EIVOK - Rádiótávközlési Szakosztály
Szakmai Fórum
EIVOK-29.

Szélessávú készenléti kommunikáció fejlődése és biztonsági aspektusai

Kardos Tamás, ÓE, BGK GBI BIT
Biztonságtudományi Doktori Iskola
Pro-M Zrt.; Instruktor: Vereckei Béla
Témavezető: Prof. Dr. Rajnai Zoltán

2022. október 20.

Fejlesztési stratégia

A Pro-M középtávú fejlesztési stratégia – az EDR evolúciós fejlődése

A stratégia félidei felülvizsgálata jelenleg folyamatban van

- **EDR 2.0 – Szélessávú adatszolgáltatás a TETRA hang mellett**

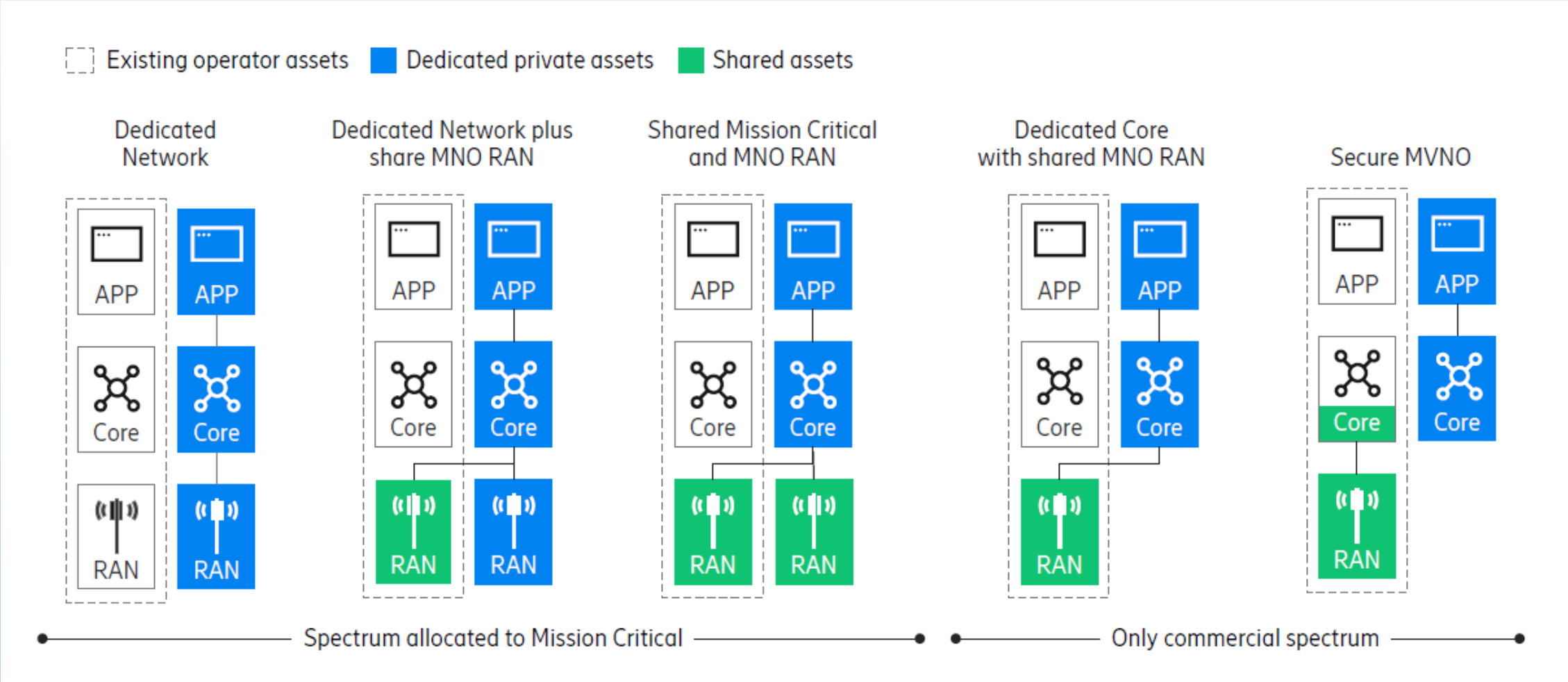
A 2020-2022 hibrid készenléti mobilhálózati modell megvalósítása, 4G LTE technológia használatával valósul meg. Saját maghálózati (core) infrastruktúra, míg a rádióhálózat (RAN) esetében részben felhasználva a meglévő 4G/5G kereskedelmi mobilhálózatok hozzáférési hálózatát.

2025-ig a TETRA technológián alapuló EDR 1.0 hálózat biztosítja a hang alapú készenléti szolgáltatást.

- **EDR 3.0 – Hang és adatszolgáltatás 3GPP szabványos szélessávú hálózaton (4G/5G)**

2025-ig cél a megfelelő önálló, dedikált 4G/5G rádiós hálózat (RAN) kiépítése, a TETRA rádiós hálózat integrációja és a forgalom átterhelése elsődlegesen a dedikált rádiós hálózatra, a publikus rádiós hálózat igénybevétel fenntartása ad-hoc igények kielégítésére.

Különböző hálózati architektúrák



https://www.ericsson.com/en/blog/2022/7/public-safety-going-4g-and-5g-broadband-the-latest-industry-trends

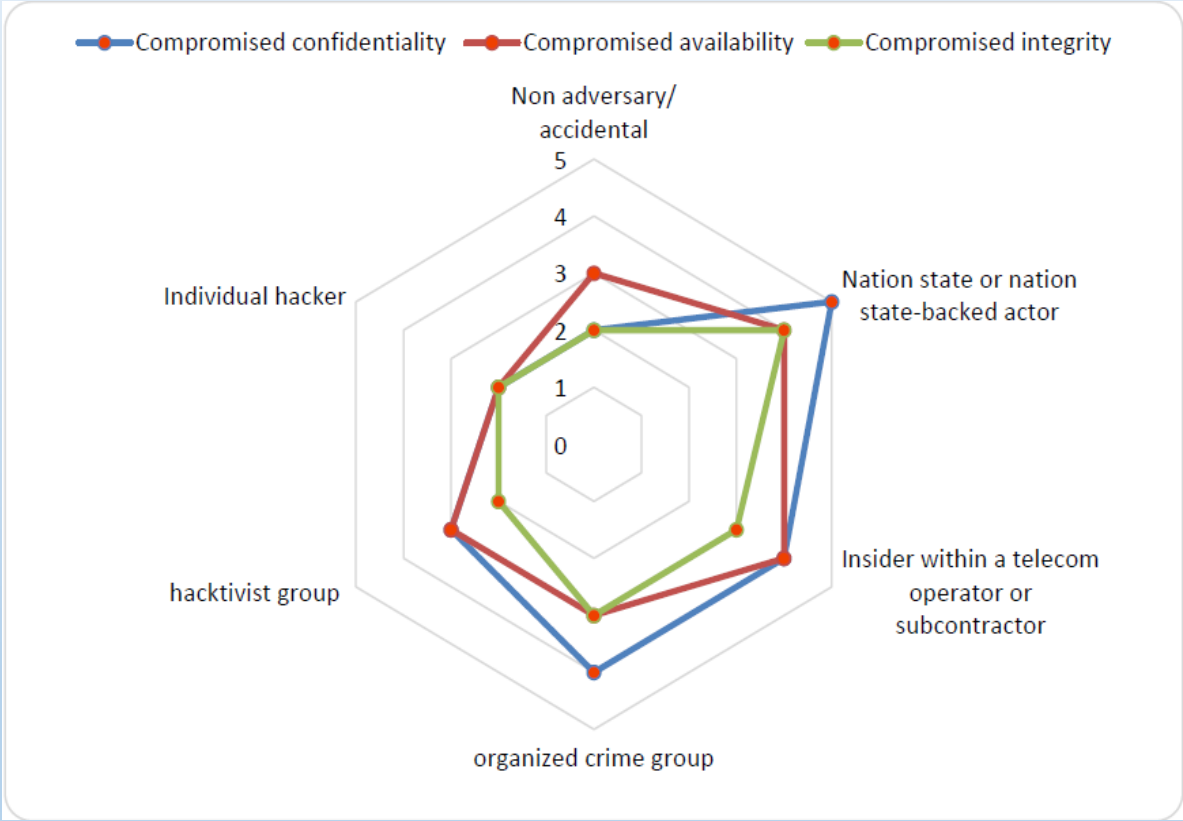
Biztonsági és megbízhatósági kérdések

- Miért nem triviális a 4G/5G használata?
  - Eddig zárt technológia, mely kiforrott, nem piaci kommersz HW-t használ
  - Szabványosítás még folyamatban (5G)
  - Érzékeny és speciális információk továbbítása, pld különleges adatok, melyek nem évülnek el
- Megfelel az 5G?
  - Igen, épp a megfelelő időben jött és még időben vagyunk! – szabványosítás folyamatban (készenléti)
  - Elegendő sávszélesség
  - Megbízhatóság és biztonság – 5G tervezési alapja!
  - Költségek csökkentése (készülék és hálózati oldalon) – több lehetséges szállító
  - Nagyobb függetlenség - több lehetséges szállító

Fenyegetések – telco operátorok

- stratégiai, hálózatot érintő és végpontokra vonatkozó technológiai, valamint a fizikai térből érkező fenyegetések

- Stratégiai:
  - Nem ellenséges/véletlen károkozó/természeti
  - Egyéni támadó
  - Hacktivista támadók
  - **Szervezett bűnözés -** állami összeköttetés?
  - **Belső támadó -** humánbiztonság
  - **Állami vagy államilag támogatott támadó**
  - Egyéb lehetséges támadók - kiberterroristák, vállalati szereplők



https://www.eeas.europa.eu/delegations/united-states-america/eu-coordinated-risk-assessment-5g-network-security_en

Sebezhetőségek - üzemeltetők, szállítók

HW/SW/folyamatok/irányelvek

- Technikai sebezhetőségek (HW/SW/folyamatok)
- 5G és nem 5G specifikus (komplexitás)
- Softwarization (SDN, SDR , whithe boxes vs network specific HW) – SW fejlesztésből adódó sebezhetőség/backdoors
- Új technológiáknak köszönhetően (SDN és NFV, cloud {helye} és konfiguráció, szeletelés)
- Hálózati szeletelek között, virtuális hálózatok között megfelelő szeparáció hiánya
- Hálózat konfiguráció miatt (jelentősen bonyolultabb)
- Képzett és felkészült üzemeltető személyzet hiánya miatt (komplexitás, változás)
- Belső biztonsági auditok, monitoring gyakorlat és biztonsági menedzsment hiánya, eszközleltár
- (Biztonsági) üzemeltetési procedúrák hiánya/nem megfelelősége (update/patch management)
- 3GPP sztenderdeknek való megfelelőség hiánya, sztenderdek nem megfelelő implementációja

https://www.eeas.europa.eu/delegations/united-states-america/eu-coordinated-risk-assessment-5g-network-security_en

Sebezhetőségek - üzemeltetők

- Nem megfelelő hálózati tervezés és architektúra
- Nem megfelelő fizikai biztonság (hálózat és IT infrastruktúra)
- Nem megfelelő hozzáférési kontroll (helyi és távoli elérés) – virtuális eszközök, támogató harmadik fél
- Nem megfelelő beszállítói kiválasztás (biztonság bizonyos megfontolások felett)
- Nem megfelelő változás kezelés (emberi hibák, jogosulatlan változtatások)

https://www.eeas.europa.eu/delegations/united-states-america/eu-coordinated-risk-assessment-5g-network-security_en

Sebezhetőségek - beszállítók

- Jelentős befolyású SW és szolgáltatás biztosítása 3. fél által – jelentős beszállítói kitettség adódhat a beszállító kockázati profiljából
- Szállítói kockázati profil felállítása:
  - EU/Nem-EU
  - Kormányzati befolyás
  - 3. országbeli (kormányzati) befolyás
  - Szankciók?
  - Tulajdonosi struktúra
  - Szállító képessége a berendezések/SW zavartalan biztosítására
  - Beszállító minőségbiztosítása, információbiztonsági jógyakorlata, saját beszállítói láncának ellenőrzésé…

https://www.eeas.europa.eu/delegations/united-states-america/eu-coordinated-risk-assessment-5g-network-security_en

Table 1: Top 30 declaring companies as to cumulative number of declared 5G patent families (granted in either EPO or USPTO) per year

Current Assignee	2015	2016	2017	2018	2019	2020	2021	2022
Huawei (CN)	71	77	791	1,369	2,187	3,634	3,738	3,754
QUALCOMM (US)	126	140	169	1,078	1,550	3,165	3,318	3,356
Samsung Electronics (KR)	23	23	38	1,148	2,187	2,798	3,214	3,215
LG Electronics (KR)	21	22	40	920	2,033	2,148	3,171	3,183
Nokia (FI)	163	177	200	1,281	1,699	2,600	2,632	2,651
Ericsson (SE)	38	53	713	772	1,128	1,202	1,293	1,337
ZTE (CN)	20	22	24	230	791	882	1,045	1,077
Oppo (CN)	0	0	1	194	405	534	906	993
Sharp (JP)	1	1	11	440	548	850	891	894
NTT DOCOMO (JP)	20	23	28	33	394	508	561	561
Apple (US)	34	63	207	274	384	469	531	531

https://www.iplytics.com/report/5g-patent-race-june-2022/

Sebezhetőségek – egyedi beszállítók

- Egyedi beszállítótól/megoldástól való függés - sokszínűség
- Monokultúra
- Egyetlen gyártótól való nagyfokú függőség (kereskedelmi nyomás, ellátási nehézség, felvásárlás, összeolvadás, szankciók)
- Korlátozott beszállítói kör okozhatja a verseny/fejlesztés/hibajavítás visszafogását is
- Korlátozott együttműködés (interoperability)

https://www.eeas.europa.eu/delegations/united-states-america/eu-coordinated-risk-assessment-5g-network-security_en

Fenyegetések– telekomm. operátorok

- A hálózatok nem megfelelő konfigurációja
- Hozzáférési kontrollok hiánya (alvállalkozó priv. jogosultságai)
- Alacsony minőségű (hibás/sérülékeny) termék kihasználása
- Beszállítói függőség (hálózati oldalon főként)
- A beszállítói lánc állami befolyásolása
- A hálózat támadása szervezett kiberbűnözői körök által
- Kritikus infrastruktúrák és szolgálatások jelentős befolyásolása
- Jelentős hálózati leállás az energiaszolgáltatást vagy más kiszolgáló rendszert érő kibertámadás miatt
- Végpontok támadása – MDM – könnyebben kivédhető esetünkben

https://www.eeas.europa.eu/delegations/united-states-america/eu-coordinated-risk-assessment-5g-network-security_en

KOCKÁZATOK - kockázatértékelés – több szintű

- 5G – uniós kockázatkezelés
- Országszintű/hatósági előírások (5G/készenléti/kritikus infrastruktúra) stb
- 5G – operátor / infrastruktúra szolgáltató kockázatkezelés – operátorok közötti információ/jógyakorlat megosztás
- Készenléti szolgáltató saját kockázatkezelése

https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

5G EU kockázatértékelés

I. – Az elégtelen biztonsági intézkedésekhez kapcsolódó kockázati forgatókönyvek	R1. – A hálózatok hibás konfigurálása R2. – A hozzáférés-ellenőrzések hiánya
II. – Az 5G ellátási lánchoz kapcsolódó kockázati forgatókönyvek	R3. – Gyenge termékminőség R4. – Az egyetlen szállítótól való függés az egyes hálózatokon belül vagy a diverzifikáció hiánya nemzeti szinten
III. – A fő fenyegető szereplők működési módjához kapcsolódó kockázati forgatókönyvek	R5. – Állami beavatkozás az 5G ellátási láncon keresztül R6. – Az 5G hálózatok kihasználása vagy a végfelhasználók célba vétele szervezett bűnözői csoportok által
IV. – Az 5G hálózatok és más kritikus rendszerek közötti kölcsönös függőségekhez kapcsolódó kockázati forgatókönyvek	R7. – A kritikus infrastruktúrák vagy szolgáltatások jelentős zavara R8. – A hálózatok súlyos hibája a villamosenergia-ellátás vagy egyéb támogató rendszerek megszakadása miatt
V. – A végfelhasználói eszközökhöz kapcsolódó kockázati forgatókönyvek	R9. – A tárgyak internete (IoT), a mobiltelefonok vagy intelligens eszközök kihasználása

https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

5G biztonsággal kapcsolatos uniós eszköztár

https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

Javaslatok – Szabályzási - Szolgáltatóknak

- A nemzeti hatóságok szerepének megerősítése – távközlési szolgáltató esetén
- A beszállítói lánc állami felügyelete/vizsgálata
- Hálózatüzemeltetők auditja és információk összegyűjtése (Ibtv hatálya távközlési szolgáltatókra való kiterjesztése? NBSZ NKI/piaci?)
- Kulcsfontosságú beszállítók kockázatelemzése, korlátozás, kockázatcsökkentés
- A kiszervezés/külső üzemeltetők biztonsági kontrolljának megvalósítása
- A beszállítók sokszínűségének biztosítása vs interoperabilitás
- A kulcsfontosságú rendszerelemek azonosítása és a diverz és fenntartható 5G ökoszisztéma létrehozása
- A sokszínűség fenntartása és fejlesztése, valamint EU szintű képességfejlesztés
- távközlési iparági együttműködés Information Sharing and Analysis Centers (ISAC)

Javaslatok – Technológiai - Szolgáltatóknak

- Alapvető biztonsági követelmények alkalmazása, biztonságos hálózati architektúra megalkotása (jógyakorlatok/ajánlások fejlesztés/konfiguráció/incidens kezelés/frissítés)
- Releváns szabványok 3GPP, ETSI ajánlások, TCCA ajánlások melyek a biztonságot érintik
- Szigorú hozzáféréskontroll használata (legkisebb jogosultság elve, szerepkörök szétválasztása, 3. felek kontrolja)
- A virtualizált hálózati funkciók biztonságának növelése, fizikai szeparáció
- A biztonságos hálózatmenedzsment, üzemeltetés és monitorozás biztosítása (NOC/SOC) Mo/EU területén – EWS (Early Warning System)
- A fizikai biztonság megerősítése, kritikus komponensek esetén mindenképp
- A szoftverek integritás-ellenőrzésével, frissítésével és a javítások menedzsmentjével kapcsolatos intézkedések megerősítése
- A beszállítókat érintő beszerzési szabályok szigorítása a biztonsági szabályok beemelésével
- Az EU tanúsítvány használata a hálózati komponensekre, a végpontokra és/vagy a szolgáltatói eljárásokra (Európai Kiberbiztonsági Tanúsítási Keretrendszer, Common Criteria)
- Az ellenállóképességgel és a folytonossággal kapcsolatos tervek megerősítése (DRP/BCP), válasz

Következtetések

Az 5G ökoszisztéma megbízhatósága és biztonsága -jelen fejlesztési/tervezési állapotában megfelelőnek tűnik a BB-PPDR rendszerekben elvárt szint biztosításához, de lehetséges, hogy további pótlólagos intézkedések, szabályozók, fejlesztések szükségesek.

Köszönöm a figyelmet!

Kérdések?