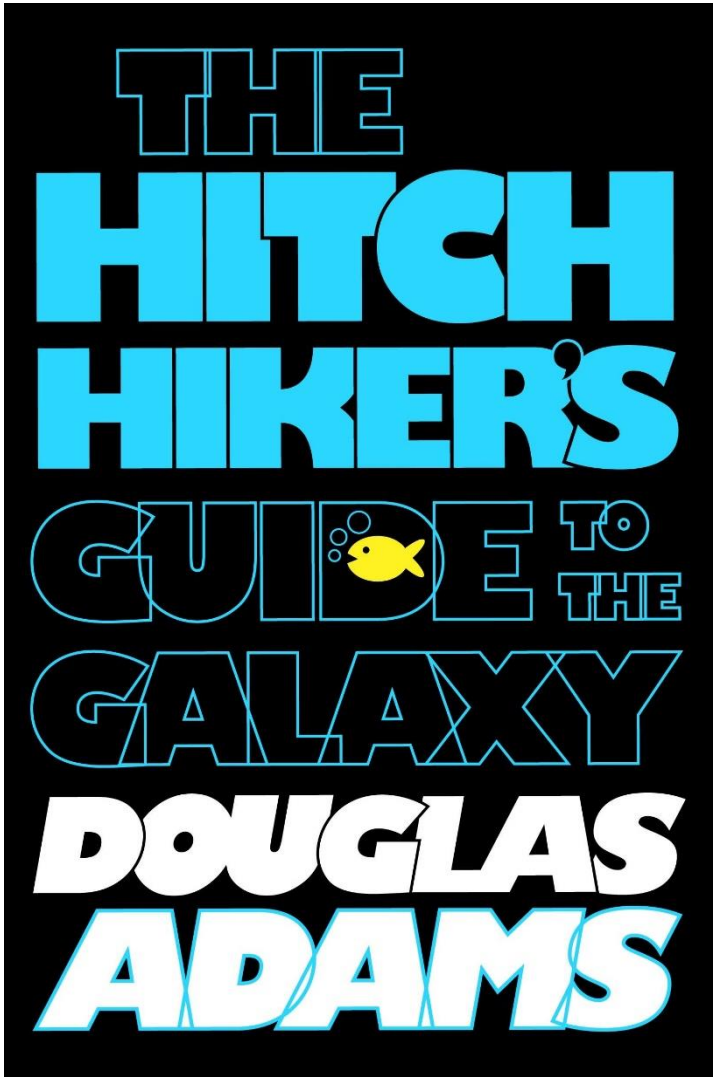
IoT (in)security
(a pessimistic view on the Future Internet)

Levente Buttyán, PhD
Laboratory of Cryptography and System Security (CrySyS Lab)
Department of Networked Systems and Services
Budapest University of Technology and Economics
www.crysys.hu


THE
HITCH
HIKER'S
GUIDE TO THE
GALAXY
DOUGLAS
ADAMS

”If you’re a researcher on this book thing and you were on Earth, you must have been gathering material on it.”
”Well, I was able to extend the original entry a bit, yes.”
”Let me see what it says in this edition, then. I’ve got to see it.”
... ”What? *Harmless*! Is that all it’s got to say? *Harmless*! One word!
... Well, for God's sake I hope you managed to rectify that a bit.”
”Oh yes, well I managed to transmit a new entry off to the editor. He had to trim it a bit, but it’s still an improvement.”
”And what does it say now?” asked Arthur.
”*Mostly harmless*,” admitted Ford with a slightly embarrassed cough.

technology review

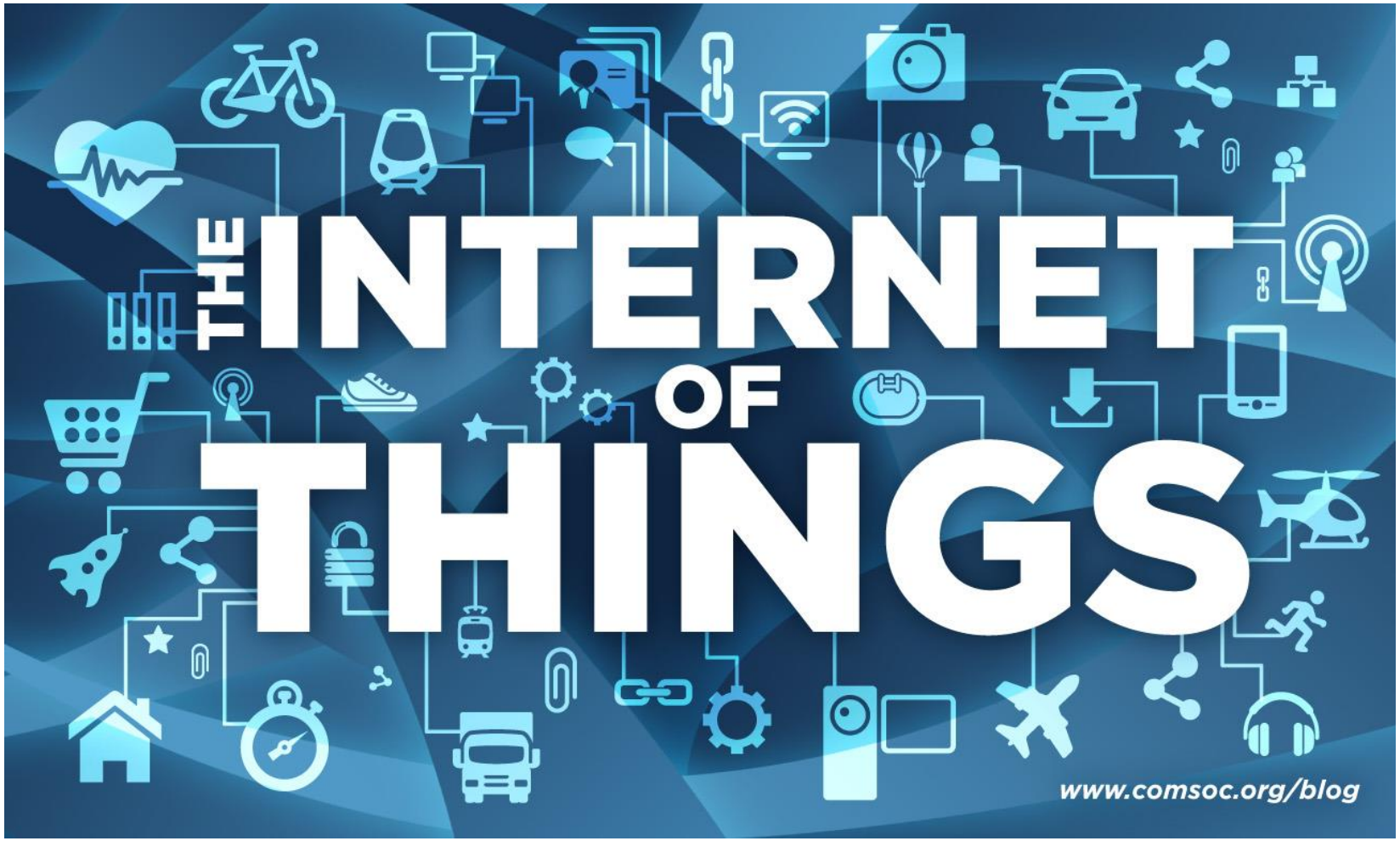
Published by MIT

The Internet Is Broken

The Net's basic flaws cost firms billions, impede innovation, and threaten national security. It's time for a clean-slate app

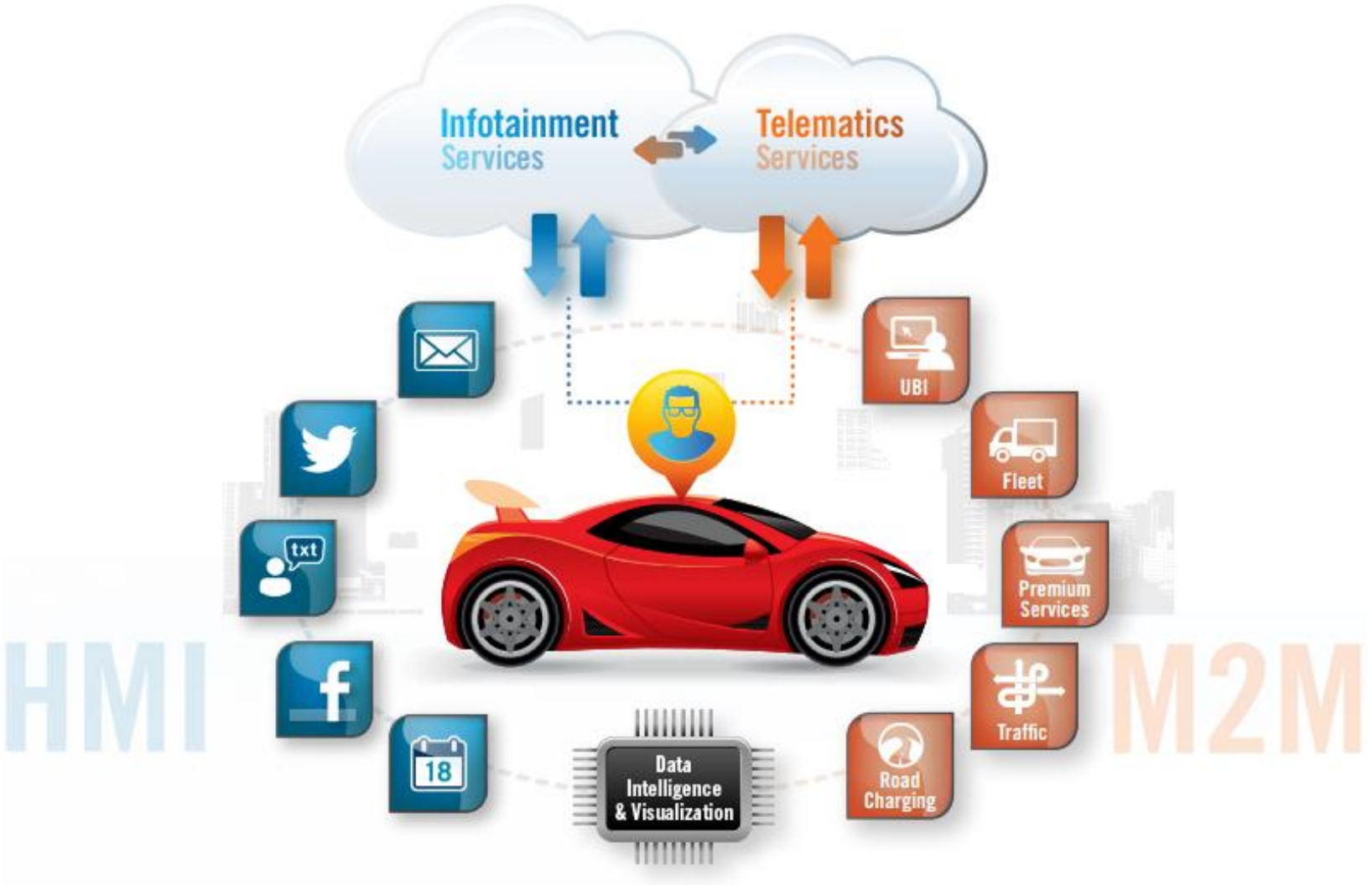
By David Talbot on February 15, 2006


technology
review
Published by MIT
still
The Internet Is Broken
The Net's basic flaws cost firms billions, impede innovation, and threaten national security. It's time for a clean-slate app
By David Talbot on February 15, 2006
2016

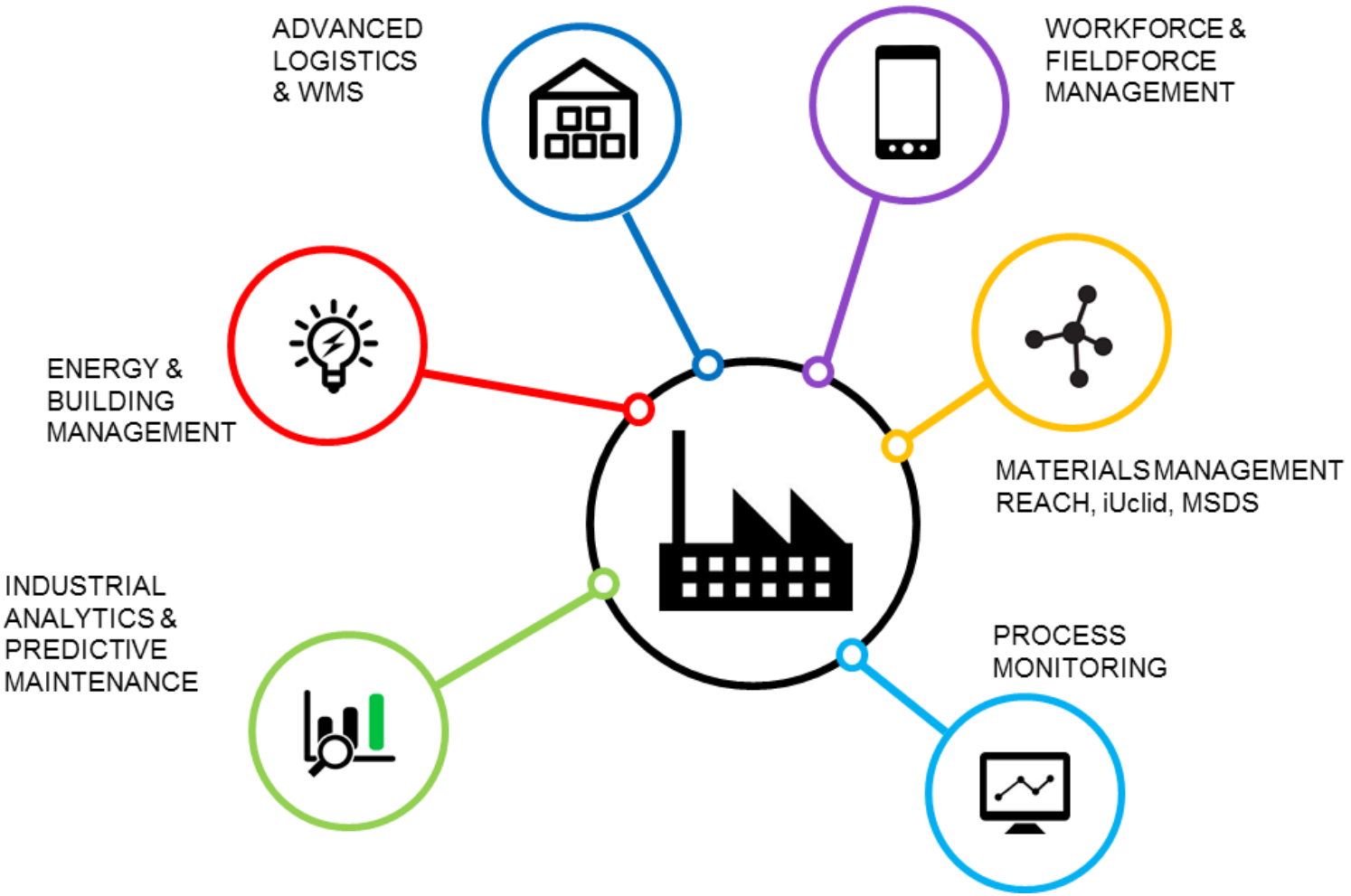

THE INTERNET OF THINGS
www.comsoc.org/blog

Smart homes

Smart vehicles (aka connected cars)



Smart factories (aka Industry 4.0)



How about security?

SECURITY

No surprise, IoT devices are insecure

By

Hacking a living room: Kaspersky Lab researcher finds

ENTREPRENEURS 8/03/2013 @ 8:08PM | 15,132 views

Hacking Insulin Pumps And Other Medical Devices From Black Hat

+ Comment Now + Follow Comments

PODCASTS

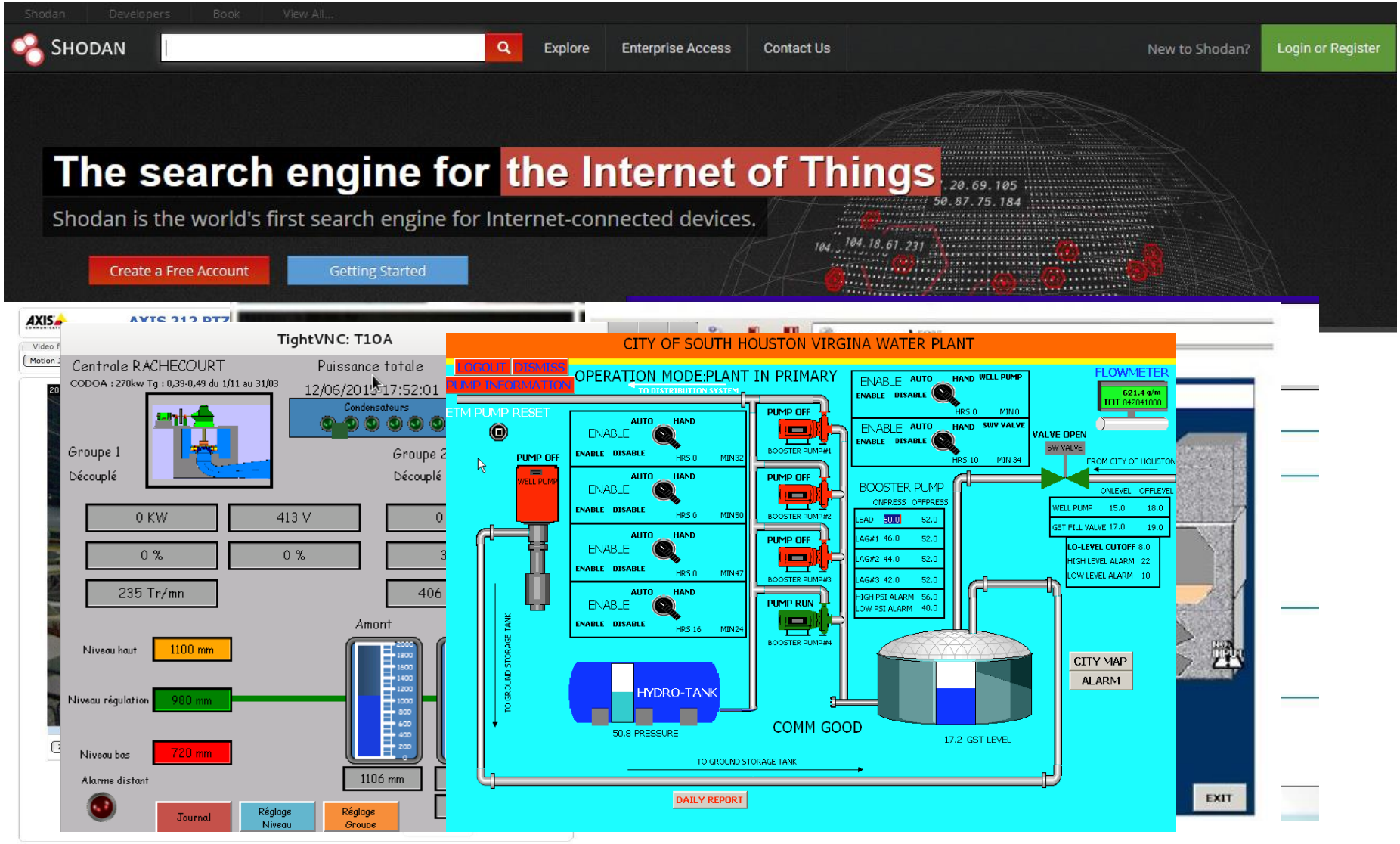
(Photo: Detroit News, file)

Traffic Monitoring Tech Vulnerable To Hacking

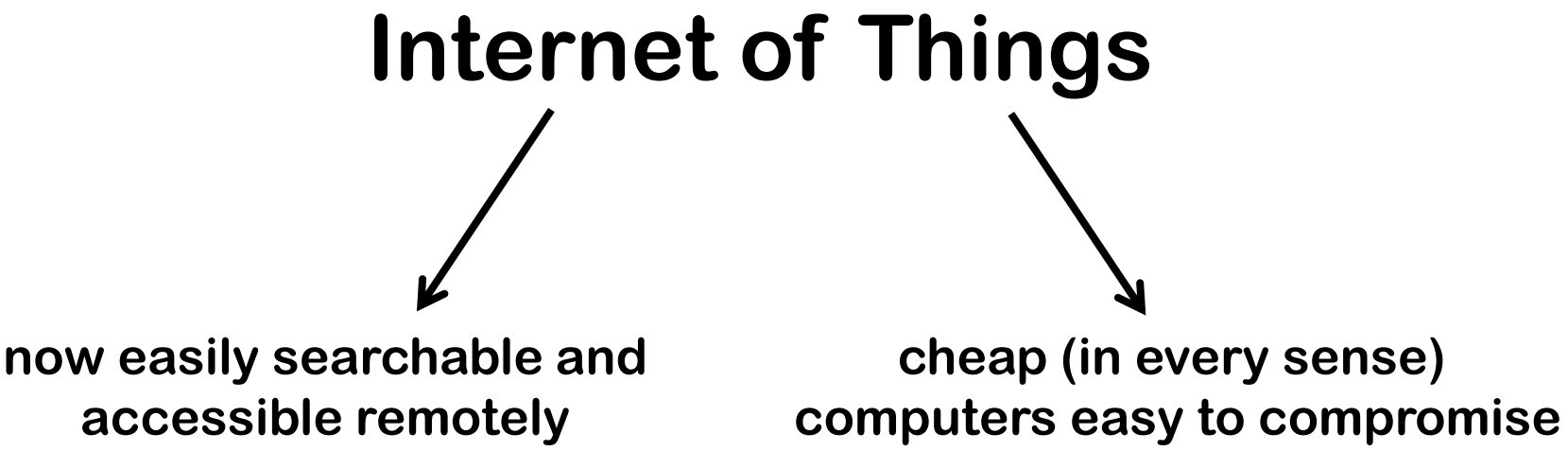
POSTED BY: PAUL MAY 1, 2014 11:36 COMMENTS OFF

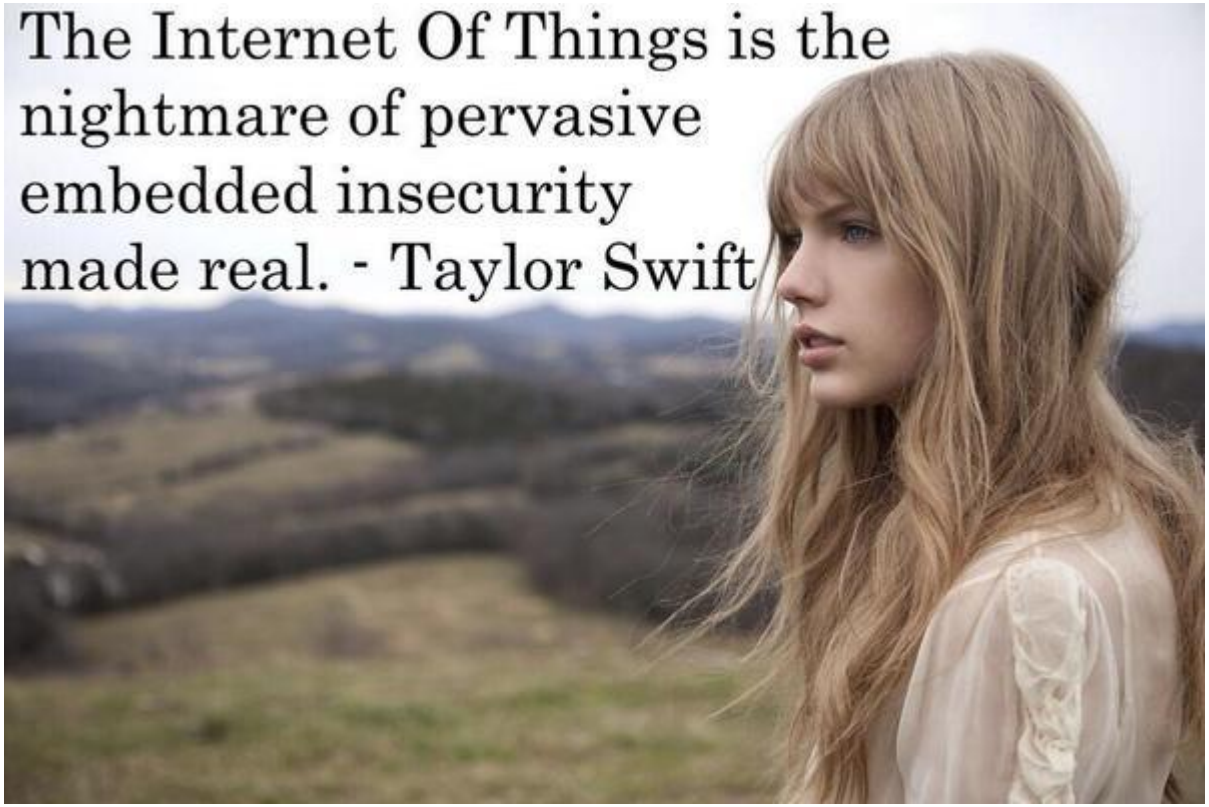
Connected cars aren't the only transportation innovation that's coming down the pike (pun intended). As we've noted before: smart roads and smart infrastructure promise even more transformative changes than – say – having Siri read your text messages to you through your stereo system.

How about security?



IoT from a hacker's perspective




The Internet Of Things is the
nightmare of pervasive
embedded insecurity
made real. - Taylor Swift

It could really be a nightmare...

WIRED Hackers Remotely Kill a Jeep on the Highway—With Me in It SUBSCRIBE

BUSINESS | DESIGN | ENTERTAINMENT | GEAR | SCIENCE | SECURITY

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

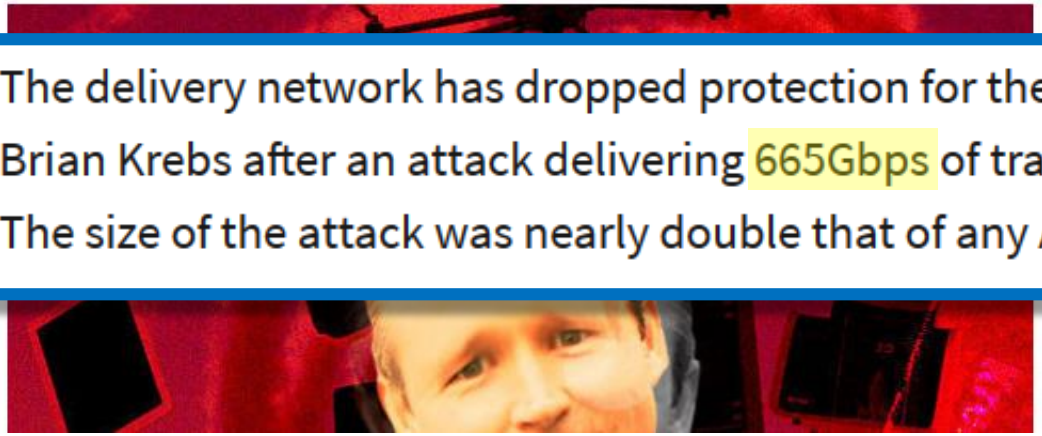
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

It could really be a nightmare...

NETWORKWORLD
FROM IDG

By Tim Greene | Follow
Network World | Sep 23, 2016 10:53 AM PT

Largest DDoS attack ever delivered by botnet of hijacked IoT devices



The delivery network has dropped protection for the Krebs on Security blog written by Brian Krebs after an attack delivering 665Gbps of traffic overwhelmed his site Tuesday. The size of the attack was nearly double that of any Akamai had seen before.

RELATED

Armies of hacked IoT devices launch unprecedented DDoS attacks

It could really be a nightmare...

PCWorld
FROM IDG

NEWS | REVIEWS | HOW-TO | VIDEO | BU

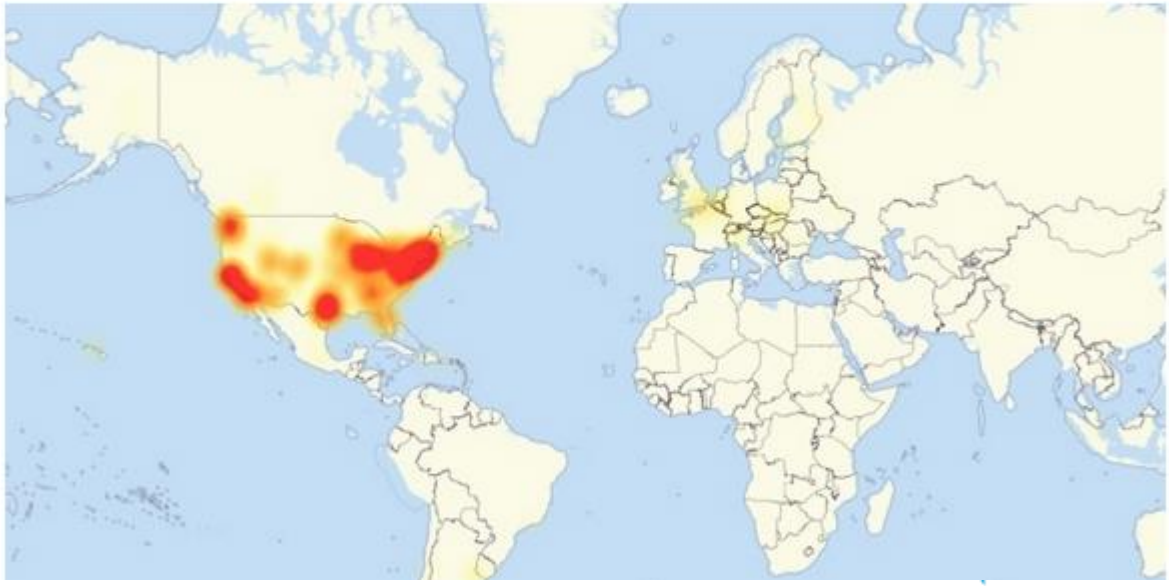
Major DDoS atta knocks Spotify, PayPal, and mor

The sound of silence.

Brad Chacos | *@BradChacos* Oct 21,
Senior Editor, PCWorld

An IoT botnet is partly behind Friday's massive DDOS attack

DVRs and other devices compromised with the Mirai malware are being the attack.



Michael Kan Oct 21, 2016 4:21 PM
IDG News Service

IoT devices became the weakest link

Default passwords

RouterPasswords.com

Welcome to the internets largest and most updated default router passwords database,

Select Router Manufacturer:

CISCO

Find Password

Manufacturer	Model	Protocol	Username	Password
CISCO	CACHE ENGINE	CONSOLE	admin	diamond
CISCO	CONFIGMAKER		cmaker	cmaker
CISCO	CNR *Rev. ALL*	CNR GUI	admin	changeme
CISCO	NETRANGER/SECURE IDS	MULTI	netrangr	attack
CISCO	BBSM *Rev. 5.0 AND 5.1*	TELNET OR NAMED PIPES	bbsd-client	changeme2
CISCO	BBSD MSDE CLIENT *Rev. 5.0 AND 5.1*	TELNET OR NAMED PIPES	bbsd-client	NULL
CISCO	BBSM ADMINISTRATOR *Rev. 5.0 AND 5.1*	MULTI	Administrator	changeme
CISCO	NETRANGER/SECURE IDS *Rev. 3.0(5)S17*	MULTI	root	attack
CISCO	BBSM MSDE ADMINISTRATOR *Rev. 5.0 AND 5.1*	IP AND NAMED PIPES	sa	(none)
CISCO	CATALYST 4000/5000/6000 *Rev. ALL*	SNMP	(none)	public/private/secret
CISCO	PIX FIREWALL	TELNET	(none)	cisco
CISCO	VPN CONCENTRATOR 3000 SERIES *Rev. 3*	MULTI	admin	admin
CISCO	CONTENT ENGINE	TELNET	admin	default
CISCO	AP1200 *Rev. IOS*	MULTI	Cisco	Cisco

Unpatched vulnerabilities

The Hacker News™
Security in a serious way

12-Year-Old SSH Bug Exposes More than 2 Million IoT Devices

Thursday, October 13, 2016 Mohit Kumar

New research [PDF] published by the content delivery network provider Akamai Technologies shows how unknown threat actors are using a 12-year-old vulnerability in OpenSSH to secretly gain control of millions of connected devices.

"New devices are being shipped from the factory not only with this vulnerability exposed but also without any effective way to fix it. We've been hearing for years that it was theoretically possible for IoT devices to attack. That, unfortunately, has now become the reality."

Factory made backdoors

Saturday, September 26, 2015

How I hacked my IP camera, and found this backdoor account

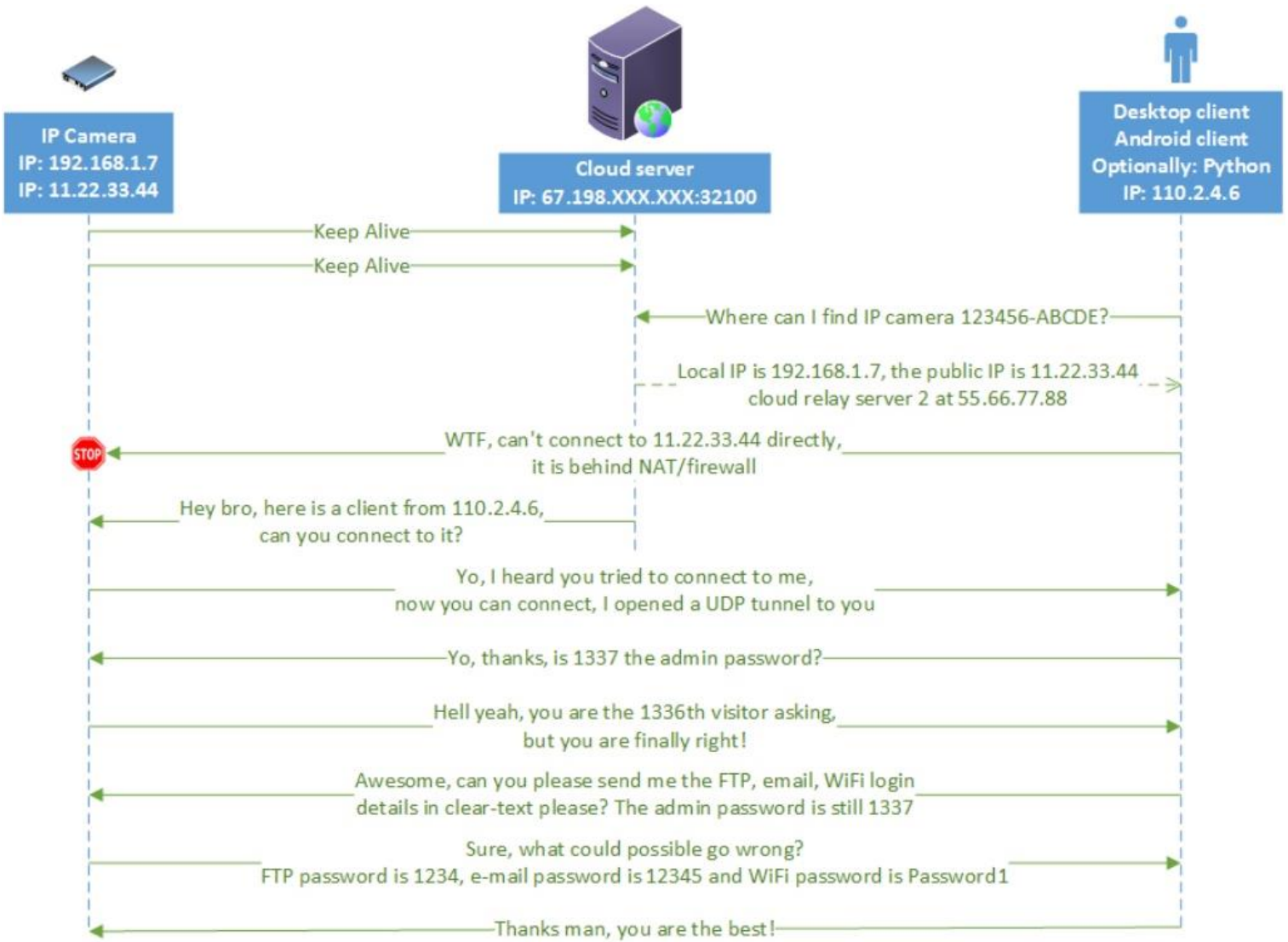
It is time to recap what we have. **There is an undocumented telnet port on the IP camera, which can be accessed by default with root:123456, there is no GUI to change this password, and changing it via console, it only lasts until the next reboot. I think it is safe to tell this a backdoor.**

With this console access we can access the password for the FTP server, for the SMTP server (for alerts), the WiFi password (although we probably already have it), access the regular admin interface for the camera, or just modify the camera as we want. In most deployments, luckily this telnet port is behind NAT or firewall, so not accessible from the Internet. But there are always exceptions. Luckily, UPNP does not configure the Telnet port to be open to the Internet, only the camera HTTP port 81. You know, the one protected with the 4 character numeric password by default.

Posted by Z at 2:02:00 PM

Firewall bypass as a feature

source: IoT security is a nightmare. But what is the real risk?
Hactivity 2016 talk by Zoltán Balázs




WHY?

KrebsonSecurity

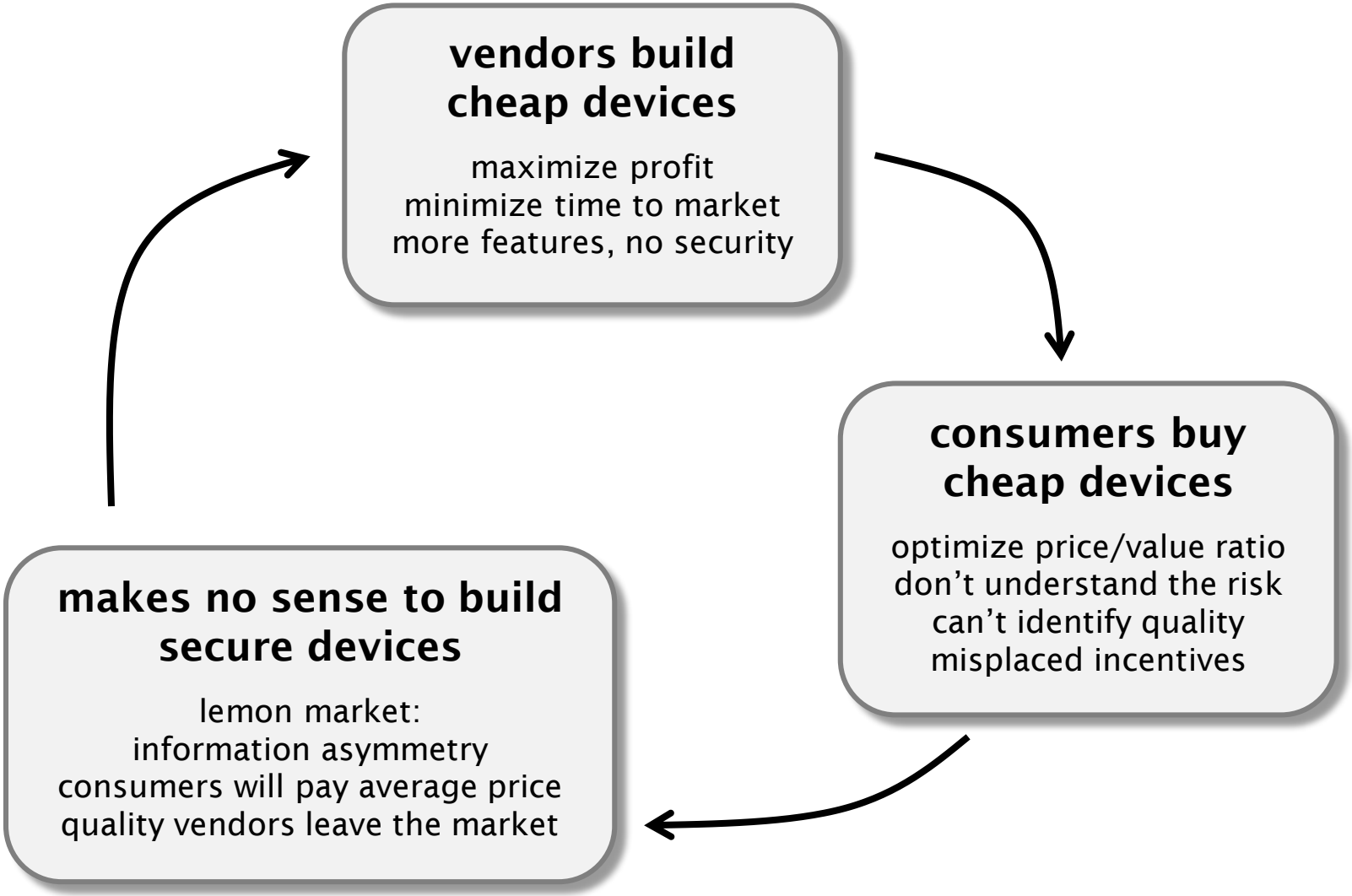
In-depth security news and investigation

In letters to the **Federal Communications Commission** (FCC), the **Federal Trade Commission** (FTC) and the **Department of Homeland Security** (DHS), **Virginia Senator Mark Warner** (D) called the proliferation of insecure IoT devices a threat to resiliency of the Internet.

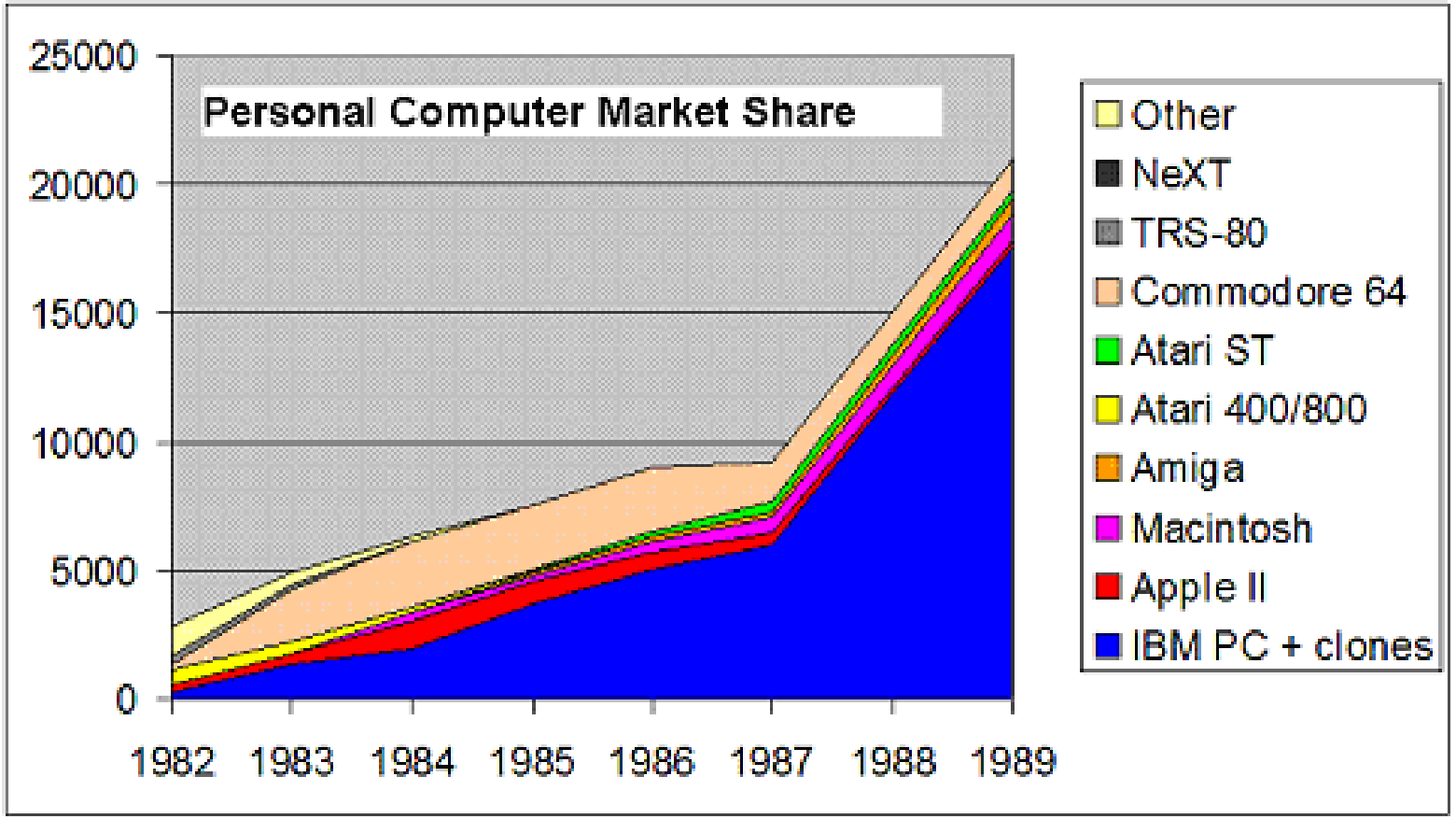
"Manufacturers today are flooding the market with cheap, insecure devices, with few market incentives to design the products with security in mind, or to provide ongoing support," Warner wrote to the agencies. "And buyers seem unable to make informed decisions between products based on their competing security features, in part because there are no clear metrics."

"Because the producers of these insecure IoT devices currently are insulated from any standards requirements, market feedback, or liability concerns, I am deeply concerned that we are witnessing a 'tragedy of the commons' threat to the continued functioning of the internet, as the security so vital to all internet users remains the responsibility of none. Further, buyers have little recourse when, despite their best efforts, security failures occur" [link added].

Security economics



Have you seen this before?



”History is just new people making old mistakes.”

— Sigmund Freud

technology review

Published by MIT

still

The Internet Is Broken

The Net's basic flaws cost firms billions, impede innovation, and threaten national security. It's time for a clean-slate app

By David Talbot on February 15, ~~2006~~ 2016


technology
review
Published by MIT
will remain
The Internet Is Broken
The Net's basic flaws cost firms billions, impede innovation, and threaten national security. It's time for a clean-slate app
2016
By David Talbot on February 15, 2006

Laboratory of Cryptography and System Security (CrySyS Lab)
Department of Networked Systems and Services
Budapest University of Technology and Economics
www.crysys.hu

contact:
Levente Buttyán, PhD
Associate Professor, Head of the CrySyS Lab
buttyan@crysys.hu