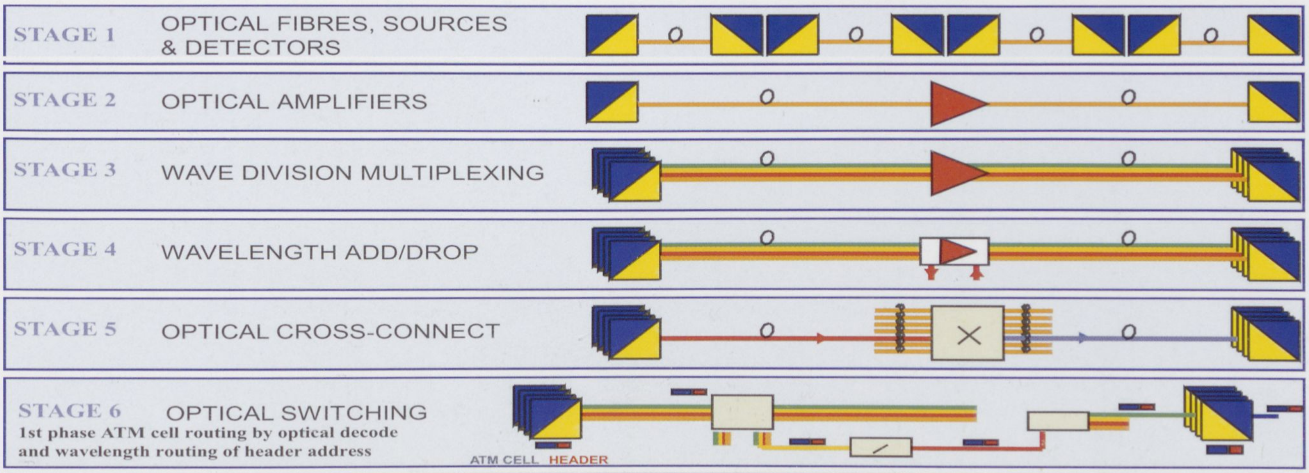
- 512x512 wavelengths, non-blocking, fast protection



Key Stages in Photonics Road Map: Stage4 C65

PIRELLI

Key Stages in Photonics Road Map: Stage 6



STAGE 1 OPTICAL FIBRES, SOURCES & DETECTORS

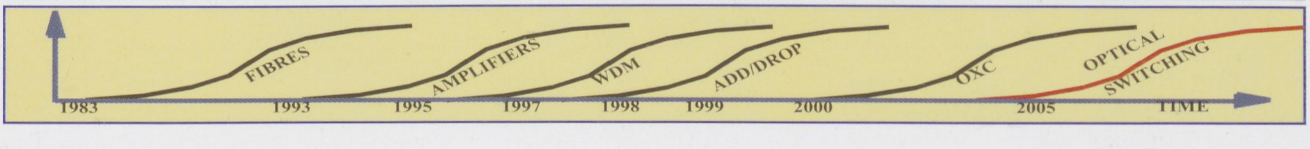
STAGE 2 OPTICAL AMPLIFIERS

STAGE 3 WAVE DIVISION MULTIPLEXING

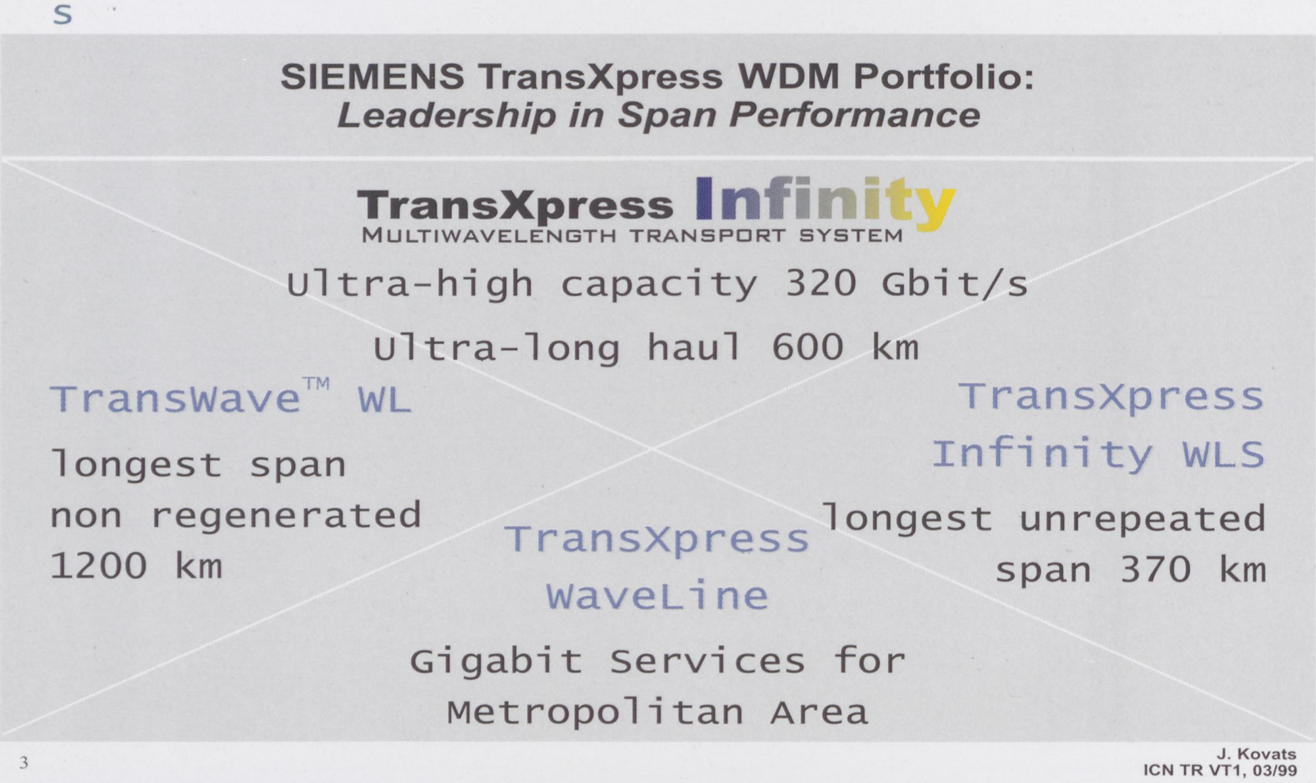
STAGE 4 WAVELENGTH ADD/DROP

STAGE 5 OPTICAL CROSS-CONNECT

STAGE 6 OPTICAL SWITCHING
1st phase ATM cell routing by optical decode and wavelength routing of header address



COMING SOON:2000/1-5



S

SIEMENS TransXpress WDM Portfolio:
Leadership in Span Performance

TransXpress Infinity
MULTIWAVELENGTH TRANSPORT SYSTEM

Ultra-high capacity 320 Gbit/s

Ultra-long haul 600 km

TransWave™ WL

longest span
non regenerated
1200 km

TransXpress
Infinity WLS

longest unrepeated
span 370 km

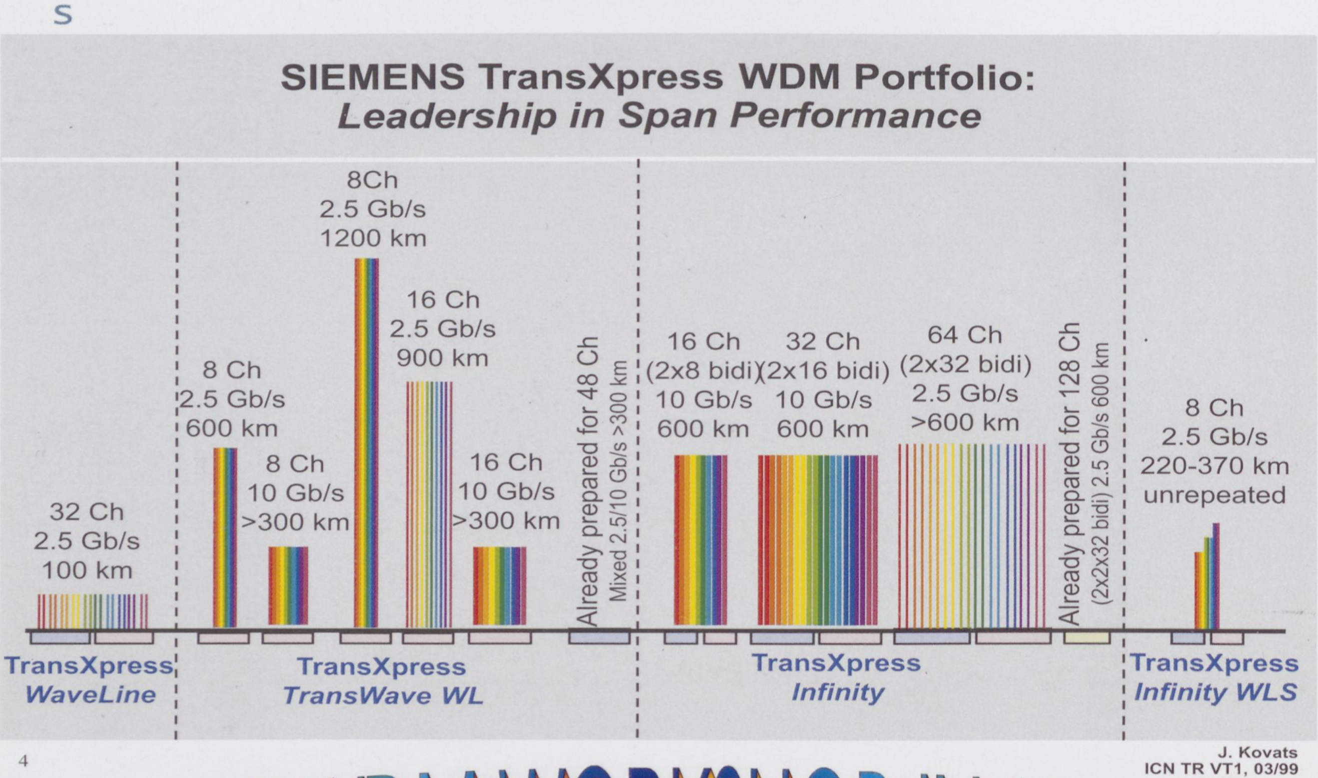
TransXpress
WaveLine

Gigabit Services for
Metropolitan Area

3

J. Kovats
ICN TR VT1, 03/99

Siemens Product Strategy D3



S

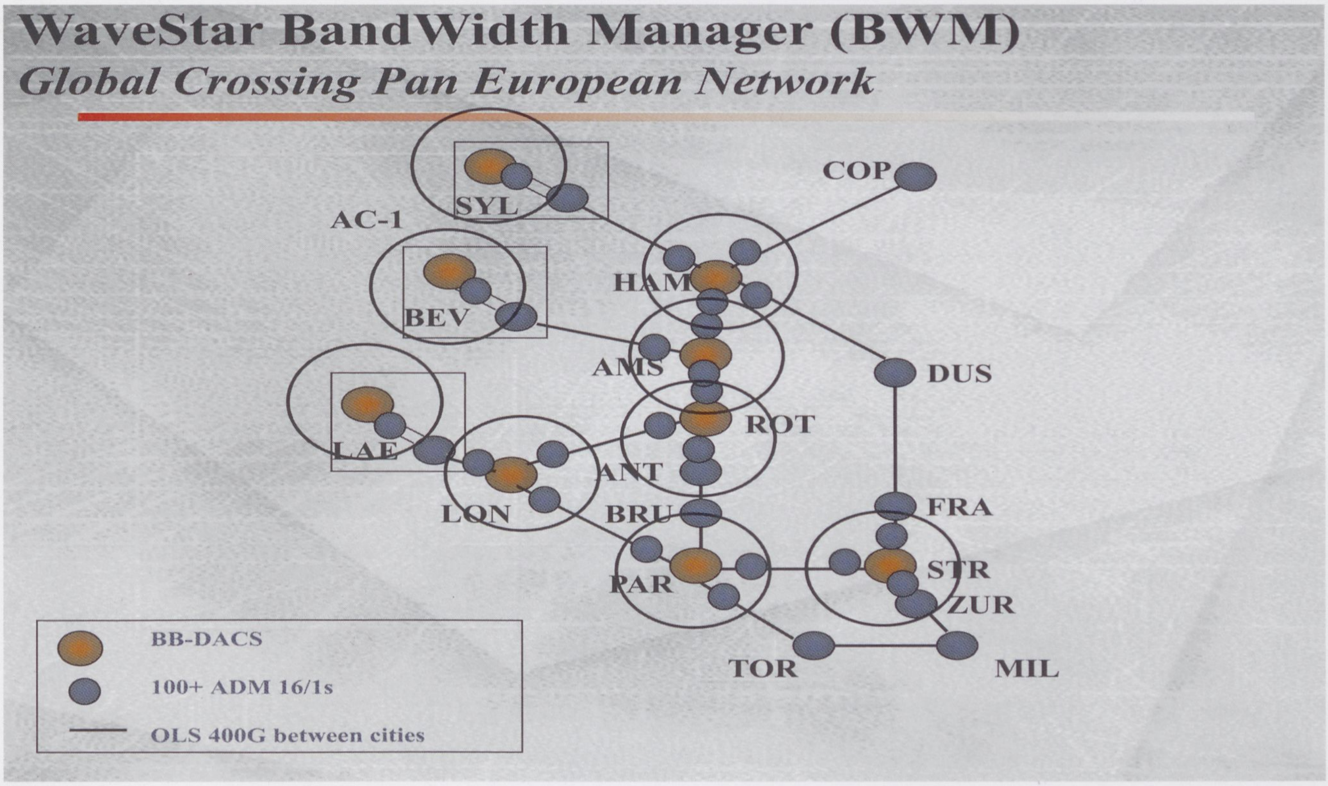
SIEMENS TransXpress WDM Portfolio:
Leadership in Span Performance

4

J. Kovats
ICN TR VT1, 03/99

THE FIRST WDM WORKSHOP IN HUNGARY

COMING SOON:2000/1-5



WaveStar BandWidth Manager (BWM)

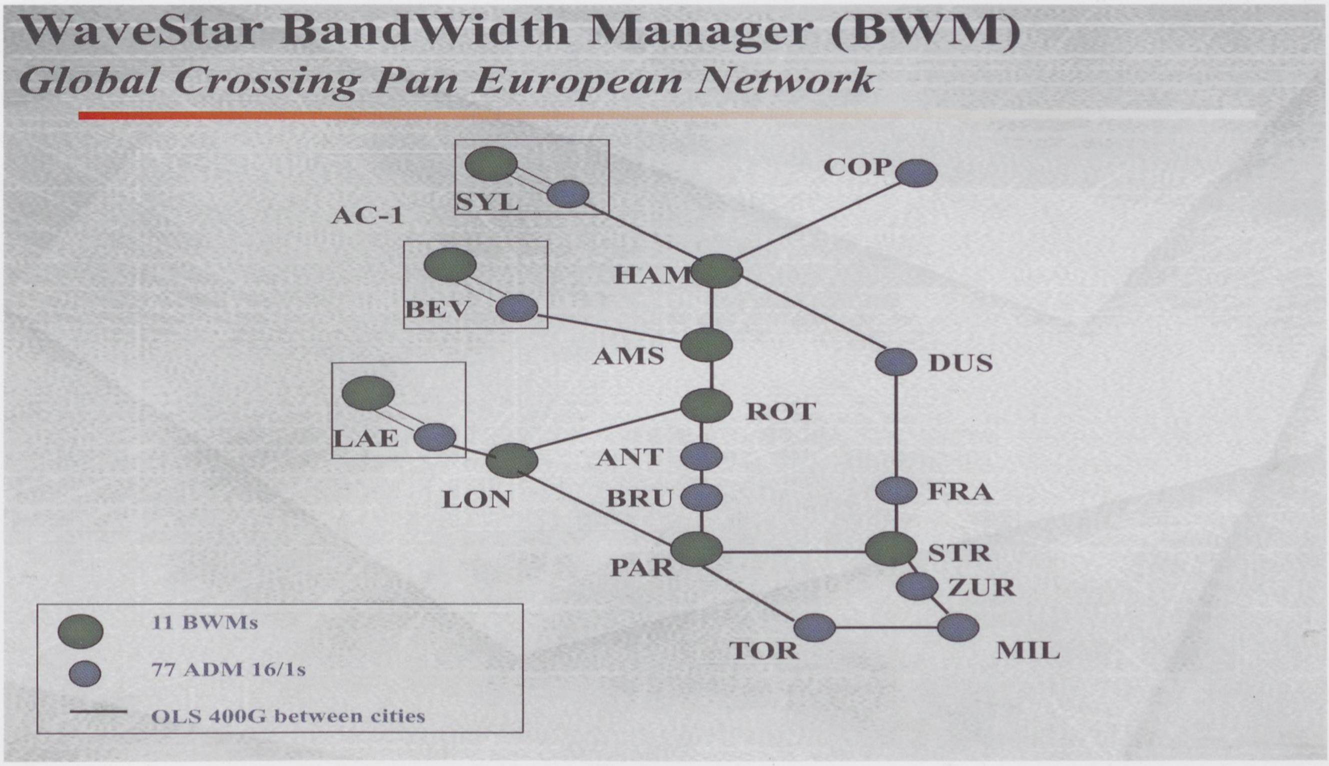
Global Crossing Pan European Network

● BB-DACS

● 100+ ADM 16/1s

— OLS 400G between cities

BWM, Global Crossing Pan European Network 2 **D34**



WaveStar BandWidth Manager (BWM)

Global Crossing Pan European Network

● 11 BWMs

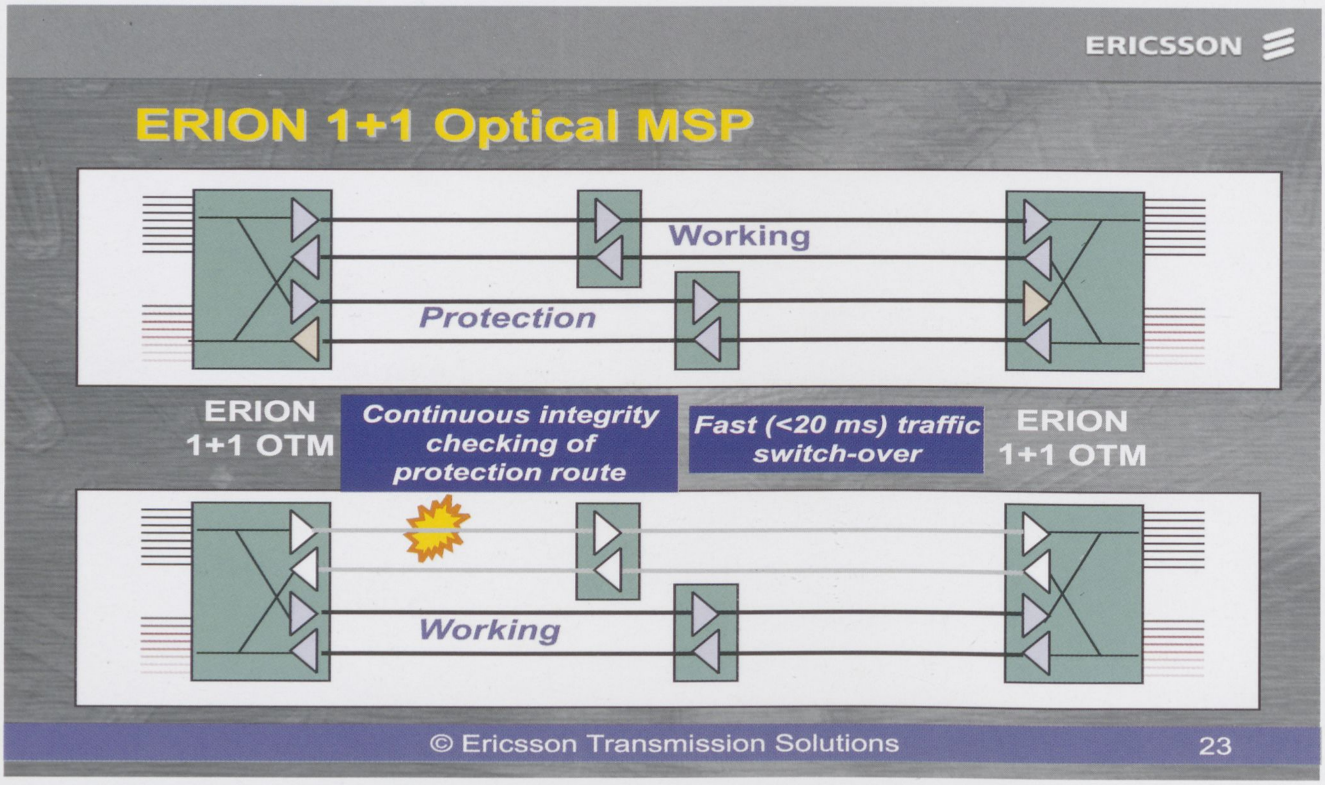
● 77 ADM 16/1s

— OLS 400G between cities

THE FIRST WDM WORKSHOP IN HUNGARY

D50

COMING SOON:2000/1-5



ERICSSON

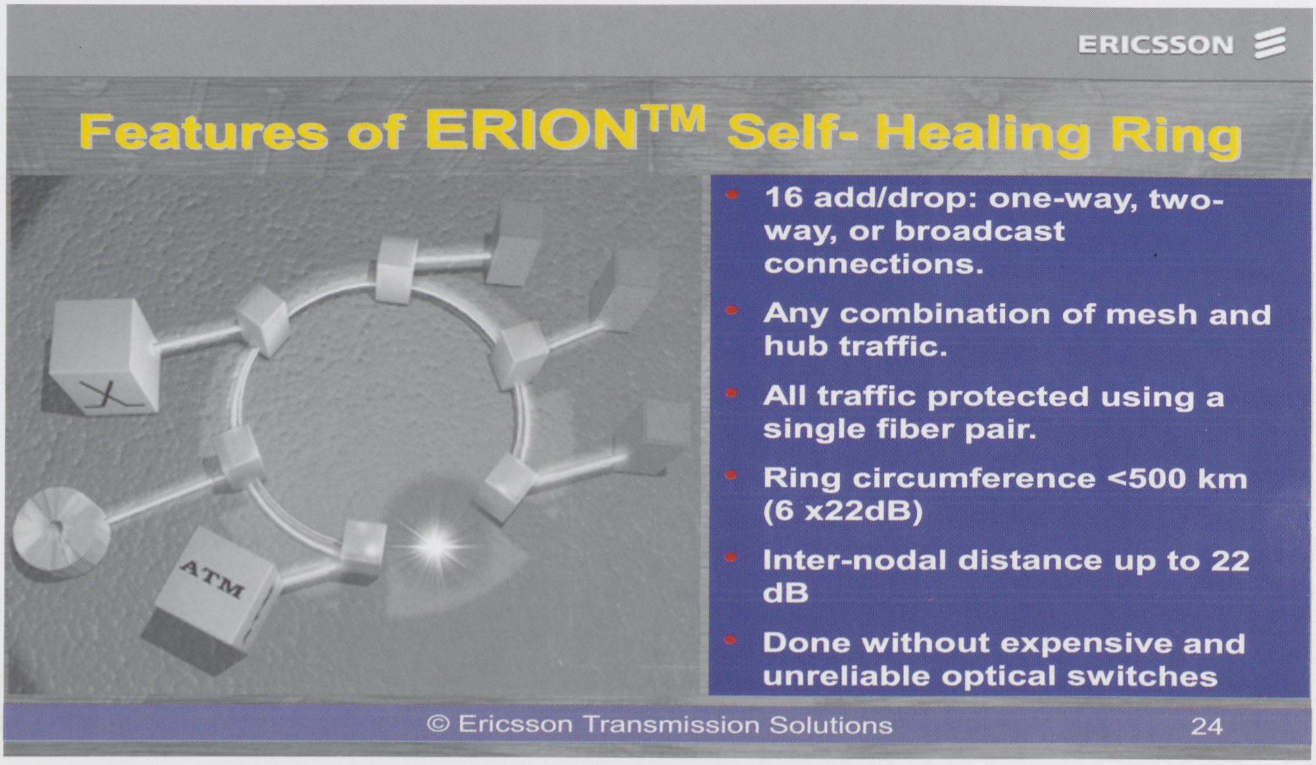
ERION 1+1 Optical MSP

Continuous integrity checking of protection route

Fast (<20 ms) traffic switch-over

© Ericsson Transmission Solutions 23

ERION 1+1 Optical MSP D50



ERICSSON

Features of ERION^{TM} Self- Healing Ring

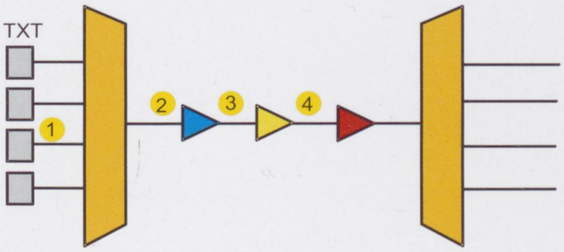
- 16 add/drop: one-way, two-way, or broadcast connections.
- Any combination of mesh and hub traffic.
- All traffic protected using a single fiber pair.
- Ring circumference <500 km (6 x22dB)
- Inter-nodal distance up to 22 dB
- Done without expensive and unreliable optical switches

© Ericsson Transmission Solutions 24

THE FIRST WDM WORKSHOP IN HUNGARY

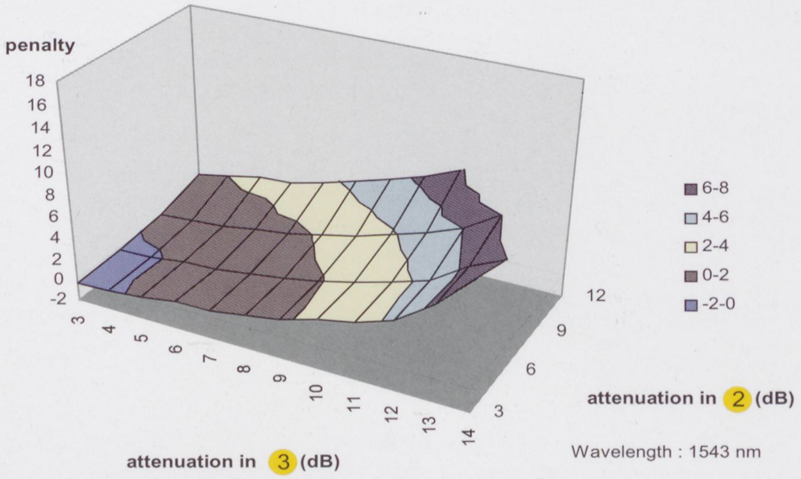
WDM link robustness

- Degradation of the optical levels in the link



- Definition of the penalty
  - » Penalty = Shift in dB of the BER curves with degraded conditions compared to the BER curves in nominal conditions

Double degradation in Paris - Rouen link



Wavelength : 1543 nm

At 9 dB attenuation in ② and 10 dB in preamplifier ③, input power is 0.3 dB lower than nominal condition ones

Technical options

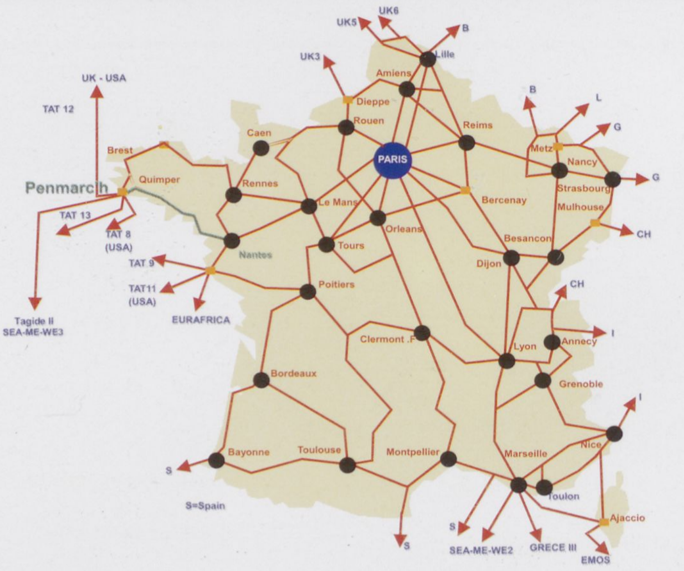
- STM 64 :
  ADM's availability ; Cost of new technology
  - » Fibre limitation (Chromatic Dispersion, PMD)
- WDM :
  - » Up to 16X STM-16 Channels commercially available
  - » MUX and de-MUX passive elements
  - » Use of transponders
  - » Flexibility of increasing the number of channels in operation in the installed wavelength multiplex
  - » Gain flatness of optical amplifiers to be considered for long links
- The FT choice today is WDM :
  - » Maturity of the technology compared to STM-64 new generation equipment

France Telecom
Branche Développement
Cnet

1rst Hungarian WDM workshop 23-03-1999

Technical options **D77**

The long distance network



France Telecom
Branche Développement
Cnet

1rst Hungarian WDM workshop 23-03-1999

3.4. Safeguards

Safeguards preclude or mitigate LAN vulnerabilities and threats, reducing the risk of loss. No set of safeguards can fully eliminate losses, but a well-planned set of cost-effective safeguards can reduce risks to a reasonable level as determined by management. Safeguards are divided into four major groups: general, technical, operational, and virus. Most of these safeguards also apply to applications as well as to LANs and WANs [7].

3.4.1. General Safeguards

General safeguards include a broad range of controls that serve to establish a firm foundation for technical and operational safeguards. Strong management commitment and support is required for these safeguards to be effective. General safeguards include, but are not necessarily limited to, the assignment of a LAN/WAN security officer, a security awareness and training program, personnel screening during hiring, separation of duties, and written procedures.

3.4.2. Technical Safeguards

These are the hardware and software controls to protect the LAN and WAN from unauthorized access or misuse, help detect abuse and security violations, and provide security for LAN applications. Technical safeguards include user identification and authentication, authorization and access controls, integrity controls, audit trail mechanisms, confidentiality controls and preventive hardware maintenance controls.

User Identification and Authentication

User identification and authentication controls are used to verify the identity of a station, originator, or individual prior to allowing access to the system or to specific categories of information within the system. Identification involves the identifier or name by which the user is known to the system (e.g., a user identification code). This identifying name or number is unique, is unlikely to change, and need not be kept secret. When authenticated, it is used to provide authorization/access and to hold individuals responsible for their subsequent actions.

Authentication is the process of "proving" that the individual is actually the person associated with the identifier. Authentication is crucial for proper security; it is the basis for control and accountability in a system. Following are three basic authentication methods for establishing identity.

1. *Something Known by the Individual.* Passwords are presently the most commonly used method of controlling access to systems. Passwords are a combination of letters and numbers (or symbols), preferably comprised of six or more characters, that should be known only to the accessor. Passwords and log-on codes should have an automated expiration feature, should not be reusable, should provide for secrecy (e.g., nonprint, nondisplay feature, encryption), and should limit the number of unsuccessful access attempts. Passwords should conform to a set of rules established by management. In addition to the password weaknesses, passwords can be misused. For example, someone who can electronically monitor the channel may also be able to "read" or identify a password and later impersonate the sender. Popular computer network media such as Ethernet or token rings are vulnerable to such abuses. Encryption authentication schemes can mitigate these exposures. Also, the use of one-time passwords has proven effective.
2. *Something Possessed by an Individual.* Several techniques can be used in this method. One technique would include a magnetically encoded card (e.g., smart cards) or a key for a lock. Techniques such as encryption may be used in connection with card devices to further enhance their security. Dial-back is a combination method where users dial in and identify themselves in a prearranged method. The system then breaks the connection and dials the users back at a predetermined number. There are also devices to determine, without the call back, that a remote device hooked to the computer is actually an authorized device. Other security devices used at the point of log-on and as validation devices on the LAN server include port-protection devices and random number generators.
3. *Something About the Individual.* These would include biometric techniques that measure some physical attribute of a person such as a fingerprint, voiceprint, signature, or retinal pattern and transmits the information to the system that is authenticating the person. Implementation of these techniques can be very expensive.

Authorization and Access Controls

These are hardware or software features used to detect and/or permit only authorized access to or within the system. An example of this control would be the use of access lists or tables. Authorization/access controls include controls to restrict access to the operating system and programming resources, limits on access to associated applications, and controls to support security policies on network and Internetwork access.

In general, authorization/access controls are the means whereby management or users determine who will have what modes of access to which objects and resources. The who may include not only people and groups, but also individual PCs and even modules within an application. The modes of access typically include read, write, and execute access to data, programs, servers, and Internetwork devices. The objects that are candidates for authorization control include data objects (directories, files, libraries, etc.), executable objects (commands, programs, etc.), input/output devices (printers, tape backups), transactions, control data within the applications, named groups of any of the foregoing elements, and the servers and Internetwork devices.

Integrity Controls

Integrity controls are used to protect the operating system, applications, and information in the system from accidental or malicious alteration or destruction, and provide assurance to users that data have not been altered (e.g., message authentication). Integrity starts with the identification of those elements that require specific integrity controls. The foundations of integrity controls are the identification/authentication and authorization/access controls. These controls include careful selection of and adherence to vendor-supplied LAN administrative and security controls. Additionally, the use of software packages to automatically check for viruses is effective for integrity control.

Data integrity includes two control mechanisms that must work together and are essential to reducing fraud and error control. These are (1) the well-formed transaction, and (2) segregation of duties among employees. A well-formed transaction has a specific, constrained, and validated set of steps and programs for handling data, with automatic logging of all data modifications so that actions can be audited later.

Two cryptographic techniques provide integrity controls for highly sensitive information. Message Authentication Codes (MACs) are a type of cryptographic checksum that can protect against unauthorized data modification, both accidental and intentional. Digital signatures authenticate the integrity of the data and the identity of the author. Digital signature standards are used in E-mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and sender authentication.

Audit Trail Mechanisms

Audit controls provide a system monitoring and recording capability to retain or reconstruct a chronological record of system activities. An example would be system log files. These audit records help to establish accountability when something happens or is discovered. Audit controls should be implemented as part of a planned LAN security program. LANs have varying audit capabilities, which include exception logging and event recording. Exception logs record information relating to system anomalies such as unsuccessful password or log-on attempts, unauthorized transaction attempts, PC/remote dial-in lockouts, and related matters. Exception logs should be reviewed and retained for specified periods. Event records identify transactions entering or exiting the system, and journal tapes are a backup of the daily activities.

Confidentiality Controls

These controls provide protection for data that must be held in confidence and protected from unauthorized disclosure. The controls may provide data protection at the user site, at a computer facility, in transit, or some combination of these. Confidentiality relies on comprehensive LAN/WAN security controls which may be complemented by encryption controls.

Encryption is a means of encoding or scrambling data so that they are unreadable. When the data are received, the reverse scrambling takes place. The scrambling and descrambling requires an encryption capability at either end and a specific key, either hardware or software, to code and decode the data. Encryption allows only authorized users to have access to applications and data.

The use of cryptography to protect user data from source to destination, which is called end-to-end encryption, is a powerful tool for providing network security. This form of encryption is typically applied at the transport layer of the network (layer 4). End-to-end encryption cannot be employed to maximum effectiveness if application gateways are used along the path between communicating entities. These gateways must, by definition, be able to access protocols at the application layer (layer 7), above the layer at which the encryption is employed. Hence, the user data must be decrypted for processing at the application gateway and then re-encrypted for transmission to the destination (or another gateway). In such an event the encryption being performed is not really end-to-end. There are a variety of low-cost, commercial security/encryption products available that may provide adequate protection for unclassified use, some with little or no maintenance of keys. Many commercial software products have security features that may include encryption capabilities, but do not meet the requirements of the DES.

Preventive Maintenance

Hardware failure is an ever-present threat, since LAN and WAN physical components wear out and break down. Preventive maintenance identifies components nearing the point at which they could fail, allowing for the necessary repair or replacement before operations are affected.

3.4.3. Operational Safeguards

Operation safeguards are the day-to-day procedures and mechanisms to protect LANs. These safeguards include backup and contingency planning, physical and environmental protection, production and input/output controls, audit and variance detection, hardware and system software maintenance controls, and documentation.

Backup and Contingency Planning

The goal of an effective backup strategy is to minimize the number of workdays that can be lost in the event of a disaster (e.g., disk crash, virus, fire). A backup strategy should indicate the type and scope of backup, the frequency of backups, and the backup retention cycle. The type/scope of backup can range from complete system backups, to incremental system backups, to file/data backups or even dual backup disks (disk "mirroring"). The frequency of the backups can be daily, weekly, or monthly. The backup retention cycle could be defined as daily backups kept for a week, weekly backups kept for a month, or monthly backups kept for a year.

Contingency planning consists of workable procedures for continuing to perform essential functions in the event that information technology support is interrupted. Application plans should be coordinated with the backup and recovery plans of any installations and networks used by the application. Appropriate emergency, backup, and contingency plans and procedures should be in place and tested regularly to assure the continuity of support in the event of system failure. These plans should be known to users and coordinated with them. Offsite storage of critical data, programs, and documentation is important. In the event of a major disaster such as fire, or even extensive water damage, backups at offsite storage facilities may be the only way to recover important data, software, and documentation.

Physical and Environmental Protection

These are controls used to protect against a wide variety of physical and environmental threats and hazards, including deliberate intrusion, fire, natural hazards, and utility outages or breakdowns. Several areas come within the direct responsibility of the LAN/WAN personnel and security staff including adequate surge protection, battery backup power, room and cabinet locks, and possibly additional air-conditioning sources. Surge protection and backup power will be discussed in more detail.

Surge suppressors that protect stand-alone equipment may actually cause damage to computers and other peripherals in a network. Ordinary surge protectors and uninterruptible power supplies (UPS) can actually divert dangerous electrical surges into network data lines and damage equipment connected to that network. Power surges are momentary increases in voltage of up to 6,000 volts in 110-volt power systems, making them dangerous to delicate electronic components and data as they search for paths to ground. Ordinary surge protectors simply divert surges from the hot line to the neutral and ground wires, where they are assumed to flow harmlessly to earth. The extract below summarizes this surge protection problem for networks.

Computers interconnected by data lines present a whole new problem because network data lines use the powerline ground circuit for signal voltage reference. When a conventional surge protector diverts a surge to ground, the surge directly enters the data lines through the ground reference. This causes high surge voltages to appear across data lines between computers, and dangerous surge currents to flow in these data lines. TVSSs (Transient Voltage Surge Suppressors) based on conventional diversion designs should not be used for networked equipment. Surge protectors may contribute to LAN crashes by diverting surge pulses to ground, thereby contaminating the reference used by data cabling. To avoid having the ground wire act as a "back door" entry for surges to harm a computer's low-voltage circuitry, network managers should consider powerline protection that (1) provides low let-through voltage, (2) does not use the safety ground as a surge sink and preserves it for its role as voltage reference, (3) attenuates the fast rise times of all surges, to avoid stray coupling into computer circuitry, and (4) intercepts all surge frequencies, including internally generated high-frequency surges.

The use of an UPS for battery/backup power can make the difference between a "hard or soft crash." Hard crashes are the sudden loss of power and the concurrent loss of the system, including all data and work in progress in the servers' random access memory (RAM). An UPS provides immediate backup power to permit an orderly shutdown or "soft crash" of the LAN, thus saving the data and work in progress. The UPS protecting the server should include software to alert the entire network of an imminent shutdown, permitting users to save their data. LAN servers should be protected by UPSs, and UPS surge protectors should avoid the "back door" entry problems described above.

Production and Input/Output Controls

These are controls over the proper handling, processing, storage, and disposal of input and output data and media, including locked storage of sensitive paper and electronic media, and proper disposal of materials (i.e., erasing/degaussing diskettes/tape and shredding sensitive paper material).

Audit and Variance Detection

These controls allow management to conduct an independent review of system records and activities in order to test for adequacy of system controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection includes the use of system logs and audit trails to check for anomalies in the number of system accesses, types of accesses, or files accessed by users.

Hardware and System Software Maintenance Controls

These controls are used to monitor the installation of and updates to hardware and operating system and other system software to ensure that the software functions as expected and that an historical record is maintained of system changes. They may also be used to ensure that only authorized software is allowed on the system. These controls may include a hardware and system software configuration policy that grants managerial approval to modifications, then documents the changes. They may also include virus protection products.

Documentation

Documentation controls are in the form of descriptions of the hardware, software, and policies, standards, and procedures related to LAN security, and include vendor manuals, LAN procedural guidance, and contingency plans for emergency situations. They may also include network diagrams to depict all interconnected LANs/WANs and the safeguards in effect on the network devices.

3.4.4. Virus Safeguards

Virus safeguards include the good security practices cited above which include backup procedures, the use of only company approved software, and procedures for testing new software. All organizations should require a virus prevention and protection program, including the designation and training of a computer virus specialist and backup. Each LAN should be part of this program. More stringent policies should be considered as needed, such as:

- Use of antivirus software to prevent, detect, and eradicate viruses;
- Use of access controls to more carefully limit users;
- Review of the security of other LANs before connecting;
- Limiting of E-mail to non-executable files; and
- Use of call-back systems for dial-in lines.

Additionally, there are several other common-sense tips which reduce the exposure to computer viruses. If the software allows it, apply write-protect tabs to all program disks before installing new software. If it does not, write protect the disks immediately after installation. Also, do not install software without knowing where it has been. Where applicable, make executable files read-only. It won't prevent virus infections, but it can help contain those that attack executable files (e.g., files that end in ".exe" or ".com"). Designating executable files as read-only is easier and more effective on a network, where system managers control read/write access to files. Finally, back up the files regularly. The only way to be sure the files will be around tomorrow is to back them up today.

3.5. WWW Security Strategies

The massive network infrastructure of the Internet is changing the way the world approaches education, business, and even leisure activity. At the same time, however, the Internet has presented a new, complex set of challenges that not even the most sophisticated technical experts have so far been able to adequately solve, yet that urgently need solutions. Achieving adequate security is one of the foremost of these challenges.

Ideally, Web browser security strategies should use a network-based security architecture that integrates your company's external Internet and the internal intranet security policies. Ensure that users on any platform, with any browser, can access any system from any location if they are authorized and have a "need-to-know".

The degree to which your Web server is secured generates some obvious trade-offs such as cost, management, administrative requirements, and time. Solutions can be hardware, software and personnel intensive.

Enhancing the security of the Web server itself has been a paramount concern since the first Web server initially emerged, but progress has been slow in deployment and implementation. As the market has mushroomed for server use, and the diversity of data types that are being placed on the server has grown, the demand has increased for enhanced Web server security. Various approaches have emerged, with no single de facto standard yet emerging (though there are some early leaders – among them Secure Sockets Layer [SSL] and Secure Hypertext Transfer Protocol [S-HTTP]). These are two significantly different approaches, but both widely seen in the marketplace.

3.5.1. Secure Socket Layer (SSL) Trust Model

One of the early entrants into the secure Web server and client arena is Netscape's Commerce Server, which utilizes the Secure Sockets Layer (SSL) trust model. This model is built around the RSA Public Key/Private Key architecture. Under this model, the SSL-enabled server is authenticated to SSL-aware clients, proving its identity at each SSL connection. This proof of identity is conducted through the use of a public/private key pair issued to the server validated with x.509 digital certificates. Under the SSL architecture, Web server validation can be the only validation performed, which may be all that is needed in some circumstances. This would be applicable for those applications where it is important to the user to be assured of the identity of the target server, such as when placing company orders, or other information submittal where the client is expecting some important action to take place. Fig. 4 diagrams this process.

Optionally, SSL sessions can be established that also authenticate the client and encrypt the data transmission between the client and the server for multiple I/P services (HTTP, Telnet, FTP). The multiservice encryption capability is available because SSL operates below the application layer and above the TCP/IP connection layer in the protocol stack, and thus other TCP/IP services can operate on top of a SSL-secured session.

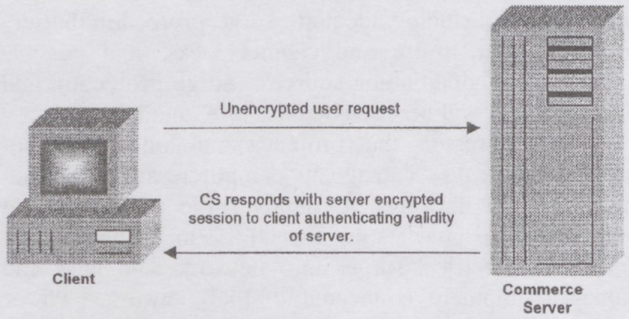

Unencrypted user request
CS responds with server encrypted session to client authenticating validity of server.
Client
Commerce Server

Fig. 4. Server Authentication

Optionally, authentication of a SSL client is available when the client is registered with the SSL server, and occurs after the SSL-aware client connects and authenticates the SSL server. The SSL client then submits its digital certificate to the SSL server, where the SSL server validates the client's certificate and proceeds to exchange a session key to provide encrypted transmissions between the client and the server. Fig. 5 provides a graphical representation of this process for mutual client and server authentication under the SSL architecture. This type of mutual client/server authentication process should be considered when the data being submitted by the client are sensitive enough to warrant encryption prior to being submitted over a network transmission path.

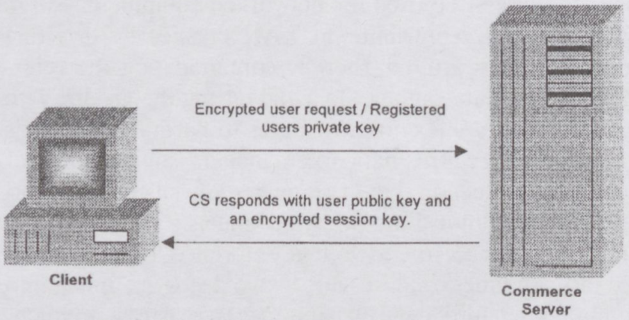

Encrypted user request / Registered users private key
CS responds with user public key and an encrypted session key.
Client
Commerce Server

Fig. 5. Client and Server Authentication

Though there are some "costs" with implementing this architecture, these cost variables must be considered when proposing an SSL server implementation to enhance your Web server security. First of all, the design needs to consider whether to only provide server authentication, or both server and client authentication. The issue when expanding the authentication to include client authentication includes the administrative overhead of managing the user keys, including a key revocation function. This consideration, of course, has to assess the size of the user base, potential for growth of your user base, and stability of your proposed user community. All of these factors will impact the administrative burden of key management, especially if there is the potential for a highly unstable or transient user community.

The positive considerations for implementing an SSL-secured server is the added ability to secure other I/P services for remote or external SSL clients. SSL-registered clients now have the added ability to communicate securely by utilizing Telnet and FTP (or other I/P services) after passing SSL client authentication and receiving their session encryption key. In general the SSL approach has very broad benefits, but these benefits come with the potential added burden of higher administration costs, though if the value of potential data loss is great, then it is easily offset by the administration cost identified above.

3.5.2. Secure Hypertext Transfer Protocol (S-HTTP)

Secure Hypertext Transfer Protocol, (S-HTTP) is emerging as another security tool and incorporates a flexible trust model for providing secure Web server and client HTTP communications. It is specifically designed for direct integration into HTTP transactions, with its focus on flexibility for establishing secure communications in an HTTP environment while providing transaction confidentiality, authenticity/integrity, and nonrepudiation. S-HTTP incorporates a great deal of flexibility in its trust model by leaving defined variable fields in the header definition which identifies the trust model or security algorithm to be used to enable a secure transaction. S-HTTP can support symmetric or asymmetric keys, and even a Kerberos-based trust model. The intention of the authors was to build a flexible protocol that supports multiple trusted modes, key management mechanisms, and cryptographic algorithms through clearly defined negotiation between parties for specific transactions.

At a high level the transactions can begin in an untrusted mode (standard HTTP communication), and "setup" of a trust model can be initiated so that the client and the server can negotiate a trust model, such as a symmetric key-based model on a previously agreed-upon symmetric key, to begin encrypted authentication and communication. The advantage of an S-HTTP-enabled server is the high degree of flexibility in securely communicating with Web clients. A single server, if appropriately configured and network enabled, can support multiple trust models under the S-HTTP architecture and serve multiple client types. In addition to being able to serve a flexible user base, it can also be used to address multiple data classifications on a single server where some data types require higher-level encryption or protection then other data types on the same server and therefore varying trust models could be utilized.

The S-HTTP model provides flexibility in its secure transaction architecture, but focuses on HTTP transaction, thus its capabilities are limited to only HTTP communications. SSL which mandates the trust model of a public/private key security model, which can be used to address multiple I/P services.

3.5.3. Internet, Intranet, and WWW security architectures

Implementing a secure server architecture, where appropriate, should also take into consideration the existing enterprise network security architecture and incorporate the secure server as part of this overall architecture. In order to discuss this level of integration, we will make an assumption that the secure Web server is to provide secure data dissemination for external (outside the enterprise) distribution and/or access. A discussion of such a network security architecture would not be complete without addressing the placement of the Web server in relation to the enterprise firewall.

Setting the stage for this discussion calls for some identification of the requirements, so the following list outlines some sample requirements for this architectural discussion on integrating a secure HTTP server with an enterprise firewall:

- Remote client is on public network accessing sensitive company data,
- Remote client is required to authenticate prior to receiving data,
- Remote client only accesses data via HTTP,
- Data is only updated periodically,
- Host site maintains firewall,
- Sensitive company data must be encrypted on public networks,
- Company support personnel can load HTTP server from inside the enterprise.

Based on these high-level requirements an architecture could be set up that would place an S-HTTP server external to the firewall, with one-way communications from inside the enterprise "to" the external server to perform routine administration, and periodic data updates. Remote users would access the S-HTTP server utilizing specified S-HTTP secure transaction modes, and be required to identify themselves to the server prior to being granted access to secure data residing on the server. Fig. 6 depicts this architecture at a high level. This architecture would support a secure HTTP distribution of sensitive company data, but doesn't provide absolute protection due to the placement of the S-HTTP server entirely external to the protected enterprise. There are some schools of thought that since this server is unprotected by the company-controlled firewall, the S-HTTP server itself is vulnerable, thus risking the very control mechanism itself and the data residing on it. The opposing view on this is that the risk to the overall enterprise is minimized, as only this server is placed at risk and its own protection is the S-HTTP process itself. This process has been a leading method to secure the data, without placing the rest of the enterprise at risk, by placing the S-HTTP server logically and physically outside the enterprise security firewall.

A slightly different architecture has been advertised that would position the S-HTTP server inside the protected domain, as Fig. 7 indicates. The philosophy behind this architecture is that the controls of the firewall (and inherent audits) are strong enough to control the authorized access to the S-HTTP server, and also thwart any attacks against the server itself. Additionally, the firewall can control external users so that they only have S-HTTP access via a logically dedicated path, and only to the designated S-HTTP server itself, without placing the rest of the internal enterprise at risk. This architecture relies on the absolute ability of the firewall and S-HTTP of always performing their designated security function as defined; otherwise, the enterprise has been opened for attack through the allowed path from external users to the internal S-HTTP server. Because these conditions are always required to be true and intact, the model with the server external to the firewall has been more readily accepted and implemented.

Both of these architectures can offer a degree of data protection in an S-HTTP architecture when integrated with the existing enterprise firewall architecture. As an aid in determining which architectural approach is right for a given enterprise, a risk assessment can provide great input to the decision. This risk assessment may include decision points such as:

- Available resources to maintain a high degree of firewall audit and S-HTTP server audit,
- Experience in firewall and server administration,
- Strength of their existing firewall architecture.

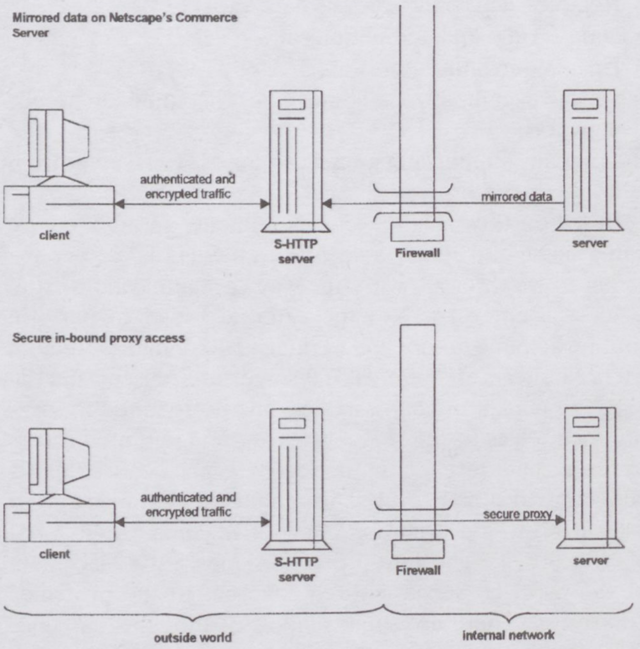

Mirrored data on Netscape's Commerce Server
authenticated and encrypted traffic
mirrored data
client
S-HTTP server
Firewall
server
Secure in-bound proxy access
authenticated and encrypted traffic
secure proxy
client
S-HTTP server
Firewall
server
outside world
internal network

Fig. 6. Externally Placed Server

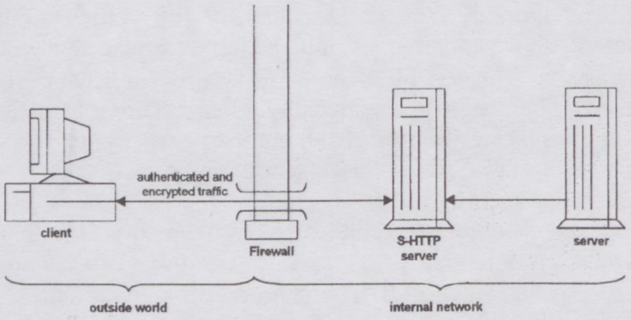


Fig. 7. Internally Placed Server

3.5.4. Secure WWW client configuration

There is much more reliance on the knowledge and cooperation of the end user and the use of a combination of desktop and workstation software, security control parameters within client software, and security products all working together to mimic the security of the mainframe and distributed application's environments. Consider the areas below during the risk assessment process and the design of WWW security solution sets:

- Ensure that all internal and external company-used workstations have resident and active antivirus software products installed,
- Ensure that all workstation and browser client software is preconfigured to return all WWW and other external file transfers to temporary files on the desktop. Under no circumstances should client server applications or process-to-process automated routines download files to system files, preference files, bat files, start-up files, etc.,
- Ensure that JAVA script is turned off in the browser client software desktop configuration,
- Configure browser client software to automatically flush the cache, either upon closing the browser or disconnecting from each Web site,
- When possible or available, implement one of the new security products that scans WWW downloads for viruses,
- Provide user awareness and education to all desktop WWW and Internet users to alert them to the inherent dangers involved in using the Internet and WWW. Include information on detecting problems, their roles and responsibilities, your expectations, security products available, how to set and configure their workstations and program products, etc.,
- Suggest or mandate the use of screen savers, security software programs, etc., in conjunction with your security policies and distributed security architectures.

This is a list of current areas of concern from a security perspective. There are options that when combined can tailor the browser to the specifications of individual workgroups or individuals. These options will evolve with the browser technology. The list should continue to be modified as security problems are corrected or as new problems occur.

3.5.5. Audit tools and capabilities

Today's auditing strategies must be robust, available across multiple heterogeneous platforms, computing and network based, real-time and automated, and integrated across the enterprise.

Today, information assets are distributed all over the enterprise, and therefore auditing strategies must acknowledge and accept this challenge and accommodate more robust and dicey requirements. As is the case when implementing distributed security control mechanisms, in the audit environment there are also many players and functional support areas involved in collecting, integrating, synthesizing, reporting, and reconciling audit trails and audit information.

The overall audit solutions set should incorporate the use of browser access logs, enterprise security server audit logs, network and firewall system authentication server audit logs, application and middle-ware audit logs, URL filters and access information, mainframe system audit information, distributed systems operating system audit logs, data base management system audit logs, and other utilities that provide audit trail information such as accounting programs, network management products, etc.

The establishment of auditing capabilities over WWW environments follows closely with the integration of all external WWW servers with the firewall, as previously mentioned. This is important when looking at the various options available to address a comprehensive audit approach.

WWW servers can offer a degree of auditability based on the operating system of the server on which they reside. The point, though, is that in order to provide some auditing the first place to potentially implement the first audit is on the platform where the WWW server resides. Issues here are the use of privileged accounts and file logs and access logs for log-ins to the operating system, which could indicate a backdoor attack on the WWW server itself. If server-based logs are utilized, they of course must be file protected and should be off-loaded to a nonserver-based machine to protect against after-the-fact corruption.

Though the server logs aren't the only defensive logs that should be relied upon in a public WWW server environment, the other components in the access architecture should be considered for use as audit log tools. As previously mentioned, the WWW server should be placed in respect to its required controls in relation to the network security firewall. If it is an S-HTTP server that is placed behind the firewall then the firewall of course has the ability to log all access to the S-HTTP server and provide a log separate from the WWW server-based logs, and is potentially more secure should the WWW server somehow become compromised.

The prevalent security architecture places externally accessible WWW servers wholly outside the firewall, thus virtually eliminating the capability of auditing access to the WWW server except from users internal to the enterprise. In this case, the network security audit in the form of the network management tool, which monitors the "health" of enterprise components can be called upon to provide a minimal degree of audit over the status of your external WWW server. This type of audit can be important when protecting data which resides on your external server from being subject to "denial of service" attacks, which are not uncommon for external devices. But by utilizing your network management tool to guard against such attacks, and monitoring log alerts on the status or health of this external server, you can reduce the exposure to this type of attack.

Other outside devices that can be utilized to provide audit include the network router between the external WWW server and the true external environment, though these devices are not normally readily set up for comprehensive audit logs, but in some critical cases they could be reconfigured with added hardware and minimal customized programming.

Another possible source of audit logging could come from "back end" systems that the WWW server is programmed to "mine" data from. Many WWW environments are being established to serve as "front ends" for much larger data repositories, such as Oracle data bases, where the WWW server receives user requests for data over HTTP, and the WWW server launches SQL_Net queries to a back end Oracle data base. In this type of architecture the more developed logging inherent to the Oracle environment can be called upon to provide audits over the WWW queries. The detailed Oracle logs can specify the quantity, data type, and other activity over all the queries that the WWW server has made, thus providing a comprehensive activity log that can be consolidated and reviewed should any type of WWW server compromise be suspected. A site could potentially discover the degree of data exposure though these logs. These are some of the major areas where auditing can be put in place to monitor the WWW environment while enhancing its overall security. It is important to note that the potential placement of audits encompasses the entire distributed computing infrastructure environment, not just the new WWW server itself. In fact, there are some schools of thought that consider the more reliable audits to be those that are somewhat distanced from the target server, thus reducing the potential threat of compromise to the audit logs themselves.

3.5.6. WWW security flaws

As with all new and emerging technology, many initial releases come with some deficiency. But this has been of critical importance when that deficiency can impact the access or corruption of a whole corporation's or enterprise's display to the world. This can be the case with Web implementations utilizing the most current releases which have been found to contain some impacting code deficiencies, though up to this point most of these deficiencies have been identified before any major damage has been done. This underlines the need to maintain a strong link or connection with industry organizations that announce code shortcomings that impact a sites Web implementation. A couple of the leading organizations are CERT, the Computer Emergency Response Team, and CIAC, Computer Incident Advisory Capability.

Just a few of these types of code or design issues that could impact a sites Web security include initial issues with the Sun JAVA language and Netscape's JavaScript (which is an extension library of their HyperText Markup Language, HTML).

The Sun Java language was actually designed with some aspects of security in mind, though upon its initial release there were several functions that were found to be a security risk. One of the most impacting bugs in an early release was the ability to execute arbitrary machine instructions by loading a malicious Java applet. By utilizing Netscape's caching mechanism a malicious machine instruction can be downloaded into a user's machine and Java can be tricked into executing it. This doesn't present a risk to the enterprise server, but the user community within one's enterprise is of course at risk.

Other Sun Java language bugs include the ability to make network connections with arbitrary hosts (though this has since been patched with the following release) and Java's ability to launch denial of service attacks though the use of corrupt applets.

These types of security holes are more prevalent than the security profession would like to believe, as the JavaScript environment also was found to contain capabilities that allowed malicious functions to take place. The following three are among the most current and prevalent risks:

- JavaScripts ability to trick the user into uploading a file on his local hard disk to an arbitrary machine on the Internet,

- The ability to hand out the user's directory listing from the internal hard disk,
- The ability to monitor all pages the user visits during a session.

The following are among the possible protection mechanisms:

- Maintain monitoring through CERT or CIAC, or other industry organizations that highlight such security risks,
- Utilize a strong software distribution and control capability, so that early releases aren't immediately distributed, and that new patched code known to fix a previous bug is released when deemed safe,
- In sensitive environments it may become necessary to disable the browser's capability to even utilize or execute JAVA or JavaScript – a selectable function now available in many browsers.

In the last point, it can be disturbing to some in the user community to disallow the use of such powerful tools, because they can be utilized against trusted Web pages, or those that require authentication through the use of SSL or S-HTTP. This approach can be coupled with the connection to S-HTTP pages where the target page has to prove its identity to the client user. In this case, enabling Java or JavaScripts to execute on the browser (a user-selectable option) could be done with a degree of confidence.

Other perceived security risks exist in a browser feature referred to as HTTP "Cookies." This is a feature that allows servers to store information on the client machine in order to reduce the store and retrieve requirements of the server. The cookies file can be written to by the server, and that server, in theory, is the only one that can read back their cookies entry. Uses of the cookie file include storing user's preferences or browser history on a particular server or page, which can assist in guiding the user on their next visit to that same page. The entry in the cookies file identifies the information to be stored and the uniform resource locator (URL) or server page that can read back that information, though this address can be masked to some degree so multiple pages can read back the information.

The perceived security concern is that pages impersonating cookies-readable pages could read back a user's cookies information without the user knowing it, or discover what information is stored in their cookie file. The threat depends on the nature of the data stored in the cookie file, which is dependent on what the server chooses to write into a user's cookie file. This issue is currently under review, with the intention of adding additional security controls to the cookie file and its function. At this point it is important that users are aware of the existence of this file, which is viewable in the Macintosh environment as a Netscape file and in the Win environment as a cookies.txt file.

4. INTERNET FIREWALLS

In the most elementary sense, a firewall is a security barrier between two networks that screens traffic coming in and out of the gate of one network to accept or reject connections and service requests according to a set of rules. If configured properly, it addresses a large number of threats that originate from outside a network without introducing any significant security liabilities. A more sophisticated firewall also controls how any connections between a host external to a network and an internal host occur. In addition, an effective firewall also hides information such as names and addresses of hosts within the network as well as the topology of the network it is employed to protect. Firewalls can defend against attacks on hosts (including spoofing attacks), applications protocols, and applications. In addition, firewalls provide a central way of not only administering security for a network, but also for logging incoming and outgoing traffic to allow accountability of user actions and for triggering incident response activity if unauthorized activity occurs.

Firewalls are typically placed at gateways to networks (see Fig. 8), mainly to protect an internal network from threats originating from an external one (especially from the Internet). In this type of deployment the goal is to create a security perimeter (see Fig. 8) protecting hosts within from attacks originating from external sources. This scheme is successful to the degree that the security perimeter is not accessible through unprotected avenues of. The firewall acts as a "choke" component for security purposes. Note that in Fig. 7 routers are in front and in back of the firewall. The first (shown above the firewall) is an external router used to initially route incoming traffic, direct outgoing traffic to external networks, and broadcast information that enables other network routers as well as the router to the other side of the firewall to know how to reach it. The other router is an internal router that sends incoming packets to their destination within the internal network, directs outgoing packets to the external router, and broadcasts information concerning how to reach it to the internal network and the external router. This "belt and suspenders" configuration further boosts security by preventing broadcasting of information about the internal network outside of the network that the firewall protects. This information can help an attacker learn of IP addresses, subnets, servers, and other information useful in perpetrating attacks against the network. Hiding information about the internal network is much more difficult if the gate has only one router because this router is the external and internal one, and must thus broadcast information about the internal network to the outside [8].

Another way that firewalls are deployed (although, unfortunately, not as frequently) is within an internal network – at the entrance to a subnet within a network – rather than at the gateway to the entire network (see Fig. 9). The purpose is to segregate a subnetwork (a "screened subnet") from the internal network at large – a very wise strategy when the subnet has higher security needs than those within the rest of the security perimeter. This type of deployment allows more careful control over access to data and services within a subnet than is otherwise allowed within the network. The gate-based firewall, for example, may allow FTP access to an internal network from external sources. If a subnet contains hosts that store information such as lease bid data or salary data, however, allowing FTP access to this subnet is less advisable. Setting up the subnet as a screened subnet could solve this problem and provide suitable security control – the internal firewall that provides security screening for the subnet could be configured to deny all FTP access, regardless of whether the access requests originated from outside or inside the network [8], [9].

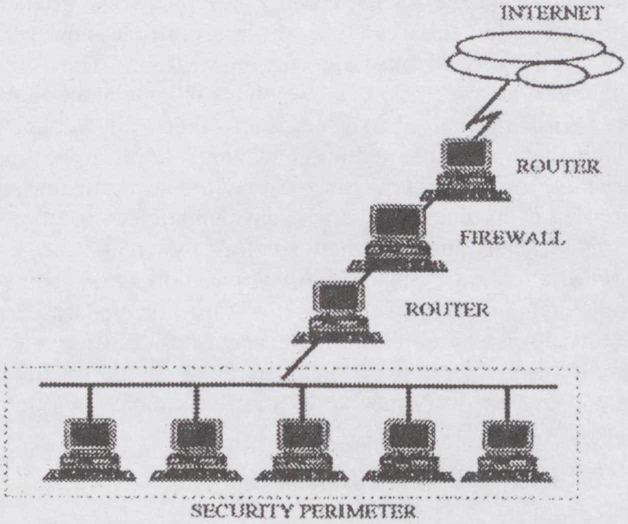


Fig. 8. A Typical Gate-Based Firewall Architecture

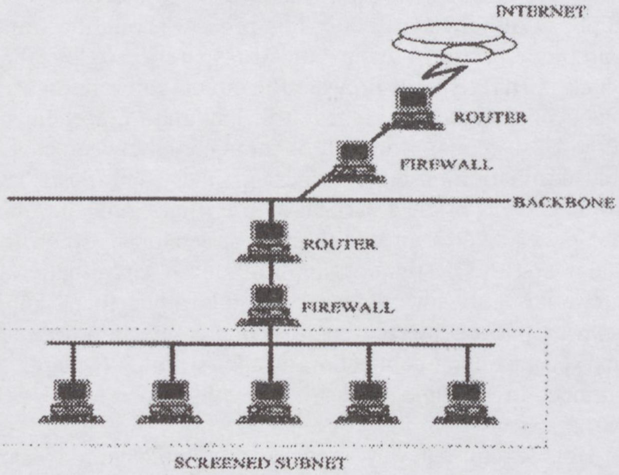


Fig. 9. A Screened Subnet

4.1. Packet Filters

The most basic type of firewall is a packet filter. It receives packets, then evaluates them according to a set of rules that are usually in the form of access control lists. The result is that packets can meet with a variety of fates – be forwarded to their destination, dropped altogether, or dropped with a return message to the originator informing him what happened. The most frequently applied filtering rules are:

- Source and destination IP address,
- Source and destination port,
- Direction of traffic (inbound or outbound),
- Type of protocol (e.g., IP, TCP, UDP, IPX, and so forth),
- The packet's state (SYN or ACK (Acknowledge)).

Packet-filtering firewalls are a good way to provide a reasonable amount of protection for a network with minimum complications. Packet-filtering rules can be extremely intuitive and can thus be easy to set up. Packet-filtering firewalls also tend to have the least negative impact upon throughput rate at the gateway compared to other types of firewalls. Additionally, they tend to be the most transparent to legitimate users; if the filtering rules are set up appropriately, users will be able to obtain the access they need with little interference from the firewall.

Unfortunately, simplicity has its disadvantages. The rules that this type of firewall implements are based on port conventions. When an organization wants to stop certain service requests (e.g., telnet) from reaching internal (or external) hosts, the most logical rule implementation is to block the port (in this case, port 23) that by convention is used for telnet traffic. Blocking this port, however, does not prevent someone inside the network from allowing telnet requests on a different port that the firewall's rules leave open. In short, firewalling schemes based on ports do not provide the precision of control that many organizations need. Furthermore, packet-filtering firewalls are often deficient in logging capabilities, particularly in providing logging that can be configured to an organization's needs (e.g., in some cases to capture only certain events, while in other cases to capture all events), and often also lack remote administration facilities that can save considerable time and effort. Finally, creating and updating filtering rules is prone to logic errors that result in easy conduits of unauthorized access to a network and can be a much larger, more complex task than anticipated.

Like many other security-related tools, many packet filtering firewalls have become more sophisticated over time. Some vendors of packet-filtering firewalls in fact now offer programs that check the logic of filtering rules to discover logical contradictions and other errors. Some packet-filtering firewalls, additionally, offer strong authentication mechanisms such as token-based authentication. Many vendors' products now also defend against previously successful methods to defeat packet-filtering firewalls. Network attackers can send packets to or from a disallowed address or disallowed port by fragmenting the contents. Fragmented packets cannot be analyzed by a conventional packet-filtering firewall, so the firewall passes them through, but then they are assembled at the destination host. In this manner the network attackers can bypass firewall defenses altogether. However, some vendors have developed a special kind of packet-filtering firewall that prevents these types of attacks by remembering the state of connections that pass through the firewall. Some state-conscious firewalls can even associate each outbound connection with a specific inbound connection (and vice versa), making enforcement of filtering rules much simpler.

4.2. Application-Gateway Firewalls

A second type of firewall handles the choke function of a firewall in a different manner – by determining not only whether but also how each connection through it is made. This type of firewall stops each incoming (or outgoing) connection at the firewall, then (if the connection is permitted) initiates its own connection to the destination host on behalf of whomever created the initial connection. This type of connection is thus called a proxy connection. Using its database defining the types of allowed connections, the firewall either establishes another connection (permitting the originating and destination host to communicate) or drops the original connection altogether. If the firewall is configured appropriately, the whole process can be largely transparent to users.

An application-gateway firewall is simply a type of proxy server that provides proxies for specific applications. The most common implementations of application-gateway firewalls address proxy services (such as mail, FTP, and telnet) so that they do not run on the firewall itself – something that is very good for the sake of security, given the inherent dangers associated with each. Mail services, for example, can be proxied to a mail server. Each connection is subject to a set of specific rules and conditions similar to those in packet-filtering firewalls except that the selectivity rules used by application-gateway firewalls are not based on ports, but rather on the to-be-accessed programs/services themselves (regardless of what port is used to access these programs). Criteria such as the source or destination IP address can, however, still be used to accept or reject incoming connections. Application-level firewalls can go even further by determining permissible conditions and events once a proxy connection is established. An FTP proxy could restrict FTP access to one or more hosts by allowing use of the get command, for example, while preventing the use of the put command. A telnet proxy could terminate a connection if the user attempts to perform a shell escape or to gain root access. Application-gateway firewalls are not limited only to applications that support TCP/IP services; these tools can similarly govern conditions of usage of a wide variety of applications, such as financial or process control applications.

Two basic types of application-gateway firewalls are currently available: (1) application-generic firewalls, and (2) application-specific firewalls. The former provide a uniform method of connection to every application, regardless of which particular one it is. The latter determine the nature of connections to applications on an application-by-application basis. Regardless of the specific type of application-gateway firewall, the security control resulting from using a properly configured one can be quite precise. When used in connection with appropriate host-level controls (e.g., proper file permissions and ownerships), application-gateway firewalls can render externally originated attacks on applications extremely difficult. Application-gateway firewalls also serve another extremely important function – hiding information about hosts within the internal network from the rest of the world, so to speak. Finally, a number of commercial application-gateway firewalls available today support strong authentication methods such as token-based methods (e.g., use of hand-held authentication devices).

Application-gateway firewalls currently are the best selling of all types of firewalls. Nevertheless, they have some notable limitations, the most significant of which is that every TCP/IP client for which the firewall provides proxies must be aware of the proxy that the firewall runs on its behalf. This means that each client must be modified accordingly, which is often no small task in today's typical computing environment. A second limitation is that unless one uses a generic proxy mechanism, every application needs its own custom proxy. This limitation is not formidable in the case of proxies for services such as telnet, FTP, and HTTP, because a variety of proxy implementations are available for these widely used services. Proxies for many other services are at the present time, however, not available, and must be custom written. Third, although some application-gateway firewall implementations are more transparent to users than others, any vendor's claim that any implementation is completely transparent warrants healthy skepticism. Some application-gatewall firewalls even require users who have initiated connections to make selections from menus before they reach the desired destination. Finally, most application-gateway firewalls are not easy to initially configure and update correctly. To use an application-gateway firewall to the maximum advantage, network administrators should set up a new proxy for every new application accessible from outside a network.

4.3. Circuit-Gateway Firewalls

As discussed previously, application-gateway firewalls receive connections from clients, dropping some and accepting others, but always creating a new connection with whatever restrictions exist whenever a connection is accepted. Although in theory this process should be transparent to users, in reality the transparency is less than ideal. A third type of firewall, the circuit-gateway firewall, has been designed to remedy this limitation by producing a more "seamless," transparent connection between clients and destinations using routines in special libraries. The connection is often described as a virtual circuit because the proxy creates an end-to-end connection between the client and the destination application. A circuit-gateway firewall is also advantageous in that rather than simply relaying packets by creating a second connection for each allowed incoming connection, it allows multiple clients to connect to multiple applications within an internal network.

Most circuit-gateway firewalls are implemented using SOCKS, a protocol that includes a set of client libraries for proxy interfaces with clients. SOCKS receives an incoming connection from clients, and if the connections are allowed, it provides the data necessary for each client to connect to the application. Each client then invokes a set of commands to the gateway. The circuit-gateway firewall then imposes all predefined restrictions, such as the particular commands that can be executed, and establishes a connection to the destination on the client's behalf. To users this process appears transparent.

As with application-gateway firewalls, circuit-gateway firewall clients must generally be modified to be able to interface with the proxy mechanism that is used. Making each client aware of SOCKS may not be an overwhelming task because of the availability of a variety of SOCKS libraries available for different platforms. The client must simply be compiled with the appropriate set of SOCKS libraries for the particular platform (e.g., UNIX, Windows, and so forth) on which the client runs.

Circuit-gateway firewalls also have limitations. First and foremost, the task of modifying all clients to make them aware of the proxy mechanism is, unfortunately, potentially extremely costly and time-consuming. Having a common interface to the proxy server so that each client would not have to be changed would be a major improvement. Second, circuit-gateway firewalls tend to provide a rather generic access mechanism that is independent of the semantics of destination applications. For example invoking the delete command to delete data in an application that reinitializes all parameter values by retrieving values from a database not accessible to users every time it is invoked is potentially not catastrophic. In other applications, however, being able to delete data is likely to be hazardous. So offering proxies that take into account application semantics would be more advantageous. In addition, SOCKS has several limitations. Most implementations of SOCKS are rather deficient in their ability to log events. Furthermore, SOCKS neither supports strong access authentication methods nor provides an interface to authentication services that could provide this function.

4.4. Hybrid Firewalls

Although the distinction between packet-filtering firewalls, application-gateway firewalls, and circuit-gateway firewalls is meaningful, many firewall products cannot be classified as exactly one type. As firewalls evolve, additionally, it is likely that some of the features in application-gateway firewalls will be included in circuit-gateway firewalls, and vice versa.

4.5. Virtual Private Networks

An increasingly popular Internet security control measure is Virtual Private Networks (VPNs), which incorporate end-to-end encryption into the network, enabling a secure connection to be established from any individual machine to any. At present, this technology is most commonly implemented in firewalls, allowing organizations to create secure "tunnels" across the Internet (see Fig. 10). Attackers who have planted one or more network capture devices anywhere along the route used to send packets between the firewalls will not gain any advantage from capturing these packets unless they can crack the encryption key, an unlikely feat unless a key that is extremely short in length is used. The chief disadvantage of the firewall-to-firewall VPN is that it does not provide an end-to-end tunnel. In this scheme packets transmitted between a host and the firewall for that host are in cleartext and are thus still subject to being captured. Increasingly, however, vendors are announcing support for end-to-end VPNs, allowing host-to-host rather than only firewall-to-firewall tunnels.

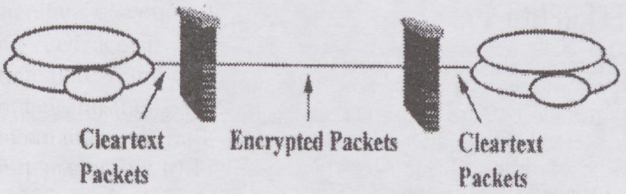


Fig. 10. A Virtual Private Network

Like any other type of Internet security control measure, VPNs are not a panacea. Anyone who can break into a machine that stores an encryption key can, for example, subvert the integrity of a VPN. VPNs do not supplant firewalls or other kinds of network security tools, but rather supplement the network security administrator's arsenal with capabilities that were not, for all practical purposes, previously available. With the PPTP (point-to-point tunneling protocol) standard currently being widely implemented in VPN products (usually in firewalls with VPN support capabilities), the task of setting up secure tunnels is at least now much less formidable than it was even recently [8].

4.6. Security Maintenance

Developing an accurate and complete firewall policy is the most important single step in using firewalls effectively. This policy provides a statement of requirements for each firewall, and should be modified and updated as new applications are added within the internal network protected by the firewall and as new security threats emerge. Maintaining firewalls properly and regularly examining log data they provide are almost certainly the most neglected facets of using firewalls, yet these activities are among the most important in ensuring that the defenses are adequate and that incidents are quickly detected and handled. Regularly performing security evaluations and testing the firewall to identify any exploitable vulnerabilities or misconfiguration are also essential activities.

Properly designing and implementing firewalls, after all, can be difficult, costly, and time consuming. The truth, however, is that firewall design and implementation are simply the beginning point of having a firewall, and that firewalls that are not properly maintained soon lose their value as security control tools. One of the most important facets of firewall maintenance is updating both the security policy and rules by which each firewall operates. Firewall functionality nearly invariably needs to change as new services and applications are introduced in (or sometimes removed from) a network. Undertaking the task of inspecting firewall logs on a daily basis to discover attempted and possibly successful attacks on both the firewall and the internal network it protects should be an extremely high priority. Evaluating and testing the adequacy of firewalls for unexpected access avenues to the security perimeter and vulnerabilities that lead to unauthorized access to the firewall itself should also be a frequent, high-priority activity [8].

REFERENCES

[1] Internet Security Protocol, 1998
[2] Security Project at the TCM Laboratory
[3] Technical White Paper Discussing Encription Definitions and Methods Used in Data Communication Systems
[4] A. Menezes, P. van Oorschot, S. Vanstone: Handbook of Applied Cryptography, CRC Press, 1996
[5] Stephen James: The Self Hack Audit
[6] Dan Thomsen: A New Security Model for Networks and the Internet
[7] Steve Blanding: An Introduction to LAN/WAN Security
[8] E. Eugene Schultz: Internet Firewalls
[9] Marcus J. Ranum: Thinking About Firewalls

AZ INTERNET HASZNÁLAT BIZTONSÁGA

GÁL RICHÁRD

ELMÉLETI VILLAMOSSÁGTAN TANSZÉK
BUDAPESTI MŰSZAKI EGYETEM
1111 BUDAPEST, EGRY J. U. 18.

Az utóbbi időben egyre több vállalat, cég próbálja felhasználni az Internetet különböző céljai megvalósításához annak ellenére, hogy az Internet alapjául szolgáló architektúra nem igazán biztonságos. A helyzetet tovább bonyolítja, hogy a gyártók, a szabványokat felügyelő és kialakító szervezetek eddig még nem állapodtak meg olyan szabványban, amely egységesen kezelné az Interneten folyó kommunikációt a megfelelő biztonságtechnikai követelményeknek megfelelően. A feladat nem egyszerű, hiszen itt egy sok szereplős, elosztott rendszerről van szó.

A WWW (World Wide Web)' még egy lökést adott az Internetet használóknak olyannyira, hogy az Interneten áthaladó forgalom ennek következtében kb. fél évente duplázódik. Köszönhető ez részben annak, hogy a WWW által kínált felhasználói interfész egységes, a felhasználói és a szolgáltatói oldal konfigurálása egyszerű, és a rajta történő megjelenés olcsó és magas színvonalú.

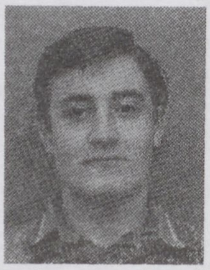
Ebben a cikkben az interneten folyó kommunikáció biztonságtechnikai szempontjait tekintettük át, különös tekintettel a biztonságos WWW technológiákra és a különböző tűzfalakkal megvalósított stratégiákra. Mindenek előtt pár szót szóltunk az internet alapját képező protokollokról.

Először a TCP/IP protokollokat tekintettük át. Ezt követően a TCP/IP és az OSI modell kapcsolata került leírásra, majd a hálózati és alkalmazás szintű protokollok vizsgálata következett. Ezek bizonyos szintű ismerete szükséges a továbbiak megértéséhez.

A következő fejezet arra koncentrált, hogy milyen okok járulnak hozzá egy számítógépes hálózati rendszer korrupciójához, ill. milyen óvintézkedések tehetők ennek megakadályozására.

Ezután kifejezetten WWW biztonságtechnikát célzó stratégiákról esett szó, úgy mint SSL, S-HTTP, illetve architekturális kérdések és auditáció.

Az utolsó fejezet a tűzfalakról adott áttekintést. Itt elsősorban a packet-filter, application-gateway és circuit-gateway típusú tűzfalakról és a virtuális magánhálózatokról szóltunk.



Richárd Gál was born in Eger. He spent his primary school studies in Füzesabony. He went to the Szilágyi Erzsébet secondary grammar school in Eger, where he attended a special english class and specialized in mathemathics. After his final exam he was accepted to the Technical University of Budapest and went to the faculty of Electrical Engineering and Informatics. His majors were telecommunication networks and multimedia. He participated on the Scientific Conference of Students in 1997 where he got 1st prize with an essay on wavelet based image compression. He wrote my diplomawork on the same topic. he got my diploma in 1999 cerifying that he is an MsC in Technical Informatics. In the autumn of 1999 he began my PhD studies in e-commerce in the same faculty of TUB.

FRAMEWORKS, TOOLKITS SOLUTIONS FOR E-COMMERCE AND E-SECURITY

ATTILA BAK

DEPARTMENT OF ELECTROMAGNETIC THEORY
TECHNICAL UNIVERSITY OF BUDAPEST
H-1111 BUDAPEST, EGRY J. U. 18.

At the outset of this article the main concepts of the Public Key Infrastructure (PKI) will be detailed. After this the abstraction of Virtual Private Networks (VPN) will be introduced and its relationship with PKI will be cleared. Since Baltimore Technologies is one of the leading suppliers and main developers in the field of e-commerce and e-security framework products, toolkits and API's will be introduced. A whole section will be devoted to the interesting connection between wireless mobile technology (WAP) and e-security. At last but not at least we will gain a short introduction into the widely used and accepted e-commerce framework (Java Commerce Framework) from Sun Microsystems, Inc.

1. INTRODUCTION TO PKI

1.1. IT Security – Threats and Opportunities

We are in the middle of an electronic business revolution. The new global culture of electronic information exchange and networking poses a greater threat than ever before of fraud, e-mail eavesdropping and data theft for both companies and individuals.

Information security is now a major issue facing today's electronic society. As the information highway transcends borders, locked doors are no longer sufficient to protect one of the corporation's most valuable assets — information. On the other hand, the Internet provides corporations with new and exciting opportunities to develop an additional channel for service delivery. The ubiquitous, low-cost nature of the Internet has caused an explosion in e-business and e-commerce activity, creating a paradigm shift in the business world. Putting business "online" opens up a whole new world of possibilities such as enhanced service levels, increased efficiency, reduced costs, improved corporate-wide communications, shorter time-to-market and wider market reach. Organizations recognize the need to respond strategically to this explosive growth, rather than reactively, carefully balancing concern for the protection of corporate data, with the desire to leverage this new medium for competitive advantage. Information security is at the heart of both of these demands. We need information security not only to protect our assets, but also to enable us to take advantage of this new market opportunity. We need to have the same levels of confidence and trust in the electronic world, as we have in the traditional world. As we move into the electronic world, how can we recognize and trust people when we cannot see them, hear them or even receive their signature? How do we keep our business transactions secret without sealed envelopes or private telephone calls? How do we know the intended person received the message intact, and has agreed to the contract?

Public Key Infrastructure (PKI) provides the key to unlock the benefits of a truly secure electronic world [1].

1.2. What is a Public Key Infrastructure (PKI)?

Securing business and communications over computer networks can be likened to an electronic equivalent of signing a letter and sealing it in an envelope. The signature proves authenticity and the sealed envelope provides confidentiality. Cryptography ensures confidentiality by encrypting a message using a secret key in association with an algorithm.

This produces a scrambled version of the message that the recipient can decrypt, using the original key, to retrieve the contents. The key used must be kept secret between the two parties. The central problem in most cryptographic applications is managing these keys and keeping them secret. Public key cryptography solves this problem by replacing the secret key with a pair of keys, one private and one public. Information encrypted using the public key can only be retrieved using the complementary private key. With this system the public keys of all users can be published in open directories, facilitating communications between all parties. In addition to encryption, the public and private keys can be used to create and verify 'digital signatures'. These can be appended to messages to authenticate the message and the sender. But public key cryptography, on its own, is not enough if we are to truly re-create the conditions for traditional paper-based commerce in an electronic world.

We also need:

- Security policies to define the rules under which the cryptographic systems should operate,
- Products to generate, store and manage the keys,
- Procedures to dictate how the keys and certificates should be generated, distributed and used.

In short — we need a *Public Key Infrastructure (PKI)*.

PKI provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the four principal security functions for commercial transactions:

- *Confidentiality* — to keep information private,
- *Integrity* — to prove that information has not been manipulated,
- *Authentication* — to prove the identity of an individual or application,
- *Non-repudiation* — to ensure that information cannot be disowned.

Lack of security is often cited as a major barrier to the growth of e-commerce, which can only be built on the confidence that comes from knowing that all transactions are protected by these core functions.

Like any new, business-critical technology, the evaluation and implementation of a PKI solution is a challenging and intricate process, which requires a great deal of planning, management and clear guidance.

Remark: It is estimated that the Digital Certificate Software and CA Service market is set for a compound annual growth rate of 80 % between 1998 and 2002.

1.3. The Components of a PKI

A Public Key Infrastructure is a combination of hardware and software products, policies and procedures. It provides the basic security required to carry out electronic business so that users, who do not know each other, or are widely distributed, can communicate securely through a chain of trust. PKI is based on digital IDs known as "digital certificates" which act like "electronic passports", and bind the user's digital signature to his or her public key.

A PKI should consist of:

- A Security Policy,
- Certificate Authority (CA),
- Registration Authority (RA),
- Certificate Distribution System,
- PKI-enabled Applications.

Security Policy

A security policy sets out and defines an organization's top-level direction on information security, as well as the processes and principles for the use of cryptography. Typically it will include statements on how the organization will handle keys and valuable information, and will set the level of control required to match the levels of risk. Some PKI systems are operated by Commercial Certificate Authorities (CCAs) or Trusted Third Parties, and therefore require a CPS. This is a detailed document containing the operational procedures on how the security policy will be enforced and supported in practice. It typically includes definitions on how the CAs are constructed and operated, how certificates are issued, accepted and revoked, and how keys will be generated, registered and certified, where they will be stored, and how they will be made available to users [1].

Certificate Authority (CA)

The CA system is the trust basis of a PKI as it manages public key certificates for their whole life cycle. The CA will:

- Issue certificates by binding the identity of a user or system to a public key with a digital signature,
- Schedule expiry dates for certificates,
- Ensure certificates are revoked when necessary by publishing Certificate Revocation Lists (CRLs).

When implementing a PKI, an organization can either operate its own CA system, or use the CA service of a Commercial CA or Trusted Third Party.

Registration Authority (RA)

An RA provides the interface between the user and the CA. It captures and authenticates the identity of the users and submits the certificate request to the CA. The quality of this authentication process determines the level of trust that can be placed in the certificates.

Certificate Distribution System

Certificates can be distributed in a number of ways depending on the structure of the PKI environment, for example, by the users themselves, or through a directory service. A directory server may already exist within an organization or one may be supplied as part of the PKI solution.

PKI-enabled applications

Examples of applications are:

- Communications between web servers and browsers,
- Email,
- Electronic Data Interchange (EDI),
- Credit card transactions over the Internet,
- Virtual Private Networks (VPNs – will be detailed later on).

1.4. Steps to Evaluating PKI Solutions

The adoption of PKI technology is still in its infancy, and will be new to most organizations. It is essential that the following areas are considered when undertaking research into implementing a PKI.

Flexibility

It is essential that all components of a PKI are interoperable, as it is unlikely that they will all be sourced from a single supplier. For example, the CA may have to interface with existing systems, such as directory servers already installed in the organization. The PKI should use open, standard interfaces such as LDAP and X.500(DAP), in order to ensure that it is capable of working with all standards-compliant directory servers. In addition, many organizations have preferred suppliers of smart cards and hardware security modules (HSMs). Again, by using open, standard interfaces such as PKCS#11 (Cryptoki), the PKI has the flexibility to work with a wide range of security tokens. In many PKI systems, face to face registration is required to provide the necessary level of trust. However, this may not always be appropriate, so remote registration may be required. The PKI should allow users to request certificates by e-mail, by using a standard web browser or automatically via network communication devices for VPNs [1].

For some large scale implementations, certificates need to be automatically created in batches – for example bank cards or national identity cards. In such instances, the PKI requires the flexibility of an automated RA process linked to the card database.

Ease of Use

Although the principles upon which a PKI system works can be complicated, the management should not be. The PKI must enable non-technical personnel, such as business administrators, to operate it with confidence. These operators should not have to deal with the intricacies of cryptographic algorithms, keys and signatures. It should be as easy as clicking on icons and letting the software application do the rest. The interface should be graphical and intuitive, assisting the management task, rather than obscuring it in complex database records. Flexibility and ease of use will seriously impact the return on investment in a PKI system as they affect issues such as training, maintenance, system configuration, integration and of course future growth in user numbers. These issues can make the cost of ownership of a PKI far higher than the initial implementation cost and therefore need to be considered in the evaluation phase.

Support for an Organization's Security Policy

PKI is becoming central to organizational security infrastructures, and any CA must be capable of reflecting and implementing the organization's security policy. A policy-driven PKI system therefore is critical in order to ensure that the certificate management process accurately reflects the roles of the CA and RA Operators and certificate users. For example, the CA Operator may decide to delegate the end-user certificate revocation to the RA Operators, whilst retaining revocation rights over RA Operator certificates [1].

Scalability

As an organization's use and reliance on PKI increases, it is essential that the PKI system can scale to match this growth. Initially, a PKI may only support a single application, however, it should be versatile enough to support further applications as they come on-line. It should also be possible to add extra CA and RA components to support an increasing number of certificates as the PKI grows. In addition, a variety of certificate types and registration mechanisms may be needed as the scope of the PKI expands to include new services.

Interoperability

PKI technology is still in development stage and it is difficult to predict with any certainty the future uses and requirements for PKI systems. Standards for PKI are still evolving and in some cases are non-existent. Therefore, in order to protect your investment and prevent future interoperability headaches, it is vital to source a PKI that is completely open, and built to the most common and advanced commercial standards. This needs to be considered at the design stage, to ensure the seamless integration with the rest of your IT infrastructure.

The Security of the CA/RA

The CA/RA systems are at the heart of any PKI. The security of these systems is of primary importance, and if compromised, the whole PKI solution will be jeopardised.

In particular, the PKI must ensure the following:

The CA's private key should be held in a tamper-resistant security module and provision made for back-up copies for disaster recovery purposes. Access to the CA and RA should be tightly controlled, e.g. using smart cards to ensure strong user authentication. It should also be possible to configure the certificate management process such that more than one operator is required to authorize certification requests.

All certificate requests should be digitally signed by strong cryptographic authentication to detect and prevent hackers from deliberately generating bogus certificates. All significant events performed by the CA/RA system should be recorded in a secure audit trail, where each entry is time/date stamped and signed, to ensure that entries cannot be falsified. The CA should be approved and verified by an independent body, for example at least to ITSEC E2, but preferably to ITSEC E3 (Information Technology Security Evaluation Criteria). ITSEC is a recognized global standard for the measurement of security products and the E3 evaluation represents the highest level of commercial security sought today.

1.5. Conclusions to PKI

E-business is now a reality. With its growth currently accelerating at such a rapid pace, PKI will soon become so commonplace that organizations will issue digital certificates and smart cards as normal practice. It is therefore essential when evaluating a potential PKI system, that thorough research is undertaken, and informed decisions are made to ensure that the fundamental criteria have been met. To succeed in the electronic business world, organizations must re-engineer their working practices, and implement systems to undertake e-commerce securely, thereby embracing tomorrow's technology — today [1].

2. VIRTUAL PRIVATE NETWORKING

2.1. Introduction to VPN technology

The Internet has revolutionised the ways in which companies do business, the Internet Protocol (IP) being undeniably efficient, inexpensive and flexible. However, the existing methods used to route IP packets leave them vulnerable to a range os security risks such as spoofing, snifing and session hijacking and provide no form of non-repudiation for contractual and monetary transactions.

Recently, companies have demanded a more secure way to conduct business and to have more internal control over Internet security. Besides securing the internal environment, organisations need to secure communications between remote offices, business partners, customers and travelling and telecommuting employees. Transmitting messages over the Internet to these different entities poses an obvious risk, given the lack of protection provided by the existing Internet backbone.

Control and management of security and access between these different entities in a company's business environment is of paramount importance. This is where Virtual Private Networks (VPNs) play a major role and are set to revolutionise security on the Internet by providing a flexible, scalable and comprehensive information security solution. A VPN is an enterprise owned and managed network solution using existing dedicated networks, the Internet or a combination of both, to securely communicate information [2].

VPN providers differ in their product offerings:

- Embedded technology such as that employed in routers,
- Application level products installed on gateways and servers,
- Desktop client applications providing security for dial-up and Internet connections,
- Firewalls with VPN capabilites.

VPNs provide the necessary data privacy, access control, data integrity and authentication services at a low level in the network and are independent of the application using the network. By using VPN links to connect two networks, they become, essentially, one secure network.

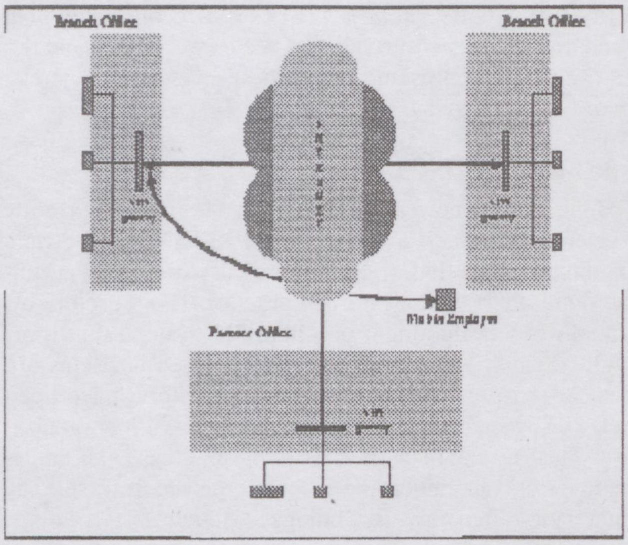


Fig. 1. VPN network securing a business, partner company and mobile worker

2.2. Tunneling Protocols

Securing traffic at the network level rather than at the application level has been a hot area of debate some time. For VPNs, three tunnelling protocols are emerging: L2TP (Layer 2 Tunnelling Protocol), PPTP (Point-To-Point Tunnelling Protocol) and IPSec. L2PT and PPTP are significant to those businesses supporting non-IP protocols, but provide weak authentication, whereas IPSec supports the IP protocol along with the Internet Key Exchange (IKE) and supports a number of identity technologies including X.509 certificates [2].

2.3. IPSec

A solution for securing all communications, irrespective of the applications generating the traffic is an ideal way to truly secure all network transactions the most important concerns being:

- Confidentiality and integrity – ensuring that data remains private and intact,
- Authentication – verifying the identity of any entity on the network, whether it be a user, application or gateway.

VPNs adhering to IPSec standards and using IPSec services provide secure, standards-based communications between different entities in a network. In their initial connection, each pair of entities negotiates the security policy that is to be used in their subsequent communications. Issues decided in this negotiation include the form of authentication, whether encryption will be used and the key lengths that will be used. This information is known as a Security Association (SA) and is referenced by a Security Policy Index (SPI) and use an established SA in any key negotiation and authentication [2].

The IPSec protocol suite uses two main components of the IP datagram to protect transmissions:

- Authentication Header (AH),
- Encapsulated Security Payload (ESP).

These two headers provide the required security features in IP transmissions and both are stored in an SA.

AHs provide authentication of both entity and data origin, integrity and replay protection, whilst ESPs provide confidentiality, authentication of data origin and replay protection. The two headers have some overlap in their functionality, the main difference being AH's provision of the strong authentication and ESP's provision of data protection.

IPSec defines algorithms for each type of header:

- AH – Authentication with static keys generated using MD5 and SHA-1,
- ESP – Encryption supporting many algorithms including DES, DES3, Blowfish.

Before a network session can begin, each party needs to negotiate the terms associated with the communication, terms to be later stored in the SA. The protocol defining this negotiation is IKE (IPSec Key Exchange, formerly ISAKMP/Oakley). IKE describes the use of key exchanges using the Diffie-Hellman algorithm with the addition of public key technology for securing the exchange, and modes of exchange.

IPSec defines IKE for authentication methods of mutual identification and includes:

- *IKE* – DSS signatures, RSA signatures, RSA encryption along with support for V3 X.509.

2.4. IPSec Authentication using a Public Key Infrastructure (PKI)

IKE authentication by itself is not secure enough. Without certificates IKE is reduced to using a pre-shared static key during authentication, this falls far short of the strength of verification required by businesses. A much stronger form of authentication is the use of public key technology to provide public key encryption techniques and digital certificates. A PKI provides the VPN with the facility to use strong authentication techniques, certificate management and support for certificate life cycles through the use of Certificate Revocation Lists (CRLs). Support for policy management within a PKI, allows the VPN to enforce strict policy control at a granular level throughout a network.

Key exchange without the use of trusted certificates received from a PKI or Trusted Third Party (TTP), is susceptible to attacks, especially the man in the middle attack (MIM). This attack involves a third party fooling each party in a connection into performing a key exchange with the attacker and not the intended party.

The certificates received from the PKI provide reliable authentication and secure key negotiation by allowing each party to verify that the host they are communicating with is indeed who they say they are. Lookup of revoked certificates is provided by support for directories, which are used to publish revoked certificates within the PKI [2].

2.5. PKI-Enabling a VPN

The PKI-Plus toolkit (described later) provides a means of building certification services and CRL lookup into any entity in a VPN, allowing full integration of a PKI to provide strong authentication.

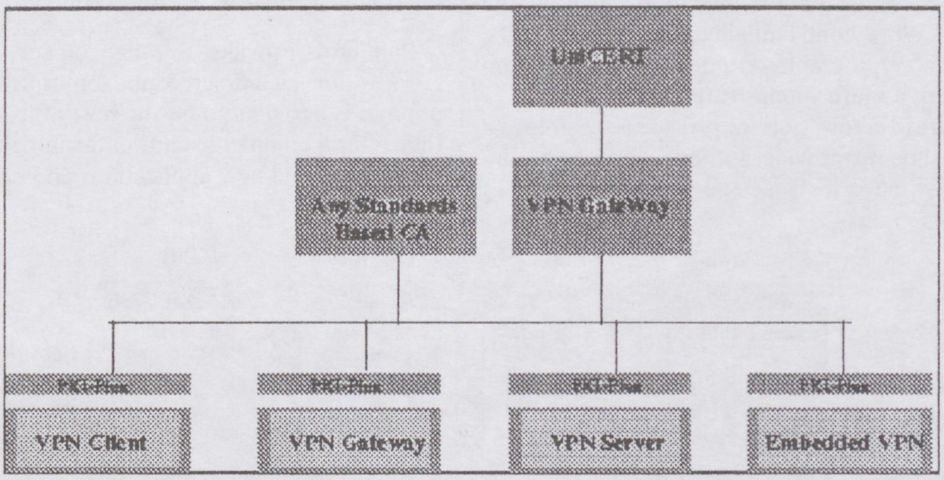


Fig. 2. PKI-Plus SDK enables VPN products to perform certificate processing to any standards-based CA

3. INTRODUCTION TO BALTIMORE TECHNOLOGIES

Baltimore Technologies is a leading supplier of security solutions for e-commerce and enterprise systems. These solutions are based on a family of products and services offered directly by Baltimore.

Each product contributes to the overall vision of Baltimore's e-security framework, which is designed to offer full security for a variety of business contexts. This security enables companies to operate more efficiently and to offer new levels of customer service.

For many software developer companies, it is essential to enable applications to work in distributed, networked environments, such as the Internet or Virtual Private Networks. This work requires changing the communications and security of the application to ensure compatibility with other applications and elements such as firewalls, proxies, etc. In the networked world, sensitive information becomes more generally available and accessible. This increase in information flow introduces a number of risks, necessitating the introduction of security solutions, which can provide both authentication of the parties involved in any transaction, and protect data while in transit or storage [7].

Software applications that are enabled to work with PKI systems will benefit from the enhanced security offered by Digital Certificates and cyptography. Additionally, applications that operate within a PKI security framework can benefit from a common security policy operated by an organisation. This can mean that a single smartcard or digital certificate can be used for a variety of systems within a company. For example, a single company-issued smartcard could be used for accessing applications, encrypting email, securing web connections and even opening doors!

3.1. Networked E-Security from Baltimore

The migration of computing environments to distributed, networked solutions has radically changed the way companies conduct business. Electric commerce has become a reality and businesses can now operate on a global basis without difficulty. Many corporations have also enhanced their legacy networks and communication infrastructure to take advantage of these new systems, with the Internet's low cost and global accessibility being of particular benefit.

For all its advantages, any networked solution results in a more open, less secure environment. Thus the usability of networks for commerce and enterprise-critical applications is limited by this lack of security. New security systems have been developed to provide applications and devices with even better security than was available on private, internal networks.

For traditional systems, security was based on restricting unauthorised access to the information or system that was being protected. This model does not work for distributed environments such as the Internet, which is completely open and allows unrestricted communications between everything connected.

For Enterprises, the security of corporate assets is paramount. Information, Intellectual Property, documentation, content, networks, data, computers, employee and customer data can all be considered part of a corporation's assets. Each of these can and should be safeguarded by a corporation to ensure it remains competitive within its marketplace [7].

For Electronic Commerce, security offers new ways of doing business with reduced risk. International supplier-to-customer relationships are now possible and security provides the necessary elements of trust to faciliate trade and communications. The advent of Trusted Third Party and Digital Signature legislation is designed to ensure that e-commerce become as viable as normal commerce.

Cryptography offers virtually unbreakable systems for security on open networks. A wide range of new Internet security systems has evolved in the past few years, which utilise cryptography for a wide variety of requirements. These technologies secure systems such as messaging, email, electronic payments, software applications and network communications.

At a basic level, security can be divided into a number of elements: confidentiality, authentication, integrity and non-repudiation. While confidentiality and integrity can be provided by basic cryptography, authentication and non-repudation require a more sophisticated system.

Public Key Infrastructure systems provide a scalable and policy based method to provide authentication and non-repudiation. PKIs have fast become the cornerstone of practically all e-commerce and enterprise security designs and are set to dominate the security landscape for the foreseeable future.

3.2. The E-Security Framework from Baltimore

Baltimore provides a range of security products and services for e-commerce and enterprise systems. Each product is designed to be the best in its class and together they offer a complete solution for integrating security into both legacy and new applications and environments [7].

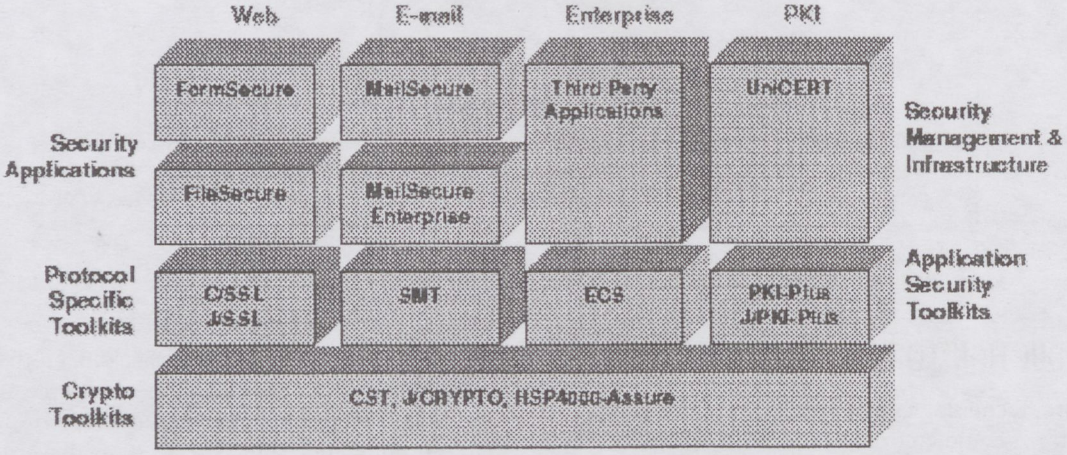


Fig. 3. Security modules and toolkits

In the followings the main modules, toolkits will be detailed.

Certificate Authority

Product: UniCERT

UniCERT is one of the world's leading CA systems and is used in PKI systems to provide full-strength security for a wide variety of e-commerce and enterprise security systems. It is a modular system which offers flexible, scalable deployment for both public and private CA systems. Using digital certificates, UniCERT provides authentication and non-repudation facilities for services such as Secure Email, Internet Shopping, Secure Web Banking, Online Trading and Virtual Private Networks. UniCERT powers both enterprise and commercial public Certificate Authority systems throughout the world and is compatible with all popular PKI-enabled applications. UniCERT also offers a unique policy-enforcement system.

Secure Applications

Products: MailSecure, FormSecure, FileSecure

These applications provide security for web and email systems within a PKI. They are designed to work with popular desktop systems (browsers, email clients) and provide full strength security based on industry protocols.

MailSecure Overview

All users may not be aware that every email travels as clear text around the organisation and across the globe. Email messages are passed between many different 'mail servers' as they travel from the sender to the receiver. Any of these mail servers could be used to capture a copy of the message for later analysis, or to alter the message in some way before sending it on to the next server [3].

It has become increasingly easy for competitors, or other outsiders, to gain information about an organization or the people within the organization, because of these loopholes. Furthermore, courts of law may accept email messages as evidence of wrongdoing, or of contract commitment.

MailSecure enables the full set of security functions to be added to email systems. These functions include:

- Confidentiality – provided by the use of 128bit DES strong encryption,
- Integrity – provided by the use of Digital Signatures,
- Authentication – provided by the use of X.509 digital certificates
- The proof of a transaction or 'Non-Repudiation' – provided by the use of a Public Key Infrastructure to issue digital certificates.

With MailSecure the organization can use email for all critical transactions. It does not matter what your organization's mail system is or the systems of your associates and partners because MailSecure provides support for most mail systems.

Control of the implementation and roll-out is provided through a centralised administration function – this limits the options which are allowed on users desktops so making system administration an easy task [3].

Full keybook and Certificate control is provided within MailSecure. This allows certificates to be stored either by each user themselves or on a central store. MailSecure supports both local and remote key and certificate generation so enabling small pilot systems to scale easily to trusted PKI implementations.

FormSecure Overview

FormSecure is a package of a number of software components easily installed from a single CD-ROM. This allows integrators and developers to choose the implementation of the security solutions best suited to their needs. Using FormSecure, the provision of a complete and integrated system for secure Web forms communication is a straightforward process. The diagrams show how the major components of FormSecure are deployed in a typical application [12].

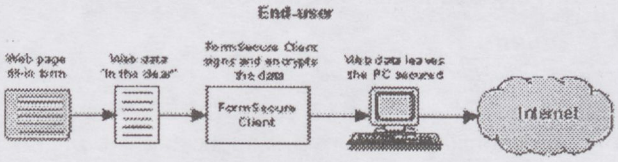


Fig. 4. FormSecure by client

FormSecure Client, which operates 'behind' the end user's existing browser, is distributed via Web download. No modification is required to the existing browser.

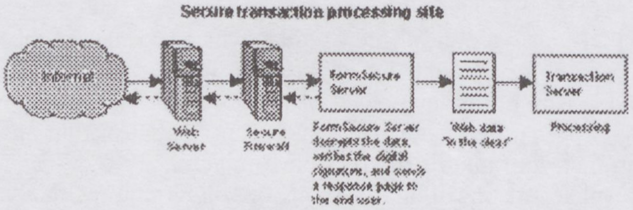

Secure transaction processing site
Internet
FormSecure Server
Transaction Server
Web Server
Secure Firewall
FormSecure Server decrypts the data, verifies the digital signature, and sends a response page to the end user.
Web data "in the clear"
Processing

Fig. 5. FormSecure by transaction server

FormSecure Server is loaded at the application transaction server site.

Other advantages of FormSecure:

E-commerce and e-business applications can only be built on the confidence that comes from knowing that all transactions are confidential and cannot be tampered with and that the senders are who they say they are and will not later be able to deny the transaction.

These functions are called confidentiality, integrity, authentication and non-repudiation. Using public key cryptography and Public Key Infrastructure (PKI), FormSecure delivers them all in an easy to use package [12].

Compared with other, commonly used security solutions only FormSecure provides all four functions combined in a widely applicable architecture (Table 1).

Table 1. FormSecure provides greatest security

	FormSecure	*SSL*	*SET*	*IPSec*
End-to-end confidentiality and integrity	Yes	No	Yes	No
User Authentication	Yes	No	Yes	No
Non repudiation	Yes	No	Yes	No
Standards based	Yes	Yes	Yes	Yes
Widely applicable	Yes	Yes	Credit card only	Yes
Signed responses	Yes	No	No	No

Secure Socket Layer (SSL) is an IP-based protocol that can only provide security between a Web browser and the Web server. It does not give 'end-to-end' security right through to the transaction processor. Further, without additional security mechanisms, SSL provides no means to identify a specific individual user, as having the right to perform an on-line transaction, for example, since SSL has no digital signature or authentication capability [12].

Secure Electronic Transactions (SET) is designed for a restricted group of related transactions and is suitable only for credit card transactions that involve a client, merchant and bank. By comparison, FormSecure offers a completely flexible solution for Web-based communication and transactions of many kinds.

IP Security Protocol (IPSec) operates only at the network level and does not provide security through to the application level, nor does it cater for user authentication and non-repudiation. While IPSec has the benefit of being easy to integrated into a system, with no need to adapt existing software, FormSecure delivers a much higher level of security, for a very modest investment in software development [12].

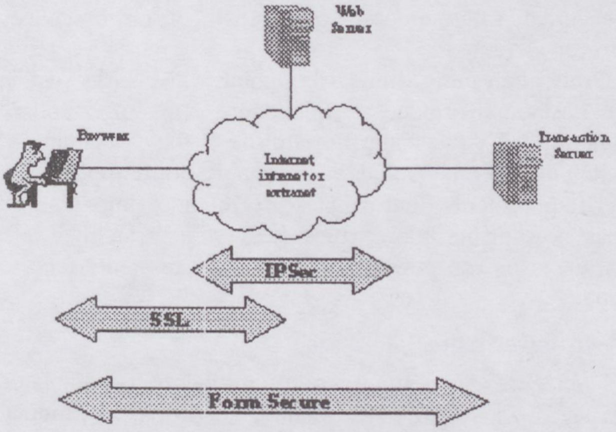


Fig. 6. Security levels

FileSecure Overview

FileSecure is a building block for integration projects. It acts as an automated, high-performance, process or 'robot'. FileSecure takes all incoming objects, which may be presented as files or email, secures them, and then presents them either to be sent out, collected or stored. Using industry-standard S/MIME and full-strength cryptography, FileSecure can sign and optionally encrypt objects, check signatures and decrypt, or just pass objects through untouched. FileSecure can handle multiple attachments in incoming and outgoing email.

A powerful management interface allows you to decide what processes-e.g. sign-only, pass-through-are applied to an object from a particular source directory or mail account, and where the resultant object will be sent [11].

The Problem FileSecure Solves

IT professionals widely understand that communicating between employees, with customers or business partners, over a public network-such as the Internet- often requires high-strength security. This applies to email, web-browsing or simple file transmission.

There are some applications available to assist this security requirement. However, many situation call for customised solutions. For example, what if many individuals, such as customers or suppliers, are sending large volumes of purchase requests, tenders, personal information updates, to your organisation? How do you deal with such requests securely and automatically, integrating with your back-end processing, without building complicated cryptographic software from the ground up?

Many integration projects now require security features. And there are not enough knowledgeable programmers to build specific applications from toolkits, within the available time.

FileSecure solves the problem. It is a self-contained building block, which provides integrators with the ability to by-pass the complexities of writing new security code into an application [11].

Who is FileSecure Designed For?

FileSecure has been developed for the convenience of system integrators who need to provide a security solution for their customers. From an end-user's perspective, FileSecure is invisible. There is no need to have a specialised programmer in order to incorporate security into the system.

Other than basic, standard, administrative tasks (which are easily performed, as FileSecure runs on standard Windows NT), the main prerequisite is the availability of someone who understands your organisation's applications and requirements, and can transform those into security rules. Applying these rules is then a straightforward matter, given the powerful and intuitive user interface to FileSecure.

Why Use FileSecure?

FileSecure allows an integration project to be completed quickly. FileSecure is a unique, server-based product. It can add high-strength, industry-standard security to products and processes with minimum integration effort. No programming is required [11].

FileSecure is high-performance tool, or building block, that offloads computer-intensive cryptographic operations, to minimise impact on performance. FileSecure separates the complex cryptographic operations from your core application, allowing you and your developers to focus on your core business. As a server process, FileSecure is invisible to the user, merely adding security when it is needed, and removing it when it is no longer needed.

How Does FileSecure Work?

The principle of FileSecure is simple, but it can be used to build sophisticated and comprehensive security projects. FileSecure takes an object from an input source, performs some cryptographic operations on that object, and outputs the resultant object to a destination.

The input source can be a directory (shared, local, remote) or an email account (i.e. waiting for incoming email) The cryptographic operations can be signing, signing and encrypting, verifying (checking the signature), decrypting, or not performing anyoperations (i.e. pass-through). The destination can be a directory (shared, local, remote), an email. The management interface allows you to set up and manage a series of rules, each one associating an input, a cryptographic operation, and a destination. In this way, a powerful and flexible security application can be constructed. Finally, FileSecure needs to be equipped with keys and corresponding certificates in order to sign messages. Since FileSecure uses standard X.509 Version 3 certificates, any compliant CA will work [11].

PKI Toolkits

Products: PKI-Plus, J/PKI-Plus

PKI-Plus (and its Java version, J/PKI-Plus) provides all the functionality necessary for applications to operate within a PKI. It provides support for cryptography, secure storage, digital certificates, directories, and certificate authorities. Its policy enforcement system enables a consistent, enterprise-wide security infrastructure to be implemented in all applications operating within a PKI [7].

PKI-Plus Overview

PKI-Plus is a radically new toolkit, which provides all the necessary functionality for applications to interact within a Public Key Infrastructure. It provides full encryption and digital signature capabilities which can be used within an Intranet, Extranet or Internet environment.

Unlike existing toolkit system, PKI-Plus requires minimum cryptographic or digital certificate knowledge on behalf of the developer. It offers a high-level API which can be readily integrated into new and legacy applications without difficulty. Additionally, its unique policy-enforcement system allows enterprises to dictate their security policy at the application and desktop level [10].

By using PKI-Plus, application developers can add full strength authentication, confidentiality, integrity and non-repundiation capabilities to any system.

PKI-Plus can be used by a wide variety of applications. Examples include:

- Email clients and systems,
- Secure Web applications,
- Access control systems,
- Digital Signature software systems,
- Virtual Private Networks,
- Certificate Registration systems.

Since PKI systems can be operated on a private and public basis, PKI-Plus is designed to work with both scenarios without difficulty.

PKI-Plus is fully object-oriented. It is available as C++ or Java classes (J/PKI-Plus). Available on Windows and Unix platforms and compliant with Java JDK 1.2, PKI-Plus can be integrated into nearly all environments, operating on multiple platforms [7].

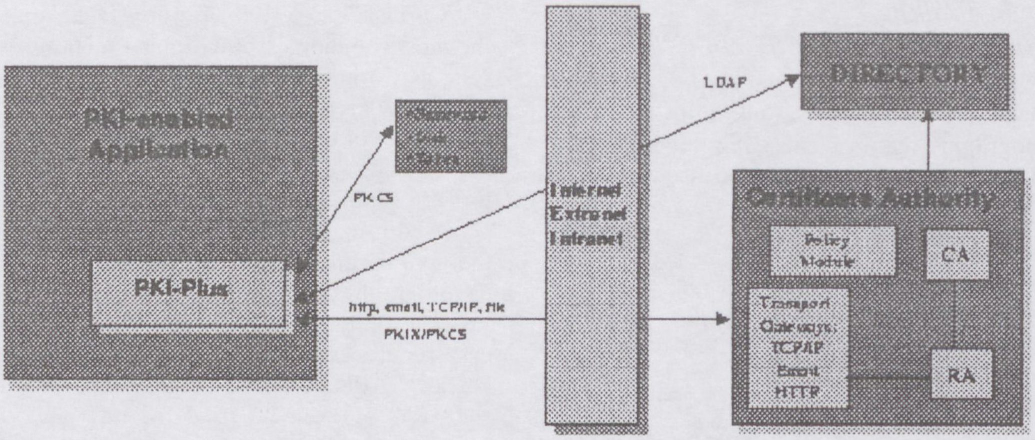


Fig. 7. PKI enabled applications using directory and certificate authority

Security Protocol Toolkits

Products: Secure Messaging Toolkit (SMT), C/SSL, J/SSL

These toolkits can be used by applications to secure messaging or socket communications. All the complexities of the security protocols are hidden from the developer to ensure rapid integration and correct implementation of security features into the application.

J/SSL Overview

J/SSL is a full strength secure communications toolkit written in 100 % pure Java and built using Baltimore Technologies award-winning J/CRYPTO cryptographic toolkit. J/SSL is a full implementation of SSL 3.0 and TLS 1.0. J/SSL provides unlimited encryption key length with no restriction on the strength of security [4].

SMT Overview

Standard e-mail applications are inherently insecure, particularly over the Internet, as it is possible for network administrators, ISP's and others to intercept, read and alter messages. Software developers who are delivering client and server email applications can use the S/MIME toolkit to protect and to enhance their e-mail services as follows [6]:

- To ensure that mail is confidential and can only be read by the receiver.
- To ensure that mail cannot be altered in transit.
- To provide sender-generated digital signature, guaranteeing the receiver that an incoming email genuinely came from its stated source.

The key features of the SMT are:

- Generation of RSA Key Pairs (512-2048 bits),
- Secure storage and retrieval of RSA key pair with passphrase protection,
- X.509 version 3 certificate interpretation,
- Session key generation and encryption,
- Message signature verification,
- Encryption and decryption of session key for multiple recipients,
- MAPI to MIME [and vice versa] conversion,
- Enhanced support for MAPI structures.

The Secure Messaging Toolkit supports the following standards, in addition to S/MIME:

- X.509 v1,v3 certificates as specified in ITU RFC 1422,
- 512, 1024 and 2048 bit RSA key pairs,
- Compliant with PKCS standards
  - PKCS#1 RSA encryption standard,
  - PKCS#5 Password-based encryption standard,
  - PKCS#7 Cryptographic message syntax Ssandard.

The specification was designed to be easily integrated into e-mail and messaging products. Secure Messaging Toolkit builds security on top of the industry standard MIME protocol according to an equally important set of cryptographic standards, the Public Key Cryptography Standards (PKCS). The fact that S/MIME was created using other standards is important for something that is likely to be widely implemented [6].

Users will benefit from the widespread adoption of S/MIME. Privacy, Data Integrity, and Authentication will be available to anyone with an e-mail package that implements S/MIME. If developers implement the standard and pay close attention to interoperability then secure messages can be exchanged between users of different email packages.

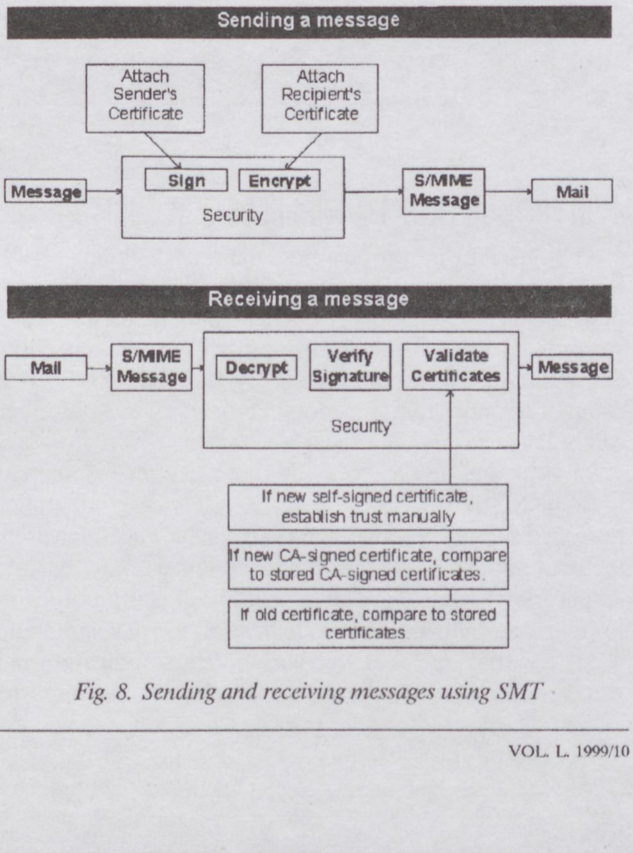

Sending a message
Attach Sender's Certificate
Attach Recipient's Certificate
Message
Sign
Encrypt
Security
S/MIME Message
Mail
Receiving a message
Mail
S/MIME Message
Decrypt
Verify Signature
Validate Certificates
Message
Security
If new self-signed certificate, establish trust manually
If new CA-signed certificate, compare to stored CA-signed certificates.
If old certificate, compare to stored certificates

Fig. 8. Sending and receiving messages using SMT

Cryptographic Toolkits

Products: Crypto Systems Toolkit (CST), J/CRYPTO, HSP4000-Assure

These toolkits are suitable for applications which have specific cryptographic requirements. A prior understanding of the principles of cryptography is essential for the correct use of these toolkits.

J/CRYPTO Overview

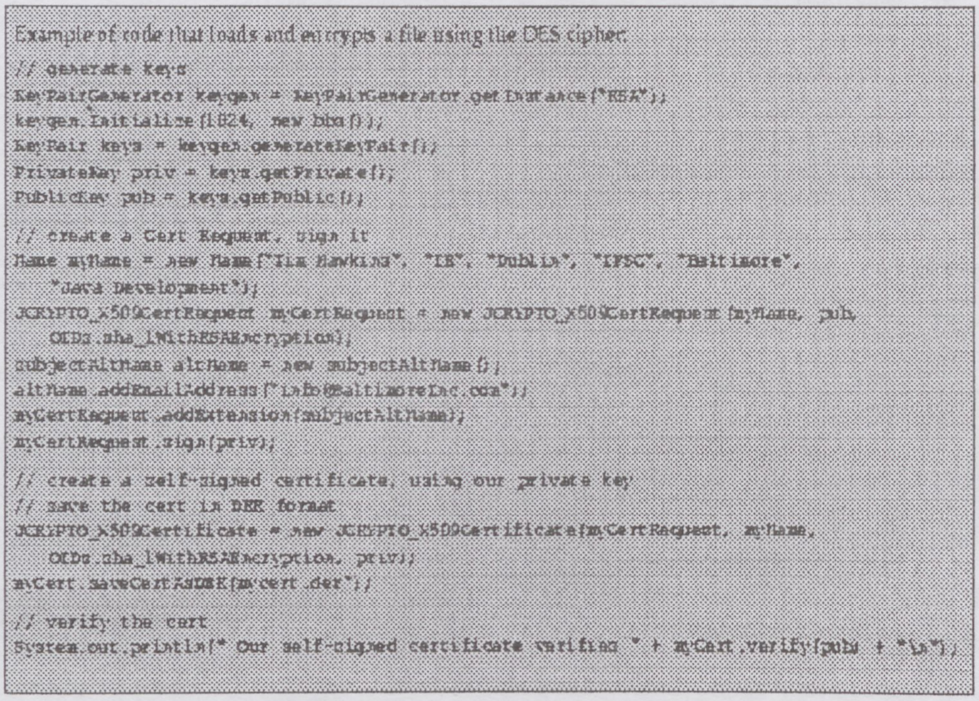
Written in 100 % pure Java, this is a high-speed, low-level toolkit that contains an intuitive, easy-to-use API [5]. Some of the new features in J/CRYPTO 4.0 include

- JCA/JCE 1.2 API Compliant Toolkit,
- Persistent applet support,
- Additional JCE 1.2 cryptographic service providers can be plugged straight in J/CRYPTO is the first cryptographic class library designed for commercial Java applications.

J/CRYPTO is a 100 % pure Java implementation of the most common cryptographic functions used in security systems worldwide. J/CRYPTO offers full strength RSA public key cryptography, DSA, RC4, RC2, Triple-DES, a wide range of cipher (asymmetric and symmetric), hashing, key exchange algorithms. Strong random number generators are supplied with the toolkit. Keys and other data can be saved using standard passphrase based encryption. All the cryptographic functions can be called via SUN's Java Cryptography Architecture (JCA).

Many of the PKCS standards are supported allowing easy secure exchange of data with other products. The low-level API allows fine manipulation of data.

J/CRYPTO can be used for any Java application or applet including Internet Communications, File Storage/-Retrieval, Digital Signature, Message Authentication, Secure Login, Data Auditing etc.



Example of code that loads and encrypts a file using the DES cipher.

```
// generate keys
KeyPairGenerator keygen = KeyPairGenerator.getInstance("RSA");
keygen.initialize(1024, new bba());
KeyPair keys = keygen.generateKeyPair();
PrivateKey priv = keys.getPrivate();
PublicKey pub = keys.getPublic();

// create a Cert Request, sign it
Name myName = new Name("Tim Hawkins", "IE", "Dublin", "IFSC", "Baltimore",
    "Java Development");
JCRYPTO_X509CertRequest myCertRequest = new JCRYPTO_X509CertRequest(myName, pub,
    OIDs.sha_1WithRSAEncryption);
subjectAltName altName = new subjectAltName();
altName.addEmailAddress("info@BaltimoreInc.com");
myCertRequest.addExtension(subjectAltName);
myCertRequest.sign(priv);

// create a self-signed certificate, using our private key
// save the cert in DER format
JCRYPTO_X509Certificate = new JCRYPTO_X509Certificate(myCertRequest, myName,
    OIDs.sha_1WithRSAEncryption, priv);
myCert.saveCertAsDER(mycert.der");

// verify the cert
System.out.println(" Our self-signed certificate verifies " + myCert.verify(pub) + "\n");
```

Fig. 9. PJ/CRYPTO source extract

4. INTRODUCTION TO WIRELESS E-SECURITY

The growth in the wireless market is being driven by the immense, universal popularity of mobile phones, personal digital assistants (PDA) and handheld PCs (HPC). According to the Strategis Group, there will be more than 530 million wireless subscribers by the year 2001. New estimates report that the number of wireless subscribers will break the one billion mark by 2004.

Services and applications for these devices are increasing rapidly. In order to deliver these services and applications in a secure, scalable and manageable way, new architectures and protocols are being designed. The Wireless Application Protocol (WAP) is a result of continuous work to define an industry-wide specification for developing applications that operate over wireless communication networks. The WAP specification is developed and supported by the wireless telecommunication community so that the entire industry and most importantly, its subscribers can benefit from a single, open specification [8].

4.1. Why WAP?

WAP has been designed to work within the constraints that mobile wireless devices have to operate in. These devices have limited display capabilities and simple user interfaces. They have limited processing power, battery life and storage capabilities. Additionally the network provision is inherently more unreliable relative to the wired world of the Internet. Overcoming these hurdles is no easy task, but it has been done. This year has heralded a spate of WAP enabled devices, service and content providers, network operators and infrastructure providers. WAP is here.

The WAP-enabled wireless world represents a huge new market for anyone involved in e-commerce. Essentially the number of users is no longer constrained to PCs connected to the Internet, which itself is a massive market. The e-commerce market is set to explode to new limits fuelled by both the astronomic growths of the Internet and the WAP-enabled wireless world.

The WAP-enabled wireless world represents an opportunity for Enterprises to benefit from new levels of communications and remote access. Now employees will be able to access applications and information from anywhere. This leads to a streamlining of business processes and makes the company more competitive e.g. sales people can have access to vital data such as the latest pricing, competitive data and product availability from customer sites, which in return reduces the sales cycle and leads to faster revenue streams [8].

4.2. Wireless e-Security

The issue of security dominates e-commerce and the enterprise. Whilst e-commerce enables businesses to operate on a global basis without physical presence, it also represents new challenges in assuring both customers and merchants that they are operating within a trusted environment. For Enterprises, the security of corporate assets is paramount. Information, intellectual property, documentation, content, networks, data, computers, employee and customer data can all be considered part of a corporation's assets. These should all be safeguarded by a corporation to ensure it remains competitive within its marketplace.

Cryptography offers virtually unbreakable systems for security on open networks. A wide range of new Internet security systems have evolved in the past few years which utilize cryptography for a wide variety of requirements. These systems secure other systems such as messaging, email, electronic payments, software applications and network communications.

The W/Secure SDK extends the ability to create such security systems from the Internet to the WAP-enabled wireless world. W/Secure SDK allows developers to build in Wireless e-Security. At a basic level security can be divided into a number of elements: confidentiality (privacy), authentication, authorization, integrity and non-repudiation. W/Secure SDK enables developers of system to build in confidentiality, integrity and authentication. Authorization and non-repudiation can also be incorporated by integrating with more sophisticated systems such as Public Key Infrastructures (PKI). W/Secure SDK has built-in functionality that makes this integration to PKIs a simple process [8].

4.3. Security in WAP

The WAP specification is a major achievement because it defines for the first time an open, standard architecture and set of protocols intended to implement wireless Internet access. Wherever possible, existing standards have been adopted or have been used as the starting point for WAP technology. Optimizations and extensions have been made in order to match the characteristics of the wireless environment.

The key elements of the WAP specification include:

- WAP Programming Model
  Very similar to the current WWW Programming Model (Fig. 10).
- Wireless Markup Language (WML) and WMLScript (WML Scripting Language)
  A markup language adhering to XML standards that is designed to enable powerful applications within the constraints of handheld devices.
- Micro-browser Specification
  A specification for a WML/WMLScript aware micro-browser in the wireless terminal that controls the user interface and is analogous to a standard Web browser.
- Wireless Telephony Applications (WTA) Framework
  This allows access to telephony functionality such as call control, phone book access and messaging from within WMLScript applets.
- WAP Stack
  A lightweight protocol stack to minimize bandwidth requirements, guaranteeing that a variety of wireless networks can run WAP applications securely (Fig. 11).

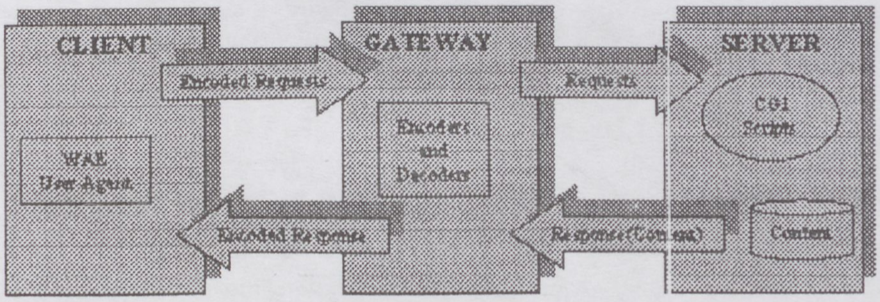


Fig. 10. WAP programming model

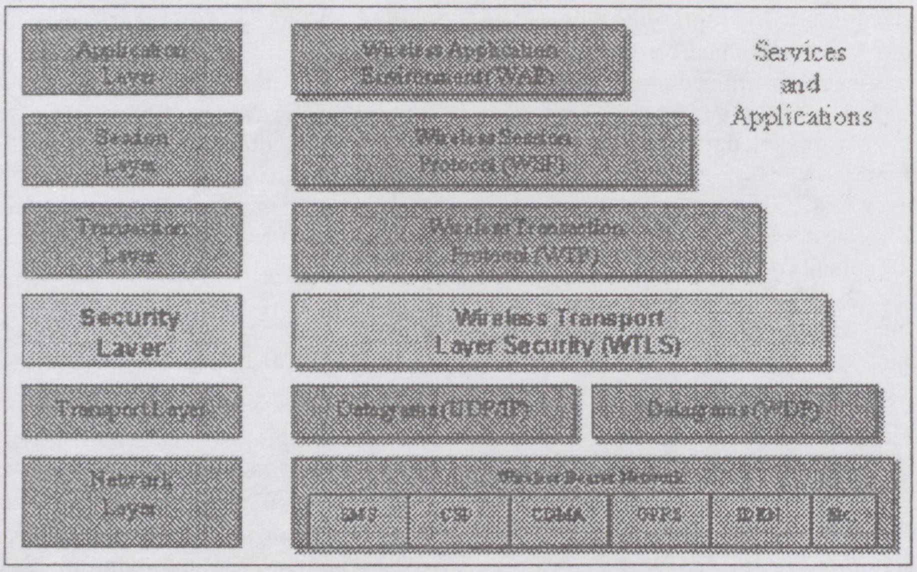

Application Layer
Wireless Application Environment (WAE)
Services and Applications
Session Layer
Wireless Session Protocol (WSP)
Transaction Layer
Wireless Transaction Protocol (WTP)
Security Layer
Wireless Transport Layer Security (WTLS)
Transport Layer
Datagrams (UDP/IP)
Datagrams (WDP)
Network Layer
Wireless Bearer Network
GSM
CSD
CDMA
GPRS
iDEN
Etc.

Fig. 11. Security within WAP is provided by WTLS

4.4. Wireless Transport Layer Security (WTLS)

Security within WAP is mandatory. It initially appears in the form of WTLS. WTLS provides the key security elements of confidentiality, integrity and authentication. WTLS is the wireless version of the industry standard Transport Layer Security (TLS), which is equivalent to the widely used Secure Sockets Layer (SSL). TLS provides a secure network connection session between a client and a server, most commonly used between a web browser and a web server.

The transformation of TLS to WTLS is based upon the need to support datagrams in a high latency, low bandwidth environment. To operate within this environment WTLS provides an optimized handshake (initiation of a secure session) through dynamic key refreshing. Dynamic key refreshing allows encryption keys to be updated on a regular and configurable basis during a secure session. This not only provides a higher level of security, but also provides considerable bandwidth savings on the relatively costly handshaking procedure [8].

The additional security elements of verified authentication, authorization and non-repudiation are provided by integration into a PKI. Baltimore Technologies range of W/Secure products allow users to implement WTLS and take full advantage of PKI systems. The W/Secure range of products supports open standard APIs and protocols to allow the widest possible interoperability with existing open standards based implementations.

4.5. W/Secure SDK Overview

W/Secure SDK is a powerful software development kit allowing application developers to create secure encrypted sessions between online networked applications. W/Secure contains an implementation of Wireless Transport Layer Security (WTLS) allowing developers to build full strength security into their WAP V1.1 client and server applications. WTLS 1.1 is the mandated security layer within any WAP v1.1 compliant product.

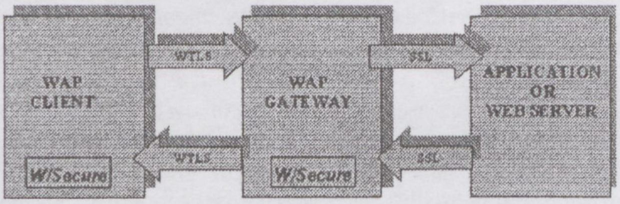


Fig. 12. WAP clients and gateways can incorporate security with the W/Secure SDK

The high level API provided in the product, abstracts the developer away from the complexities of cryptography, and allows them to concentrate on the core functionality of the applications they are building. Underlying security can easily be integrated into applications being built for the wireless world. Basic certificate handling functionality is provided as a standard part of the product. This allows applications built using the W/Secure SDK with an excellent foundation to enter the now widely adopted world of PKI. The W/Secure SDK allows the developer to integrate WTLS data encryption capabilities into any online networked application. This entails the ability to configure the security parameters to be used for authentication data security, and to initiate and receive WTLS-secured connections.

The W/Secure SDK API includes fully configurable support for:

- Session caching,
- Security re-negotiation,
- Temporary key reuse,
- Dynamic re-configuration during a session,
- Integration into datagram layers defined in the WAP specification i.e. UDP/IP and WDP.

W/Secure SDK supports a number of standards regarding the secure storage of private keys and digital certificates. These include PKCS#1, #7, #8 and #12, allowing both private keys and certificates to be integrated into security applications from all major industry-standard formats. This again emphasizes Baltimore's commitment to fully follow and implement all relevant standards in our products. The W/Secure API also contains support for token-based private keys, allowing private key operations (for example: signing) to be performed using any private key mechanisms available to the developer. Thus smartcards and hardware tokens can now be integrated using W/Secure (typically using a PKCS#11 interface) allowing even greater security when establishing a WTLS session. W/Secure SDK supports a wide range of public key cryptographic algorithms, which can be configured within its cipher suites:

- RSA,
- Diffie-Hellman,
- RC5,
- DES, Triple DES,
- IDEA,
- SHA-1,
- MD-5.

The key strength used by these suites is configurable to suit the level of security required.

4.6. W/Secure Architecture

There are two major concepts involved in the use of W/Secure SDK: W/Secure sessions and W/Secure support services. A W/Secure session is a single WTLS-secured connection with a remote host; data can be securely read from and written to a W/Secure session. A W/Secure support service is a utility object that provides support for W/Secure sessions; support facilities include providing security parameters, CA certificates, session caching facilities, etc.

Before you can establish a W/Secure session with a remote host, you must decide what cipher suites you will accept, what Certification Authorities you will trust, etc. W/Secure allows you to do this by creating and configuring a W/Secure Support object. A single support service can be used to support multiple W/Secure sessions. When creating a support service, you must initially specify whether your application is an WTLS server or an WTLS client. The distinction is usually obvious: a client makes outgoing connections to WTLS servers; a server receives incoming connections from WTLS clients [8].

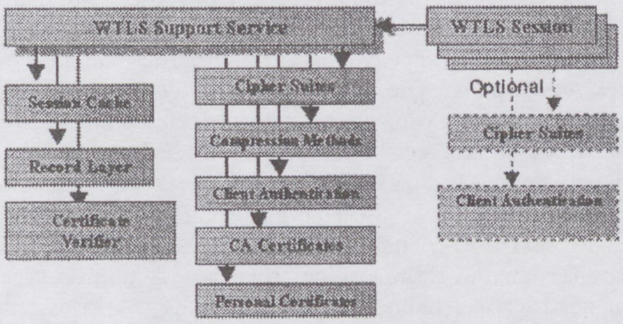


Fig. 13. W/Secure SDK architecture is based around session and support service objects

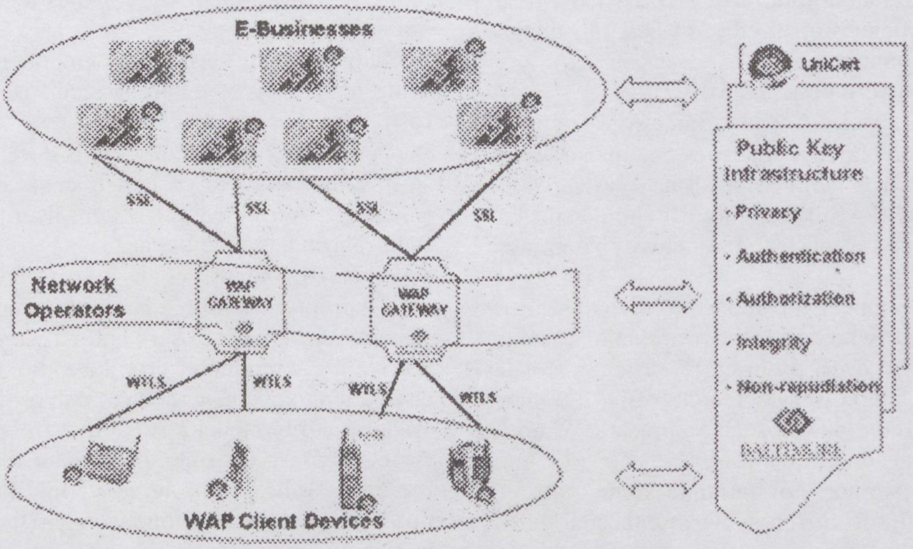


Fig. 14. Wireless e-commerce with complete security

4.7. E-Commerce and PKI Integration

The WAP specification is an ongoing process. Some of the basic elements of security such as confidentiality, authentication and integrity have now been addressed with the publication of the WTLS specification. Baltimore Technologies is one of the first companies to market with products that meet this specification. However full participation in e-commerce requires that the additional security elements of authorization and non-repudiation be addressed. In real terms this implies integration with PKI systems that have already been deployed and new systems for the future. In the wireless arena these systems will be defined in WAP. Interoperability with these different systems is a key design principle with any of Baltimore's e-security products.

W/Secure SDK contains the seeds to begin this integration and will be enhanced in the future to make this as seamless as possible. Underlying protocol and format changes are hidden from the developer, so they can be easily introduced when the time is necessary [8].

5. THE JAVA WALLET

5.1. Design goals for Java Wallet

The Java Wallet is a client-side architecture designed to bring together pluggable commerce components to enable complex and secure online transactions of value and information in a platform-independent environment. The Java Wallet, as an open platform for purchasing, banking, and finance, is broadly extensible, providing a framework whose functionality can be extended to accommodate the needs of a variety of institutions and end users in the rapidly evolving world of electronic commerce [9].

Unlike recently developed electronic "wallets", the Java Wallet can be extended to support sophisticated electronic commerce operations using a variety of value transfer instruments and protocols. The list of operations possible using the Java Wallet is limited only by the ingenuity of Java developers. The Java Wallet was developed in response to the growing demand for effective vehicles for electronic commerce. With projections for online commerce running to $66 billion by the year 2000, new technologies are required to make electronic commerce both secure and user-friendly. Sun Microsystems, JavaSoft's parent company, is the leading provider of solutions to the financial services industry. Because of this, Sun was one of the first to understand the problems faced by financial institutions trying to take advantage of the new opportunities that electronic commerce presented. In the winter of 1995, a team of technologists started work on a suite of application programming interfaces (APIs) that would solve many of the problems involved in successfully implementing electronic commerce.

Specifically, the APIs were designed to:

- Create a secure, flexible software framework for purchasing, banking, and finance that runs on any hardware platform, from environments as small as smartcards to systems as large as IBM mainframes. It should specifically be able to run on the planned network computer platforms.
- Provide complete support for applications that involve online transactions, whether those transactions occur within corporations over proprietary systems and/or intranets or in the marketspace created by the Intranet.
- Make it easy to create downloadable applets to charge for information and content delivery.
- Provide complete support for multiple value transfer mechanisms, both those currently in existence and those that will be developed over time.

The value of this work to the marketplace was quickly recognized and the development team was transferred to JavaSoft in early 1996 to commercialize the technology. The result is a new set of tools and enabling technology bundled under the heading Java Commerce. Today, developers of financial server applications are faced with a multitude of competing standards, protocols, and value transfer types. Java Commerce provides an open platform which can support all standards and payment protocols running concurrently in the same environment. Any developer who wishes to create support for a specific technology, for example IBM's Cryptolope technology or First Virtual's payment protocols (to name just a few), can do so easily and with the confidence that, because they are using Java, their implementation will run everywhere, including browsers like Netscape Navigator and Microsoft Internet Explorer, hand- held devices, and transactional servers. Of equal importance, Java Commerce provides developers with tools which greatly reduce costs, effort, and time in implementing new electronic commerce solutions. Merchants, financial institutions, and others who wish to enable online transactions via the Java Wallet have a lot of latitude in configuring commerce servers. As long as a commerce Web site is configured to send commerce information in the format developed for the Java Wallet, users can interact with the site, making purchases using secure protocols, transferring value to or from a smart card, engaging in microtransactions, using merchant-specific coupons, etc. If a developer creates a new operation, for example, Java Wallet users need only download the cassette containing that Operation Commerce component to extend the functionality of the Java Wallet. Some examples of Java Wallet extensibility are the following [9]:

- A bank designs a component that enables Java Wallet users to interact with an online ATM with a user interface exactly like that of the bank's real ATM. The Java Wallet user could download the component and, using a physical smart card reader, transfer funds to and from an electronic cash card or a smart card.
- A merchant designs a component that includes a coupon that JCC users download and use toward discounts on the merchant site. The component keeps track of how much the Java Wallet user spends at the site and give discounts accordingly.
- A utility company develops a component for paying bills using a number of different credit cards or electronic cash cards.
- A microtransaction component is developed that allows Java Wallet users to exchange small amounts of value (money, tokens, even frequent-flyer miles) for time spent playing a game online.
- A software company designs a portfolio analysis component that interacts with a bank's financial portfolio component. Java Wallet users enter their financial data in the bank's component, download the portfolio analysis component, and allow the two to interoperate. The Java Wallet security model assures that the portfolio analysis cassette has access only to the data that the bank and the Java Wallet users agree upon. For example, the portfolio analysis component might have access to tax information alone, or to stock holdings and transactions.

Cassettes could also be developed to enable:

- CFO cash management,
- Foreign exchange,
- Loan origination,
- Business-to-business purchase orders,
- Interbank settlement,
- Tax management across states,
- Automobile financing or mortgage payments.

5.2. Java Wallet Subsystems

The following are the main components of the JCC architecture:

- The *Java Commerce Client (JCC)*: The JCC is a container for Commerce JavaBeans components, consisting of Java classes that extend the JDK specifically to enable secure electronic commerce. The JCC contains interfaces that support Commerce JavaBeans components, a database, user interfaces, the Gateway Security Model, and Java Commerce Messages.
- A *Database*: a basic relational database for storing user information, for registering cassettes and cassette compatibility, and for transaction logging.
- *Operations Protocols, and Instruments*: The JCC is designed to carry out commerce operations. An operation is a procedure that uses protocols and instruments to accomplish a task. Examples of operations include purchase, ATM transfer, financial planning, etc. Operations use protocols to carry out the basic transfers associated with commerce operations. For example, a purchase operation could use the SET protocol to transfer credit card information to the appropriate parties. Protocols use instruments to transfer data necessary to a transaction. In general, an instrument represents some private user information and a relationship with an institution. For example, a credit card instrument represents both private user information (billing address, credit card number) and a user-to-bank relationship (credit card number, bank name, bank brand, etc.) In the JCC, protocols "act on" instruments to perform transfers. The JCC databases maintains relations among compatible operations and protocols, and among compatible protocols and instruments. In the JCC, operations, protocols, and instruments are Commerce JavaBeans components contained in cassettes [9].
- Any number of *Cassettes/Commerce JavaBeans*: Cassettes are digitally signed Java archive (JAR) files that contain one or more Commerce JavaBeans components and the resources (shared interfaces, graphics, etc.) used by the Bean(s). Commerce JavaBeans are modular bodies of Java code that extend the JavaBeans component model. A Commerce JavaBeans component is a reusable commerce component that extends the functionality of the JCC while meeting specific interface requirements. Once installed, a cassette and its constituent Bean(s) are persistent on the client. With Commerce JavaBeans, developers can compose commerce-enabled applications that can be easily installed in the JCC. The JCC defines interfaces for the following Commerce JavaBeans components:
  - Operations,
  - Instruments,
  - Protocols,
  - Services,
  - Preferences,
  - Wallet UIs,
  - Gates.
- *User Interface* (including one or more graphical user interfaces): a secure wallet-like interface that allows users to easily edit preferences, perform electronic commerce operations, select and edit instruments, review transactions, control cassette downloads, modify an address database, and so on. This UI functionality can be extended by installing new UI Commerce JavaBeans components in the JCC. The graphical user interface that displays is controlled by a UI Commerce JavaBeans component. The UI Commerce JavaBeans component contains all of the views that are implemented by the JCC to display the GUI. JCC users can install a number of different UI cassettes and select one as the preferred GUI. Institutions can also develop heavily branded GUIs that display when JCC users interact with the institution's Web site. UIBeans developers have a great deal of freedom in customizing the look and feel of the JCC GUI.
- The *Gateway Security Model*: a system of gates and permits that restricts access among Beans and between Beans and the JCC according to the Limited Trust Model of security. Gates control access to resources in the JCC and in cassettes by passing permits to code based on the roles for which the code is digitally signed. Permits provides access to methods that act on the resources protected by the gate. Roles are established based on contractual agreements between parties involved in commercial relationships. The Gateway Security Model extends Java platform security, refining the "sandbox" model of applet containment to implement fine-grained access control. Within the JCC, the roles with which a cassette is signed determine the cassette's level of access into the JCC and into other cassettes.
- *Java Commerce Messages*: a format in which commerce servers communicate with the JCC. A JCM is specific to an operation and contains the information required for the successful execution of an electronic transaction. The reception of a JCM instantiates the JCC and causes it to begin executing an operation. A JCM requests that the JCC perform an operation (such as an ATM transfer), provides information about protocols and instruments that can be used to complete the operation, and provides data necessary for a successful operation. A JCM is a text file, either static or dynamically created by applets, CGI programs, or servlets, sent to the JCC in response to a transaction call placed by a JCC user (for example, when a JCC user selects PAY on a merchant site or TRANSFER FUNDS on a bank's Web site) [9].

REFERENCES

[1] Introduction to PKI; http://www.baltimore.com
[2] VPN White Paper; http://www.baltimore.com
[3] MailSecure Brochure; http://www.baltimore.com
[4] J/SSL Brochure; http://www.baltimore.com
[5] J/CRYPTO Brochure; http://www.baltimore.com
[6] SMT Brochure; http://www.baltimore.com
[7] PKI-Plus Product Description; http://www.baltimore.com
[8] W/Secure Documentation; http://www.baltimore.com
[9] The Java Wallet Arechitecture; http://web2.javasoft.com
[10] The PKI-Plus Brochure; http://www.baltimore.com
[11] The FileSecure Documentation; http://www.baltimore.com
[12] The FormSecure Documentation; http://www.baltimore.com

E-COMMERCE ÉS E-SECURITY FRAMEWORK, TOOLKIT MEGOLDÁSOK

BAK ATTILA

ELMÉLETI VILLAMOSSÁGTAN TANSZÉK
BUDAPESTI MŰSZAKI EGYETEM
1111 BUDAPEST, EGRY J. U. 18.

A cikk elején bemutattuk a publikus kulcsrendszert, mint egy olyan infrstrukturális biztonságtechnikai megoldást, amely az elektronikus kereskedelem és az elektronikus biztonság körében felmerülő problémákat hatékonyan orvosolhatja. A publikus kulcsrendszer, mint rendszertechnikai megoldás nemcsak a titkosítás technikai részleteit foglalja magában, hanem az ezekkel kapcsolatos ügyviteli teendőket is.

A következő fejezetben a Virtuális Privát Hálózat (VPN) fogalmát tisztáztuk. Azt is bemutattuk, hogyan lehet ilyen hálózatokat publikus kulcsrendszerű infrastruktúrával megvalósítani.

Az ezt követő fejezetben a világ egyik legjelentősebb elektronikus kereskedelemmel és elektronikus biztonsággal foglalkozó cége – a Baltimore Technologies – néhány jelentősebb és mindenképpen figyelmet érdemlő termékének mély részleteit tártuk az olvasó elé. Külön figyelmet érdemel a mobil eszközök és az elektronikus kereskedelem, illetve az elektronikus biztonság kapcsolatával foglalkozó szekció. Ebben részletesen bemutattuk a WAP (Wireless Application Protocoll – vezetéknélküli alkalmazásszintű protokoll) néven ismert technológiát, amely nagyon könnyen a jövő kiemelkedő mobil elektronikus kereskedelem alaptechnológiájává is válhat.

Végezetül megismerkedtünk a Sun Microsystems, Inc. cég által kifejlesztett, Java alapokon nyugvó elektronikus kereskedelmi keretrendszer alapjaival is.

HÍRADÁS A SZÁZADVÉGI „ANGOLKÓRRÓL”

MOLNÁR JÁNOS

MOL RT. TÁVKÖZLÉST SZOLGÁLTATÓ EGYSÉGE, SIÓFOK
TELEFON: 15 949, (84) 505 949

A külföldi cégek magyarországi térfoglalása nyomán a soha nem látott bőségben áradó fogyasztási cikkek elképesztően széles választéka, nem utolsó sorban a különböző számítógépes programok terjedése, valamint a hiányos nyelvtudás és a fogyatékos szakmai ismeretek eredményeként a magyar sajtóban, a hivatalos iratokban és általában a magyar nyelv használata kezd kimenni a divatból. Helyét valami olyan angol–magyar keverék foglalja el, amely már nem a gondolatok szabatos közlését segíti, hanem inkább a beszélő tényleges hiányosságait igyekszik leplezni. A cikk bemutatja néhány kiragadott terület (MOL, kereskedelem, posta, egészségügy stb.) gyakorlatának görbetükörbeli képét. A fordítás nehézségei nem újkeletűek és nem csak a magyarok szenvednek miatta. Ezért az anyanyelv oktatása és a nyelvápolás mellett fokozott gondot kell fordítani a szakmai ismeretek terjesztésén túl a tudatformálásra, az általános igényességre, azaz a nemzeti kultúrára is. Ezt kívánja segíteni ez az írás.

1. VÁLTOZUNK

Valamikor budapesti voltam: a Józsefvárosban születtem, a Ferencvárosban tanultam, a lágymányosi Dunaparton kaptam mérnöki okleveleimet és első munkahelyeim is a fővárosban voltak. Tavaszonként nekem is nyíltak Kosztolányi Üllői úti fái, azok árnyalták eszmélésemet, számomra is azok adtak kedvet, tusát, azok voltak az ifjúság. Most, frissen borotvált, jólfésült (WELLA DESIGN, AFTER SHAVE, OLD SPICE HIGH, IRISCH MOOSEAU DE COLOGNE) *gyütt-ment*-ként egy Balaton-menti betonpanel társasházban csészényi INSTANT DOUWE EGBERTS (vagy OMNIA vagy RICORE, nem mindegy?) mellett csodálom a távolkeletiek kultúráját; a kínai kézzel írt kiegészítések és a krix-kraxos postabélyegző tanúsága szerint Pekingben feladott, tökéletes magyar helyesírással (é, á, í, ó ékezetes betűk!) nekem címzett, egyébként angol nyelvű levelet. Adható ennél több? Kell ennél még több?

Igen, nekem kell! Apai ágú felmenőimtől (tisztes foglalkozású molnár, asztalos, iparos őseimtől) ugyanis csak magyarul hangzó családnevemet örököltem, anyai ágról is csak a magyar anyanyelvet. Én meg most már azt sem tudom, mi a nevem. Az INTERNET-es – WINDOWS-os „írógépek” és a szolgáltató cégek adatbázisai, nyomtatói jóvoltából olyan gépi nyilvántartásokba kerültem, ahol a kisbetű, a nagybetű, a szóköz és a pont különleges jelentéssel bír. Csakhogy ezekre a helyekre nem én írtam be (egységesen) a nevemet, hanem a SERVER-ek, a DOMAIN-ok és a POP-ok gazdái, azaz számomra ismeretlen keresztapák improvizáltak valamit.

Ezért aztán drmolnar janos, Dr. Molnar Janos, Dr Molnár, János, Janos Dr Molnar, János Molnár dr, jmolnardr, Molnár János III; továbbá ezen lényegében kisbetűs alapváltozatok nagybetűs, sőt az ékezetes részek miatt még többféle módon rejtjelezett változataival (pl. MOLn-r Jβnos) létezem. A PASSWORD-ok, PINCODE-ok, jelszavak, névre szóló belépési jogosultságok ily módon igen bő választékából adódó gondjaimat érdemlegesen szaporítja a környezetemben dolgozó további két Molnár János, a szomszédomban lakó harmadik Molnár János meg még néhány nem János Molnár és a többi MJ monogramos munkatárs. A gyakran pontatlan címzésekről, az alkalmi kézbesítők olvasási képességeiről nem beszélek.

Gondjaim vannak más honfitársaimmal is, a somogytanyasi születésű *károlájn*-okkal, a zalaborzasztói *betty*-kkel és *dzsó*-kkal, a kárpátaljai *kitty*-kkel. Nem értem a neves magyar művelőket (?) és a műveiket sem. Akiket hallgatok, amiket olvasnék. Munkatársaimat is csak ritkán értem. Ők írásba adták, hogy *„olyan individuum vagyok, aki a tesztelt tájmintervallumban különös szenzitivitást mutatott a kollegiális és perszonális kommunikációk szintaxisa és a használt kódrendszer kapcsán tapasztalható globális anomáliák iránt”*.

Hallom, hallom, de nem értem, fel nem foghatom.

2. MINDEN OLYAN MÁS

A magyar Hírközlési és Informatikai Tudományos Egyesület szakmai lapjának, a HÍRADÁSTECHNIKA-nak a szerkesztési elvével sem vagyok tisztában. Hiszen az újság elvileg magyar és angol nyelvű, de a címlapon lévő név (egy szó) nincs lefordítva; a grafikás C5 engem egy alifás propángyökre emlékeztet, ám címlapi szövegkörnyezete valamiféle angol nyelvi játékot sugall. A belső címlapon egyértelműen angolos a lap neve. A tartalomjegyzéke se nem magyar, se nem angol. Vannak benne angol szavak és mondatok, meg magyar szavak és mondatok, akárcsak a lapban. A nem szószerinti és a nem teljes körű magyar/angol, illetve angol/magyar fordítás még nem lenne baj, ha a fordítás az eredeti szöveg szellemét tartalmazza, de miért nem lehet rendes, kétnyelvű lapot csinálni? Legalább az első oldal végéig, az impresszumig bezárólag?

A HTE Hírlapja sem különb: a magyar egyetemeken rendes matematikai tananyagként tanított és az oroszból fordított Matematikai zsebkönyvben is több tárgyszóval kiemelt, Csebisev féle polinomok névadójának születési centenáriumáról megemlékezve megtudhatjuk, hogy *„1894-ben halt meg P. L. TSCHEBYSEW (1821-1894) orosz matematikus, a SZentpétervárI matematikai iskola megalapítója”*.

Nem értem az országon belüli telefonjaimat felvevő- fogadó gépeket, urakat és hölgyeket sem. Legalábbis egy jó ideig. Mert az udvariaskodó bejelentkezés szövegét sikkes 1-2 idegen nyelven az automatával elmotyogtatni (miközben a díjszámláló az én zsebemre ketyeg és a nagyzenekarral előadatott céghimnusz hangjai még azt is elnyomják, ami esetleg érthető lenne), utána jöhet mindez esetleg magyarul is. Az élő anglomán üdvözlést könnyebb túlélni, mert beleszólással meg lehet szakítani, sőt gyakran még magyarra is lehet váltatni. De érteni akkor sem lehet, hiszen a sok angoloskodó nevű, magyar nyelven kimondhatatlan ILYEN–OLYAN HUNGARY meg a SOMEKIND OF HUNGARY KFT, csapat, vagy az ABCDE MAGYARORSZÁG RT. központi OFFICE-jében, netán CALL CENTER-ében, DIRECT HUNGARY-jében (a panelház 9. emeletén, balra a második lakásban) az ügyfelek értetlenkedő kérdezősködéseitől (*„betűzze kérem, mert nem értem”*) kellően zaklatott ügyintéző (vagy a központkezelő, vagy a HELP DESK-es, vagy a HOT LINE tanácsadó, esetleg a FULL SERVICE szolgáltatást nyújtó egyszemélyes mindenes, azaz egy MANAGER ASSISTENS) számára magától értetődő, hogy ő hol és kinek dolgozik, a saját neve meg még inkább (ezért azt már el sem hadarja). Nekem, tudatlan, vadidegen, kíváncsi, süket ismeretlennek meg mi közöm mindehhez a sok, bizalmas céginformációhoz...

Nem értem az országon belüli faxaimat küldő–fogadó LIMP HOME intelligenciájú, FULLDUPLEX gépeket (és gazdáikat) sem. A TRANSMISSION OK, ST TIME, TO USAGE, és még ki tudja milyen üzenetek mellett szereplő dátum sem magyar: *11/12* november 12. napját, vagy december 11. napját jelenti? Egy fax esetén (ha friss) viszonylag könnyű ezt eldönteni, de ha a Hivatalnak (Illeték, APEH, Bank, Bíróság, ...) még az ügyintéző nevét, esetleg levélszámot, dátumot sem tartalmazó, de *aláírás nélkül is hiteles* záradékkal ellátott, ajánlottan feladott ám a kerítéslécek közé kézbesített végzésében az szerepel, hogy a fellebbezésre a kézhezvételt követő 15 napon belül van mód s a postabélyegzőt sem a magyarok fura szokása szerintire faragták?

Egy csöppnyi, japán számítástechnikai szerkezet (fényképezőgépem hátlapja) nevével (hardver) ellentétben rugalmas: apró kapcsolóval tetszés szerinti (azaz német, angol vagy magyar szokás szerinti) sorrendben kiírt dátumot tudok nagybecsű alkotásaimra varázsolni. De nem ezért háborgok. Már a magyar Hivatalok, intézmények vezetői, a közhivatalnokok, egyetemi oktatók kézzel írt magánleveleiket is gyakran angolkórosan keltezik! Igaz, a MATÁV telefonkönyveiben sem az szerepel mindig és mindenhol, hogy *Magyar Posta*. Somogyban a Posta Rt, Magyar meg az Önkormányzat, Városi változat a divatos. Ezen nem kell csodálkozni: nyelvismeret híján a MATÁV-nak üzletszabályzata sincs. Csak Üzletszabályzat (MATÁV Rt.) van, meg CALL CENTER, HELP DESK, OFF LINE, meg HOT LINE.

3. HIÁNYZIK

Nem értem, hogy a Magyar Olaj- és Gázipari Részvénytársaságnak a jó IMAGE ellenére miért nincs vezetősége és miért nincs személyzete? Igaz, a működtetéséért az EXECUTIVE COMMITTEE meg a CHIEF INFORMATION OFFICER, a pénzügyekért a CFO (CHIEF FINANCIAL OFFICER) a felelős. Azért, hogy az INPUTokra megfelelő legyen az OUTPUT. Úgy általában azért van VEZETÉS és ÜGYVEZETÉS is, meg HUMÁN, sőt HR (HUMÁN RESOURCES RENDSZER), de vezetőség mint olyan, az sincs. Van viszont BENCHMARKING, ARIS, IUFACOST, CASHFLOW, MOVING MAP. A cégen belül UPSTREAM illetve DOWSTREAM ÜZLETCSOPORT-ok működnek, a SHOP-okhoz FUEL-t szállítanak. A korszerű szervezetátalakítás jegyében és a ragozási (illetve a ragozhatatlan) minták miatt egyre több az *Elemzés, Előkészítés, Fejlesztés, Felügyelet, Gazdálkodás, Gyártás, Jog, Koordináció, Kezelés, Művelés, Növelés, Rendszer, Régió, Szervezet, Szolgáltatás, Tervezés*, LAKOSSÁGI DIVÍZIÓ, PLATFORM, TRANZAKCIÓ, LOGISZTIKA, BACK OFFICE, esetleg STRATÉGIA és más hasonló megnevezésű valami a csoportok, osztályok, főosztályok, igazgatóságok stb. helyett. Legjobban hangzik (egyesek szerint) a *Csoport* TREASURY *Irányítás*, mint olyan.

Természetesen számtalan TEAM tevékenykedik még a központban és van bőségesen ALLOKÁCIÓ, PUBLIC RELATION, HERMES, CORPORATE, TREASURE és TREASURY, KONTROLLING és CONTROLLING, PUBLIC AFFAIRS, ENGINEERING, sőt MOL RC REINSURANCE COMPANY LTD.; SPE HUNGARIAN SECTION, NON CORE érdekeltség és CAPTIVE *biztosító*. Ha osztály, akkor legalábbis *Beszerzési export import osztály I.* vagy *II.* legyen a neve, netán KUMMI. A cégazonosító kézikönyv példamutató alkotás (DESIGN), bár gyakran a *cegjelyeses*, papírra írt hivatalos levelek és a MOLnβr-hoz hasonlóan *rejtjelezettek* a MULTIFUNKCIONÁLIS raktári bizonylatok is az 1 SAP R/3 VÁLLALAT hasznára, dicsőségére. A MENEDZSER-szerződéses ISSUE MANAGEMENT (BOARD) azért rendszeres tájékoztatást kap a társaság TREASUER-e által ellenjegyzett OPPORTUNITY COST, LIZING, FACTORING, SALE AND LEASEBACK, DHL LIMIT, valamint a LIMIT feletti TREASURY és HEDGELÉS-i ügyletekről, a baleseti FREKVENCIÁ-ról, különös tekintettel a GÁZCENTRUM SZOLNOK és a COST CENTER-ek KONSZOLIDÁLT KOMMULATÍV összegeinek TREND-jére, nyilván a HEADOFFICE-beli KONZISZTENCIA biztosítása érdekében, hogy minél sikeresebb lehessen pld. a NONSTOP TELECOMMUNICATIONS OUTSOURCING AND COSOURCING STRATEGIES TENDER, amit a TERMÉKMENEDZSMENT TEAM irányít a sajátmaga által TESZT-elt KNOW-HOW szerint.

Vannak MARKETING elemek, melyekből SZINERGIÁkat kell kiaknázni a STRATÉGIAI PROJEKT-javaslatok (vagy a PROJEKTSTRATÉGIÁk?, esetleg a PROJEKTUMOK?) szerint. Az eredmények a ROADSHOW-ok alkalmával PREZENTÁL-tatnak. A haszonból a Társaság a *mecenatúra* jegyében mint első számú kiemelt főSZPONZOR sokmindent támogat: sportot, ACCOUNT-ot, PROMOCIÓ-t, DM-et stb. A ROAMING-olás során megéhezettek a MOL FRANCHISE-s SNACK-jában akár BRAQUETTE-tet is ehetnek méterszámra. Az üzlet előtt lévő háromnyelvű hirdetőtáblán *Small Pizza* és *Kleine Pizza* közt *Pizza kicsi* van, hirdetvén, hogy Magyarországon nincs különbség a *nagy marha* meg a *marha nagy* között. (Hol van egy magyarul legalább kicsit tudó festősegéd, ha már a tervezőintézeti mérnökök együttesen [tervezők + ellenőrök + tervzsűri] még kicsit sem tudnak?)

Ezek a tünetek egyébként az egészségügyiek szerint is a teljesen normális állapot jellemzői. Az egyik pesti egyetem klinikájának DOUBLE DUMMY RANDO-

MIZÁLT, PLACÉBO CONTROLLÁLT, KETTŐS VAK, MULTICENTRIKUS TESZTELÉS (STUDY NO: ABC 123 XYZ) előre nyomtatott magyar nyelvű (?) kérdőívén (vagy más lapokon, jelentéseken is gyakran) a személyazonosító rovat imígyen néz ki: ... KERESZTNEV; ... VEZETEKNEV; ... NAP; ... HONAP; ... EV. (Külön szakmai élvezet lehet az eredeti, jogtiszta német kiértékelő szoftverbe ágyazott dátumkezelő családfájának gyökereit kutatni: német? angol? amerikai? mit és hogyan csinál 2000-ben?).

4. SZÓLJON A DAL

Nem értem a rádiót sem, pedig már speciális HIFI HEADSET *szettegység*-et és távvezérlő CONTROLLER KIT *készlet*-et is beszereztem, minek következtében a *vételi érzékenységem*, azaz a *hatásfokom* maximális (legalábbis a használati leírás szerint). Idézek a Kossuth adón sugárzott Esti Krónikából: Az európai Unióban a *személyek szabad áramlása* a cél. (Nem az emberek kötetlen *közlekedése, a vándorlás, a kóborlás, a kirándulás, a bolyongás, a mozgás, a munkavállalás, a lehetőség, az utazás*; nem az őrizetlen, a jelképes, az átjárható határ; nem az európai egység, hanem a *szabad áramlás*.

Igaz, az áramlásméréssel foglalkozó MSz ISO 5167-1/1994 magyar szabvány a 6.2.1. pontjában kijelenti (mindenféle lektori javításom és szabvány-szerkesztői tiltakozásom ellenére!) hogy: *„A mérendő folyadék lehet összenyomható folyadék (gáz) vagy összenyomhatatlannak tekintett folyadék (cseppfolyós anyag).”* Kossuth rádió másnap (harmadnap, vagy akármikor): JúROP felé haladás jegyében a Miskolcon alapítandó (új színházi) tagozat célkitűzése: operát csak az eredeti nyelven fogunk előadni és színházi VORKSOPot is szervezünk az EU kulturális bizottságának igényei szerint. Színmű, színjáték, daljáték, színdarab, népszínmű, előadás, magyar igény szerinti dal, dallam, dalolás, éneklés, Kodály, Bartók, magyarnóta, népdal, népdalest, cigányzene, muzsika, ötórai tea, vagy valami hasonló ritkább, mint a fehér holló, de van MUSICAL, POP-ROCK-RAPP-WORLD MUSIC, HEAVY METALL, BEAT, PERFORMANCE, DISCO és UNITED GAMES JÁTÉKOK annál inkább.

Amíg az EU szerencsétlen igénye utol nem ér, addig a kaposvári BUSINESS PRINT CORPORATION FREE műsorfüzetét böngészem. A DARK CITYbeli BEAUTY FARM-ban mint kezdő PÁJONÉR (majdani YUPPI) a SWEET CHARITY SUPERSTARja, a LOST IN SPACE, MULAN, CALLANETICS, Xy DJ (DISC JOCKEY), THRILLER, MUSICAL, SCI-FI stb. nyújtotta lehetőségek közt válogathatok a CHIPKATONÁK felügyelete alatt. Vagy inkább a kaposvári CENTRÁL PARK PUB 29 DANCEFLOOR VALENTINE DAY STRICTLY NIGHT-ot, esetleg a CLUB FREE HOUSE NEW TONE MULTIMOVIE MULTIFILTER BARDON LINK-jét válasszam ha kultúráltan kívánok szórakozni?

Vagy a HOSPITALI DESK mellől egy műszőke HOSTESS-t, egy GO-GO GIRL-et, netán a PUB-ból egy barnabőrű ESCORT hableányt? Siófoki ínyenceknek németesch cégtábla szerinti ajánlatok isch vannak: STREAPTISE SCHOW a vízparton, HAB- ÉS HÓPARTY A PALACE-ban (TWO IN ONE TICKET). Budapesti program esetén egyszerűbb lenne a helyzetem, hiszen a fővárosi moziműsort közvetlenül a FREE LEISURETIME GUIDE oldalain böngészhetem és karosszékből kereshetem a *Dinódilit* és az *Űrdinkák*at is. A győri MEDIAWAVE-n a lehetőségek egyenesen határtalanok. A közeli határ miatt erős nyugati hatásra hirdetett — rendezett *ország falu*bolondja verseny amatőr és profi résztvevői a hivatásos PERFORMER-ek INSTALLÁCIÓja előtt rendezett színpadi versenyben saját idiotizmusukat (!) bizonyíthatták és elismertethették a szakértő zsűrivel, valamint a még nem eléggé idióta és ezért nem versenyképes nézőkkel.

A tengerentúli (amerikai) fútbal ligák legfrissebb eredményeivel és a jövő-menő kosárlabda sztárok szeretőikkel és HIV vírusaikkal egyetemben mégis csak- csak emberibbek, mint a különböző *„magyar szakmai”* folyóiratok, például a MAGASYN, QUALITÁS, PUBLIC RELATIONS, ONLINE, UPDATE, FIRST CLASS, stb. cikkeiben, cégismertetőkben vagy a felsőfokú tankönyvekben hemzsegő PATCHWORK, SYSOP DEROGÁCIÓ, BIG-BANG, BAD-FIX, CASH FLOW ASSISTANSE és egyéb INTERFACES izék.

5. FALU VÉGÉN KURTA KOCSMA?

A NONSTOP HYPERMARKET-ek MULTINACIONÁLIS CENTER-ek, PLAZA-k, MALL-ok, SUPERMARKET-ek, vagy a nyírségi egyszemélyes bt, családi kft. DESIGN-es DISCOUNTE SHOP-ja inkább *üzlet, bolt, kereskedés, műhely, üzem*, netán *áruház, üzletház, szaküzlet, vásárcsarnok, piac vagy ilyen-olyan udvar*, esetleg *mészárszék, a sarki fűszeres*. Egyszóval a *Józsi bácsi boltocskája* a helybéli magyarok körében nem BUTIK, MARKET, BOUTIQUE és legfőképpen nem belsőépítész által tervezett esztétikum hordozója, hanem a *„fenn az ernyő, nincsen kas”* szellemében berendezett *kóceráj*. Az ópesti-újbudai-hajógyári Sziget EVENTS HALL-jában az eredményes WORKSHOP-os ROADSHOW és a bevezető HEPPENING után a DEALER-ek, BUSINESSMAN-ok, netán az interregionális DISTRIBUTOR-ok árubemutatót tartanak (a várható nagy érdeklődésre való tekintettel és a felhajtás kedvéért a helyi, magyar POLICE-től bérelt egyenruhás lovasrendőrök szakfelügyelete alatt). Ezt követően színes, szagos, szélesvásznú, szemkápráztató, vibráló, dübörgő, mézesmázos, floridai pálmafás, dalmatás (top101 kiskutyás) és macskás, hupikék törpikés, szupertisztaszárazságérzetű, agymosó, agresszív közszolgálati hírreklám riportokat zúdítanak a nyakamba oldalszám (vagy garantáltan és óránként maximum 12 percig [ez 20 ugyanennyi idő és legalább 120 decibell).

A NEWSDA, a MUSIC TIME, a MUSIC BOX CLASSIC, a HANGOLKA, a HBO, a CITY KRÓNIKA, a SÓ, a TALKSÓ, a SHOWMŰSOR, a SHOWDER, meg az egyéb magyar sajtó és a rádió — tv műsorok vajon miért felelős por- meg sószóró szerkesztője, művelt MENTORa, TUTORja, MODERÁTORa, TERMINÁTORa, PERFORMER-je, okos-ügyes bemondója, beszélője, mellébeszélője, beszédhibása, csinoskája, előadója, felolvasója, fontoskodója, hadaróbajnoka, idétlenkedő párosa, játékvezetője, kikiáltója, mesélője, megrendelője, mindenese, nyelvelője, pénzelője és még ki tudja kinek a mije (nem megfelelő rész törlendő; akinek nem inge, ne vegye magára, ez a felelősségelhárítás helye) boldog lehet: nemcsak a zsebe tele, nekem még a hócipőm is.

Tényleg nem értem a szigorúan tárgyszerű közszolgálati (közcélú? magánszolgálati? magáncélú?) hírek heroldjait és kiötlőit. Ha a kitágított világ valamennyi nyelvén (de az európaiakon felül a kínai, az arab, a arámi, a héber és a japán a minimum) nem vagyok tökéletesen író–olvasó–beszélő hírelnyelő, akkor a magyaroknak magyarul (?) írott sajtótermékek és a hallott szövegek összevetésének a lehetősége/kényszere már elveszi a kedvem és időm java részét. A szövegek megértéséről, megfeleltetéséről, netán az ellenmondások összevetéséről, a hiányzó láncszemek megkereséséről (azaz a gondolkodásról) még szó sincs (ne is legyen?!). Hiszen a hazai hírek legtöbbje nem a tények teljes értékű, szakszerű közlése (ki–mikor–mit–hol–hogyan csinált), hanem a megfogalmazó számára sem ismert (háttér) eseményekhez fűzött (féltitkos) vélemények cáfolatainak kommentálásaira utaló viszontválaszok elkésett reflexióira való óvatos utalások a személyiségi jogok legteljesebb figyelembe vétele mellett. Vagy a rágalmazási, erkölcsi, megrontási, kártérítési ellenperek indítási lehetőségeinek fenyegető előjelzései. Vagy mindezek szemrebbenés nélküli, határozott és kemény cáfolása. Vagy sejtetése.

6. MUNKÁT, KENYERET

Én új helyen, új életet akarok kezdeni. A napi hírek után az országos MEDIAban (ez többes számban van már, egyes száma: MEDIUM, szótári fordítása: közeg, eszköz, anyag; magyarul *sajtó*, átvitt értelemben *tájékoztató eszközök*), a magyar lapokban magyar nyelvű álláshirdetéseket olvasok (minthogy a Siófoki Hírek című lap is megszűnt, helyette csak Siófok Hírlevél van). Ezek szerint életrajzokat vár és SENIOR SALES HW DISZTIBÚCIÓ (*bruttó fizetés havi 600 eFt + kompenzációs csomag*), KEY ACCOUNT MANAGER (*550 eFt + kompenzáció*), MAJOR ACCOUNT MANAGER (*450 eFt + kompenzáció*), HDD FAILURE ANALYSIS ENGINEER, AREA SALES ENGINEER (SALARY + COMMISSION), HIGH-TECH ÜZLETÁGFEJLESZTŐ, vagy TREASURER, SUBPROJECT MANAGER, TOPMANAGER, P-AFFAIRS esetleg PUBLIC RELATIONS szakértő, FLOTTAMANAGER, sőt POWERSCREEN RENDSZERGAZDA beosztásba keres jelentkezőket a budapesti illetékes CLIENT SERVICE MANAGER vagy a HUMAN RESOURCES MENEDZSER.

Aki már kóstolt a TREASURY világból, ért a CASH FORECAST készítéshez és agilis, ill. egyetlen vágya a kötelező mellébeszélés: DEALER-ségre (a DEALING DOOM-on belüli MONEY MARKET FX ügyek kezelésére), vagy a TERMELÉSI IGAZGATÓ ACÉLSZERKEZETEK munkakörre a biztos siker reményével pályázhat. Igénytelenebbek havi 150 ezerért ASSOCIATE-ként dolgozhatnak, hiányosabb műveltségűek előbb szakirányú szakizé szakismereteiket szaporítsák a TQM, a NEMZETKÖZI MARKETING KOMMUNIKÁCIÓ, QUQLITY (!) MANAGER, IMÁZSMENEDZSMENT stb. tudományok felsőfokú terjesztésére szakosodott intézményeinkben! De van más iskolában, más kerületben, akárhol Magyarországon EURO-DIPLOMA és MASTER OF BUSINESS ADMINISTRATION FOR ENGINEERS képzés; TARZERT oklevél is szerezhető a megfelelő UNIVERSITY OF ... KNOW-HOWja alapján. A korszerűség jegyében a BME nem mindig ad ki oklevelet. Helyette partnereinek MBA (MASTER OF BUSSINESS ADMINISTRATION) CERTIFICATE-jét lehet megszerezni az államilag *akkreditált másoddiplomás* szakirányú PROGRAMtól. A nagy hagyományokkal bíró, Műegyetem rakparti Mérnöktovábbképző Intézet (amíg még van!) tanfolyamainak java részét sem a Duna-parton lehet látogatni. Stílusosan a környéken lévő BCN LTD. (a nem odavalók kedvéért a BUSSINESS COMMUNICATIONS NETWORKS KFT.-ről van szó, megközelítésére ajánlott a FOUNDATION FIELDBUS) vette át szerepköre egy részét. Természetesen előnyben van az, akinek léte legzsengébb szakaszaiban a budapesti MAGYAR–BRITISH INTERNATIONAL SCHOOL ALAPÍTVÁNYI ÓVODA ÉS ÁLTALÁNOS ISKOLA adta az anyanyelvi és a tudati alapozást, majd a TUNINGot, hiszen sok munkahelyen igény a *fejlődési potenciál*!

Kamaszkori nevelés ma már nincs, csak TINÉDZSER-kori INTENZÍV TRÉNING, FULL SERVICE; esetleg átképzés, a JOB divat. Sportiskolákban a JUNIOR és KADETT kór dúl. Ám az sem kifejezett hátrány, ha valaki a Magyar Televízió teletext adásainak svéd ábécéjén csiszolgatja (tompítja) máshol szerzett helyesírási ismereteit, vagy már élvezte a CWI, ASCII, IBM, 852 és egyéb kódlapok, valamint a 84-85-101-102 gombos írógépelgető számítógép billentyűzetek, illetve a kalapos betűk nemzeti és nemzetközi szabványai nyújtotta egyéni, de főleg páros-társas örömöket (ő úgy írt, az én gépem meg így tud). Az oktatási segédletek, füzetek, borítók garafikája, színvilága, szellemisége külön tanulmányt érdemelne. OKÉ?

Vannak másfajta gyöngyszemek is. Negyed oldalas magyar nyelvű, szellemes szövegű hirdetésben egy globális innovatív gyógyszergyár (címe: szakmai rejtvény megfejtése!) életrajzokat vár az angolul profi szinten beszélő, író és olvasó, magyarul is Aranyul tudó hasonszőrű cimboráktól. (Kár, hogy globális és innovatív a gyár s még egyetlen magyarul tudó munkatársa sincs. De remélem, majd lesz.)

Nem értem a kereskedő cégeket és reklámjaik, árjegyzékeik nyelvezetét sem. Attól, hogy csak BAR NONSTOP (0–24) amivel találkozhatom, de jóformán nincs egy tejcsarnok, ahol pohárnyi tejet ihatnék. Az éjszaka nyitva tartó BAR nem éjszakai mulató, hanem egy éjjeli gyorsétkezde (ki mer éjszaka egy szendvicsért elmenni?).

De a boltok polcain sorakozó téglákban sincs normális tej. Legfeljebb TEJITAL, NORMÁL. A védett márkanevekkel is talán megbarátkoznék valahogy. EXLUZÍV (esetleg EXCLUSIVE), MOBILE FORCE SALONokban Krém Classic, Twist, Vanille, Nemes szalámi turista és hasonlóan nevezett harapnivalók találhatók, de a LA GRANDE CUISINE, LIGHT-LINCO-LIGHTFRUIT OF THE LOOM, BOCCIA, STRECH, SOISZA MASTER, GIFTIGKÍGYÓ, PRET-A-PORTER EDT jellegű, „értelmességeket” már nem veszi be sem a szemem, sem a gyomrom (a lejárati dátum érvényességi idején belül sem). Mindegy hogy mi az, csak vegyük már, vigyem? (A „CASH & CARRY” érdemi fordítása ezek szerint *„eszi – nem eszi, ej de veszi!”*?). Ráadásul egyre több helyen tegeződnek, szóban és írásban: személyesen merev faarccal és személytelenül, a reklámokban meg őrült lelkesedéssel. Öröm az ürömben: egyre kevesebb a pénztár ahol a pénzt lehetne költeni; pályaudvar, állomás, megálló se nagyon, repülőtér sincs már. Van viszont számtalan TERMINÁL és BANKOFFICE, SALEPOINT, HOMEBANK, CHIPCARD, CREDITCARD, CHARGECARD és DEBIT (debil?) CARD meg MESTER KARD az OFFICE DEPOT-ban. Mindezeket nem ellensúlyozza a pultok méretének radikális csökkentése. A sok rágó- és egyéb gumi, lufi, elem, betét, zsemlye stb. mellett már annyi üres hely sem marad az önkiszolgálásomhoz, hogy a kártyatartó tárcámat letegyem. Még akkor sem, ha 1-2 izét *véletlenül* leverek...

7. A SZAKMA

Ma már ki tudja miféle napi aktualitású reklámismeretek és széleskörű magyarázat nélkül a magyar lapokat (szabványokat, telefonkönyvet, akármit) csak nézni lehet. Olvasni, megérteni nem. Szak(ál)ismeretekkel sem mindig, mert akkor meg a röhögéstől fulladozik az ember. Vagy a dühtől. Mert például a meglehetősen gyakori épülettüzek okozóira (az ilyen-olyan módon szabályozott hegesztési körülményekre és a rendszerint 8 elemit végzett hegesztőkre) a következő előírás is vonatkozik:

„MAGYAR SZABVÁNY MSZ EN 287-1 :1992 Hegesztők minősítése ... Nemzeti előszó :... A hazai gyakorlatnak megfelelően, bár e szabvány nem teszi kötelezővé, a hegesztőknek elméleti vizsgán kell bizonyítaniuk megfelelő szakmai felkészültségüket. ... A szabvány magyar nyelvű változata az angol eredeti alapján készült, így vitás esetekben az angol szöveg a mértékadó, továbbá a minősítési bizonyítványok vagy más kapcsolódó dokumentumok második nyelve angol. ...”

És ez még a jobbik eset, mert *van* magyar nyelvű változat! (Az a költségcsökkenés, ami a szabványok le nem fordítása miatt a szabványügyi szervezetnél jelentkezik, csak látszólagos, mert a szükséges szabványokat itt—ott, így is, úgy is sebtiben lefordítják. Annyiszor és annyiféle szóhasználattal, ahány cégnél szükség lesz rájuk.) Számtalan olyan magyar híradástechnikai és egyéb szabvány is létezik, amelynek angol nyelvű eredetije (az ISO, az EN stb. kiadványa) kapott egy honi MSz-EN, MSz-ISO előtagot az eredeti hivatkozási száma elé, s ezzel kész a magyar nemzeti szabvány. Akkor, amikor statisztikai adatok és pedagógiai tapasztalatok mutatják, hogy a trianoni határokon belül élők mintegy 20 (egyesek szerint 50!) százaléka gyakorlatilag analfabéta az anyanyelvén! ([1.] szerint *„még az egyetemisták is félanalfabéták lehetnek és kimutatták, hogy az amerikai college-okban tanuló diákoknak kereken három százaléka analfabéta”*.) A határokon kívül, medencén belül élő—lévő magyarok elemi anyanyelvhasználati jogáról és a nagy eredményként elkönyvelt néhány kétnyelvű utcanév tábláról vagy bizonyítványról nem szólok, csak családommal együtt irigylem a legalább a hivatalos állami nyelven írott bizonyítványok tulajdonosait. Nekem ugyanis vannak olyan Budapesten kiállított papírjaim, amelyek kizárólag angol nyelven tanúsítják, hogy a Magyarországon, heteken át tartott INTERNAL AUDITOR COURSE meg a REGISTERED LEAD ASSESSOR TRAINING keretében szerzett minőségügyi ismereteim okán a Brit Minőségbiztosítási Intézet nyilvántartásba vett. Ennek ellenére (vagy ezért?) fogalmam sincs arról, hogy egy sajtófigyelőből vett eme tömörítmény miről akar tájékoztatni (a szóalakok nem az én másolási hibáim!):

A cég WORLD WIDE WEB megjelenése MARKETING eszköz, a MARKETINGKOMMUNIKÁCIÓs WEB alkotója. A vállalat honlapja támogatja a PR-tevékenységet, a SZPONZORÁCIÓt. A WORLD WIDE WEB szöveg alapú MÉDIA, ahol a hangsúly az információ átadásán van. Az ONLINE reklám különbözik a DIREKT MARKETINGtől. A WEBREKLÁM legelterjedtebb típusa a szalaghirdetés (BANNER). Az ONLINE SZALAGREKLÁMnál a reklámozó dönt a tartalomORIENTÁLT és a látogatóiszám-ORIENTÁLT SITE-ok között. Érdemes a PORTAL SITEokat alkalmazni. Az internet-szolgáltatók szerint az üzenetek 10-30 százaléka SPAM. SPAM az, aki ugyanazt a mondatot ismételgeti.

AGENT LINE szolgáltatásait a CTI-re épülő CALL CENTER, TELEBANKING és TELEBROKING ATM átvitel FORE SYSTEMS eszközei valósítják meg THIRD GENERATION WIDEBAND CODE DIVISION MULTIPLE ACCESS (WCDMA — harmadik generációs, széles sávú, közös kódhasználatú és többszörös hozzáférésű) technológiával, mert így az ESCON csatornái a COMPUTERM kiterjesztő egységén keresztül jól látják egymást. on.

Valahol a vadnyugaton kitalált vagy távolkeleten gyártott, de mindenképpen tengerentúli és nem európai nyelven elnevezett izé nevének lefordítása (oda-, ide- vagy átferdítése) kétségtelenül nem könnyű feladat sem a szakember, sem egy nyelvész, sem egy műfordító (tanár, újságíró, ...) számára. Különösen nem könnyű feladat ez az eltérő nyelvi, kulturális környezet utalásait is tartalmazó kifejezések, mondatok (értsd: 4-5, darabonként 5—10—20 jelentésű főnév/igenév/akármi, egyike-másika nagy (kezdő) betűvel írva, helyenként ponttal dekorálva, de mindenkép affektáltan elhadarva) fordítása a nyelvtanulási időszakot kihagyó, relaxációs szuggerálással villámgyorsan felszedett néhány tucatnyi kifejezéssel büszkélkedő, újsütetű manegérnek.

Hát még mekkora tehertétel egy olyan (kényszerből akármire) vállalkozó embernek, aki a mindennapi hajszában nemhogy a kenyeret nem tudja megkeresni, de még a héjat sem könnyen leli. Igaz, nem kell mindent lefordítani. Az új, de méginkább a megmaradt fogalmakat, fogalmak nevét, ha az beleilleszthető a nyelvbe (és a hétköznapi, köznyelvi használatba), lefordítani nyilván nem érdemes (de lehet: a németek ismerik a rádiót, de csak a *rundfunk*-ot használják, mert a *gömbszikra* nem annyira latinos; a helikopter egyenesen lökött találmány, hiszen a németek *hubschrauber [emelőcsavar]*-ja kifejezetten szemléletes). A tranzisztort és annak emitterét, kollektorát felesleges és zavaró lenne *átalakító*ra és annak *kibocsátójára, gyűjtőjére* magyarítani, ám a toolbox önmagában sehogy, szerszámosládaként, szerszámként nehezen, segédprogramként, javítóprogramként könnyedén elfogadható (sőt: csak így, mert ezek a szavak árnyaltabban képesek rámutatni a pontos tartalomra, mint az angol gyűjtőfogalom). A redox potenciál szószerinti magyarítása sem a vörös ökör nemzőképességét minősíti.

8. HA

Ha maga a szakma, a bármilyen területen tevékenykedő szakemberek meghatározásaikat szabatosan és egységesen használnák,

Ha legalább a szakmai szövegekben azt és úgy mondanák, amire gondolnak s ezt még a szakmán belüliek is ki tudnák mondani, netán értenék amit mondanak,

Ha a szavak hangzása és írásképe egységes lenne és mernénk legalább most, Európával való újraegyesülésünk alkalmával átvenni ilyen jellegű (nem a derogáció hatáskörébe tartozó) szokásokat is – egye a fene az új fogalom új nevét, használjuk.

Ha a fordító (a tanár, az újságíró, ...) tudja (tudhatja? tudhatná?), hogy miről szól a standard, válogathat a szabvány, szabványos, irányadó mérték, mértékadó, minta, sablon, etalon, színvonal, súly, alapvető, szabályos, tipikus, helyes, kánon, kívánatos, klasszikus, hiteles, sőt: zászló, lobogó szavakból. A test lehet mérés, ellenőrzés, vizsgálat, próba, elemzés vagy kísérlet. A project lehet beruházás, elgondolás, befektetés, elképzelés, feladat, létesítmény, megvalósítás, munka, objektum, tárgy, téma, terv, tervezet, tervrajz, vázlat, vetület (de akkor, ha az embernek beszélhetnékje van, de se gondolata, se mondanivalója nincs sem magyarul, sem angolul, akkor a legszabatosabb magyar fordítása: izé). A slide értelme is változhat szövegbeli környezetétől függően az oldal, lap, fólia, kép, ábra, dia, szöveg(részlet), vázlat, rész, fejezet, magyarázat szerint.

Ha a fordító (a tanár, az újságíró, ...) egyáltalán tudja, tudhatja, melyik szó milyen fogalmat takar, mi mit jelent, ha a kifejezések, szavak, rövidítések, betűszavak, képletek, kódok, jelek, jelképek, szimbólumok, cégjelek, címerek és cégérek közti különbséget ismeri és ha eldöntötte (képes erre?), hogy szószerinti, értelem szerinti vagy nemzeti–szakmai észjárás szerinti műfordítást fog csinálni, s tisztában van az eredeti és a befogadó nyelvi környezet legfontosabb szintaxisaival, asszociációs, hangzási, irodalmi, szakmai, történeti kontextusaival is csak akkor van meg annak a reménye, hogy elfogadható fordítás (és nem széles körben terjesztett nyelvrontás és tudatrombolás) lesz a végeredmény.

Nem említem a magyar igék ragozási rejtelmeit és vonzatait, avagy azt a nyűgöt, hogy sok angol szó szótári, sőt használati alakjából nem következik mondatbeli szerepe: lehet az főnév, melléknév vagy akár ige. Ritkán ragozva vagy ragozatlanul, főleg szenvedő szerkezetekben ám mindenkép magyar füleket fájdító, elferdített szókapcsolatokban. [Szakszótárból idézek: „Alapértelmezés az amerikai angolságú Call Center, ami brit angolul call centre, ezek magyar fordítása: magyar neve még nincsen”.] Egy magyar fül számára ma még, talán, nem azonos jelentéstartalmú a felújítódik kijelentés azzal, hogy valamit felújítani kell, vagy netán valaki felújítja, esetleg majd fogják felújítani.

Azt azért meg kell jegyeznem a fordítás kínjaiba keveredett lelkiismeretes írástudók védelmében, hogy e nyelvi–gondolkodásmódbeli nehézségek nem újak és nem csak a magyar nyelv technikai nyűgei.

Egy angol! példa jól mutatja, hogy mennyire gondosnak kell(ene) lennie egy szakszerű fordítónak. Beda Venerabilis Historia Ecclesiastica című, 731-ben latinul megjelent művének angol fordításában ez áll: „Urunk megtestesülésének 664. évében egy napfogyatkozás volt, május 3-án reggel 10 órakor”. A fordító automatikusan a mai időszámításra gondolt, holott az eredetiben hora circiter decima diei van, azaz a nap 10. órájában, ami az akkori szokás szerint napkeltétől napnyugtáig 12 órára osztott nappal alapján a mai 16 órának felel meg. Oppolzer számításai igazolták, hogy valóban 16 órakor volt látható a napfogyatkozás Nagy-Britanniában.

9. FILE

Valószínűleg a műszakiak meg(nem)fizetettségére (nem megbecsülésről van szó!) vezethető vissza, hogy az ámítástechnikusok soha életükben nem jártak vendéglőben és nem ettek ott halat. A filézett hal, a hal filéje, a halszelet ugyanazt a file szót tartalmazza, amit ámítástechnikusul fájl-nak kellene mondanom. De én ezt nagyon fájlalom, mert beletörik a nyelvem, ha egy fájlt érintő tevékenységről kell beszélnem. Ezért én maradok a hosszabb állomány, esetleg a szöveg , de leginkább a file mellett. Akár halról, akár a bacon baconról (kolozsvári szalonna szeletről), akár VincsEszterről (?) van szó.

Szinte mindegyik foglalkozási ág (céh) kialakította a maga szakmai zsargonját (tolvaj nyelvét) önkifejezési igényei, megkülönböztetési vágyai, egyes esetekben a kívülállóktól való elkülönülési szándéka, esetleg felsőbbrendűségének kinyilvánítási céljából. Röviden sznobizmusból. Mentséget erre mindaddig lehetett találni, sőt el is lehet fogadni, amíg ezek a mesterségbeli tájszólások (nyelvek, nyelvhasználati szokások s az ezzel összefüggő viselkedés!) viszonylag szűk körben maradva szakmai kérdésként (vagy társadalmilag úgy-ahogy elfogadott jelenségként) kezelhetők. Ám mindegyik szakma összefügg sok másikkal, s mindegyik szervesen beépül egy adott ország kultúrájába.

Tömegében ezek a hatások már nem tekinthetők jelentékteleneknek. Ez már rendszer, amelyben a szakmai részelemek minőségileg többet jelentő halmazzá állnak össze. A gépesített ámítástechnika, az informatika, a sugárzott és nyomtatott sajtó, a reklám, a drótos vagy a drótnélküli telefon, a kereskedelem vitathatatlanul egyre összetettebb szakma, mely nem mélyen benyomul a családok mindennapjába, rátelepszik minden emberre. Ezért ma már nem tudom elfogadni a túlburjánzó (főleg anglomán, angolkóros) idegen-nyelvűséget. Ez már nem olyan szakmai belügy, mint a latinul celebrált liturgia, vagy a hypotalamus, netán az ulcus duodeni. Ez a beszéd alapvető céljának, egymás megértésének a megcsúfolása; a lét, az én- és öntudat, a nemzeti kultúra semmibe vevése.

10. HA ÉS HA

Ha a hivatásos beszélők (vadidegeneket vihogva tegező–hadaró hírolvasók, szelypegő újságírók, makogó–motyogó színészek és franciásan raccsoló ripacsok, politikusok, tanárok, a több diplomával büszkélkedő FEANI főmérnökök...) tudnának magyarul és nem nyávognának, nem sziszegnének; nem idétlenkednének, ha a kutya és a könyv meg a gép helyet nem ŐT, hanem AZT mondanának és csak a személyre az Ő-t, sőt: Kovács Károly sem csak a Kovács lenne a hírekben, hanem Kovács úr, netán Kovács Károly Elnök úr; (igaz, gyakran hallani, hogy XY BETÖRŐ úR, ami kétségtelenül nem kutya)...

Ha a hivatásos beszélők ismernék és használnák a magyar hangsúlyokat, az írásjeleket és a szóközöket, ha ismernék a csend hatását, ha netán minderről tanúságot is tennének a szavak között, a mondatok és a bekezdések, a gondolatfüzérek végén....

Ha az igazgatóságok tagjai, de legalább a fővezérelnökigazgató (esetleg egy-egy tanszék vezetője) különbséget tudna tenni a vezetőség, a vezető és a vezetés között s a magyar igék, sőt a segédigék vonzatait és a főnevek ragozásának fortélyait is ismerné, netán használná (nemcsak a saját KNOW HOW IMAGEjét)...

Ha nem kellene az amerikai és az ausztrál angol, valamint a tengerentúli angol angol, továbbá az európai baszk, cseh, dán, finn, francia, flamand, vallon, 2 féle holland, portugál, 2 féle spanyol, katalán, tucatnyi német, 2 féle norvég, olasz, meg a nemzetiséginek is tekinthető horvát, orosz, román, roma, szerb, szlovák, szlovén, ukrán, no még a klasszikus latin, ó- és újgörög, a kelet- és nyugatpatagón, valamint japán, kínai és arab, esetleg további afrikai és ázsiai nyelveken beszélni (netán nyelvjárásaikban is, sőt, nemcsak ilyen nyelven írni és olvasni, hanem eszerinti gondolatvilágokkal létezni)...

Ha nem kellene nagyítóval olvasni és közben betűrejtvényeket fejteni az embernek ahhoz, hogy legalább a mucsajtanyai önkiszolgáló hypermarket árúházban (szatócs bazárban) ki tudja választani a tejtermékek garmadájából a megfelelő napi túrót vagy sajtot, s ne tejszínt vegyen tej helyett (vagy fordítva, majd otthon ordítva)...

Ha a reklám igaz és helyénvaló, magyarokhoz szóló, netán ízléses, nem sértő, szakszerű, érthető, mértéktartó stb. volna...

Ha a Nyugati pályaudvar oldalánál épülő harmadméretű Niagara vízesés helyett a peremkerületi földutak legalább harmadát portalanítanánk, ha már csatornázásuk nincs...

Ha a számítástechnikai alkotásokat és szolgáltatásokat a mérnöki munka gyümölcseinek tekintenék legalább a létrehozóik, azaz ezeket is jól megterveznék, szakszerűen dokumentálnák, majd minősítenék, továbbá nem lopnák ugyanúgy, mint más gyártmányokat...

Ha a kokakolát kortyoló kaubojok és aranyásók külsőségeit kritikátlanul követő hajdan erős magyar romlásnak indult, mai diszlexiás, diszkós, nyeszlett kamaszai számára nem bundás indulatokat, káromkodó és kajánkodó úri lócsiszárokat, hanem követendő kárpát-medencei példaképeket állítanánk...

Ha a c, ch, h betűket látva nem kellene törni a fejemet és a nyelvemet, hogy a cé, céhá, csé, écs, há, ká, es, esz, szi hangok közül melyiket illik(?) használni...

Ha sok lakásban (a szívekben!) a csillagos-sávos zászlóplakát helyett nemzeti színű lenne a díszítmény, ha már ilyen lobogó a lakberendezési ízlés...

Ha legalább őőőő az értelmiségiek őőőő a beosztottaik és munkatársnőik számára őőőő nemcsak egy rövid parancsot használnának őőőő kötőszóként...

Ha hinnénk abban, hogy az Eugaron való vad rohanás izzadt pézsmaszaga ellen nem EU dezodor kell, hanem tiszta forrásvíz, fürödni abban...

Ha a binárisan aláosztott műveltségű szakemberek (fél- , negyed-, nyolcad műveltségű szakbarbár szakokleveles ámítástechnikusok) és a 95 puha pici kisablakon egerésző, munkabíró, de betegek (sebesen és vakon író, Windows 95 vizsgás, átképzett 1/2 analfabéták) nem követnék olyan gyorsan a prófétahajlamú puha-árújú keményeket...

Akkor biztosan mások lennénk, más világban élnénk. Más lenne a kultúránk.

11. IMÁDSÁG

De addig is kellene tenni valamit – biztatom magam. Elmegyek hát egy templomba imádkozni, türelmet tanulni. Útközben elér a vadonatúj PREPAID SIM CARDos ONE TOUCH COM EFT kódolt PDA PALMTOP PRIVAT CLASSIC PRO GSM PRAKTIKUM-jának jóvoltából egy ONLINE SMS: nem üres az E MAI Lom. (Milyen jó, hogy csörgött, illik vibrálásra átkapcsolni.)

A templomban kezdetben engem kissé zavar, hogy a sok apróságot (és szüleiket!) nem zavarja a környezet kívánta áhítat s emiatt inkább óvodában vagy önkiszolgáló étteremben lévőnek érzem magam (hiszen a levegőben is valamiféle csipsz vagy kentáki csikken szag terjeng tömjén illat helyett). Végül is megnyugszom. Igaz, nem illik a templomban szaladgálni, de miért ne lehetne rohangálás, majszolás meg ICETEA szörcsöltetés közben imádkozni? Csak (mise)bort szabad a templomban inni? Nem elég a türelemről papolni: tanulni, gyakorolni is kell!

Vége a misének, magam maradnék, tovább merengenék. Nem megy. Kis csoport marad még s lelkigyakorlatot tart az atya vezetésével. Azt is mondhatnám, pszichoterápiás csoportfoglalkozásba csöppentem. A profi módon kézben tartott beszélgetést, a helyzetelemzéseket figyelmesen hallgattam. Tanultam a hétköznapi, házastársi lélektant. Később kiderült, megérzésem jó volt: az atya sokáig amerikában élt és tanult, majd hazaköltözött és most egy magyar MARRIAGE ENCOUNTER EUROPE TEAMot vezet. De az a vég! Csak azt tudnám feledni!: Jól begyakorolt, kotta nélkül énekelt spirituálék; wadnyugati kántri dallamok, JAZZritmusok, angol szövegek. Magyar virágénekek, hagyományos zsoltárok, Károli-féle fohászok, esetleg gregorián művek helyett.

12. ELMEGYEK...

Máshová megyek (no nem a magyar MOLTRAVEL ALL INCLUSIVE, avagy a helybéli TRAVEL TEAM hónapokra előre hirdetett LAST MINUTE ROAMING ajánlatára). A többnapos hazai rendezvény címe érdektelen, mert sem a téma, sem a szakma, sem bármi a körülményekből nem egyedi, a jelenség és a jelleg tipikus, általánosítható, kétségbe ejtő. A színhely Magyarország valamelyik vidéki, régi–új kastélyszállodája. Jó pénzért jó ellátás, profi szervezés. Pályakezdők és aktív nyugdíjasok, ismerősök vagy sem, eladók vagy vevők, elnökök, igazgatók, tanárok, 20–50–200 fő a szakma krémjéből. Szolid elegancia, szakmailag értékes előadások; színvonalas kiállítás, színes, hasznos ismertetők a legújabb termékekről. Intelligens, érdeklődő, humorra kész, válogatott, dolgos magyar társaság a hallgatóság. Az előadók zöme is magyar. A külföldi cégek főleg magyar kirendeltségük vezetőjével, esetleg anyaországbeli előadókkal szerepelnek. Az idegen nyelvű szöveget jól fordítják, majdnem egyidejűleg a beszélővel.

De azért az ilyen-olyan SYSTEM rendszerről, sőt SYSTEMSrendszerekről, TENDERajánlatokról, CENTERközpontokról, MENEDZSELT felügyeletekről, hierarchikus struktúrákról, SLIPszámlákról és TOPlistákról folyik a szó; mert ami nem rendszer és nem TOP, az már egy szóra sem méltó, hisz duplázva-kettőzve az igazi-igazi, kettősen duplázva (méginkább ikresítve) az igaziak, a legeslegoptimálisabbak a kérészéltű siker, a csúcsos sikerek vágyott-elképzelt reményei. Az I/O, I/A, HART, DELTAV, COUGERPLUS, INFOSYS, EXANTE, WALL WASHER, TOPSYS, ETS, PLC, OKJ, BASESTAR OPEN, VODB, PODB, API, BIT, PDAS, CAxx és más, intelligens, okos izék tengere meg árad a magyar tannyelvű felsőoktatási intézmények tekintélyes tanárainak ajkairól a némán pislogó magyar hallgatókra. A betűszavakat természetesen mindenütt angolosan ejtik, betűzik, de már magyarul ragozzák. A tisztes tanítási szándék egyébként nyilvánvaló jele, hogy néha elhangzanak a rejtvények megfejtései: a betűszavak angol feloldásait, netán további és bővebb, esetleg hosszú magyarázatokat lehet hallani kémbriddzsi vagy Rigó utcai vagy palóc-angol tájszólásban. Merthogy mi mit jelent, azon még egy ausztráliai angol is vitatkozik egy indiai vagy oxfordi angollal (minőségügyi világkonferencián hallgattam ezt az élvezetes, ki miben tudós veszekedést!), nemhogy egy magyar (neofita anglomán) szakértő egy másikkal. Ezért aztán a szakmai részek (szavak, betűrejtvények) fordítását gyakran meg sem kísérlik.

Mielőtt még mezei magyar mérnök vagy metrológus olvasóm kaján kárörvendéssel kuncogni kezdene, egy villámkérdés: mit takarnak a következő magyar, méréstechnikai fogalmak és ki mire jogosult ezek közül: átállítás, beállítás, beszabályozás, érvényesítés, hitelesítés, igazolás, irányítás, kalibrálás, képesítés, képességvizsgálás, megerősítés, megfelelőség, meghatározás, mérés, minősítés, módosítás, tanúsítás, vizsgálás?

(Quick quiz for quiet Quikers: Which is what: auditation, calibration, confirmation, installation, installing, inspecting, qualification, modification, notification, presentation, validation, verification, qualifying, testing?)

Az már szinte kötelező a korszerűség jegyében, hogy pásszvördös szkriptek futkározzanak, projectek, projektek, prodzsektek, managementek, menedzserek, manegerek, sztenderdek és stenderdek meg standardok, updaték és upgradék; interfacék interfészekkel, routerekkel, néha kapukkal és csatolókkal meg proxi ágensekkel elegyedjenek, az illesztőket ragozatlanul elkerülve downlink. Ez azt akarja jelenteni, hogy a hallgatóság felé szlájdossanak és röpködjenek az előadók szájából. Ők zenére, szóra (de legalább képre) szeretnék bírni a rendszerint nem ismert, ki tudja hogy működő, de milliókba kerülő, legújabb gigantomán, mikropuha szoftveres, kivetítős, sztereo dolbyszavú legeslegszámítógépesítettebb hordozható lapos top bemutatórendszerüket, hogy a hallgatóság a meg nem jelent háttér-kulik (beosztott munkatársak) kemény munkája eredményeként összekalapált vázlatokat és ábrákat élvezhesse az „előadás" és az előadó, azaz a meggyőzés, az újdonság, a gondolatok helyett. Ha végre sikerül az installálás és a helybéli hardverek, inkompatibilis processzek, portok meg fájlok megadták magukat a jövevényeknek, akkor sincs a legtöbb látványban hallvány köszönet sem.

Van olyan (ma még) magyar egyetem, ahol legalább fél éven keresztül tanítják a bemutatók, előadások elkészítésével, vetítésével, elmondásával kapcsolatos tudnivalókat. A kívánatos betűnagyságot, a szín- és formakontrasztot, a nyomdászat esztétikai és technikai kultúráját (azaz egy szakmát!), a vetítés és a képernyőkezelés ergonómiáját, az előadás technikáját és még sok minden kapcsolódó és hasznos tudnivalót. Az egyik előadó (tanár!) éppen ezekről mesél. Röviden és kivonatosan, de igen sok görbét, részletes táblázatot felvillantgatva. Halkan hadarva a fal felé fordultan, mint amikor egy tanuló izzad az utóvizsgán, a tábla előtt. Eközben a jól világított teremben libegő vásznon gyenge fényű, kontraszt nélküli életlen képek és vörös lézerszemű szürke szellemárnyak pantomimot táncolnak. Esetleg halványkék (vakítóan világos) háttérre írt világossárga betűket sejteni. Vagy mélykék, állandóan visszatérő cégemblémás alapon sötétbíbor vagy fekete görbéket, 8 számjegyre pontos, sűrű Excel táblázatokat. A jobbára ötletszerűen választott vadneon színeket pasztell árnyalatok puhítják. Az egyébként követhetetlen, álháromdimenzós oszlopok, vázlatpontok, ábrák és táblázatok egy legalább 150 oldalnyi, főleg folyóírással sebtiben papírra vetett (firkált), lábjegyzetekkel is ellátott mű kiragadott lapjai, vegyesen angol és magyar nyelven, továbbá német és francia keverékben (hiszen Párizs volt az előző előadási, városlátogatási helyszín, a leghasznosabb irodalmi forrás meg német ...). Egy mondatban: a legtöbb előadás formájában élvezhetetlen és kimerítő, tartalmában meg elég pontos bemutatója annak, hogy mit, hogyan nem szabad csinálni. A máskor és máshol is „élvezett" előadások sorából ez is csak azért lóg ki, mert éppen azt magyarázza: mit hogyan kellene csinálni.

A szünetben beszélgetés, névjegycsere. Az ismerősök azért cserélik ki legújabb adataikat, mert hol van az az idő, amikor én ott és azt... A bemutatkozók meg azzal a reménnyel, hogy hátha sikerül valami kis üzletet összehozni. Ha nem itt és most, hát majd később. A névjegyek zöme színes, mondhatnám tarka-barka; esetleg fényképes. Kevés kivételtől eltekintve anglomán nyelvű (a Budapesti Műszaki Egyetem sem BME már, hanem TUB: TECHNICAL UNIVERSITY OF BUDAPEST). A keresztnév elől, vezetéknév hátul, s már nemcsak az ohiói bányában bicsaklik meg a kéz, gyakran lehull nevedről az ékezet szülőhazádban is, neved foszlik, szakadoz, különösen akkor, ha ez felsőfokú, egyetemes egyetemi divat.

Minek e végeláthatatlan, egész életünkön átkígyózó, mindent behálózó sort tovább idézni? Teljes körűen lehetetlen, meg felesleges, csemegének meg így is már túl keserű, hisz mindenkinek keserves személyes tapasztalatai lehetnek nemcsak a mellébeszélés, a nemtudás, az álkorszerűség, a butaság, a nagyképűség, az áltudományosság, az átverések, a gondolattalanság, a tautológia (az ismétlések) és az eufemizmus (a megszépítő hazugság), hanem a sznobizmus, a gyermekes majmolás és a képregényes rajzfilmfigurák lelkiélete köréből.

Mert e „nemcsak térkép-táj" szülőföldemen szeretnék még sokáig magyarul írni és magyarul olvasni, honfitársaimmal magyarul szót érteni.

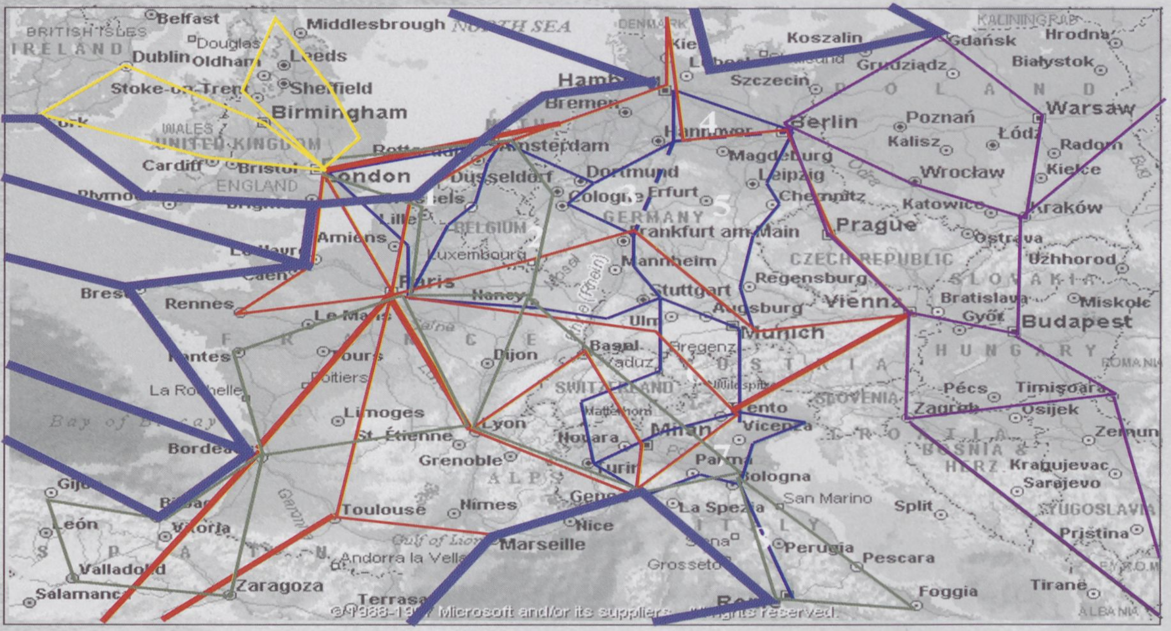
HIVATKOZÁS

Inge Uffelmann: Mindentudó illemtudó. Fordította: Rónaszegi Éva. Panoráma – Medicina Könyvkiadó; Budapest, 1995. (I.m.: 175 oldal) A mű eredeti címe: Gute Umgangsformen in jede Situation, FALKEN-Verlag; Niederhausen, 1993.

D26

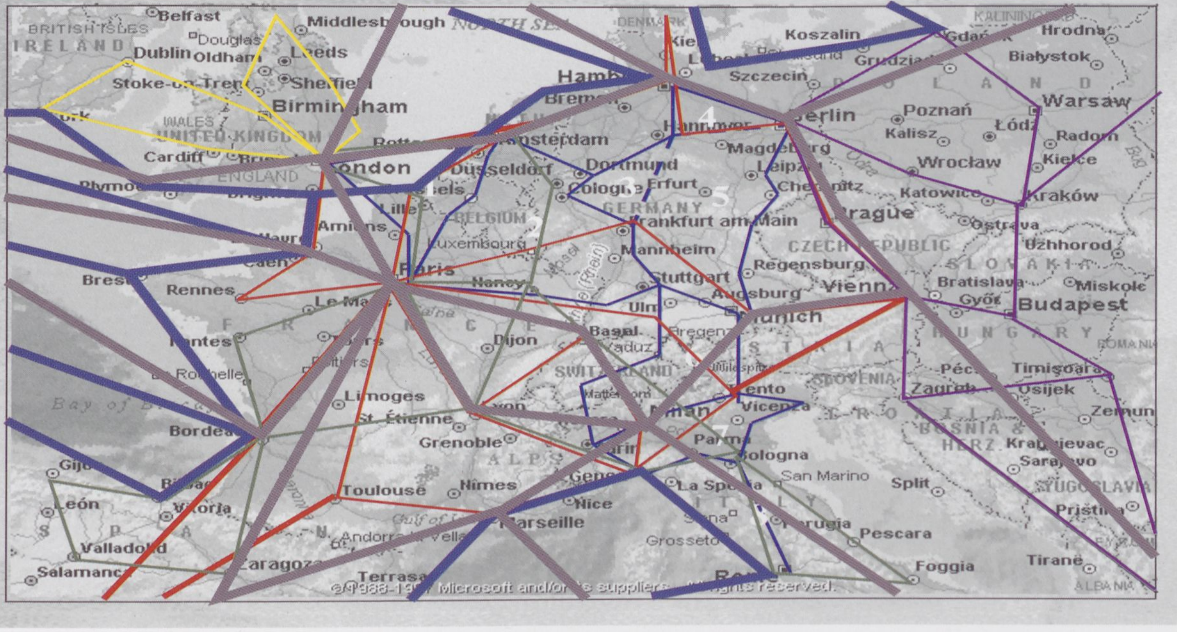
COMING SOON: 2000/1-5

Supply-side Capacity comes to Europe



Supply-Side Capacity comes to Europe D26

Supply-side Capacity comes to Europe



THE FIRST WDM WORKSHOP IN HUNGARY

D24&25

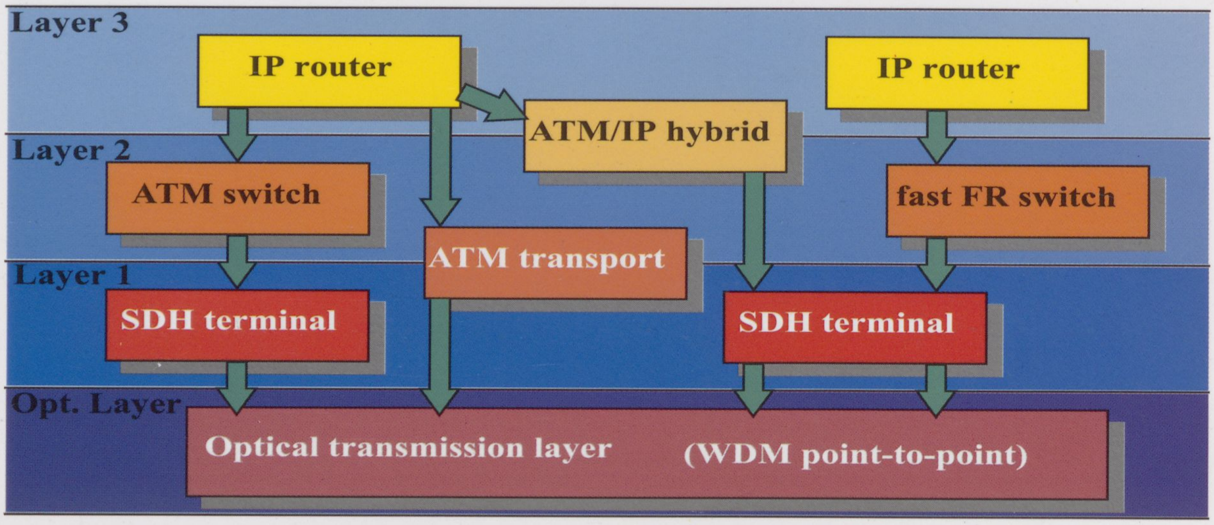
COMING SOON:2000/1-5

EURESCOM

1st Hungarian WDM Workshop, 23 March 1999, Budapest

swisscom

Traffic Layering Today



Layer 3

IP router

ATM/IP hybrid

IP router

Layer 2

ATM switch

fast FR switch

ATM transport

Layer 1

SDH terminal

SDH terminal

Opt. Layer

Optical transmission layer (WDM point-to-point)

Marcel Schiess
24 / 26 U-CITCTATS-2

Corporate Technology

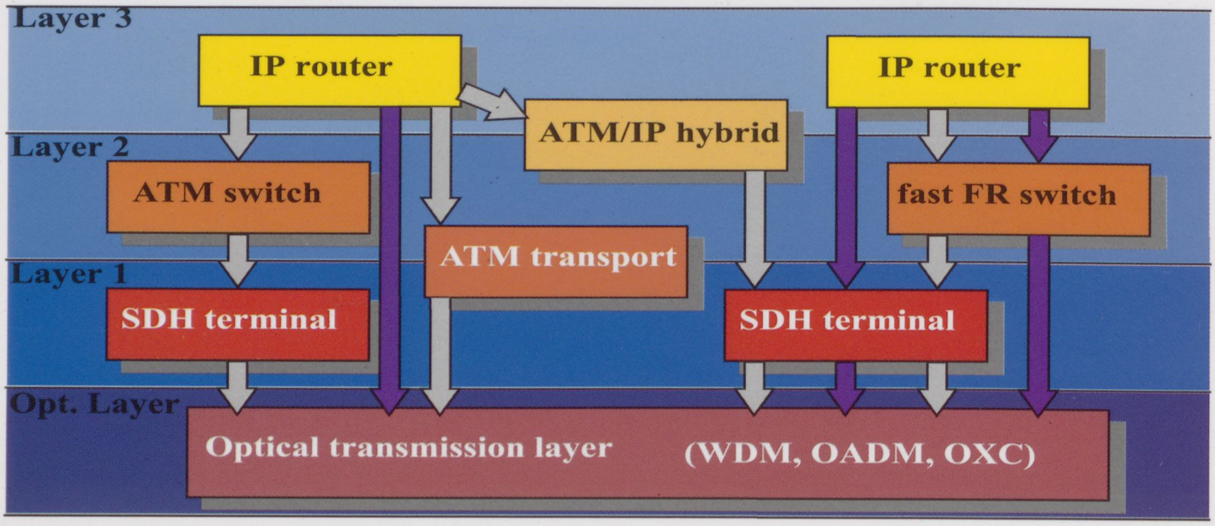
Traffic Layering Today-Tomorrow D24&25

EURESCOM

1st Hungarian WDM Workshop, 23 March 1999, Budapest

swisscom

Traffic Layering Tomorrow



Layer 3

IP router

ATM/IP hybrid

IP router

Layer 2

ATM switch

fast FR switch

ATM transport

Layer 1

SDH terminal

SDH terminal

Opt. Layer

Optical transmission layer (WDM, OADM, OXC)

Marcel Schiess
25 / 26 U-CITCTATS-2

Corporate Technology

THE FIRST WDM WORKSHOP IN HUNGARY