A NEMZETI KÖZSZOLGÁLATI EGYETEM KIADVÁNYA

Kommunikáció 2013
Communications 2013

14

SCI-Network Távközlési és Hálózatintegrációs Zrt.

http://www.scinetwork.hu/
info@scinetwork.hu

A SCI-Network Távközlési és Hálózatintegrációs Zrt. hálózati rendszerintegrációval foglalkozó szakértő vállalkozás. A szűkebb értelemben vett hálózati rendszerek mellett a cég alaptevékenységébe tartozik a mikrohullámú átvitel, a hálózati biztonság és a rendszerfelügyelet is. A SCI-Network teljeskörű szolgáltatást nyújt ügyfeleinek a hálózatok terén a feladat felmérésétől kezdve, a tervezésen, eszközszállításon, üzembehelyezésen, oktatáson keresztül a garanciális és garancián túli szolgáltatásokig. A folyamatosan gyarapodó létszámmal, bővülő ügyfélkörrel és növekvő forgalommal rendelkező vállalat az informatikai vállalkozások felső harmadába tartozik.

A SCI-Network célja, hogy ügyfelei számára magas színvonalú megoldásokat biztosítson, valamint megismertesse kiváló minőségű termékeit és szolgáltatásait leendő ügyfeleivel.

A vállalat kiemelt figyelmet fordít a minőségbiztosításra, melyet ISO 9001 és AQAP2110 minősítése is tükröz.

SCI-NetWork
Telecommunications & Networking Inc.
H-1142 Budapest, Erzsébet királyné útja 125.
phone: +36-1 467-7030 • fax: +36-1 467-7049

Testre szabott kommunikációs megoldások? A Kapsch ideális partner! Legyen szó integrált beszéd- és adatátviteli rendszerekről, innovatív modulokról és komponensekről, távközlési szolgáltatók számára kifejlesztett megoldásokról, vagy akár közlekedéstelematikáról – a Kapsch intelligens megoldásai a legmagasabb minőségi követelményeknek is megfelelnek és világszerte megtalálhatók. **www.kapsch.hu**

kapsch >>>
always one step ahead

Nemzeti Közszolgálati Egyetem

Budapest, 2013. november 13.

A tudományos kiadványt lektorálták:
Prof. Dr. Pándi Erik r. ezredes, f. tanár
Dr. Fekete Károly mk. alezredes, e. docens
Dr. Kerti András mk. alezredes, adjunktus
Dr. Szöllősi Sándor ny. okl. mk. őrgy, e. docens

Szerkesztette:
Dr. Fekete Károly mk. alezredes, e. docens

Felelős kiadó: Prof. Dr. Patyi András, rektor
Megjelent a Nemzeti Közszolgálati Egyetemi Kiadó gondozásában
Készült Nemzeti Közszolgálati Egyetem nyomdájában, 100 példányban
Felelős vezető: Tóth-Baltási Péter
Levelezési cím: 1581, Budapest, Pf.: 15.
nke@uni-nke.hu

ISBN 978-615-5305-16-0

TARTALOMJEGYZÉK

A tudományos konferencia támogatói:

Alcatel-Lucent Magyarország Kft.

Hungaro DigiTel Kft.

Equicom Kft.

SCI-Network Távközlési és Hálózatintegrációs ZRt.

NATIONAL INSTRUMENTS™

Biztonságpolitikai Szakkollégium

TOTALTEL Távközléstechnika Kft.

SPESYS Network Security Company

Hírközlési és Informatikai Tudományos Egyesület

ELSINCO Budapest Kft.

HM EI Zrt.

Kapsch Telecom Kft.

HM CURRUS Zrt.

HM ARMCOM Kommunikációtechnikai Zrt.

HM ARZENÁL Zrt.

A NEMZETKÖZI KONFERENCIA HÁTTÉR INFORMÁCIÓI

A konferencia fővédnöke:
Vas Sándor dandártábornok
Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnökség csoportfőnök

A konferencia támogatói:
ALCATEL-LUCENT Magyarország Kft.
Hírközlési és Informatikai Tudományos Egyesület
Hungaro DigiTel Kft.
Kapsch Telecom Kft.
Equicom Kft.
NATIONAL INSTRUMENT™
SCI-Network Távközlési és Hálózatintegrációs Zrt.
TOTALTEL Távközléstechnikai Kft.
ELSINCO Budapest Kft.
SPESYS Network Security Company
Biztonságpolitikai Szakkollégium
HM EI Zrt.
HM ARMCOM Kommunikációtechnikai Zrt.
HM ARZENÁL Zrt.
HM CURRUS Zrt.

A konferencia rendezői:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Üzemeltetési Intézet Híradó Tanszék
Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnökség
Hírközlési és Informatikai Tudományos Egyesület NKE Egyetemi Csoport

A szervező bizottság elnöke:
Dr. Fekete Károly mk. alezredes, e. docens

A szervező bizottság titkára:
Dr. Farkas Tibor fhdgy., adjunktus

A szervező bizottság tagjai:
Dr. Németh József, adjunktus
Jobbágy Szabolcs szds., tanársegéd

az Ön ICT méréstechnikai szakértője

Az EQUICOM Méréstechnikai Kft. 2000 óta van jelen a magyarországi ICT piacon telekommunikációs, informatikai és kábeltelevíziós méréstechnikai megoldásokkal.

Világviszonylatban is vezető pozíciót elfoglaló beszállítói innovatív megoldásokat kínálnak az adatátviteli és kommunikációs hálózatok létesítési és üzemeltetési méréséhez, analíziséhez, és monitorozásához. Az évről-évre növekvő piaci jelenlét az ügyfeleikkel kialakított jó kapcsolat, a technológia központú szemlélet, és a hozzáadott érték növelésére való törekvés mellett a beszállítók folyamatos fejlesztési munkájának is köszönhető.

A beszállítók meghatározó jelenléte révén olyan területeken értünk el jelentős sikereket, mint a hozzáférési optikai hálózatok mérése, az új generációs transzport technológiák analízise, vagy a vállalati informatikai hálózatok mérése és monitorozása. A kanadai központú **EXFO** kezdetekben optikai kézi műszereiről volt ismert, mára azonban a szolgáltatói hálózatok minden szegmensére fejleszt méréstechnikai megoldásokat. A **Fluke Networks** hasonlóan széles spektrumon fedi le az informatikai hálózatok analízisét és monitorozását, a fizikai szinttől a vezeték nélküli technológián át egészen az alkalmazás teljesítmény menedzsmentig. A **FITEL Furukawa Electric** optikai szálhegesztőivel, valamint a **VeEX** kábeltelevíziós analizátoraival, és szolgáltatói hálózatok üzemeltetésére szánt kézi műszereivel lesz teljes a megoldások tárháza.

EQUICOM Méréstechnikai Kft.
1162 Budapest, Mátyás király utca 12.
Tel.: +36 1 272 1234 ● Fax: +36 1 272 1232 ● E-mail: info@equicom.hu

www.equicom.hu

BEVEZETŐ

A KOMMUNIKÁCIÓ nemzetközi szakmai-tudományos konferencia-sorozat tizennegyedik évfordulóján tisztelettel köszöntjük Önt!

Az elmúlt néhány évben az infokommunikáció területén a gazdasági visszaesés és stagnálás volt jellemző, melynek eredményeként egyrészt szűkültek a technológiai megújulás lehetőségei, másrészt a tervezhető és végrehajtható fejlesztések megfontoltabban, kiérleltebben és komplexebb szempontrendszer érvényesítésén keresztül valósultak meg. A főként gazdasági alapokon nyugvó technikai akadályok leküzdését gyakran mélyreható szervezeti átalakulások segítették, azonban kizárólag átszervezéssel egyre kevésbé lehet a kor színvonalán tartani és főként érdemben fejleszteni a Magyar Honvédség híradó és informatikai rendszerét. A két, szakmailag egyre kevésbé elváló területet az információbiztonság gyorsan változó és nagyon forró kérdései hatják át és erősít meg bennünket abban, hogy a kérdéskört kizárólag komplexen, a mindenkori aktuális helyzetnek megfelelően és még talán annál is egy lépéssel előbbre látva kell kezelni.

Örömmel jelenthetjük a konferencia tisztelt résztvevőinek, hogy oktatási alapegységünk - a megújult egyetemi struktúrán belül - továbbra is létezik, őrzi a „szakma lángját". Rendszeressé váltak az információbiztonság szakmai kérdéseit tárgyaló tavaszvégi konferenciáink, a hálózat és rendszercentrikus gyakorlati híradó és informatikai képzést – az egyetemünkön kizárólagosan – a Híradó Tanszék végzi. A hagyományteremtés rögös útján túl vagyunk, a megalapozott, teljes vertikumú tanfolyami, alap, posztgraduális és doktori képzés nehéz, de megtisztelő feladatait végezzük.

Ebben az évben ismét lehetőségünk nyílt különkiadványt készítenünk. Szerény példányszámban, de valódi papíralapú változatban, az előadások napján foghatjuk kézbe. Tisztelettel és azzal a nem titkolt szándékkal ajánljuk rendezvényünk résztvevőinek a kötetet, hogy - az előadókon és a meghívott vendégeken túl - minél szélesebb szakmai körhöz jusson el a mai konferencia mondanivalója.

Budapest, 2013. 11. 13.

A szervező bizottság

NYIKES Zoltán[1]

AZ RFID ÉS AZ INFORMÁCIÓBIZTONSÁG

Rezümé

A szerző az RFID2 történetének és működésének bemutatását követően az eddig felmerült általános és biztonsági kérdéseket megfogalmazva, azokra keresek megoldási lehetőségeket. Figyelembe véve és azt bemutatva, az általános biztonsági és azon belül az információbiztonsági területet veszi vizsgálat alá. Ezt a területet mélyebben vizsgálva, a konkrétan felmerülő információbiztonsági kérdésekre talált megoldási lehetőségek és eddig beváltan alkalmazott információvédelmi technológiákat tanulmányozza és mutatja be. Az alkalmazási lehetőségek széles tárházából a jelenleg nagy fejlődés elé néző dokumentációvédelmet és adminisztratív biztonságot választotta. A papír alapú dokumentációt a mindennapi életből egyelőre teljesen kizárni nem lehet. Ezért mindenképen muszáj ezen területnek is biztosítani a már rendelkezés álló technológiák alkalmazhatóságát a saját a közérdek kívánalmai alapján. A közokiratok és bankjegyek vonatkozásában nagy fejlesztés látható, viszont ezek a biztonsági elemek a mindennapokban még nem jelentek meg. Gondolva itt az „intelligens" papír és a digitális vízjel alkalmazásának lehetőségeire a védelmi szférában. Eljutva a „hogyan tovább?" kérdésig, azt vizsgálva mutat be néhány valószínű alternatívát, melyet a szakma prognosztizál az elkövetkezendő időn belül.

Kulcsszavak

RFID; rádiófrekvenciás azonosítás; RFID-cimkék; tag; transzponder,; aktív-, passzív-, alacsony frekvenciás-, magas frekvenciás-, ultra magas frekvenciás-, mikrohullámú RFID; biztonság; információbiztonság; információvédelem; személyes adatok védelme; dokumentumvédelem, adminisztratív biztonság, információbiztonsági kockázat; szimmetrikus-, aszimmetrikus hitelesítés;

Az ipari társadalmat a XX. század végén, a XXI. század elején felváltotta az információs, tudásalapú társadalom. Ezt a mindennapjainkban szinte a bőrünkön érezzük. Mobil telefonon tartjuk a kapcsolatot az ismerőseinkkel, családtagjainkkal. Ha autóban utazunk már-már elengedhetetlen a GPS[3] alapú navigációs rendszerek használata. Az Internet már a mindennapjaink részévé vált, napi sok 10 vagy akár 100 üzenetet kapunk, küldünk. Az Interneten vásárolunk, intézzük banki ügyleteinket, rendezzük az adóbevallásunkat, foglalkozunk a biztosításainkkal, mindamellett hogy filmet nézünk, zenét, rádiót hallgatunk, vagy éppen híreket olvasunk rajta. Nem is említve a napjainkban egyre népszerűbb közösségi oldalak látogatását, csak hogy néhány lehetőségét említve a napról napra fejlődő világhálónak. Ugyanakkor egy másik digitális megoldás lépett be mindannyiunk nappali-

1 Magyar Honvédség 54. Veszprém Radarezred Információvédelmi központ, központparancsnok, nyikes.zoltan@mil.hu

2 RFID (Radio Frequency IDentification) Rádiófrekvenciás azonosítás

3 GPS (Global Positioning System) Globális Helymeghatározó Rendszer

jába a digitális tévézés és rádiózás lehetőségével, ami új korszakot indít el a média világában.

A számtalan említett és nem említett lehetőségek vonatkozásában nem szabad megfeledkeznünk a biztonság kérdéséről. A rengeteg információ, ami elektronikusan vagy egyéb formában keletkezik, védenünk szükséges. Ezen megállapítás senki számára nem hagy kétséget. Egyedül a mikéntje az, amit a társadalom a szakemberektől vár. Az IT[4] napjaink egyik dinamikusan fejlődő szegmense a rádiófrekvenciás azonosítás, az RFID. A „civil" kereskedelmi és logisztikai alkalmazása mellett a védelmi szektorban is szükség van az alkalmazására, viszont a biztonság kérdése itt még hatványozottabbá válik, mint bárhol máshol.

Az RFID biztonságát vizsgálva, véleményem szerint a rendelkezésünkre álló számtalan kommunikációs és informatikai lehetőségek biztonságossága vagy azzá tétele fölöttébb nagy innovációt és szabályozottságot igényel. Ennek jó alapot teremt a 2009. évi CLV törvény a minősített adat védelméről, valamint a hozzá kapcsolódó kormányrendeletek, melyek mind a papír alapú adatkezelést, mind az elektronikus minősített adat kezelést szabályozza, valamint a 2013. évi L. törvény a az állami és önkormányzati szervek elektronikus információbiztonságáról, ami jó kiinduló alapja lesz a védelem biztosításának. Ezen felül számos más nemzetközi és hazai szabvány áll a rendelkezésre, melyek az információbiztonság területének szabályozottságához biztosítanak keretrendszert.

Az RFID általános bemutatása

Az RFID „radio frequency identification" az angol kifejezés rövidítése, aminek a magyar jelentése rádiófrekvenciás azonosítás. Hatalmas gyakorlati jelentősége abból adódik, hogy közvetítésével adatokat lehet nyerni az adathordozó megérintése, sőt „láthatósága" nélkül – az adatátvitel elektromos vagy mágneses hullámok közreműködésével történik. Az RFID rendszer összetétele egy adatolvasó és egy ún. transzponder.

Az azonosítandó tárgyon található az RFID-transzponder, egy kis méretű computerchip-ből és egy antennából áll, melyek egy öntapadós címke segítségével kerülnek általában az azonosítandó tárgyra (RFID címke vagy „tag"). A transzponder lehet aktív, tehát önálló energiaforrással ellátott, illetve passzív, önálló energia ellátás nélkülöző.

Az RFID rövid története

Az első rádiófrekvenciás – ma RFID néven ismert – elven alapuló azonosításra szolgáló technológiát a második világháborúban fejlesztettek ki. Sir Robert Alexander Watson[5] fedezte fel, és tökéletesítette a radart, ami csak detektálásra volt használható, azonosításra nem (gyakorlatilag nem tudtak megkülönböztetni az ellenséges és a saját repülőgépeket).

Véletlenszerű volt az 1939-es felfedezése Nagy-Britanniában annak a ténynek, hogyha egy pilóta himbáló mozgást végez a repülőgéppel, megváltozik a

4 IT (Information technology) Információs technológia

5 Sir Robert Alexander Watson – 1892.április 13.– Inverness (Skócia), 1973. december 5.) Életműve meghatározó hatást gyakorolt a XX. század második felének katonai repülésére.

visszavert rádióhullámok alakja, ezáltal a radar[6] képernyőjén megkülönböztethetővé válnak a saját és ellenséges gépek. Ez tekinthető a legelső passzív RFID rendszernek, mely végül Watson vezetésével az első aktív repülőgép felismerő rendszer, az IFF[7] kifejlesztéséhez vezetett.

Az 1970-es években történt RFID „robbanáshoz" az 1960-as évek volt az „előjáték". R. F. Harrington[8] elektromágneses mezőkkel foglalkozó tanulmányai alapozták meg az RFID későbbi elterjedését. Rengeteg kutató foglalkozott ekkor RFID-vel kapcsolatos – a fizikai hullámterjedést leíró módszerekkel folytatott – kísérletekkel.

A kereskedelmi alkalmazások az 1960-as évek elején indultak. A Sensormatic[9] nevű cég élenjárt a korai RFID megoldások területén. Az EAS[10] néven megjelent áruvédelmi lopásgátló rendszer napjainkban is széles körben alkalmazott technológia. Előnye rendkívüli olcsóságában és könnyű használhatóságában rejlett. A mikrohullámú, vagy induktív csatolás alapján működő EAS rendszerek vezettek az RFID széles körű elterjedéséhez.

A '70-es években komoly fejlesztések folytak mind Amerikában, mind Európában. A fejlesztések állatok nyomon követése valamint, jármű és gyártási folyamatok nyomon követése irányában folytak. A gazdák körében nagyon népszerű állataik nyomon követése RFID segítségével. A Los Alamos-i kutatóintézet nukleáris eszközök nyomon követésére is kifejlesztett egy rendszert ezekben az években. A fejlesztésekbe, kutatásokba bekapcsolódott cégek és egyetemek sorába olyan cégeket is megtalálunk, mint pl. a Los Alamos Tudományos Laboratórium, a Northwestern Egyetem, a Svéd Mikrohullámú Kutatóintézet, a Raytheon[11], az RCA[12] és a Fairchild[13], valamint a GE[14] és a Philips[15].

A '80-as évekre a kutatási-fejlesztési fázist felváltotta az új eredmények implementációja, a termékekben történő alkalmazása. Az Egyesült Államokban elsősorban a szállítási folyamatok nyomon követésére, személyes hozzáférésre, állatok azonosítására alkalmazták. Európában az állati nyomon követés mellett az ipari és üzleti alkalmazások is igénybe vettek RFID megoldásokat.

Az RFID alkalmazások köre a '90-es években tovább bővült: az autópálya díjfizetés mellett indításgátlókban, (sí)bérletekben alkalmazták, de egyes beléptető rendszerekben is elterjedt. Sok cég lépett be az RFID piacra, olyanok, mint a Texas Instruments[16],az IBM[17], a Micron[18], a Philips, az Alcatel[19], a Bosh[20] és a

6 Radar – (Radio Detection And Ranging), Rádióérzékelés és Távmérés, rádiólokátor

7 IFF – (Identification, Friend or Foe), Idegen barát felismerő rendszer

8 R. F. Harrington – a Syracuse University kutató professzora

9 Sensormatic – az amerikai tulajdonú Tyco cégcsoport tagja

10 EAS – (Electronic Article Surveillance) elektronikus árufelügyelet

11 Raytheon Company, USA védelmi és ipari vállalat

12 RCA – (Radio Corporation of America) elektronikai vállalat volt 1919-1986 között.

13 Fairchild Corporation – USA vállalat 1920.-ban alapították

14 GE – (General Electric Company), USA multinacionális vállalat

15 Philips – (Koninklijke Philips Electronics NV) multinacionális holland elektronikai vállalat.

16 Texas Instruments Inc. – USA elektronikai és félvezető gyártó cég

17 IBM – (International Business Machines) USA multinacionális társaság

Combitech[21]. 1990-ben alakult meg az E-Z Pass[22], mely egységesíteni kívánta egy saját fizető-ellenőrző rendszer kiépítésével a különböző útdíj fizetési módszereket. Ez a technológia Európában is egyre népszerűbb lett.

Az első, CMOS[23] áramkörre integrált mikrohullámú Schottky diódák[24] lehetővé tették az egyszerű, egyetlen IC[25]-ből álló mikrohullámú RFID tag-ek létrejöttét, ami nagyobb olvasási hatótávolságot és gyorsabb adatátvitelt biztosított.

1999-ben az UHF[26] RFID lendületet kapott, amikor az Auto-ID Center[27] megalapításra került, és a cég kifejlesztette az olcsó, mikrochip-et is tartalmazó RFID tag-et. A tag-ben csak egy sorozatszámot tárolnak, ami a kis memória következtében olcsóbb, és a sorozatszám alapján egy Internet alapú adatbázisból kereshető ki további információ a termékről. Addig egy RFID tag egy mobil adatbázis volt. Az RFID-t hálózati technológiává fejlődött azzal, hogy a tárgyakat a tag-ek révén az Internethez kapcsolta. Az üzleti életben ez jelentős változást hozott, mert lehetővé vált az, hogy a termék útja a két fél által folyamatosan követhető legyen.

Az RFID teljes körű bevezetését tervezik a multinacionális kereskedelmi cégek, mint pl. a Metro[28], a Tesco[29], vagy a Wal-Mart[30]. Mellettük az USA Védelmi Minisztérium (DoD31) ugyanúgy érdeklődik e technológia iránt, mint egyes kisebb gyógyszeripari vállalatok, vagy autógumi gyárak. Az igazán széles körű elterjedés napjainkban várható, miután az EPCglobal[32] jóváhagyta a második generációs szabványokat. [9]

AZ RFID alkalmazásának lehetőségei

A mai életünk szinte teljes vertikumát magába ölelő lehet az RFID alkalmazásának a lehetősége. Ehhez kellett az információs technológiák robbanásszerű fejlődése is. Az Internet és a mobiltelefonos valamint a GPS technológiák alkalmazásával a mindennapi életünk, háztartásunk ugyanúgy be van hálózva, mint az ipari tevékenységek, gyártási technológiák vagy a banki-üzleti világ. De elsősorban a logisztikai folyamtokban kapott szerepe mellett a védelmi szféra is jelentősen érdekelt a technológia fejlődésében.

Az RFID jelenlegi alkalmazásának főbb területei:

---

18 Micron Technology, Inc.- USA multinacionális félvezető gyártó cég

19 Alcatel-Lucent – globális távközlési vállalat

20 Robert Bosch GmbH – Stutgartban alapított multinacionális vállalat

21 Combitech – Svédország egyik vezető technológiai és műveletek tanácsadó cége

22 E-ZPass Interagency Group (IAG) – USA elektronikus autópályadíj-beszedési rendszert működtető cég

23 CMOS – (Complementary Metal–Oxide–Semiconductor), integrált áramkör technológia

24 Schottky dióda – Elsősorban tranzisztorok telítődésének megakadályozására alkalmazzák

25 IC – (Integrated Circuit) integrált áramkör

26 UHF – (Ultra High Frequency) deciméteres hullámtartomány

27 Auto-ID Center – Hét kutatóegyetem laboratóriumai által alapított kutatási központ

28 Metro AG – 1964-ben Düsseldorfban alapított kis-és nagykereskedelmi cégcsoport

29 Tesco plc – 1919-ben az Egyesült Királyságban alapított kis-és nagykereskedelmi cégcsoport

30 Wal-Mart Stores, Inc. – USA kis-és nagykereskedelmi cégcsoport

31 DoD (vagy USDOD, DOD) – Az Egyesült Államok Védelmi Minisztériuma

32 EPCglobal – (Electronic Product Code (EPC)) a technológia alkalmazására alapított közös vállalat

- Logisztika, kereskedelmi raktárak;
- Könyvtári és irattári alkalmazások;
- Vagyontárgyak nyomkövetése, tárgyi eszköz leltár;
- Gyártás-optimalizálás;
- Ellátási lánc menedzsment;
- Kiskereskedelem;
- Díjfizető rendszerek;
- Biztonsági és beléptető rendszerek;
- Állattenyésztés. [4]

Az RFID fő típusai

A **passzív RFID** tageknek nincs adó egysége, a (modulált) rádióhullámokat csak az olvasóból kisugárzott energia révén verik vissza. Egy mikrochip van beépítve, ami egy antennával van ellátva. Tokozásuk számtalan lehet: A nyomtatható smart-label RFID címkét egy hordozó rétegre felerősített papír címke és ragasztóréteg közé helyezik. A transzpondert lehet plasztik kártyába ültetni, kulcstartóra fűzni vagy műanyag dobozba rögzíteni, hő és kémiai behatások elleni védelem miatt. [13]

Az **aktív RFID** tagek egyéni adóval és többnyire egyéni energiaforrással rendelkeznek, a mikrochip-jükben tárolt információt rádióhullámok útján sugározzák. Ilyen rendszereket használnak például nagy értékű konténerek, vasúti kocsik, követésére. Szélesebb értelemben véve kétféle aktív tag létezik: a transzponder és a beacon. [13]

Az RFID olvasó rádióhullámaira ébred fel az **aktív transzponder**, máskülönben nem sugároz. Ezek többnyire beléptető és autópálya díjfizető rendszereknél használatosak. Ha egy jármű a beléptető kapu előtt elhalad, a kapunál elhelyezett olvasó által kibocsátott rádióhullám eredményeként a szélvédőn elhelyezett transzponder felébred, és kisugározza az egyedi azonosítóját. Azzal növeli a transzponder az elemének élettartamát, hogy csak az olvasó jelének hatására kezd el sugározni. [13]

A **beaconok** valósidejű helymeghatározó rendszerekben (real-time locating system = RTLS) alkalmazzák, ahol nagy értékű eszközök pontos helyének meghatározása az elsődleges. Az RTLS alkalmazásával a beacon rendszeres időközönként leadja az egyedi azonosítóját, ami három másodperc vagy egy nap is lehet, típustól függően. Az eszköz pontos helye könnyen meghatározható, hogyha a beacon jeleit legalább három különböző vevő veszi egyszerre. Ezt a rendszert nagy értékű járműveknél alkalmazzák a lopások megelőzésére. [13]

Rendszerek fő típusai és alkalmazásuk előnyök és hátrányok

Az ***alacsony frekvenciás RFID***, vagyis a 9-135 KHz közötti frekvenciatartományban a használata elsősorban az élőállatok azonosítási területén terjed el, a könyvtári könyvek azonosítása mellett. Az autóipar fejlődése során kezdték el alkalmazni először a prémium kategóriás, majd szinte az összes kategóriánál az Auto Key and Lock megoldásokat. A biztonságtechnikai alkalmazások esetében is sok esetben használják a biztonsági és beléptető rendszerek telepítése során.

A raktári környezetben a használata az alacsony olvasási távolság miatt nem alkalmazható jól illetve az ePC használatánál nem szabványosított. Ellenben világviszonylatban elfogadott, széles körben elterjedt, és fémes anyagok közelében is működő képes. [6][8]

A ***magas frekvenciás RFID*** egy 13,56 MHz-es alkalmazás. Világviszonylatban elfogadottságából adódóan, valamint a nedves környezetben történő jó alkalmazhatósága miatt a raklapok és csomagok azonosítására használják elsősorban a légi forgalomban. E mellett különböző beléptető rendszerek, továbbá az áruvédelem területén, könyvek és ruházat védelmére is használják.

A fémes környezetben a hatékonysága alacsony. Az olvasási távolsága 1,5 m alatti.[6][8]

Az ***ultra magas frekvenciás RFID,*** vagyis a 1,5 m feletti olvasási távolság miatt a 300 és 1200 MHz közti frekvencia jól alkalmazható nedves környezetben, amely miatt a kereskedelmi alkalmazása is jelentősen megnőtt. Elsősorban konténereknél, szállító járműveknél valamint járművek nyomon követésénél alkalmazzák. A dokumentáció menedzsmentben is jelentős a szerepe. Az alkalmazás még Japánban nem elfogadott, valamint a sugárzott jel elnyelődése számottevő.[6][8]

A ***mikrohullámú RFID,*** vagyis a 2,45 és a 5,8 GHz-es alkalmazást a nagy olvasási távolsága miatt elsősorban a gépjármű beléptetéseknél alkalmazzák. Egyéb alkalmazásaihoz még számos fejlesztés szükséges mert jelenleg bonyolult rendszer kiépítése szükséges hozzá. Az EU bizonyos részein nincs kereskedelmi használatra szóló megegyezés vele kapcsolatban.[6][8]

Felmerülő kérdések, aggályok az RFID-vel kapcsolatban

Az RFID személyazonosításra való alkalmazása évek óta vita tárgya. Főként adatvédelmi aggályokat vetnek fel. Többen fenyegetést látnak abban, hogy az RFID bélyegek anélkül olvashatók, hogy a tulajdonosa észlelné, mivel a bélyeg egyedi azonosítója összekapcsolható a tulajdonos személyes adataival. Ezen felül, az RFID címkéket úgy lehet a tárgyakra helyezni, hogy az azokat megszerző egyén nem is tud róluk. A címkéket távolról is le lehet olvasni, ráadásul olyan olvasókkal, amik el vannak rejtve a környezetben, így az egyén gyakorlatilag azt sem tudja, hogy mikor „olvassák le”.

Például egy áruházban a termék vásárlója nem tudja hatástalanítani az azonosítót. Bankkártyás fizetés esetén pedig a termék összekapcsolható lenne a vásárlóval. Ebből következik, hogy a vásárló már név szerint is beazonosíthatóvá válna. Így a vásárlás után már nemcsak a termék, hanem a vásárló is követhető lenne akár nagyobb távolságból is. Már léteznek (például az áruház kijáratánál elhelyezhető) különböző deaktivátor kapuk, de ezek hatásfoka még kétséges.

Szintén nem elhanyagolható a biztonság kérdése, mivel jelek távolról, tudtunk nélkül is leolvashatóak. Természetesen a rádiófrekvenciás jelek is titkosíthatóak különböző kriptográfiai módszerekkel, de például a passzív címkék memóriakapacitása ennek gátat szabhat.

Az magánélet védelme mellett a másik fontos kérdés, hogy az RFID az egészségre és a környezetre ártalmas lehet-e. Az RFID-vel kapcsolatos elektro-

mágneses mezők (EMF[33]) általában gyengék, így a lakosság jóval kisebb mértékben van kitéve e sugárzásnak, mint amit a hatályos szabványok megengednek. A vezeték nélküli alkalmazások száma azonban mostanra jelentősen megnövekedett.[4][5]

A biztonság

A biztonság mindig valamilyen érdekellentét kontextusában merül fel, valamiféle fenyegetésekkel kapcsolatban. A fenyegetés lehetőség olyan (aktív) cselekedetre valamilyen ellenfél részéről, amely neki hasznot, a vizsgált rendszernek pedig kárt okoz. A megvalósult fenyegetést *támadásnak,* végrehajtóját pedig *támadónak* nevezzük. A támadó szemszögéből a támadásnak van valamilyen (várható) költsége és (várható) haszna. A támadót biztonsági tervezéskor racionálisnak feltételezzük, azaz arra számítunk, hogy költségeit minimalizálni, hasznát pedig maximalizálni próbálja a rendelkezésére álló információ alapján. Biztonsági (más szóval védelmi) intézkedésnek nevezzük mindazt, ami a támadás költségeit növeli. Ezek két nagy csoportba oszthatók: a *proaktív biztonsági intézkedés*ek a támadás végrehajtásához szükséges erőforrások növelésével rónak költségeket a támadóra, a *reaktív biztonsági intézkedés*ek pedig a támadás végrehajtása miatt okoznak kárt a támadónak. Az RFID technológiák mindkét fajta biztonsági intézkedés megvalósításához eredményesen alkalmazhatók. Egy biztonsági rendszer (biztonsági intézkedések összessége) akkor sikeres, ha megakadályozza, hogy a fenyegetésből támadás legyen. [12]

Az információbiztonság

A biztonság témakör két, az IKT[34]-k iránti bizalom megteremtését szolgáló területet fog össze. Az egyik az információbiztonság, a másik pedig a magánélet-védelem. Ez utóbbi terület európai viszonyok között leginkább a személyes adatok védelmének kérdéseként értelmezhető a gyakorlatban. Az információbiztonság a szervezeti értelemben vett biztonság megteremtésének eszköze, míg a személyesadat-védelem a felhasználóknak és az ügyfeleknek az egyre növekvő kiszolgáltatottsággal szembeni biztonságérzetének megőrzését elősegítő eszköz.

Az információbiztonság egyik maghatározó pillére az informatikabiztonság, amely alatt az informatikai rendszerek és eszközök (szoftver, hardver vagy ezek együttese) elvárt működését (biztonságos működését) akadályozó vagy veszélyeztető kockázatok (cselekmények, külső hatások vagy ezek következményeként előálló állapotok) elleni védettség értendő. Az informatikabiztonság (biztonságos működés) – definíció szerint – csak a konkrét használati cél alapján egyedileg meghatározható minőség, ami ugyanakkor azonban nem zárja ki a tipizálás lehetőségét. Az „informatikai rendszer és termék" kifejezés az üzemeltetést és használatot is átfogó széles értelemben használatos, ahol az informatikai rendszerekbe az internetes alkalmazások és szolgáltatások növekvő szerepére való tekintettel beleértendők az adatátviteli-távközlési hálózatok is.

Az információbiztonság és a személyes adatok védelme az IKT világában szorosan összekapcsolódik. A két terület egyszerre van egymást kiegészítő és

33 EMF – Elektro Magnetic Field – elektromágneses mező

34 IKT – Infokommunikációs technológia

egymásnak ellentmondó viszonyban. A kiegészítő viszony annak köszönhető, hogy a személyes adatok kezelése során az adatok védelme információbiztonsági megoldások nélkül elképzelhetetlen. A kezelt személyes adatok védelmének nézőpontjából az információbiztonság egyike azon kérdéseknek, amelyek megfelelő kezelése elengedhetetlen tényező a személyes adatok védelmében. A magánélet védelmének azon aspektusa azonban, amely a személyes adatok kezeléséhez való jogosultság megszerzéséhez kapcsolódik már ellentmondásokhoz vezet a két terület között. Az információbiztonság megteremtésében ugyanis rendkívül fontos szerepet játszik a felhasználók megfelelő azonosítása, valamint a felhasználókról történő kiterjedt adatgyűjtés az egyes biztonsági eseményekért való felelősségnek a későbbi megállapíthatósága érdekében. Az információbiztonság megteremtésének nézőpontjából ezért a személyes adatok védelme az információbiztonság megteremtését *akadályozó tényező*ként is jelentkezik a gyakorlatban. A Magyar Parlament, az Európai Uniós jogharmonizáció szellemében elfogadta a 2011. évi CXII. törvényt az információs önrendelkezési jogról és az információszabadságról, mely a fenti probléma megoldását is szolgálja.[1]

Az ***információbiztonsági kockázatok*** könnyen számszerűsíthetők, mivel az információ, egy-egy dokumentum illetéktelenek kezébe vagy nyilvánosságra kerüléséből, továbbá informatikai rendszerek rosszindulatú támadások eredményeként előálló időleges vagy végleges működésképtelenségéből potenciálisan származó kár mértéke elég jól meghatározható. Az információbiztonsági kockázatok változása ezért szorosan összefügg az informatikai eszközök és rendszerek üzleti értékével, sőt megállapítható, hogy az IKT üzleti folyamatokban betöltött szerepének növekedésével együtt nőnek az információbiztonsági kockázatok. Tekintettel arra, hogy az üzleti folyamatok IKT-függősége folyamatosan nőni fog a következő évtizedben, az információbiztonsági kockázatok tartós növekedésére lehet számítani. Az információbiztonsági kockázatok jövőbeli alakulása azonban a technológiai változások mellett a potenciális támadók körének jövőbeli alakulásától is függ. Az informatika korai időszakát jellemző individuális elkövetők helyébe az elmúlt időszakban egyre inkább a professzionális, jól szervezett, elkövetői csoportok léptek. Ez a folyamat várhatóan tovább fog erősödni. [1]

Az ***információbiztonsági technológiák*** köre igen széles. Ide sorolhatók mindazok a hardver- és szoftvereszközök, amelyek az információbiztonsági kockázatok csökkentését segítik. Egyes reaktív információbiztonsági eszközök (például vírusirtó, tűzfal) használata mára már általánossá vált. Az azonosítási megoldások is sokat fejlődtek az elmúlt évtizedben. Ennek a területnek a következő évtizedben tapasztalható nagy változása lesz, hogy az egyfázisú azonosítást fokozatosan és általánosan kiváltják a kétfázisú azonosítási megoldások.

A biztonsági kockázatok elleni proaktív védekezés előtérbe kerülése a technológiák szintjén elsősorban a szoftverfejlesztés átalakulásában ragadható meg. Ennek a változásnak egyik legfontosabb eredménye az lesz, hogy a következő évtized második felére általánossá válik az információbiztonsági szempontok figyelembe vétele a termékek és rendszerek tervezése során is. [1]

A különböző ***információbiztonsági értékelési és tanúsítási*** megközelítések egyre fontosabb szerepet játszanak az IKT biztonsága és megbízhatósága tekintetében, amelyeket részben *állami szabályozás* ír elő, részben bizonyos gazdasági

szektorok, területek *önszabályozás*a révén válik kötelező előírássá. Ilyen a NATO[35]-beszállítók előzetes értékelése és tanúsítása.

További konszolidáció várható a jelenleg versengő biztonsági szabványok és tanúsítási rendszerek között (ISO/IEC 27001[36], a COBIT[37] és az ISO/IEC 15408 [38]– Common Criteria[39]), és egyre inkább a piacon maradás feltétele lesz a megfelelő tanúsítvány megléte. E megközelítések közös jellemzője, hogy *komplex átfogó megoldások*at kínálnak az információbiztonsági problémák kezelésére. Fontos azonban azt is látni, hogy az egyes megközelítések esetében a hangsúlyok eltérnek. Így például a Common Criteria az IKT rendszerek és -eszközök *biztonsági értékelés*e használatos, az ISO/IEC 27001 elsősorban az *információbiztonság menedzsmentfolyamatai*nak megítélésére, a COBIT-ot pedig a felelős, számonkérhető és *átlátható IT-irányítás* vizsgálatánál alkalmazzák.

Várható, hogy ez a *munkamegosztás tovább erősödik*, ugyanakkor az egyes elemek jobban fognak egymáshoz illeszkedni. A jelenleginél is határozottabban elválnak a menedzsmentjellegű, a rendszer- és eszközszintű biztonsági szabványok, és az ezekre épülő értékelési és tanúsítási rendszerek, valamint az egyes szinteken történő értékelést és tanúsítást támogató technológiák. Ezzel párhuzamosan általánossá válik a biztonsági követelményeknek való megfelelőséget vizsgáló és ellenőrző, a biztonsági előírások kikényszerítését támogató *IT-alkalmazások használata*. [1]

Biztonsági szabályozás és kutatások

A fejlesztések elsősorban az RFID-rendszerek biztonságának növelése irányába mutatnak. Ezekben a rendszerekben fontos szempont, hogy a jogosulatlan személyek ne férhessenek hozzá más felhasználók adataihoz. A következő támadások lehetnek:

- Lehallgatás: a címke (tag) és a reader közötti rádiójeleket dekódolják.
- Zavarás: az adatcsere megszakadhat árnyékolás, vagy a transmitter zavarása miatt.
- Azonosítás hamisítása: a hamisító hozzájut az azonosítási és biztonsági információkhoz, és azt a látszatot kelti, hogy ő, mint reader fér hozzá a címkéhez (tag-hez).
- Tartalom hamisítása: az adat könnyen hamisítható a jogosulatlan írási hozzáférés által.
- Blokkolás: az ún. blokkoló címke (tag)-ek több címke (tag) jelenlétét szimulálják, és ezáltal lehetetlenné teszik a reader működését.

Az RFID-címkéket meg kell védeni az illetéktelen leolvasásoktól, és az illetéktelen beírásoktól, a számítógépes vírusoktól és az identitáslopásoktól; különö-

35 NATO – The North Atlantic Treaty Organization – Az Észak-atlanti Szerződés Szervezete

36 ISO/IEC 27001 – Az információbiztonság irányítási rendszerei. Követelmények

37 COBIT – Control Objectives for Information and related Technology – informatikai szabályozási keretelvgyűjtemény

38 ISO/IEC 15408 – Az informatikai biztonságértékelés közös szempontjai

39 Common Criteria – Közös Szempontrendszer – nemzetközileg elismert biztonsági szabálygyűjtemény

sen akkor, ha személyes vagy egészségügyi információkat hordoznak. Ehhez az RFID-chipen tárolt információkat kötelezően kódolni kell, ha ilyen információ hordozását tervezik rajtuk. [7]

Európai megállapodás az RFID-címkék etikus használatáról

Az Európai Bizottság önkéntes megállapodást írt alá az ipar és a civil társadalom képviselőivel, az Európai Hálózat- és Információbiztonsági Ügynökséggel (ENISA), valamint a magánélet- és adatvédelemmel foglalkozó európai szervezetekkel olyan iránymutatások kidolgozására, amelyek az európai vállalatoknak még az intelligens címkék (rádiófrekvenciás azonosító eszközök, RFID) forgalomba hozatala előtt segítenek megoldani a címkék használatából adódó adatvédelmi kérdéseket.

A megállapodás előzménye, hogy 2009 májusában az ipar, a szabványügyi testületek, fogyasztóvédelmi szervezetek, civil társadalmi csoportok és szakszervezetek valamennyi érdekeltje egyetértett abban, hogy tiszteletben tartja az intelligens címkék használatára vonatkozó magánélet- és adatvédelmi elvek megállapításáról szóló európai bizottsági ajánlást. Az ajánlásban többek között az is szerepel, hogy amikor a fogyasztók intelligens címkékkel ellátott termékeket vásárolnak. Ezeket a címkéket automatikusan, azonnal és a díjmentesen hatástalanítani kell, kivéve, ha a fogyasztó kifejezetten igényli aktiválásukat.

A szabályozás szükségességét alátámasztja, hogy az intelligens címkék használata óriási ütemben. Világszerte mintegy 2,8 milliárd intelligens címkét értékesítettek 2011-ben, ennek körülbelül a harmadát Európában. Az iparági becslések szerint azonban 2020-ra akár 50 milliárd, RFID-címkét tartalmazó elektronikus eszköz is lehet.[4]

Hasznos, de veszélyeztetheti a magánéletet

A mobiltelefonokban, számítógépekben, hűtőszekrényekben, e-könyvekeben és gépkocsikban lévő RFID-címkék sok potenciális előnnyel járnak a vállalkozások, a közszolgáltatások és a fogyasztói termékek számára. Példaként hozhatók fel a következők: a termékek megbízhatóságának javulása, az energiahatékonyság fokozása és az újrahasznosítási eljárások hatékonyabbá válása, az autópályadíjnak a díjfizető kapunál való megállás nélkül történő kifizetése, a reptéri csomagkiadásnál töltött idő csökkenése, valamint a termékek és szolgáltatások környezeti hatásának mérséklése.

Az RFID-címkék ugyanakkor magánélet-védelmi, biztonsági és adatvédelmi kockázatokat jelenthetnek. Ide tartozik az is, hogy egy harmadik fél az engedélyünk nélkül juthat hozzá személyes adatainkhoz (például a tartózkodási helyünk koordinátáihoz). [4]

RFID és a biztonság

Az utóbbi időben az RFID rendszerek magas biztonsági fokú alkalmazásokban történő felhasználása került előtérbe. Gondoljunk a napjainkban egyre jobban elterjedő PayPass[40] bankkártyás fizető-rendszerekre, vagy betegazonosításra. Ezen megoldások elengedhetetlenné tették olyan biztonsági kiegészítések integ-

40 Olyan, egy érintéssel működő, bankkártya alapú fizetési technológia, amely megkönnyíti és felgyorsítja a fizetést.

rálását a meglévő rendszerekbe, melyek megakadályozzák a jogosulatlan hozzáféréseket, belépéseket.

A korszerű hitelesítő rendszerek a titok birtoklásának tényét állapítják meg (jellemzően kulcs alapú módszerek). Egy megfelelő algoritmus alkalmazásának a célja megakadályozni a titkos kulcs feltörését. Napjaink magas biztonságú RFID rendszereinek rendelkeznie kell a felsorolt képességgel, ezzel megelőzve az alábbi támadásokat.

- Illetéktelen hozzáférés az adathordozóhoz, a tárolt adatok duplikálása, illetve módosítása céljából.
- Ismeretlen eredetű adathordozó elhelyezése a zónán belül a hitelesítő algoritmusok kijátszásával.
- A rádiós adatforgalom lehallgatása, illetve annak visszajátszása egy hiteles adathordozó látszatának keltése céljából („replay and fraud").

Az alkalmazni kívánt RFID rendszer kiválasztásakor mérlegelnünk kell a fenti szempontok figyelembevételével a használat során megkövetelt biztonsági szükségleteket, illetve azok kielégítésének lehetőségeit. Egy alkalmazást, mely nem igényel nagy biztonsági szintet (pl. ipari automatizáció), feleslegesen drágítana e funkciók integrálása. Ezzel szemben egy nagy biztonságigényű alkalmazás számára elengedhetetlen e funkciók megléte a magasabb költségek árán is. [9]

Kölcsönös szimmetrikus hitelesítés

A kölcsönös szimmetrikus hitelesítés az olvasó és a transzponder között az ISO 9798-2[41] által elfogadott háromlépéses, kölcsönös szimmetrikus hitelesítésen alapuló eljárás, mely egy időben ellenőrzi mindkét fél tudását a titkos kriptografikus[42] kulcsról.

A művelet alapelve szerint minden – az alkalmazást alkotó – tag és olvasó birtokában van ugyanannak a titkos kriptografikus *k* kulcsnak (innen a szimmetrikus eljárás elnevezés). Egy, a zónába újonnan belépő tag-ről nem elképzelhető, hogy a többivel azonos alkalmazáshoz, azokkal megegyező biztonsági feltételekhez tartozik. Az olvasó tekintetében nagyon fontos, hogy megvédje saját alkalmazási körét a jogosulatlan felhasználóktól, ezzel esetlegesen adatforgalmának manipulálásától. Ezzel együtt a transzponder vonatkozásában is fontos a tárolt adatok jogosulatlan hozzáférésének megakadályozása. [9]

Származtatott kulcsokon alapuló hitelesítés

Az előzőekben bemutatott hitelesítő módszer egyik legnagyobb hibája, hogy minden – azonos alkalmazáshoz tartozó – transzponder ugyanazt a *k* titkosító kulcsot használja. Minden hasonló megoldás számára – mely nagyon nagyszámú transzpondert alkalmaz – potenciális veszélyt hordoz ez a tulajdonsága. Mivel ezek a transzponderek gyakorlatilag mindenki számára korlátozás nélkül hozzáférhetők, számolni kell a kulcs kompromittálódásának veszélyével. Amennyiben ez végbemegy, a fent tárgyalt művelet teljesen hatástalanná válik.

41 ISO 9798-2 – Információ-technológiai, információbiztonsági szabvány

42 Kriptogárfia – Informatikai tudományág, mely a rejtjelzéssel, titkosírásokkal, kódolással, azok előállításával és megfejtésével foglalkozik

Amennyiben minden transzpondert saját kulccsal látunk el, a biztonság nagymértékben megnő. Ennek elkészítéséhez előbb kiolvassák a transzponder szériaszámát. A K_X titkos kulcs egy K_M mesterkulcs, valamint egy kriptográfiai algoritmus alkalmazásával kerül előállításra. Ennek következtében minden transzponder saját ID-jéhez[43], valamint a K_M mesterkulcshoz kapcsolt szériaszámot kap a downlink csatornán.

A közös hitelesítés első lépéseként az olvasó lehívja a transzponder azonosítóját. Az olvasó speciális titkosító modulja (SAM[44]) a K_M mesterkulcs segítségével előállítja az olvasó titkos kulcsát, amire a hitelesítés első fázisában lesz szükség. [9]

Titkosított adatkapcsolat

Az előző fejezetekben megismert összetétel most egy potenciális támadóval kerül kiegészítésre.

Ekkor a támadóknak is két fajtáját kell megkülönböztetnünk. Az első – nevezzük *Támadó*$_1$-nek – megkísérel a háttérben maradni és lehallgatásos módszerekkel, passzív módon, értékes információkat kinyerni az adatfolyamból. A *Támadó*$_2$ viszont aktívan részt vesz az adatcserében, és saját (vagy más) hasznára módosítja is annak tartalmát.

Kriptográfiai megoldások mindkét támadó ellen megoldást nyújtanak. Az átviendő adatot (nyílt szöveg) ezért rejtjelzésnek vetik alá, mely eredményeképp a támadó nem vonhat le következtetéseket annak eredeti tartalmáról.

Az adatkapcsolat rejtjelzése is ugyanezen az elven működik. A nyílt szöveget egy *k* titkosító kulcs és egy rejtjelező algoritmus segítségével titkosított szöveggé alakítják. A támadó nem következtetheti ki az eredeti szöveg tartalmát a titkosító algoritmus és annak *k* kulcsának tudása nélkül.

A titkosított adat csak a vevőben kerül visszaalakításra a dekódoló algoritmus, valamint egy titkos *K'* kulcs birtokában.

Amennyiben *k* és *K'* azonos, úgy szimmetrikus kulcsú algoritmusról beszélünk, míg ha *k* kulcs nem nyújt segítséget a visszafejtéshez, úgy az algoritmus aszimmetrikus. RFID rendszerek régóta csakis szimmetrikus kulcsú elven működnek.

Ha minden karakter külön-külön kerül titkosításra, az eljárást szekvenciális kódolásnak, míg ha egy karakterblokk, úgy blokk kódolásnak nevezzük. Mivel azonban a blokk kódolók hallatlanul számításigényesek, RFID alkalmazásokban betöltött szerepük jelentéktelen. Titkosított adatforgalmú RFID rendszerek legnagyobb nehézsége a szimmetrikus *k* kulcs szétosztásának mikéntje, még annak felhasználása előtt.[9]

A ***folyamkódolók*** olyan kriptográfiai algoritmusok, melyek a nyílt szöveg karaktereit egymást követően, de más-más függvény révén titkosítják. A folyamkódolót még az első világháború alatt, 1917-ben találta fel Gilbert Sandford

43 ID – (identification) azonosító

44 SAM – (Secure Application Module) speciális titkosító modul

Vernam[45]. Az ideális folyamkódolót „one-time-pad”-nek (OTP), vagy feltalálója után Vernam ciphernek is nevezik.

Elsőként egy *k* véletlen kulcs kerül generálásra, mely az osztott kulcs lesz az információcserében részt vevő felek között. A kulcsot, ezután *XOR*[46] kapcsolatba állítják a nyílt szöveg karaktereivel. A véletlenszerű *k* kulcs hossza legalább a nyílt szövegével azonos kell legyen, ellenkező esetben az esetleges ismétlődő minták statisztikai támadása feltételezhető. Ezen kívül minden kulcs csak egyszer kerül alkalmazásra, ami a kulcselosztás magas fokú biztonságát követeli meg. Ebben a formában a folyamkódolás teljesen alkalmatlan RFID rendszerek számára.

Ahhoz, hogy legyőzzék a kulcselosztás és generálás okozta komplikációkat, a valódi véletlen szám generátorok helyett „álvéletlen” generátorokat, ezzel együtt „álvéletlen” kulcsokat kezdtek használni. Mivel egy folyamkódoló által alkalmazott függvény minden pillanatban (minden karakter után) megváltozhat, így a függvény kimenetének nem csak az aktuális karaktertől, hanem egy belső *M* állapottól is függenie kell. A belső *M* állapot értéke minden lépés után átformálódik a $g_{(k)}$ transzformációs függvény kimenetének eredményeként. Az „álvéletlen” generátor tehát a $g_{(k)}$ függvényből és az *M* állapotból tevődik össze. A kódolt adat biztonsági foka tehát $g_{(k)}$ komplexitásától és az *M* belső állapotok számától függ.

Az $f_{(K)}$ kódoló függvény ezzel szemben nagyon egyszerű felépítésű, kizárólag *XOR*, vagy *ÉS*[47] kapukból épül fel, a gyakorlatban állapotgépekkel könnyen kivitelezhető.

Ha egy állapotgép *n* számú tárolóval bír, abban az esetben *2n* db belső *M* állapot megkülönböztetésére képes. Az állapot-transzformációs $g_{(K)}$ függvény kombinatorikai logikai elemekből áll. Az állapotgépek fejlesztése és implementálása rendkívül leegyszerűsödik, ha lineáris visszacsatolt shiftregisztereket[48] használunk.

A shiftregiszterek flip-flopok[49] soros, és időzítő bemenetek párhuzamos kapcsolásaként tekinthetők, ahol az *n.* kimenet az *n+1.* bemenettel van kapcsolatban A flip-flopok celláinak tartalma minden órajel következtében 1-gyel eltolódik, a kimenetet pedig az utolsó flip-flop adja. [9]

Egyéb biztonsági javaslatok

A ***Hash[50]-alapú hozzáférés-vezérlés*** esetében, az olcsó smart címkék[51] erőforrás-gazdálkodását figyelembe véve az alábbiakban egy egyszerű – egyirányú hash függvényeken alapuló – biztonsági eljárás kerül bemutatásra. Az séma megvalósítása jellemzően hardveres. A zárolt vagy feloldott állapotban is működő tag-

45 Gilbert Sandford Vernam – 1890. április 3 - 1960. február 7 ideális folyamkódoló szabadalmát tartják minden idők legjelentősebb kriptográfiai szabadalmának.

46 XOR logikai művelet – Kizáró vagy, Aritmetikai logikai egység

47 ÉS kapu– logikai alapműveletet megvalósító áramkör

48 Shiftregiszter – A bemenő bitje az utolsó kimeneti bittől függ.

49 Flip-flop – (bistabil multivibrátor) digitális hálózati elem

50 Hash – Egy olyan informatikában használt matematikai algoritmus, amely végtelen hosszúságú adatot véges hosszúságra képez le.

51 smart címkék – egy öntapadós címkéből áll, melybe ultra-vékony hártyaként van beágyazva egy RFID tag.

ek mindegyike egy kis szeletet különít el memóriájából ún. *metaID*[52]-k tárolására. Egy tag zárolásához annak tulajdonosa egy véletlen kulcs *hash*-elt változatát, mint a tag *metaID*-jét tárolja el a transzponderben. *(metaID ‹ hash(kulcs))*. Ez történhet akár RF[53], akár – a megnövelt biztonság miatt – közvetlen fizikai módszerrel. A zárolást követően a felügyelő mind a kulcsot, mind pedig a *metaID*-t egy *back-end*[54] adatbázisban menti el.

A transzponder a *metaID* vételekor zárolja sajátmagát. Ebben az állapotban minden kérésre kizárólag *metaID*-jével válaszol, egyéb aktivitás nem jelentkezik.

A feloldáshoz a gazda lehívja a tag *metaID*-jét, az adatbázisában megkeresi a alkalmas kulcsot, majd ezt visszaküldi a transzpondernek. A tag hash-eli a kulcsot, aztán összehasonlítja a saját *metaID*-jével. Amint ez a két hash megegyezik, úgy feloldja önmagát, és teljes funkcionalitást nyújt a környező olvasók számára. A nem zárolt tag-ekkel történő visszaélések megakadályozásához a tag-eket csak az információfolyam idejére érdemes feloldani a zárolás alól.

Az egyirányú hash invertálásának nehézségét kihasználva a módszer biztos védelmet nyújt az illetéktelen hozzáférések ellen. A *spoofing*[55] kísérletek ellen azonban védelmet nem, csak detektálási lehetőséget biztosít. A támadó előbb lehívja a tag *metaID*-jét, majd a visszajátszásos támadás során egy hiteles olvasónak láttatja a tag-et. A lekért *metaID*-hez a valóban hiteles olvasótól megkapja az ID-t, amit alkalmaz a *spoofolt* olvasónak küldött lekérdezések során a kiszemelt tag-gel való kapcsolatfelvételhez.

Továbbá az olvasó a tag-ek tartalmát is ellenőrizheti a *back-end* segítségével. Bármilyen inkonzisztencia esetén riasztást küld az olvasónak egy esetleges *spoofing* támadásról.

Az algoritmus nagyon egyszerű: mindössze a hash függvények implementálását igényli a transzponderekben, valamint egy terjedelmesebb nyilvántartást a *back-end* adatbázisokban. Az eljárás rendkívül rugalmas, könnyen bővíthető pl. többszörös hozzáféréssel, vagy éppen írás-felügyelettel.

A *metaID*-k egyszerű lekérdezhetősége ugyanakkor könnyű háttéradatbázis kiépítési lehetőséget kínál *thirdy-party*[56] gyártók részére, ezzel egyidejűleg a *metaID*-k egyedisége könnyű azonosítási lehetőséget is nyújthat.[9]

Véletlenszerű hozzáférés-vezérlés esetén, ez a séma egy kisszámú tagpopuláció esetén hatékonyan működő egyirányú hash függvényeket használó megoldás, mely megelőzi a jogosulatlan lekéréseket, míg a hiteles olvasók kéréseire változatlanul válaszképesek maradnak a tag-ek.

Míg az előzőekben transzponderei egyirányú hash függvények számítására voltak alkalmasak, úgy itt ezen felül véletlen számokat is generálhatnak. Az olvasó kérésére a transzponder itt előbb egy véletlen számot, majd az ID és a véletlen szám egy beírtjának hash-sel képzett kivonatát adja vissza, tehát *(r,h(ID||r))*-t.

52 metaID – meta azonosító

53 RF – (Radio Frequency) rádiófrekvencia

54 A back-end adatbázis tárolja az adatokat, de nem tartalmazza a végfelhasználói alkalmazás elemeket.

55 spoofing – adatkommunikációs teljesítményjavításra használt protokoll

56 „Harmadik fél” gyáró – nem kapcsolódnak a felhasználóhoz

Az olvasó *brute-force*[57] módszerrel megkeresi a kiválasztott transzpondert. Ehhez lehívja adatbázisából az összes ID-t, majd hasheli a tag-ektől kapott *R* számok ismeretében. Kisszámú létszám mellett ez egy igen gyors és hatékony megoldás. A gyakorlatban elegendő is lehet ez a séma, elméleti robosztusságát vizsgálva azonban aggályok merülnek fel.

Az egy irányú hash függvények magukban hordozzák azt a problémát, mely a kimenet inverzének előállításakor jelentkezik. Nincs garancia a diszkrécióra, mivel technikailag engedélyezett a bemeneti bitek felfedése. Az séma biztonságát erősebb alapokra kell helyezni, hogy megbizonyosodhassunk az ID bitjeinek titkosságáról. [9]

Az aszimmetrikus kulcsegyeztetés esetében, az olvasók sokat nyerhetnek az uplink és downlink[58] csatorna közötti aszimmetriából, lehallgatásra érzékeny adatok átvitele során. Ha egy olvasó üzenetet akar küldeni egy kiválasztott transzpondernek (az üzenetet jelöljük *v*-vel), elég, ha a tag egy véletlen *r* számot generál, majd visszaküldi az olvasónak. Ebből az *r* értékből az olvasó kiszámít, majd elküldi ezt a tag-nek. A visszirányú csatorna hatósugarán kívül eső lehallgató csak ezt a *vΘ r*-t hallja, amiből nem következtethet az eredeti *v* értékére.[9]

Chaffing és Winnowing59 módszer a lehallgatókat zavarja meg úgy, hogy a kommunikációt haszontalan tölteléküzenetekkel, ún. chaff-ekkel zavarja meg, melyet a transzponderek egy egyszerű MAC[60] segítséggel folyamatosan szűrnek (winnowing), amennyiben hasznos adat küldésére kerül sor.[9]

Észlelő egységek használata során az RFID rendszerek felszerelhetők olyan eszközökkel, melyek alkalmasak a jogosulatlan leolvasások észrevételére. Az erős downlink jel miatt más olvasók észlelése sem okoz gondot. A polcokba szerelt speciális felismerő egységek segítségével az esetleges szolgáltatásmegtagadással járó támadások (Denial-of-service, DoS[61]) idejében detektálhatók.[9]

Sikító tag-ek esetében szintén DoS támadások ellen alkalmazható sikerrel a fent említett egységek továbbfejlesztése, mely képes a kikapcsolt transzponderek észlelésére. Beállítható, hogy ezen állapotba kerüléskor a tag-ek egy adott frekvencián „sikítsanak", melyet az olvasó észlel, tudomást szerezve ezzel a nem üzemszerű leállásokról.[9]

A fenti felismerő egységek, mint ***„biztonsági ügynökök",*** bármely RFID olvasóba beépíthetők, de sikerrel alkalmazhatók mobil telefonokban és PDA[62]-kban is. Ebből adódóan a hiteles olvasó monitorozni, logolni[63] és szűrni tudja más olvasók lekérdezéseit, kiszűrve ezzel az esetleges illetéktelen kéréseket, de átengedve a hiteles forrásból származókat. Így az olvasók és transzponderek tulajdon-

57 brute-force – A teljes kipróbálás módszere, egy, a titkosító rendszerekkel szemben alkalmazott támadási mód, ami elvileg mindig eredményes.

58 uplink és downlink – Föld-levegő közötti telekommunikációs adatkapcsolat

59 Chaffing és Winnowing – „megtréfál és kiszűr" – Ez egy titkosítás nélküli „titkosítási" technika.

60 MAC – (Media Access Control) Közeghozzáférés vezérlés

61 DoS – (Denial of Service) Szolgáltatás nyújtását megtagadó támadási fajta

62 PDA – (Personal Digital Assistant) Kézi számítógép

63 Logolás – Adatnaplózás

képpen egy WPAN[64]-t alkotnak, és akár gateway[65]-ként is működhetnek a WPAN és a külvilág között. A leolvasási sebesség is növelhető egy helyi egységgel, mely a környező tag-ek tartalmát tárolja, így feleslegessé válik az összes tag hosszas lekérdezése. Juels[66], Rivest[67], valamint Szydlo[68] javasolja egy "blokkoló tag" alkalmazását is, mely néhány átlagos tag szimulációjával blokkolni képes az illetéktelen leolvasásokat. [9]

A produktum belsejébe ***nyomtatott master-kulcs*** teljes funkcionalitást biztosít a felhasználónak. Visszahozhatják a tag-et a hash-lock állapotból, unlockolhatják azt. A kulcs a termék belsejében kerül elhelyezésre, így megvétel előtt nem fedezhető fel. Esetlegesen a technika leszűkíthető kizárólag fizikai kontaktusra, eliminálva ezzel az RF csatorna tulajdonságaiból adódó biztonsági kockázatokat.[9]

Az RFID alkalmazása a dokumentum biztonság vonatkozásában

A biztonság *(Security)* és a veszélyeztetés nélküli állapot *(Safety)* fogalma ebben az esetben a digitális, a nyomtatott és másolt adatbiztonságot, a márka- és a csomagolttermék-biztonságot *(Digital and/or Photocopied/Printed Data Security/Information Security)* jelenti a jogosulatlan hozzáférés, az illetéktelen módosítás, a részleges vagy teljes törlés, rongálás, illetve a megsemmisülés ellen. Ami az adatok/termékek bizalmasságának, rendelkezésre állásának és sértetlenségének a teljes körű védelmét jelenti.

Az adatbiztonsági és védelmi eszközök rendszere

A védelmi eszközök – az észlelhetőség módjától és mértékétől függően – az alábbi csoportokat különböztetjük meg:

- szabad szemmel észlelhető *(Overt Security Solutions)* típusok;
- szabad szemmel nem észlelhető, nagyítóval, mikroszkóppal érzékelhető *(Covert Security Solutions)* típusok, például a nyomtatott mikrokarakterek, mikrokódok;
- csak gépi eszközök segítségével rekonstruálható karakterekből, vonal-, szín-, mágneses vagy egyéb kódjelsorozatokból álló, megfelelő sugárzások (lézer-, UV-, infra-, rádió-, röntgenes elektronsugár) segítségével, továbbá kémiai reagensekkel láthatóvá tehető karakterek és jelek.

Mivel a digitális adatok, nyomtatványok és másolt dokumentumok ellen támadást intézők is folyamatos innovációban vannak, a támadások technikái, technológiái folytonos változásban vannak. Így a védelmi eszközök sem lehetnek állandóak, hanem – a vírusirtó programokhoz hasonlóan – folyamatos fejlesztésükre van szükség. [2]

64 WPAN (Wireless Personal Area Network) – Vezetéknélküli priváthálozat

65 gateway – Átjáró

66 Dr. Ari Juels – RSA Laboratories Vezető tudósa és igazgatója

67 Ronald Linn Rivest – Professzor, USA

68 Michael Szydlo – kriptográfiai szoftverfejlesztő

RFID megoldások a dokumentumkezelésben

Dokumentumok RFID matricával történő azonosítása:

- Az RFID azonosító matrica formájában kerül a dokumentumra
- Az ütközésmentes technológia alkalmazásával akár több száz dokumentum azonosítása is megtörténhet másodpercenként, ideális irattári alkalmazás
- Magas biztonsági fokú iratok kezelése, a matrica rögzítheti, hogy kinek, mikor és meddig volt hozzáférése a dokumentumhoz [8]

Elektronikus festékek (E-Inks), mint a folyadékban diszpergált, pozitív töltésű fehér és negatív töltésű fekete részecskéket tartalmazó mikrokapszulákból álló anyag, amely a ráható mágneses vagy villamos erőtér polaritásától függően válik fehérré, illetve feketévé, annak síkbeli eloszlásától függően pedig értelmezhető vizuális információvá.[2]

Folyékony rádiófrekvenciás (RFID) festékek (RFID Ink Solutions). A Cross ID Communication Materials[69] által kifejlesztett anyag az általa le - adott rádiófrekvenciás jelek által azonosítja azt az anyagot, terméket, amelyhez belevegyítik. Nyomtató- és másolófestékbe keverten, hamisíthatatlan, biztonsági nyomdatermék előállítását biztosítja.[2]

Az „intelligens" papír (The Smart Paper), a jövő nyomathordozó-típusa, amely az anyagában, illetve a felületén elhelyezett félvezető polimerek, mikrocsipek, rádiófrekvenciás eszközök, nyomdai úton előállított integrált elektronikai elemek segítségével programozható.[2]

A Digitális vízjel a nyomtatott, másolt termékek piacán legelőször 1992-ben jelent meg. Állhat például csak géppel rekonstruálható szám- vagy kódkombinációkból és digitális aláírásból. A nyomathordozó-felületen elhelyezett vagy annak anyagába beépített (embedded), látható vagy nem látható vízjel és annak információtartalma, a védelmi céltól függően, a következőek lehetnek:

- szoftveresen védett, gépi karakterfelismerő (OCR) eszközökkel értelmezhető;
- optikailag változó (UV-, IR-fluoreszcens, foszforeszcens) nyomat;
- RFID-festékkel nyomtatott;
- a közfelhasználás részére elérhetetlen speciális (pl. nano-) festékkel nyomtatott;
- mágneses kód és jelkép (logo), vonalkód vagy színkód;
- holografikus/OVID-elem;
- beépített vagy nyomtatott mikrocsip;
- beépített vagy nyomtatott mikro-RFID;
- digitális vízjelek esetében: digitális aláírás, digitális szám-, mikro-karakterkombináció (mikro - szöveg), digitalizált mikrokép;
- végül lehet integrált rövid audio- és videotartalom is, illetve a felsorolt lehetőségek kombinációiból álló megoldás is.[2]

69 Cross ID Communication Materials – Fejlesztő cég, USA

Elektronikus biztonsági elemek integrálása a nyomtatott termékbe. Mikrochip-ek, rádiófrekvenciás eszközök, nyomtatással előállított integrált áramköri elemek, nyomtatott áramforrások stb.[2]

Nyomtatott integrált áramköri elemek felvitele a védett nyomatfelületre (Printable Integrated Electronics)Ez a megoldás alkalmazása is folyamatos emelkedést mutat. Elterjedése fokozatosan kiválthatja a korábbi integrált áramköri elemeket és áramkörgyártmányokat, alapjaiban megváltoztatva mai technológiai gyakorlatot, végképpen elektronikai jellegű iparággá átformálva a nyomda ipart is.[2]

A Jövő

Az egész világ izgatottan várja az RFID címkegyártó technológia robbanásszerű fejlődését. A kockázat, mely minden címkefeldolgozó piacra való belépését fenyegeti, a sok megválaszolatlan kérdésben keresendő, mint például:

- Mikor lesz az RFID-címkék ára gazdaságos és elfogadható olyan szinten, hogy be lehessen velük törni a tömegfogyasztás piacaira?
- Mikor jön el a megfelelő idő az RFID-technológiába való befektetéshez, hogy a befektetés jövedelmezzen is? Mikor lesz túl késő erre a lépésre?
- Mi a legjobb alkalmazható technológia az ügyfelek számára? Vajon képes leszek-e azt a technológiát kínálni, amit az ügyfelek elvárnak?

Amint az RFID-címke piac egyre jobban kifejlődik, úgy egyre több faktor fog érinteni a napról napra történő fejlesztés. Az új, második generációs chiptechnológiától, az új vezetőképes festék technológiától az új elképzelésekig, melyek az RFID felhasználását célozzák, egészen a törpülő világpiacig, egyszerűen nincs recept, ami alapján meg lehetne mondani, merre tart az RFID-technológia. De az tény, hogy valamerre tart, és fejlődik! És a mozgatórugókkal párhuzamosan haladva, a feldolgozók képesek lesznek válaszolni a piac és a technológia mozgására. Így egyben képesek is lesznek a legjobb döntés meghozatalára, mely megmutatja, hogy milyen szerepet is játszanak az RFID-címkék feldolgozásának terén.[11]

Várható fejlődés

A várható fejlődést két szinten lehet megfogalmazni: az eszközök képessége és az alkalmazások elterjedése szintjén.

Az egyedi rádiófrekvenciás eszközök (címkék, érzékelők) és rendszerek (nyomkövetők, irányítók) képességei mind memóriakapacitásban, mind a feldolgozási képességben növekednek. Ennek következtében egyre több információ tárolható a tárgyakkal (személyekkel) együttmozgó címkéken. Másik következmény, hogy – mivel az információ kódolható, a lekérdezéseknél visszakérdezhető a kérdező identitása, lehetségessé válik a naplózás – ez az információtárolás egyre biztonságosabb lehet.

A rádiófrekvenciás azonosító eszközök és rendszerek építőelemként vesznek részt nagyobb rendszerekben, alkalmazásokban. Széleskörűen elterjednek a tárgy-azonosító rendszerek, és ezekre hatékony logisztikai alkalmazások épülnek, amelyek megbízhatóbbá teszik az üzleti és kereskedelmi folyamatokat, valamint a védelmi szférában történő alkalmazhatóságukat. A személyazonosításban a rádió-

frekvenciás azonosítást elsősorban a meglévő szolgáltatási viszonyok és a jogosultságok ellenőrzésében használják. Tartós személyazonosításhoz ezek a technológiák csak, mint hordozó technológiák jelennek meg és kombinálódnak más személyazonosítási technológiával, például biometrikus adatok tárolásával és ellenőrzésével. A jogosultság-ellenőrzés nemcsak az üzleti életben, de a közszolgálatban és az intelligens otthonokban is elterjed. [7]

A védelmi szektorban történő várható alkalmazása főleg abban az esetben fog megnőni, amennyiben a korábban tárgyalt információbiztonsági technológiák beépülnek a mindennapi használatba. Abban az esetben a katonai logisztikában, főként a raktározásban kaphat egyre nagyobb szerepet. De a dokumentációvédelemben is várható az elterjedése, főleg a minősített adathordozók nyilvántartásában, valamint annak az életút-követésében. A nem minősített, de fokozottan érzékeny információkat tartalmazó dokumentumok, úgy, mint a személyes adatokat tartalmazó nyilvántartások, és a pénzügyi- analitikus kimutatások és nyilvántartások területén is várható az elterjedése.

Összegzés

A felölelt téma aktuális elemzése a jelen és a jövő fejlődő rádiófrekvenciás azonosítási és nyilvántartási rendszerek fejlesztéséhez járulhat hozzá. A minőségbiztosítás illetve az informatika által csökkenthető költségek kormányzatilag is támogatottak és egyre nagyobb szerepe lesz mind egyéni és vállalati szférában, mind a közszférában, azon belül is a honvédelmi szférában. Tehát a rádiófrekvenciás azonosítás és annak védelme információbiztonsági szempontok alapján az elkövetkező években mindinkább előtérbe helyeződik, fejlődik, és a cél olyan azonosítási eljárások kidolgozása, létrehozása, mely a felhasználók érdekeit leginkább védi és nem sérti a személyes adat védelméről szóló törvényt és megállapodásokat.

A bemutatott védelmi lehetőségek alkalmazásával, ez a technológia is megfelelően és megnyugtatóan biztonságossá tehető a mindennapi használathoz. Az alkalmazhatóság széles tárházából a dokumentumbiztonság területét szélesebb aspektusban megvizsgálva számos olyan lehetőség alkalmazhatóságát mutatta be, ami nem túl nagy innovációt követően megfelelően kielégítené a korunk elvárt védelmi kívánalmait.

A hétköznapokba is bevonuló megoldások legtöbbje utópisztikusnak hangzik, s némelyek még vitatottak is, de egyértelmű hogy az RFID terjedése megállíthatatlan. Az internet, a mobiltelefonok, a különféle elektronikus eszközök felforgatták az életünket, de ez semmi ahhoz, amit egy új technológia, a rádiófrekvenciás azonosítás alkalmazása fog majd okozni. A mindenre felragasztható, mindenhová beültethető, mindenre rányomtatható nagyfrekvenciás rádióhullámokkal kommunikáló chipek a logisztikától a kereskedelemig, az egészségügytől a határőrizetig, az oktatástól a büntetés végrehajtásig mindenhová betört és még be fog törni, s mérhetetlen mennyiségű feldolgozható adatot állít elő. Egyesek szerint azonban ez már egy megvalósuló utópia, a (cseppet sem) szép új világ kezdete. Ezért kell a technológiát a jogi háttérnek is minél szorosabban követnie, hogy adataink, információink védettek legyenek az arra illetéktelenekkel szemben.

Felhasznált irodalom:

[1] Biztonság http://www.nhit-it3.hu/index.php?option=com_content&view=article&id=6433%3Ait3-1-4-1&catid=17%3Abiztonsag&Itemid=900&lang=hu letöltve: 2011. július 20.

[2] Eiler Emil – A biztonsági nyomtatás a digitális adat, a védett márka és dokumentum , a csomagolt termék és a fogyasztó védelmére, MAGYAR GRAFIKA 2007/7

[3] Füzesi István - Herdon Miklós – RFID az élelmiszerek nyomonkövetésében http://terinformatika-online.hu/index.php?option=com_content&task=view&id=225&Itemid=46 letöltve: 2011. július 20.

[4] IT café – Európai megállapodás született az RFID-címkék etikus használatáról http://itcafe.hu/hir/eu_eb_rfid_intelligens_cimke_kroes.html letöltve: 2011. július 20.

[5] Juhász Éva – RFID - egy aktuális kérdés (2011. július 20.) http://krono.inaplo.hu/index.php/inter/8-networkstudies/916-rfid-egy-aktualis-kerdes

[6] Kis Attila – RFID Megoldások-[Online] http://www.allaminyomda.hu/file/1000098 letöltve: 2013. október 10.

[7] Kósa Zsuszanna – Rádiófrekvenciás azonosítás (és ami utána következik) http://www.nhit-it3.hu/index.php?option=com_content&view=article&id=6479%3Ait3-2-2-3-u&catid=61%3Aradiofrekvencias-azonositas-es-ami-utana-koevetkezik&Itemid=913&lang=hu letöltve: 2011. július 20.

[8] Rácz László – RFID-Radio Frequency Identification-[Online] http://www.allaminyomda.hu/file/1000185 letöltve: 2013. október 10.

[9] RFID rendszerek vizsgálata felhasználás és technológia szempontjából – Egyetemközi Távközlési es Informatikai Központ (ETIK), BP. 2006. szeptember

[10] Sárkány Márta – Automatikus azonosítás -AUTOMATIC identification, Elektronikus tananyag GDF hallgatói CD.

[11] Szabó Szabolcs – RFID, amit egy címkegyártónak feltétlenül tudnia kell, MAGYAR GRAFIKA 2007/2

[12] Sziklai Péter – Nagy Dániel – Ligeti Péter – Rádiófrekvenciás azonosítás és biztonság, Magyar Tudomány, 2007/07 904. o.

[13] T-SYSTEMS – RFID rendszerek és felhasználásuk-[Online] http://www.t-systems.hu/static/sw/download/RFID_rendszerek.pdf letöltve: 2010. november 12.

[14] Zsámboki Gábor – A papír nélküli, digitális világ már hamarosan elérhető [Online] http://www.any.hu/file/1000184 letöltve: 2010. november 12.

[15] 2009. évi CLV. törvény a minősített adat védelméről

[16] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[17] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

[18] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[19] ANSI/INCITS/ISO/IEC 9798-2-1999– Információ-technológiai, információbiztonsági szabvány

[20] Common Criteria MSZ ISO/IEC 15408 – Az informatikai biztonságértékelés közös szempontjai

[21] COBIT 4.1 – Control Objectives for Information and related Technology – informatikai szabályozási keretelvgyűjtemény
[22] MSZ ISO/IEC 27001 – Az információbiztonság irányítási rendszerei. Követelmények
[23] Az Európai Közösségek Bizotságának 2009/387/EK számú ajánlása (2009. május 12.) a magánélet- és adatvédelmi alapelveknek a rádiófrekvenciás azonosítás által támogatott alkalmazások területén történő alkalmazásáról
[24] ITIL – IT INFRASTRUCTURE LIBRARY MSZ ISO/IEC 20000-1:2007 szerinti tanúsítás Informatika. Szolgáltatásirányítás

Alcatel-Lucent Magyarország Kft.

A COORDINATED VIRTUAL INFRASTRUCTURE FOR SDN IN ENTERPRISE NETWORKS

Software Defined Networking (SDN), OpenFlow and

Application Fluent Programmable Networks

STRATEGIC WHITE PAPER

Increasing agility and automation in the data center to optimize application delivery requires a complete, end-to-end, coordinated virtual infrastructure. This infrastructure will allow applications and the physical network to collaborate, thereby providing a high quality experience for users and enabling optimization of resources. The ideal solution should follow a Software Defined Networking (SDN) approach. This will allow it to bridge the gap between the network world and the newly virtualized compute world by defining a framework that uses standardized interfaces between applications and networks. Likewise, it should be flexible enough to leverage multiple methods, including OpenFlow, to provide direct access to all virtual and physical objects in the data center and enable manipulation of the forwarding plane of physical and virtual network devices, such as switches and router.

Increasing Agility and Automation in the Data Center

A completely disruptive technology has been introduced to data center computing over the last decade. Virtualization has provided enormous flexibility, including the ability to dynamically optimize resource utilization based on workloads. As a result, application architectures have evolved. Applications can now be decomposed into components that run in their own virtual machine containers while sharing the same physical server. Virtual machines delivering a single application can be spread across multiple servers in the data center (or even between data centers) and moved rapidly between servers to optimize delivery performance. In effect, virtualization has enabled significant automation and cost reduction in the data center.

Unfortunately, this new found flexibility at the data center computing level has not been matched by an equivalent capability within the physical network. Today's data center network has very little awareness of the applications that are generating traffic and, conversely, the new virtual application control systems are unaware of the conditions prevailing within the network. Thus the network and the applications are operating in silos and any attempt by the network or the application controllers — the hypervisor — to improve network resource utilization usually leads to sub-optimal results.

With automation and the ability to rapidly shift workloads between servers in the data center come new requirements that the network and network management systems were never designed to handle.

All nodes in the network of today possess a limited view of the global state of the network because they operate solely by distributed control schemes. This results in a very robust solution for delivering highly available networks. But optimizing delivery performance for applications that are spread across several servers, rather than deployed on a single server, requires a global view of the conditions prevailing within the network. In many cases, time-intensive and error-prone manual intervention on the part of the network team is required when a virtual machine is moved. In other cases, network teams have been able to deploy maintenance intensive in-house solutions using scripting tools. This effectively defeats the intended goal of rapid compute workload optimization.

Increasing agility and automation in the data center to optimize application delivery can best be achieved with a complete, end-to-end, coordinated virtual infrastructure. This infrastructure will allow applications and the network to collaborate to provide a high quality experience for users and enable optimization of resources. To support this architecture the network must be equipped with:

- **Programmability,** which will provide a link between the application control and network control layer. This will enable an orchestrated capability to optimize application delivery performance and increase visibility.
- **Application fluency,** which will allow the network to automatically identify and provision applications and react to any subsequent movement of compute resources, such as virtual machines. This will unleash the workload optimization capabilities now available for computing and enable the network to dynamically adjust to application traffic flows, thereby tuning the network to provide a high quality user experience.
- **Global control view,** which will be maintained by the network to provide application and network control systems a global view of network conditions. This can be used to improve local decisions made by individual network nodes on how to treat traffic streams of a particular application, as well as improve decisions made by application control systems concerning placement of virtual machines.

This paper outlines a practical approach to delivering a Software Defined Network (SDN) for enterprises with a coordinated virtual infrastructure. It provides an overview of SDN and OpenFlow to de-mystify these terms. And it outlines the Alcatel-Lucent Enterprise perspective on how programmability, application fluency and a global control view can be achieved for an enterprise with smaller scale computing needs than those in service provider or Web scale data centers.

Software Defined Networking (SDN) and OpenFlow

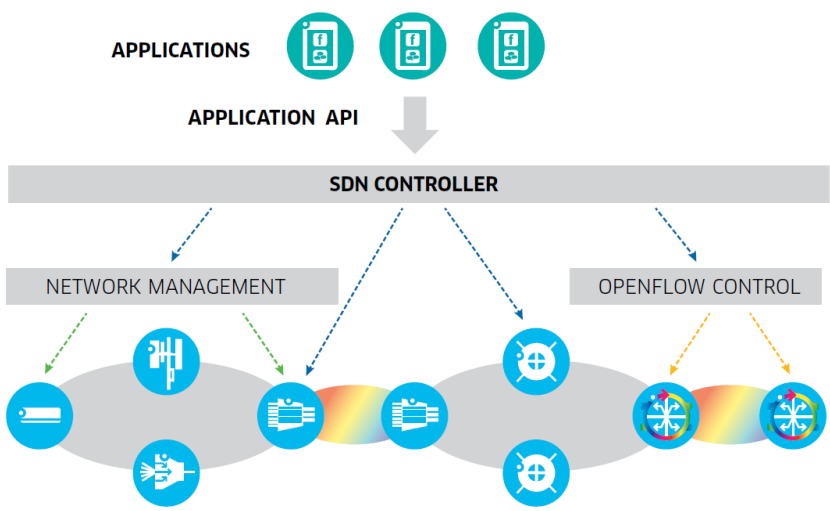
SDN and OpenFlow have been introduced to the networking world in an attempt to automate configuration changes in data center networks. To date, these new network additions have been used in very large scale computing environments, such as public clouds and web scale data centers. SDN and OpenFlow are quite different and should not be referred to interchangeably.

What is SDN?

SDN is an approach to bridging the gap between the network world and the newly virtualized compute world by defining a framework that uses standardized interfaces between applications and networks. Currently, industry attention is focused on southbound Application Programming Interfaces (APIs) that detail how an SDN framework interacts with the network. A number of communication protocols and interfaces, including existing protocols such as NetConf and Simple Network Management Protocol (SNMP), as well as new approaches based on web services, such as Representational State Transfer (RESTful) and Simple Object Access Protocol (SOAP) APIs are being discussed and can be used to realize this. OpenFlow is another such protocol.

SDN also implies developing an understanding of a global control view for the network and managing the network as a single unified abstraction. With the introduction of APIs and a global control view, SDN makes the network control plane remotely accessible and modifiable via applications that leverage open protocols. Network control and decision making can become partially centralized in SDN controllers, which maintain a global view of the network. As a result, the network appears to the virtualized application control layer as a single, logical switch (Figure 1).

Figure 1. Software-Defined Network Architecture



At the time of writing, it was not clear if this new centralized control view should be maintained as a separate SDN controller or become a function of the network provided by an existing network element for enterprises where the scale requirements are less than that of public cloud providers or providers of web scale applications.

What is OpenFlow?

OpenFlow is a technology. More specifically, it is a protocol being standardized by the Open Networking Forum. It provides direct access to and manipulation of the forwarding plane of network devices, such as switches and routers, over a network. This includes both physical devices and virtual switches. In this way, it allows the path of network packets through network switches to be determined by software running on multiple routers.

The OpenFlow protocol is based on a completely centralized control plane that is separated from the forwarding plane of the network nodes, unlike the networks of today where control and forwarding planes are both distributed in each network node. This centralization of control enables more sophisticated traffic management than is feasible using access control lists (ACLs) and routing protocols at each individual switch.

An SDN controller can use the OpenFlow protocol if it is realized on both the SDN controller and network nodes implementing the forwarding plane. OpenFlow allows the SDN controller to adjust the operation of the forwarding plane on a per flow basis.

At the moment, OpenFlow is primarily focused on data center and isolated enterprise network implementations. Google® is deploying an intra-D.C. network with OpenFlow, where the protocol is used as a traffic engineering tool, similarly to what Multi-Protocol Label Switching (MPLS) has been used for so far. Other implementations are focused on network virtualization in cloud computing environments where OpenFlow is used to control overlay networks. At present, potential service provider use-cases are around traffic-steering and hybrid-cloud/cloud-bursting, although there is no clear view on whether existing network features/protocols can be re-used or a new set of control and forwarding toolkits must be defined.

SDN and OpenFlow

SDN is an approach, OpenFlow is a technology and they are complementary.

The goal of SDN is to enable existing networks to become more adaptable to applications. More importantly, it can be used to bridge the gap between application control and network control elements, thereby allowing a coordinated effort to optimize application delivery performance. It can also provide an evolutionary path to complete network programmability by application control platforms. In addition, it can provide the means to add application level programmability to existing networks, as well as OpenFlow-enabled networks.

OpenFlow is one of several mechanisms that can be used to enable control of the forwarding behavior of network nodes by external elements. It is certainly one of the potential building blocks that can be used to deliver SDN. It provides a basic mechanism to program flow entries in a network node from an external controller. But it should be noted that several other methods already exist to achieve the same functions. OpenFlow alone is not sufficient to realize SDN, but SDN can be realized without OpenFlow. OpenFlow is focused initially on the interaction between the network control plane and forwarding plane. It leaves “northbound” APIs to application control platforms for later versions. OpenFlow assumes all control capabilities are removed from network nodes, providing forwarding

without offering a sufficient scalability model for the newly proposed network architecture. Also, OpenFlow does not define mechanisms for interacting with existing control planes in today's network elements, a necessity for environments that must have backwards compatibility with existing network infrastructures. In addition, OpenFlow does not consider how the new SDN control plane should interact with current network management platforms.

Building a Coordinated Virtual Infrastructure in Enterprise Networks

Defining the requirements

To build a coordinated enterprise virtual infrastructure, one must first consider the scale of the network in question, as well as desirable properties of current networks that should be maintained. For example, an enterprise network infrastructure is highly resilient and provides high performance in terms of bandwidth and ability to monitor application flows. This infrastructure, based on standard protocols, provides a resilient distributed control capability with a high degree of scalability and rapid recovery times upon failures. Therefore, any new solution that follows an SDN approach to deliver increased automation and coordination between the network and the applications should capitalize on existing capabilities and enhance them with additional functionality.

Understanding the limitations of current approaches

Efforts to date to realize SDN using OpenFlow and orchestration platforms, such as Open Stack and Cloud Stack, which have been focused on very large scale data centers have required large teams of experts to deliver the final solution. There are significant limitations to these solutions when the requirements of a typical enterprise are taken into account:

- A completely centralized control model as proposed with OpenFlow is not scalable, especially from the perspective of monitoring application flows.
- Smaller enterprises typically require simpler solutions with higher levels of automation built-in.
- There is no model for deployment alongside existing networks, which implies a "rip and replace" strategy is required for conversion of existing networks.
- There is a limited model for how OpenFlow-enabled networks interface with existing network management platforms and troubleshooting tools.

All of these issues must be addressed in a complete solution that can be successfully deployed in today's enterprises.

Desirable properties for a coordinated virtual Infrastructure

The ideal way to deliver automation to the network following an SDN approach is to provide programmability, application fluency, and a global control view, which will make it easier to virtualize the network and establish a control model that parallels the one established for applications. This solution should make use of standardized interfaces between applications and networks, as they become

available, and provide a "plug-and-play" environment with a single pane of glass for management across applications and the network.

Programmability

Programmability will enable an orchestrated capability to optimize application delivery performance and provide increased application performance visibility for both the net- work and application control platforms, thereby removing the current division between applications and the network.

Increased programmability will require a rich set of capabilities from the network to link with application control platforms to share a global view of network status derived from information collected at each network node. And it will require the application control platform to issue requests to the network. These links can be delivered by network management platforms or from one of the network nodes, such as a core switch within a data center network in smaller enterprises or a separate network element in larger enterprises.

Application Fluency

Application fluency will allow the network to automatically react to the movement of compute resources, such as virtual machines, to unleash the workload optimization capabilities now available for computing and dynamically adjust to application traffic flows to provide a high quality user experience

An application fluent network benefits from increased autonomous decision making capabilities of network nodes making use of a rich feature set for user, device, virtual machine and application profiling. Profiles allow the network to collect and act upon information on the types of users, devices, virtual machines and applications that connect across the network to ensure a high quality experience. The profiles should provide the network with provisioning information, the security profile required by each user or device, the quality of service (QoS) requirements, and the priority of each user or device within the network.

By using profiles, the network can recognize users, devices, virtual machines and applications to automatically bind them to a profile, and to take autonomous action based upon the perceived state of an application. The network is also able to automatically discover the location of a user or device by monitoring traffic on a specific switch port. It can automatically provision the user and device on that switch port, including security and initial QoS parameters. And it can designate conversations initiated by a particular user on a specific device that are to be measured for actual QoS received.

Global Control View

A global control view will improve local decisions made by individual network nodes on how to treat traffic streams of a particular application, as well as improve decisions made by application control systems concerning placement of virtual machines.

Providing a global control view requires a continued migration to a model for network control that should follow a hybrid approach, while maintaining a degree of autonomy and distributed control within each network node. This is in contrast

to a completely centralized control model. The global control view will be assembled by collecting event information at each network node and assembling an abstract view of end-to-end net- work status. This view can be shared with each network node to improve local decision making and via standard APIs to application control platforms.

The Alcatel-Lucent Coordinated Virtual Infrastructure

For some time now, Alcatel-Lucent has recognized the need for enterprise networks to be more aware of the applications that they transport. It has developed an Application Fluent Programmable Network optimized to provide programmability, application fluency, and a global control view for enterprise scale networks.

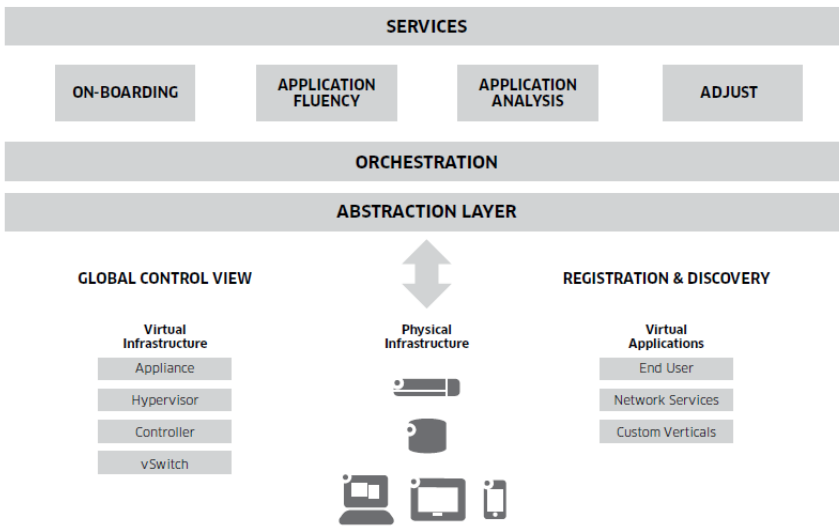
The Alcatel-Lucent solution follows an application fluent approach that:

- Increases embedded information on the types of users, devices and applications that connect across a network through embedded network profiles: User Network Profile (uNP) and Virtual Network Profile (vNP)
- Improves the ability of each network node to take autonomous action based upon the perceived state of the application through:
    - Automatic binding of devices and users upon network access to a uNP to support automatic assignment of security and QoS policy
    - Automatic binding of vNPs to virtual machines in the data center to support automatic provisioning, assignment of security and QoS policy with the network to allow the network to automatically adapt to virtual machine movement
- Enables links between existing network management platforms and application control platforms for improved visibility on virtual machine location and movement with the Alcatel-Lucent OmniVista™ Virtual Machine Manager (VMM).

The Alcatel-Lucent framework for delivering a coordinated virtual infrastructure is shown in Figure 2. Three types of operational elements are located in the data center:

- Virtual infrastructure, which is comprised of appliances, such as WAN optimization, hypervisors, controllers, such as OpenFlow controllers, and virtual switches
- Physical infrastructure, which is comprised of servers and switches
- Virtual applications, which is comprised of end user applications, such as unified communications and virtual desktop, services, such as security, and vertical specific applications, such as media control.

Figure 2. One coordinated virtual infrastructure



Network capabilities specific to delivering a coordinated virtual infrastructure include:

- An abstraction layer that removes detail from upper layers of the framework concerning the interfaces of each element in the data center and the programmable capabilities that each element possesses. Each element in the data center can either be discovered or will register itself with the fabric establishing a two way communication with the fabric.
- An orchestration layer that controls the delivery of SDN like applications.
- A services layer that can be expanded as new SDN use cases relevant to the enterprise are discovered. The initial service categories that support current SDN use cases include:
    - On-boarding, which are services targeted to bring into service all the elements in the data center, such as boot services, Dynamic Host Configuration Protocol (DHCP), IP address management and Domain Name System (DNS)
    - Application fluency, which are services that discover context (user, device, business priority of the conversation) for each application using the network and direct how to fine tune the network to provide a high quality end user experience
    - Application analysis, which are services that measure and make visible actual service levels provided to applications using the network

- Adjust, which are services that tune how the traffic flow of a specific application is treated by the network

Finally, when considering the entire physical infrastructure for application delivery, the end user devices must also be included, as shown in Figure 2.

The Alcatel-Lucent approach encompasses the goals of SDN while resolving the capability gaps that exist in current approaches. It envisions a role for SDN in enterprise networks that extends beyond the data center to include the entire corporate network. It also goes past simply automated configuration of network elements to focus on the entire user experience. With this approach:

- The scalability of current networks is maintained because individual network elements can continue to operate and make autonomous decisions on how to handle application traffic — even if the global control view becomes unavailable
- Enterprises that do not have teams of skilled programmers can benefit from a solution that is designed for their current size, leveraging existing management platforms and switches with additional automation built-in
- Existing network architectures, physical elements and management platforms can be easily and cost-effectively leveraged through an evolutionary approach to network development, rather than a revolutionary approach

Conclusion

Today's data center network has very little awareness of the applications that are generating traffic and, conversely, the new virtual application control systems are unaware of the conditions prevailing within the network. Thus the network and the applications are operating in silos and any attempt by the network or the application controllers to improve resource utilization usually leads to sub-optimal results.

To date, SDN has been used primarily on service provider and web-scale data centers to bring automation to the network for configuration. But there are limitations to cur- rent approaches to implement SDN, such as scalability and compatibility with existing networks. These limitations often make current solutions not applicable for a typical enterprise network.

The ideal solution to delivering automation to an enterprise network using an SDN approach is to provide programmability, application fluency, and a global control view. This will allow the network to be virtualized and establish a control model for the net- work that parallels the control model established for applications. This solution should make use of standardized interfaces between applications and networks, as they become available, and provide a "plug-and-play" environment for the network with a single pane of glass for management across applications and the network.

Alcatel-Lucent has recognized the need for enterprise networks to be more aware of the applications that they transport and has developed an Application Fluent Programmable Network optimized to provide programmability, application fluency, and a global control view. The Alcatel-Lucent approach to application fluent network infrastructures encompasses the goals of SDN while resolving the capability gaps that exist in the current approaches to SDN. In addition, the Alcatel-Lucent vision for SDN in enterprise networks extends beyond the data center to include the entire corporate network. It goes past simply automated configuration of network elements to focus on the entire user experience.

Acronyms

Term	Definition
ACL	access Control List
API	application Programming Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
MPLS	Multi-Protocol Label Switching
RESTful	Representational State Transfer
SDN	Software Defined Networking
SOAP	Simple Object Access Protocol
SNMP	Simple Network Management Protocol
QoS	quality of service
uNP	user network profile
vNP	virtual network profile

References

[1] ONF White Paper – dated April 13, 2012. Software-Defined networking: The New Norm for Networks https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf www.opennetworking.org

[2] Alcatel-Lucent SDN-OpenFlow Position Statement – May 2012-07-26

SZILÁRD Anikó[1]

SZEMÉLYES ADATOK VÉDELME AZ INTERNETEN

Rezümé

Napjainkban az információs társadalom korát éljük, ami a globalizáció hatására világméretűvé nőtte ki magát. Az internet az információs társadalom alapvető kommunikációs közege, ami megkönnyítheti mindennapi életünket, munkánkat, de lehetnek árnyoldalai is. Felvetődnek olyan megoldandó problémák, kérdések, miknek megválaszolása szabályozása nem csupán egy ország belügye, hanem a világhálót használó nemzetek megoldásra váró problémája. Közös konszenzust kell kialakítanunk, majd ezt követnünk például a személyes adatok védelme területén.

Az alábbiakban e problémakör nehézségeit próbálom bemutatni. Az emberek személyes adataik kezelése szempontjából országonként rendkívül eltérően bíznak meg kormányukban, illetve a vállalatokban. A személyes adatai védelméhez mindenkinek joga van, az ezzel való visszaéléseket szankcionálni kell. Meghatározásra kerül, hogy mit is tekinthetünk pontosan személyes adatnak. Láthatunk néhány példát, hogy a világhálón egy hétköznapi felhasználóról mennyi adatot gyűjtenek, elemeznek és értékelnek ki cégek, vagy akár magánszemélyek. Bemutatásra kerül a számítási felhő használata, ahol személyes adataink védelme jelenleg csak a bizalomra épülhet.

Bevezetés

A személyes adatok védelme emberi jog, érvényes rá az emberi jogok és az alapvető szabadságjogok védelmére vonatkozó egyezmény. Ami megállapítja a magánélet, családi élet tiszteletben tartásához való jogot, kiterjed a magán és személyes információkra és adatokra. A személyes adatok védelméhez való jogot az EU Alapjogi Chartájának 8. cikke elismeri, hogy

„(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

(2) Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.

(3) E szabályok tiszteletben tartását független hatóságnak kell ellenőriznie."

Személyes adatnak számít minden olyan – akár a magán-, akár a szakmai vagy közösségi életre vonatkozó – információ, amely egy adott személyre vonatkozik. Ez lehet név, fotó, e-mail cím, banki adat, egészségügyi információ, a közösségi oldalakon megjelenő üzenet vagy akár számítógépének IP-címe is, mivel az IP címből egyértelműen be lehet határolni az általunk használt számítógépet, úgy funkcionál, mint a lakóház utca, ház száma.

A digitális korban a személyes információk gyűjtése és tárolása elkerülhetetlen. Minden vállalkozás használ fel adatokat, a biztosítótársaságoktól a bankokon keresztül a közösségi oldalakig, keresőprogramokig.

1 MH Pápa Bázisrepülőtér, Híradó és informatikai részleg, Információvédelmi tiszt, aniko.szilard@gmail.com

Az adatok harmadik országokba való továbbítása a mindennapi élet egyik meghatározó kérdésévé vált. Az interneten nincsenek határok a felhő alapú számítástechnika (angolul „cloud computing") használata azzal is járhat, hogy az egyik országból elküldjük az adatokat feldolgozásra egy másik országba majd azok egy harmadikban kerülnek tárolásra.

Mi is az a cloud computing?

A felhő alapú számítástechnika a számítástechnika egy ágazata. Többféle felhő alapú szolgáltatást különböztethetünk meg, a közös bennük az, hogy a szolgáltatásokat nem egy dedikált hardvereszközön üzemeltetik, hanem a szolgáltató eszközein elosztva, a szolgáltatás üzemeltetési részleteit a felhasználótól elrejtve. Ezeket a szolgáltatásokat a felhasználók hálózaton keresztül érhetik el, publikus felhő esetében az interneten keresztül, privát felhő esetében a helyi hálózaton vagy az interneten.

A felhő alapú szolgáltatások három fő csoportja létezik:

- Szoftver szolgáltatás

A szoftvert magát nyújtja szolgáltatásként. Ezeket az alkalmazásokat általában http protokolon keresztül, egy böngészővel lehet használni.

- Platform szolgáltatás

Az alkalmazás üzemeltetéséhez szükséges környezetet biztosítja, terheléselosztással és feladatátvétellel, kezelő felülettel, ezek rendszeres biztonsági frissítésével.

- Infrastruktúra szolgáltatás

Virtuális hardvert (szervert, blokk-tárhelyet, hálózati kapcsolatot, számítási kapacítást) szolgáltat.

Hozzáférhetőség alapján:

- Publikus felhő

Publikus felhő esetén egy szolgáltatótó a saját eszközállományával (tárhely, hálózat, számítási kapacítás) szolgálja ki ügyfelei szerverigényeit. Publikus felhők esetén különösen fontos a különböző ügyfelek izolálása.

- Privát felhő

Saját vagy bérelt erőforrásokon lehet saját felhőt is építeni. Ez megoldást jelent a publikus felhők problémáira, viszont az üzemeltetésről a privát felhő tulajdonosának kell gondoskodnia.

- Hibrid felhő

privát és publikus felhők kombinációja. Ez lehetővé teszi átmeneti teljesítményigény esetén a számítási felhő kiegészítését publikus szolgáltató által kínált megoldással.

Egyéb kategóriák:

- Tárhely szolgáltatás

A tárhelyet adja, mint szolgáltatást.

Ide sorolhatjuk a biztonsági mentéseket és szinkronizácós szolgáltatásokat is.

A felhő alapú számítástechnika a 2010-es évek egy fő irányának számít. Manapság a személyes adatok vonatkozásában kell egy közös egyfajta „etikai kódexet" kialakítani. Erre természetesen a kezdeti lépések már megtörténtek. Érdemes belepillantani az európai adatvédelmi biztos véleményének összefoglalójába „A

számítási felhőben rejlő potenciál felszabadítása Európában" című bizottsági közleményről. – ben a következőket olvashatjuk:

„A számítási felhő a külső távoli IT-erőforrások igénybevétele révén számos új adatkezelési lehetőséget kínál a vállalkozások, a fogyasztók és a közszféra számára. Ezzel egyidejűleg számos kihívást jelent, különösen a számítási felhőkben feldolgozott adatokra vonatkozóan biztosítandó megfelelő adatvédelmi szint tekintetében. A számítási felhő-szolgáltatások igénybevétele komoly kockázatot jelent a tekintetben, hogy –amennyiben nem elég egyértelműek az uniós adatvédelmi jogszabályok alkalmazhatósági feltételei, és túl szűken határozzák meg vagy értelmezik a számítási felhősségét, vagy azt nem érvényesítik hatékonyan – a számítási felhő-szolgáltatást nyújtó szolgáltató által végzett feldolgozási műveletekkel kapcsolatban nem állapítható meg a felelős. Az európai adatvédelmi biztos hangsúlyozza, hogy a számításifelhő-szolgáltatások nem indokolhatják a hagyományos adatfeldolgozási műveletekre vonatkozóhoz képest alacsonyabb szintű adatvédelem alkalmazását." [1]

„ Az európai adatvédelmi biztos végül hangsúlyozza, hogy kezelni kell a számítási felhő által nemzetközi szinten támasztott kihívásokat. Arra bátorítja a Bizottságot, hogy indítson nemzetközi párbeszédet a számítási felhő által felvetett kérdésekről, beleértve a joghatóságot és a bűnüldöző szervek általi hozzáférést is, és felveti, hogy a véleményben érintett több kérdéssel a különböző nemzetközi vagy kétoldalú megállapodásokban, például a kölcsönös segítségnyújtási megállapodásokban és a kereskedelmi megállapodásokban is foglalkozhatnának. A bűnüldöző szervek adatokhoz való hozzáférésére vonatkozó minimális feltételek és elvek megállapítása érdekében nemzetközi szintű globális normákat kell kidolgozni. Az európai adatvédelmi biztos emellett támogatja hatékony nemzetközi együttmű ködési mechanizmusok felügyelőhatóságok általi kialakítását, különösen a számítási felhővel kapcsolatos kérdések terén." 2

Miért fontos az adatvédelem a személyes szabadság szempontjából?

Ha a 40-es, 50-es években találkoztak az emberek egymással, annyi információjuk volt a másikról, amennyit saját maguk elmondtak, vagy a szűkebb környezet megosztott velük.

Ma azonban információt gyűjtenek rólunk, ha belépünk egy bankba, internetezünk, bankkártyával fizetünk, de számos esetben elég, ha csak végigmegyünk az utcán.

Adataink megadását esetenként törvény írja elő, máskor megkönnyíti életünket, de előfordul, hogy tudtunkon kívül megszerzik őket. Ha adatainkat megadjuk egy harmadik személynek léteznie kell olyan szabályozásnak, amely meghatározza, ki, mely adatainkat és milyen célra jogosult felhasználni vagy továbbadni. A szabályozásnak tartalmaznia kell a mi jogainkat is, tehát annak a személynek (érintett) a jogait, akire az adatok vonatkoznak. Magyarországon a fent említetteket a 2011. évi CXII. törvény tartalmazza, egyértelműen meghatározza továbbá azt is, hogy mi is az a személyes adat:

2 Az európai adatvédelmi biztos véleményének összefoglalója „A számítási felhőben rejlő potenciál felszabadítása Európában" című bizottsági közleményről

„személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

különleges adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat; ”

Ha globálisan gondolunk a személyes adatok védelmére, hisz az internet használatával mást nem is tehetünk, napjaink problémája egy egészséges egyensúly kialakítása.

Az adatok szinte korlátlan mennyiségben egyszerűen továbbíthatók akár kontinensek között is, ez lehetővé teszi a nemzeti adatvédelem megkerülését egyszerűen úgy, hogy az adatot olyan ország szervereire juttatják el, ahol alacsonyabb szintű az adatvédelem. A személyes adataink árucikké váltak. Például a cégek árucikkeivé, hisz egy célirányos reklámkampány kidolgozásához jobb adathalmaz nem is kell, mint a szokásaink, szükségleteink megfigyelése. Ennek a globális adat halmaznak a gátlástalan fel- és kihasználása csak mindenki számára betartott ajánlásokkal, törvényekkel szabályozható.

Tegyünk egy kis visszatekintést a hazai adatvédelemben

1989. végén az alkotmány már elismeri a személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jogot Az adatvédelem, más néven az információs önrendelkezési jog az egyén „azon joga, hogy alapvetően maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról.” - mondta ki a 15/1991. (IV.13.) határozat.

Az állam, a gazdaság működéséhez, a társadalmi tevékenységek tervezéséhez, szervezéséhez egyre több információra van szükség és egyre több áll rendelkezésre. Az informatika rohamosan fejlődött.

Hiányzott egy átfogó szabályozás az adatok feldolgozásával és nyilvántartásával kapcsolatban. Az Országgyűlés megalkotta és 1992. november 17-én kihirdette a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényt, közismertebb nevén az adatvédelmi törvényt (Av.tv.). A törvény 2004. január 1-jétől hatályos módosítása átültette a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK európai parlamenti és tanácsi irányelvet.

2011.-ben az országgyűlés elfogadta az új adatvédelmi törvényt, amely hatályon kívül helyezte a 1992. évi LXIII. törvényt.

Az új adatvédelmi törvényben bővült a fogalom meghatározások köre az érintett fogalmával.

„Érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy.„ Új fogalomként jelenik meg az adatmegjelölés, amely az adat azonosító jellel való ellátása annak azonosítása céljából.

A törvény bevezette az adatfelelős intézményét is

Egy a XXI. században bevezetett törvénynél, vonatkozzon az bármely ország állampolgárainak személyes adataira - ami manapság még globálisan megoldatlan jogi, etikai, gazdasági problémákat feszeget, hisz az internetnek nincsenek határai, nincs egyértelmű tulajdonosa – elengedhetetlen, hogy a földrajzi országhatár ne szabjon gátakat a személyes adatainkkal kapcsolatos jogaink érvényesítésében.

Így például az új adatvédelmi törvény (Magyarországot tekintve) fogalom meghatározásai között szerepel az EGT – tagállam is, amely az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez.

Az adatkezelés elve

Az adatkezelés legfontosabb irányelve a célhoz kötöttség. A személyes adat kizárólag meghatározott célból kezelhető, csak a cél megvalósulásához szükséges mértékben és ideig.

Természetesen nem feledkezhetünk meg a tájékoztatási kötelezettségről sem. Ezt a 2011. évi CXII. törvény szintén részletesen szabályozza, melynek lényege, hogy az érintettel előzetesen közölni kell, hogy az adatkezelés vagy hozzájáruláson alapul vagy törvényi előírások betartása végett kötelező. Egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről az érintettet, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

Magyarországon jogorvoslatra ad lehetőséget a Nemzeti Adatvédelmi és Információszabadság Hatóság. A Hatóság feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése.

Személyes adataink kezelésének legsérülékenyebb pontja az internet

Az internetet tágabb értelemben információ megosztására és információ szerzésére használjuk. Így a kapcsolatteremtés gyakori és elengedhetetlen része az internet használatnak. Kapcsolatfelvétel során különféle személyes adatokat adunk meg.

Egy holnap felkeresésekor számítógépünk egyedi azonosító IP számát a felkeresett szerver a naplóállományában rögzíti.

Egy e-mail elküldésével nevünk, e-mail címünk továbbításával szintén továbbítódik IP számunk, mely alkalmas arra, hogy behatárolják pl. földrajzi elhelyezkedésünket.

Egy egyszerű hírlevélre történő feliratkozással is kialakul egy adatkapcsolat, mivel egy adott holnap tulajdonosai, szerkesztői a felhasználóval hosszabb távú kapcsolat kialakítására törekednek. A felhasználóikat rendszeres időközönként tájékoztatják aktuális ajánlataikról, akciókról, új szolgáltatásaikról, így hírleveleket küldenek ki. A hírlevélre való feliratkozáshoz általában az igénylő email címére és

nevére van szükség. A regisztrációt az igénylést követően kapott e-mailben kell megerősíteni. A fenn említett törvény értelmében a hírleveles oldalakat adatvédelmi nyilvántartásba kell venni, az oldalnak lehetőséget kell adnia, hogy a felhasználó bármikor ki tudjon jelentkezni és adatait töröltetni tudja az oldalról.

A regisztrációs űrlapok akár több tucat adat megadását is kérhetik. Az adatok köre lehet személyes adat (név, nem, születési adatok, lakóhely, e-mail, telefonszám, végzettség, foglalkozás, fény-kép, stb.), nem ritkán különleges adat (pl : káros szenvedélyre vonatkozó adatok).

Az érdeklődési terület vizsgálatához üzleti érdekek fűződnek, ugyanis a marketingnél ezek az adatok fontos szerepet kapnak, sokat érnek.

Internetes marketinget segítő eszközök például a cookiek.

„A cookie-k segítenek szolgáltatásaink biztosításában. Szolgáltatásaink igénybe vételével Ön beleegyezik a cookie-k használatába. „

Ismerős a fenti mondat? A Google -nál olvashatjuk minden keresés alkalmával!

Hogyan használja a Google a cookie -kat?

A cookie egy rövid szöveg, amelyet a felkeresett webhely küld el böngészőjébe. Segítségével a webhely megjegyzi a látogatásával kapcsolatos információkat, például a használt nyelvet és egyéb beállításokat. Ezáltal gördülékenyebbé válhat a következő látogatás, és könnyebb lesz a webhely használata.

Többféle célra használja fel a google a cookie-kat. Használatukkal például megjegyzi a biztonságos keresésre vonatkozó beállításait, hogy ezáltal releváns hirdetéseket jelenítsenek meg számunkra, számlálja, hogy hány látogató érkezett az adott oldalra.

Eközben minden olyan gép IP címe rögzítésre került, melyeken a hirdetés megjelent, így a felhasználók könnyen beazonosíthatóvá válnak.

Az adatgyűjtési módszerek száma kifogyhatatlan, mint ahogy felhasználási módjuk is.

Miért globálisak a problémáink?

Nemrég szinte bizonyosnak tűnt, hogy az uniós adatvédelmi reformmal kapcsolatban nem lesz egyhamar előrelépés. A megegyezést felgyorsította az Edward Snowden által kirobbantott amerikai megfigyelési botrány, amely nagy port kavart Európában is.

Az Európai Bizottság Angela Merkel német kancellár vezető szerepének elfogadását kérte a többi 27 tagállamtól az európai adatvédelmi reform kapcsán.

Merkel keményen kritizálta az amerikai internetes cégek, többek között a Google és a Facebook gyakorlatát azért, hogy európai ügyfeleik adatait kiszolgáltatták az USA hatóságainak. A fő probléma, hogy csak annak a tagállamnak az adatvédelmi szabályozására kell tekintettel lenniük a tengeren túli cégeknek, amely tagországban be van jegyezve európai részlegük. Így a szigorú német szabályozást megkerülhették például azzal, hogy a sokkal lazább kereteket szabó Írországban jegyezték be magukat.

Az egységes uniós szabályozás hatályba lépése után az ilyen kiskapuk megszűnnének.

Ugyanakkor a jelenlegi helyzetből üzletileg profitáló írek és britek nehezen adják fel saját, megengedőbb szabályozásukat. Lord McNally brit igazságügyi miniszter szerint a tervezett uniós adatvédelmi rendelet jelen formájában „nem biztosítja a kellő egyensúlyt" az üzleti érdekek és a személyes szabadságjogok védelme között.

Az Európai Unióban téma a „the right to be forgotten" néven emlegetett alapjog, mely alapján a felhasználók töröltethetnék a róluk szóló, nemkívánatos tartalmakat az internetről. A megoldást Facebook- szabálynak is nevezik, mivel főleg a közösségi oldalakat érinti. Magyarországon eddig nem igazán foglalkoztak vele, ahogy az itthoni vállalatok a megfelelő törlésekről sem gondoskodnak.

Ami az internetre egyszer felkerül, azt többé nem lehet letörölni: nagyjából ez a mai, találó közvélekedés.

De tényleg mindennek fenn kell maradnia a neten? Joga van-e a Facebooknak ahhoz, hogy a feltöltött képeket örökre eltárolja? Joga van a Google-nek ahhoz, hogy minden egyes kattintást eltároljon? Vagy ez a jog a felhasználóé? Melyik a fontosabb érdek: hogy a különböző emlékek, amiket gyártunk, az emberiség történelmének egy része örökre megőrződjön, vagy legyen jogunk hagyni, hogy tetteink feledésbe merülhessenek?

Felelniük kell e a tiniknek esetleg „csak egy fotóért" tíz, vagy húsz évvel később?

A Google volt vezérigazgatója szerint igen, az Európai Unió viszont nem osztja e véleményt.

Az Unió új rendeletének központi eleme az angolul „the right to be forgotten"-nek nevezett jog: a jogászok felejtés jogaként, illetve töröltetési jogként hivatkoznak rá.

A kifejezés lényege, hogy a személyes adatok kezeléséhez kifejezett személyes hozzájárulásra lesz szükség, ami ráadásul visszavonható, azaz a szolgáltatónak minden olyan esetben törölnie kell majd az eltárolt információkat, ha azok megőrzése egyértelműen nem indokolható.

Ha a szolgáltatók nem teljesítik a törlési kérelmeket, 2014-től mérlegelés után egységesen maximálisan éves globális bevételük két százalékára büntethetőek, ami jelentős összeg a Google vagy a Facebook esetében. Közintézményeknél és magánszemélyeknél az összeg felső határa 1 millió euró.

Az egész szabályozáshoz kapcsolódó probléma, hogy manapság, bár egyre több ehhez kapcsolódó incidensről hallani, gyakorlatilag nagyon kevesen foglalkoznak biztonságos adattörléssel. A használt számítógépeken tömegesen maradnak rajta személyes vagy céges adatok.

Hiányos adattörléssel kapcsolatban rengeteg példát találhatunk. Ma már szinte mindenkinek van okostelefonja, amely működéséből adódóan rengeteg személyes információt, kapcsolati adatokat telefonszámokat, képeket tárol. Ezekben SD - kártya van, az adat helyreállítás itt is megvalósítható.

2013. augusztus 25-én hatályba lépett az Európai Bizottság 611/2013/EU számú rendelete, amely részletesen szabályozza, hogy a nyilvános elektronikus hírközlési szolgáltatást nyújtó szolgáltatóknak milyen módon kell eljárniuk az előfizetők és egyéb magánszemélyek személyes adatainak megsértése (data breach) ese-

tén. A rendelet minden európai uniós tagállamban, így Magyarországon is hatályos és közvetlenül alkalmazandó.

Irodalomjegyzék

[1] A számítási felhőben rejlő potenciál felszabadítása Európában , 2012.09.27-i bizottsági közlemény Letöltve: 2013.09.29.

[2] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról Letöltve: 2013.08.23.

[3] http://eur-lex.europa.eu/lexuriserv/lexuriserv.do?uri=oj:c:2013:253:0003:0007:hu:pdf Letöltve:2013.10.02.

[4] http://www.jogiforum.hu/publikaciok/540 Letöltve:2013.10.04..

[5] http://www.pointernet.pds.hu/ujsagok/evilag/2002/00/evilag-16.html Letöltve:2013.10.05.

[6] http://www.kovacsvg.hu/c_adatvedelem-szemelyes-adat-vedelme Letöltve:2013.10.02.

[7] http://eur-lex.europa.eu/johtml.do?uri=oj:l:2013:173:som:hu:html Letöltve:2013.10.05.

[8] http://advocatus.dlapiper.hu/?p=1145 Letöltve:2013.10.02.

[9] http://advocatus.dlapiper.hu/?p=1024 Letöltve:2013.10.02.

[10] http://hu.wikipedia.org/wiki/Adatv%C3%A9delem Letöltve:2013.10.02.

[11] http://hu.wikipedia.org/wiki/felh%c5%91_alap%c3%ba_sz%c3%a1m%c3%adt%c3%a1stechnika Letöltve:2013.10.03.

[12] http://iothu.sharedby.co/eca2d8b5750bc009/?web=7dc72c&dst=http%3A//index.hu/tech/2013/06/23/vegre_torolhetjuk_magunkat_a_google-bol/ Letöltve:2013.10.03.

[13] http://iothu.sharedby.co Letöltve:2013.10.02.

KERTI András[1]

AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATKEZELÉS OKTATÁSÁNAK BUKTATÓI

Rezümé

Jelen cikkben a NKE HHK Híradó tanszéken évek óta folyó információbiztonsági kockázatkezelés oktatása során szerzett tapasztalatokat dolgozom fel, kiemelt figyelmet fordítva a tananyag elsajátítását nehezítő problémákra.

Kulcsszavak

Kockázatmenedzsment, kockázatkezelés, oktatás.

Bevezetés

A NATO minősített információk védelmi követelményeit meghatározó C-M(2002)492 dokumentum „B" mellékletében a kockázatelemzés mint alapkövetelmény szerepel:

„- a biztonsági kockázat menedzsment a NATO polgári és katonai testületeinél kötelező, amelynek az alkalmazása a nemzeti rendszereknél javasolt"[14]

Mivel a Honvédelmi Minisztérium és a hozzákapcsolódó szervezetek és a Magyar honvédség alakulatai több NATO információ feldolgozó rendszert is üzemeltetnek, a HM Információbiztonság szakirányításra jogosult szervezete, a Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző kar jogelőd intézményeivel karöltve, a különféle szervezetek előtt álló kockázatkezelési feladatok sikeresebb végrehajtása érdekében, 2008-tól Kockázatelemzési tanfolyamokat szervez.

A tanfolyamok tananyagának kidolgozása a fellelhető szakirodalom feldolgozásával megtörtént. Azonban mivel ez a szakterület az oktatók számára is új területnek számított, a tananyag, az oktatási és kockázat kezelési módszer folyamatosan, a felmerült kérdések, a végrehajtott kockázatelemzések során változott. A tanfolyamokon részt vett személyi állomány többségéről el lehet mondani, hogy az információbiztonság szakterületén jártas szakemberekről van szó, így az ő általuk felvetett kérdések, problémák a tanfolyam vezetők „katedra ízű" felfogását is befolyásolták. A következő cikkben szeretném bemutatni, hogy a hátunk mögött levő tanfolyamok során melyek azok a problémák, amelyek az információbiztonsági kockázatkezelés tananyag elsajátításában problémát jelentenek, mik az információbiztonsági kockázat elemzés buktatói. A cikkem során nem célom bemutatni a kockázat elemzés folyamatát, és a különböző módszerek közötti különbségeket sem.

1 adjunktus, kerti.andras@uni-nke.h

2 A C-M(2002)49 UNCLASSIFIED jelöléssel van ellátva, amely alapján a nyilvánosságra hozatala, vagyis interneten történő megjelenítése és a dokumentumra való hivatkozás, engedélyhez kötött. Ezt az engedély a NATO felhatalmazott szerve, 2004. szeptemberben megadta.

Az információbiztonsági kockázatkezelés szabályozása

Mielőtt rátérnénk a kockázat elemzés buktatóira nézzük meg, hogy milyen előírások vannak az információbiztonsági kockázat előírásaira, milyen kiinduló anyagok álnak rendelkezésre a tanfolyam megszervezéséhez!

NATO előírásai

A NATO a már citált alapelvén kívül a C-M(2002)49 „F" melléklete sem sokkal bőbeszédűbb: „Azokat a NATO civil és katonai szervezeteiben ahol NATO minősített információkat kezelnek alá kell vetni kockázat felmérésnek és kockázat menedzsmentnek, a (C-M(2002)49-t) támogató direktíváknak megfelelően."3 [15]

A támogató direktívák idézése egy teljesen nyilt cikkben nem célszerű, de ezekben a direktívákban le van írva a NATO hivatalos elképzelése a kockázat menedzsment munkafolyamatairól, elvárt dokumentumairól és szervezéséről, de konkrét módszertani ajánlás nincs.

Az Európai Unió előírásai

Az Európai Unióban az információbiztonsági kockázatkezelést nagyon komolyan veszik, erre a legjobb példa a minősített információk védelmével kapcsolatos alapdokumentum a „TANÁCS HATÁROZATA (2011. március 31.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2011/292/EU)".

A dokumentumban sok helyen és bőven szó esik a kockázatkezelésről. Az alapdokumentum4 18 cikkéből az 5. teljes egészében a biztonsági kockázat kezelésről szól. még két további példa az elmondottakra:

„A Főtitkárság és a tagállamok egyaránt kockázatkezelési eljárást alkalmaznak az EU-minősített adatoknak a saját területükön történő védelmére, a felmért kockázattal arányos mértékű fizikai védelem biztosítása érdekében."[16]

„A biztonsági kockázatkezelés célja olyan biztonsági intézkedések alkalmazása, melyek eredményeképpen kielégítő egyensúly teremthető a felhasználók igényei, a költségek és a fennmaradó biztonsági kockázatok között."[17]

Bár a dokumentum sokat foglalkozik a kockázatkezeléssel, konkrét módszertani útmutatót nem ad annak végrehajtására. Ebben valószínűleg az is szerepet játszik, hogy ezen a téren is megindult a különböző cégek piac szerzése. A 2004-ben az Európai Parlament és Tanács 460/2004/EK rendeletével létrehozott Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) honlapján a cikk írásakor 13 kockázatkezelési módszer és 25 eszköz (szoftver) alapvető leírását lehetett megtalálni.[18]

A kockázat elemzés megjelenése a hazai jogszabályokban

Kifejezetten információbiztonsági kockázatkezelésről a jogszabályok kevés szót ejtenek, de az általában vett, és az információbiztonsági kockázatkezelést is magában foglaló, kockázatok kezeléséről több jogszabályban is szó van. Ezért, bár

3 Ez eredeti szöveg:" Systems handling NATO classified information, in NATO civil and military bodies, shall be subject to risk assessment and risk management in accordance with the requirements of directives supporting this policy."

4 A határozat gyakorlatilag az elfogadó nyilatkozatból, a határozatból és a mellékletekből áll. A határozat 18 cikkben rögzíti a policy szintű alapkövetelményeket, amelyeket aztán a hat, a különálló területeket részletező, melléklet és négy függelék támaszt alá.

ez a cikk kifejezetten az információbiztonsági kockázatkezelésről szól, azonban nem szabad elfelejtkezni a kapcsolódó jogszabályokról sem.

Az államháztartásról szóló 2011. évi CXCV. törvény és a végrehajtására kiadott 370/2011. kormányrendelet, és a speciálisan a honvédelmi szervezetekre vonatkozó 39/2012. HM utasítás a kockázat kezelést, mint a belső kontrollrendszer részét a vezető felelősségévé teszik:

„A belső kontrollrendszer a kockázatok kezelése és tárgyilagos bizonyosság megszerzése érdekében kialakított folyamatrendszer, ….. A belső kontrollrendszer létrehozásáért, működtetéséért és fejlesztéséért a költségvetési szerv vezetője felelős …"[19]

„A költségvetési szerv vezetője felelős a belső kontrollrendszer keretében – a szervezet minden szintjén érvényesülő – megfelelő… kockázatkezelési rendszer,….. kialakításáért, működtetéséért és fejlesztéséért."[20]

„A honvédelmi szervezet … kockázatkezelési szabályzatot készít. A honvédelmi szervezet kockázatkezelési szabályzatában kell rögzíteni a kockázatkezelés feladatait és eljárásrendjét, valamint el kell készíteni a kockázat-nyilvántartást, amely az egyes tevékenységek vonatkozásában a beazonosított kockázatokat tartalmazza."[21]

A szabályzókból nem, de a Pénzügy Minisztérium által kiadott segédletből egyértelműen kiderül, hogy a kockázatkezelés körébe beletartoznak a szervezet információs, és ezen belül az információbiztonsági kockázatai is.

Az információbiztonsággal foglalkozó jogszabályok közül a nem minősített információk biztonságával foglalkozók - levéltári törvény, iratkezelési kormányrendelet stb..- nem foglalkoznak a kockázatok kezelésével. A kockázatkezelés a minősített adat elektronikus biztonságával foglalkozó kormányrendeletben jelenik meg, de a véleményem szerint, ott sem kellő súllyal.:

„A biztonsági vezető a rendszer életciklusának kezdeti szakaszában megkezdi a biztonsági dokumentáció kidolgozását, és a rendszer megvalósítása során, valamint a rendszer életciklusának további szakaszaiban, kockázatelemzés és kockázatértékelés alapján a szükséges mértékben kiegészíti vagy módosítja."[22]

Ebből az idézetből az derül ki, hogy a jogalkotó úgy képzeli el a kockázatkezelés folyamatát, hogy azt csak a tervezés fázis megkezdése után, csak a kivitelezési fázisban kell elkezdeni. Ez ellentmond annak a – mind a NATO-s, mind az EU-s valamint szabvány alapú- elképzelésnek, hogy a kockázatkezelést a rendszer lehető legkorábbi életciklus állomásában el kell kezdeni. A jogszabály továbbá semmiféle támpontot nem ad a kockázatkezelés módszerérére, menedzsmentjére, dokumentációjára sem.

Mivel a tanfolyamainkon kifejezetten a honvédségi szervezetek részére képezünk szakembereket, még a továbbiakban meg kell vizsgálnunk a Honvédelmi Minisztériumi szabályozást is. A Honvédelmi Minisztérium és alárendelt szervezetei számára az információbiztonsági intézkedések legfelsőbb szintjét a honvédelmi tárca információbiztonsági politikája jeleneti.5 Az információbiztonsági politika az első szabályozás amely valamilyen utasítást ad a:

- Módszerre:

5 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról

„Az adatkezelő rendszerekre vonatkozó kockázatkezelést a nemzeti ajánlások szerint kell végrehajtani. A NATO, EU adatkezelő rendszerei esetében a kockázatkezelés során a vonatkozó NATO-, EU-irányelveket is figyelembe kell venni."[23]

„A fenyegetéseket, sebezhetőséget és az előfordulási valószínűséget rendszerszintű, általános kockázatelemzés esetében 1–5 közötti értékskála alkalmazásával, részletes vizsgálat esetén a használt módszertan szerinti szélesebb értéksála alkalmazásával kell megjeleníteni." [23]

- A felelősségekre:

„Adatkezelő rendszer létesítése esetén a kockázatelemzés és értékelés a hadműveleti vagy alkalmazói követelmények alapján a műszaki követelményeket meghatározó honvédelmi szervezet feladata." [23]

„Az adatkezelő rendszer kockázatelemzési, -értékelési, és folyamatos kockázatkezelési feladatainak végrehajtásáért az adatkezelést végző honvédelmi szervezet vezetője a felelős." [23]

„A kockázatelemzést

a) minősített adatokat kezelő rendszer, több szervezet által közösen használt vagy üzemeltetett rendszer, MH-szintű rendszer esetében kötelezően,

b) egyéb adatkezelő rendszerek esetében a NATO, EU, nemzeti elektronikus adatkezelésre feljogosított rendszerek felügyeletét ellátó hatóság, illetve az információvédelem szakmai felügyeletét ellátó honvédelmi szerv döntése szerint kell végrehajtani." [23]

- Menedzsmentre:

„A kockázatok felmérésére és a maradványkockázatok kimutatására – elemzésből és az elemzéstől független ellenőrzésből álló – kétszintű eljárást kell alkalmazni.

A kockázatelemzést az adatkezelő rendszer sajátosságainak, üzemeltetési környezetének figyelembevételével kétévente legalább egy alkalommal végre kell hajtani. Új kockázati tényező megjelenésekor a kockázatelemzést soron kívül el kell végezni.

A kockázatelemzés során meghatározott védelmi rendszabályokat, a maradványkockázatokat az adatkezelő rendszer biztonságáért felelős honvédelmi szervezet vezetőjének jóvá kell hagynia, az adatkezelő rendszer akkreditálása esetében jóváhagyás céljából az illetékes hatóságnak meg kell küldeni." [23]

- A kockázatfelmérés eredményinek felhasználására:

„A kockázatelemzés során meghatározott védelmi rendszabályokat, a maradványkockázatokat az adatkezelő rendszer biztonságáért felelős honvédelmi szervezet vezetőjének jóvá kell hagynia, az adatkezelő rendszer akkreditálása esetében jóváhagyás céljából az illetékes hatóságnak meg kell küldeni.

A honvédelmi szervezet adatkezelésre vonatkozó kockázatelemzési adatai, a védelmi rendszabályok, valamint azok hatékonyságára vonatkozó ellenőrzési adatok mint döntés megalapozását szolgáló adatok nem nyilvánosak.

A kockázatelemzésre vonatkozó dokumentációt az adatkezelő rendszer biztonsági dokumentumaival együtt kell kezelni." [23]

Véleményem szerint egy politika szintű dokumentum ennél többre nem is vállalkozhat.

Az oktatás buktatói

1. Buktató: miért kell kockázat menedzsment, amikor konkrét előírások vannak?

A tanfolyamok tapasztalatai alapján elmondható, hogy minél jobban ismeri valaki az információbiztonsági szakmát, annál nehezebb számára elmagyarázni a kockázatelemzést. Ennél az állománycsoportnál merül fel a leggyakrabban az a kérdés: „Értem én, hogy a különböző előírások miatt szükség van a kockázatelemzésre, kockázatmenedzsmentre, de mi ennek az értelme és a gyakorlati haszna?"

Ez nem valamiféle „Öreg kutya ne tanuljon új kunsztokat" hozzáállás eredménye, hanem az az információvédelmi ellenintézkedésekről szóló előírások részletes elméleti és gyakorlati ismeretéből adódik.

Annak ellenére, hogy mind az ajánlások és szabványok, mind a NATO és EU előírások alapján a kockázatfelmérést már az életciklus elején meg kell kezdeni, és az eredményei alapján kell kialakítani az információvédelmi rendszert, ez a honvédségi rendszerek esetében legtöbbször másképp történt.

A NATO-ba lépésünk idején, a NATO biztonsági gondolkodását még mindenki –szakmai vezetés, beleértve az országos és katonai vezetést is, és a végrehajtó állomány is- csak tanulta. A kiépítésre kerülő rendszereknél megelégedtünk az előírások lehető legpontosabb betartásával. Sem elégé képzett szakember gárda, sem elég idő és tapasztalat sem állt rendelkezésre, a szövetségi rendszer által elvárt munkafolyamat betartására.

Az is igaz, addig, míg egy versenyszférában levő szervezet, az információvédelmi ellenintézkedéseket megválaszthatja, a kockázatelemzése és a rendelkezésére álló források alapján, addig a NATO minősített adatot kezelő szervezetnek a NATO előírások, bár hagynak lehetőséget a költséghatékony ellenintézkedések kidolgozására, ez a mozgástér eléggé kicsi, és a minimum követelményeket6 mindenképpen be kell tartani. Innentől nehezen látható be a kockázat menedzsment szükségessége, főképp akkor, ha hozzávesszük a következő vélekedést is:

„Ha betartjuk a jogszabályban előírt ellenintézkedéseket, akkor már nem vonhatnak bennünket felelősségre."

2. Buktató: tudom az előírásokat, ehhez alakítom a fenyegetéseket. Fordított gondolkodás

A 27001-s szabvány szerint, az információbiztonsági menedzsment rendszer kidolgozása során, miután a hatókört és a főbb jellemzőket meghatároztuk az alábbi munkasorrendet kell betartani:[24]

- Meg kell határoznia, hogy a szervezet milyen megközelítést alkalmazzon a kockázatfelmérésre
- Azonosítania kell a kockázatokat.
- Elemeznie kell, illetve ki kell értékelnie a kockázatokat.
- Ki kell választania a kockázatok kezelésére szolgáló szabályozási célokat és intézkedéseket

6 A minimum követelmények a C-M(2002)49-ben és a támogató dokumentumaiban vannak leírva.

Vagyis az információbiztonsági kockázat elemzés eredményeiből kiindulva kell meghatározni a kockázatokkal arányos ellenintézkedést. Ez gyakorlatilag megegyezik a NATO által írásba foglalt elvekkel is. A gyakorlati megvalósítás azonban mást mutat. A különböző minősített adatot feldolgozó rendszer kialakításakor a kockázat kezelés nem kapott szerepet, azt vagy el sem készítették, vagy csak utólag.

A minősített adatkezelő rendszerek esetében már eleve benn van egy kockázat kezelési eredmény, nevezetesen maga a minősítés. Ugyanis minősített adat minősítésének meghatározásakor az okozott kárt vesszük figyelembe.

Mivel a rendszerben már eleve benn van egy kockázat elemzési eredmény, nevezetesen az adatok minősítési szintje. Ezekhez a minősítési szintekhez az előző buktató során már emlegetett eléggé konkrét előírások vannak. Nagyon sokszor előfordul, hogy a gyakorlati foglakozás keretében végrehajtott kockázat elemzés során a tanfolyami hallgatók az előírt ellenintézkedésekhez próbálják igazítani a fenyegetéseket. Mit jelent ez? Hagyjuk egy kicsit figyelmen kívül az előírásokat és tételezzük fel, hogy a vizsgált területen rossz a bűnügyi helyzet, ebből következik a vagyontárgyak fizikai kockázata (eltulajdonítás) nagy. Következtetés: megfelelő biztonságot nyújtó rácsot kell a nyílászárókra szerelni a fizikai kockázatok csökkentése érdekében. Ez a gondolatmenet jelentené a normál kockázatkezelési gondolkozást. Azonban a minősített adatkezelés fizikai biztonságát előíró kormányrendelet, a minősítési szinteknek megfelelő konkrét rács típusok használatát írja elő. A gyakorlatlan kockázat kezelő számára ez a rács használat nem következik az általa végrehajtott kockázatkezelési feladatból. Ahhoz, hogy az ellentmondást feloldja, visszanyúl a kiindulási adatokhoz és megnöveli a veszélyeztető tényezőt, jelen esetben a bűnügyi helyzet állapotát. Így már mindenki láthatja, hogy ő jól végezte el a feladatát, mert az az eredmény jött ki, amit a jogszabály egyébként is előír.

3. Buktató: nincs királyi út, több módszer létezik

Az általunk tartott kockázatmenedzsment tanfolyamokon, néhány szabályt erősítő kivételtől eltekintve, hívatásos és szerződéses katonák kerülnek beiskolázásra. Ez a tény is gátja néha a tananyag elsajátításának. Mi katonák, főképpen az idősebb korosztály, ugyanis megszoktuk, hogy az élet minden területe szabályozva, sőt néha túlszabályozva van. Ehhez képest, amikor a kockázat elemzés konkrét módszerének oktatására kerül a sor, nagyon sokan meglepődve tapasztalják, hogy egynél több módszert muszáj bemutatni, mivel sem honvédségi szinten, sem állami szinten nincs egységes elfogadott módszertan. Ebből kifolyólag még nem volt olyan tanfolyamunk, hogy ne hangzott volna el a következő kérdés: „Miért nincs központilag kialakított, és kiadott módszertan?”

4. Buktató: Milyen mélységig elemezzek?

Az információbiztonsági kockázat elemzés oktatásának ezen buktatójánál, az arany középút megtalálása okoz gondot. A hallgatók mentalitásbeli különbségét figyelembe véve két szélsőség adódik: a „nagyvonalú” és „túl precíz” gondolkodásmód.

A „nagyvonalú” gondolkodásmódú hallgatóknál a probléma abból adódik, hogy ők a kockázatelemzésüket a végletekig leegyszerűsítik és kiindulási alapnak az egész információ feldolgozó rendszert egy kalap alá veszik, függetlenül attól, hogy az egy darab offline számítógépből áll, vagy egy egész országot lefedő rendszer. Ebben a gondolkodásmódban sem okoz gondot, mert ugye öt kockázat lehetséges: sérülhet a rendszer és az információ rendelkezésre állása és sértetlensége, illetve az információ bizalmassága. Már csak meg kell becsülni az ezekből adódó kockázatok nagyságát és kész is a kockázat elemzésünk, a tanfolyam hátralevő három napjában pedig mehetünk sörözni. Az ilyen kockázatelemzési gondolkodásmódnak köszönhetően nincs is szükség a helyi szervezet specifikus kockázat elemzés végrehajtására. El kell készíteni egy kockázatelemzést központilag és azt ki kell adni minden alakulata számára, mert az minden rendszer számára használható.

A „nagyvonalú” szemléletben elveszik a lényeg, ami az lenne, hogy a kockázatelemzést végrehajtó szervezet a saját szervezet, hely és rendszer specifikus információbiztonsági kockázatait feltárja és azokra megfelelő ellenintézkedéseket dolgozzon ki. A „túl precíz” gondolkodásmód ezt a problémát kiküszöböli, legalábbis elvileg. Őnáluk minden rendszer alrendszerekre bomlik, ami elsőre nem is lenne baj. A baj ezzel a gondolkodásmóddal akkor kezdődik, amikor a számítógép egerének a kockázatait kezdik elemezni: az egérnek mint rendszerelemnek sérülhet a rendelkezésre állása, és az integritása tűz, víz, elemi csapás, képzetlen felhasználó által. Gondoljuk csak el ebben az esetben csak az egér kockázati tényezője nyolc különféle tényező. És akkor még nem beszéltünk az alaplap, billentyűzet, nyomtató, a nyílt-, nem nyílt, és a minősített információkról, hálózati csatlakozókról, táppellátásról és a többiről. Ezzel a gondolkodásmóddal egy „rendes” kockázat elemzés végrehajtása, bár mindenre kiterjedne, de hónapokig tartana.

Befejezés

Annak ellenére, hogy a felmerült problémák, buktatók mindegyike, szinte minden egyes tanfolyamon előkerül, a válaszok és a megoldások függenek a kérdést felvető hallgatói állomány felkészültségétől, mentalitásától. A tanfolyami tanárok válaszainak helyességére utalhat egyrészt, hogy a tanfolyamokat záró vizsgát a hallgatók sikeresen teljesítik. Másrészt azok a csapatoktól érkező pozitív informális visszajelzések, amelyeket a tanfolyam oktatói kapnak volt hallgatóiktól.

Felhasznált irodalom:

[14] C-M(2002)49 Security within the North Atlantic Treaty Organisation (NATO) Enclosure „B” 9. (c) Internet letöltés http://www.nbf.hu/anyagok/jogszabaly/C-M%282002%2949.pdf

[15] C-M(2002)49 Security within the North Atlantic Treaty Organisation (NATO) Enclosure „F” 15. Internet letöltés http://www.nbf.hu/anyagok/jogszabaly/C-M%282002%2949.pdf

[16] A TANÁCS HATÁROZATA (2011. március 31.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2011/292/EU) II. Melléklet Fizikai biztonság 3. pont

[17] A TANÁCS HATÁROZATA (2011. március 31.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2011/292/EU) IV. melléklet A CIS-en kezelt eu-minősített adatok védelme

[18] rm-inv.enisa.europa.eu/rm_ra_methods.html

[19] 2011. évi CXCV. törvény az államháztartásról 69. §
[20] 370/2011. (XII. 31.) Korm. rendelet a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről 3.§
[21] 39/2012. (VI. 8.) HM utasítás a honvédelmi szervezetek operatív belső kontrolljai rendszerének kialakításáról, működtetéséről és fejlesztéséről 3.§
[22] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól 58. §
[23] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról 16. §
[24] MAGYAR SZABVÁNY MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények 4.2. Az ISMS kialakítása és irányítása

DOBÁK Imre

TECHNOLÓGIAI FEJLŐDÉS - TITKOSSZOLGÁLATOK

Rezümé

Az emberiség történelmét, jelenét és minden bizonnyal jövőjét is végigkísérik a titkosszolgálatok, amelyek rendeltetésükkel, működésükkel tagadhatatlanul részesei az adott társadalom egyes folyamatainak. Technikai eszközeik, rendszereik állandó változáson mennek keresztül, új információgyűjtő megoldások és lehetőségek jelennek meg, amelyek szolgálatba állítása – megfelelő jogi szabályozás és egyéb garanciális elemek mellett – hozzájárulhatnak az adott nemzet biztonságához. A szféra működését számtalan tényező befolyásolja, amelyek közül az egyik leghangsúlyosabb a technológiai és technikai környezet módosulása, a kapcsolódó globalizációs folyamatok. A határok technikai értelemben való elmosódása, valamint az adatgyűjtési képességek térbeli kitágulása is megállíthatatlanul formálja a titkosszolgálatok jelenlegi és jövőbeli működését. Jelen tanulmány a technológiai fejlődés és a titkosszolgálatok közötti összefüggésekre kíván néhány gondolat erejéig rávilágítani, különösen a képességek szerepére, valamint a titkosszolgálatok működéséhez kapcsolódó korlátok előtérbe kerülésére.

Kulcsszavak

technológia, fejlődés, biztonság, titkosszolgálat, kommunikáció

Bevezetés

A titkosszolgálatok1 sajátos rendeltetésük és feladatrendszerük révén fontos szerepet töltenek be az államok működésében. Szervezeteik, funkcionális felépítésük az egyes országok viszonylatában azonban alapvető eltéréseket mutatnak. Mivel titkos (titokban működő, titkos módszereket alkalmazó, titkos feladatokkal rendelkező, stb.) szervezetekről beszélünk a nyilvánosság felé megjelenített külső kép mögött meghúzódó „belső tartalom" érthető módon a társadalom szélesebb rétegei számára ismeretlen marad. Ennek okai között az állam azon érdeke jelenik meg, amely ezen szolgálatok működtetéséhez, az általuk biztosítandó speciális feladatokhoz és információs igényekhez kapcsolódik. A mélyebb, mögöttes tartalom nélkül is megfogalmazható azonban két fontos, a titkosszolgálatok működését formáló szempont: a korlátok és a képességek jelentősége. Ezek értelmezésére pedig többek között technikai, jogi, földrajzi, gazdasági értelemben is sor kerülhet. Jelen tanulmány a technológiai fejlődés és a titkosszolgálatok közötti néhány összefüggésre kíván röviden rávilágítani, különösen a képességek szerepére, valamint a titkosszolgálatok működéséhez kapcsolódó korlátok előtérbe kerülésére.

A titkosszolgálatok eszközrendszerei feladataikkal összhangban, a külső technikai lehetőségek mentén folyamatosan változnak. Fejlődésük alapját az adott kor tudományos és műszaki ismeretei képezik, kialakításuk és fejlesztésük a civil tár-

1 szerz. megj.: A tanulmány általános értelemben vizsgálja a címben jelzett kérdéskört, így a titkosszolgálatok kifejezést is általánosan, gyűjtőfogalomként használja (ide sorolva elnevezéstől függetlenül mind a hazai, mind egyéb országok titkosszolgálatait, nemzetbiztonsági szervezeteit).

sadalomban meglévő mérnöki ismereteken alapulnak, amelyek azután a speciális titkosszolgálati célokhoz igazítva elvezethetnek az adott feladatra alkalmas eszközök(rendszerek) létrehozásáig. Mindez azonban rendkívül összetett folyamat, ahol a szükséges szaktudás és humán képességek koncentrálása, az erőforrások biztosítása és az új technológiákhoz való hozzáférés lehetősége együttesen képezhetik az alapját a korszerű, zárt titkosszolgálati rendszerek2 kialakításának.

A titkosszolgálatok technikai fejlődése mindenképpen sajátosnak tekinthető, hiszen:

- Feladatrendszerükből adódóan céljaik, szakmai igényeik speciális jellegűek, amelyek egyedi fejlesztési irányokat eredményezhetnek.
- A szolgálatok működéséhez, így eszközrendszereikhez is nagyfokú konspiráció kapcsolódik, amely nem csak az alkalmazás időszakában, hanem már a fejlesztések során is jelentőséget kap.
- Az állam (és szervezetei) oldaláról jelentkező információs igényeket kell kiszolgálniuk, amelyek technikai feltételrendszerének megteremtése állandó változásra és fejlődésre készteti a szervezeteket.
- Működésük nem elválasztható a külső környezetben végbemenő folyamatoktól, így az információforrások körének állandó bővülése előrelépésre (vagy legalább lépéstartásra) készteti a szervezeteket.
- A fejlődés alapfeltételeként jelennek meg a gazdasági-költségvetési források, a tudásbázis és a magasan képzett humánerőforrás (szakembervonzat).

Fentiek figyelembevételével a titkosszolgálatok éppúgy, mint minden más állami szervezet a társadalom részeként számtalan irányból jelentkező külső hatás mentén látják el feladataikat, amelyek többek között:

- a társadalom irányából (pl. érdekek módosulása, elvárások változása);
- az állam irányából (pl. állami berendezkedés, politikai rendszer, szabályozás változása);
- a gazdaság irányából (pl. erőforrások rendelkezésre állása, költségvetés kérdései);
- a nemzetközi szegmens és a biztonsági kérdések irányából (pl. együttműködések, rendkívüli események bekövetkezése, biztonsági veszélyek jellemzőinek változása – pl. új terrorista módszerek);
- vagy akár a technológiai környezet módosulásának irányából érkezhetnek.

A jelzett hatások a titkosszolgálatok működésére, annak jogszabályi kereteire, szervezetük átalakítására is befolyással lehetnek. Gondoljunk csak egyes nemzetközi példákra, amelyek azt mutatják, hogy a külső környezetben végbement változások alapjaiban formálták át a szolgálatok helyét és szerepét. Ide sorolható egy-egy kiemelt, a társadalom tagjainak biztonsági helyzetét hátrányosan érintő esemény bekövetkezése, vagy az attól való félelem. A biztonság, mint alapvető érték

2 A témakörben kevés hivatalos nyílt információ áll rendelkezésre, így forrásként a médiahírek mellett az azóta már nyílttá vált korabeli hivatalos anyagok szolgálhatnak (pl. The National Security Archive (The George Washington University) http://www2.gwu.edu/~nsarchiv/ vagy akár a The National Archive (UK) - http://www.nationalarchives.gov.uk/about/

erőteljesebb felszínre kerülése, a társadalom tagjai biztonságának szavatolása, a nemzeti vagy akár szövetségi értékek és érdekek védelme elmozdulásokat eredményezhet a közösség fokozódó biztonságának irányába. Számos példát lehetne itt megemlíteni, így többek között az Egyesült Államokban, vagy Európa több országában is elkövetett terrorcselekményeket3, amelyeket követően a társadalom választ várt a szervezetektől. Újragondolták képességeiket, áttekintették vonatkozó stratégiájukat4 és lépéseket tettek a hosszabb távon is megfelelő reagálást biztosító megoldások kialakítására. A nemzeti és nemzetközi szinteken kiszélesedő titkosszolgálatok közötti információcsere, a bűnügyi irányok felé történő egyfajta nyitás, vagy akár a megelőzés és reagálás lehetőségét növelő képességek kialakítása (fejlesztés, képzés, információcsere, stb.) mind a társadalom biztonsági érdekeinek kielégítését szolgálják.

A történelemben visszatekintve látható, hogy a titkos szervezetek mindig is szem előtt tartották a kor fejlett technikai eszközeinek használatát. Amíg az ókorban, vagy akár a középkorban is egy-egy titkos feladat elvégzéséhez (pl. kémkedés – hírszerzés) fizikai - földrajzi közelség kellett, addig napjainkban a „távolról végezhető" megoldások arányának emelkedése jellemző. Ennek gyökerei egészen a konfliktusokkal teli XX. század első feléig vezetnek vissza. A hírszerzés és felderítés, valamint az ezek ellen folytatott elhárító funkció felértékelődésével, továbbá a technikai-kommunikációs eszközök széleskörű elterjedésével párhuzamosan szükségszerűen fordultak a szolgálatok a technikai fejlesztések irányába. Addig nem létező technikai hírszerzési és felderítési területek alakultak ki, új eszközök, rendszerek és együttműködések5 jelentek meg felölelve a kor legfejlettebb tudományos-mérnöki ismereteinek felhasználását és azok szolgálatába állítását. Az évszázad első felének sajátossága az eszközök miniatürizálására, rejthetőségének és mobilitásának kialakítására való törekvés, valamint az ellenségről információkat gyűjtő, tevékenységük felderítését segítő (pl. radar6) eszközök és rendszerek elterjedése. Az „elektronikus kommunikáció" ellenőrzése pedig ebben az időszakban még a vezetékes kommunikációhoz (pl. telefonvonalak), illetve a rádiózás terén főként a rövidhullámú sávtartomány használatához kapcsolódott.

3 A terrorcselekmények sorában kiemelkednek a 2001. szeptember 11-én az Egyesült Államokban elkövetett öngyilkos merényletek, a 2004. március 11-ei madridi-, valamint a 2005. július 7-én a londoni metróhálózatban elkövetett robbantás sorozatok.

4 Ezek között talán a legjelentősebb az USA felderítésének keretrendszerét kiszélesítő George W. Bush által 2001. októberében aláírt Patriot Act, de ide sorolhatóak többek között egyéb amerikai és más nemzeti szintű stratégiák is (pl. National Strategy for Combating Terrorism, Febr. 2003 és Sept. 2006, National Strategy for Counterterrorism June 2011, A Strong Britain in an Age of Uncertainty: The National Security Strategy, 2010.)

5Így például az Egyesült Államok és az Egyesült Királyság között megkötött 1946-ban megkötött (később kibővülő: Kanada, Ausztrália, Újzéland), külföldi vonatkozású (SIGINT jellegű) kommunikációk ellenőrzésére és megfejtésére irányuló ún. BRUSA/UKUSA megállapodás, vagy akár később 1955-től a szocialista blokkon belül is kiteljesedő, technikai kérdéseket is érintő állambiztonsági kapcsolatrendszerek.

http://www.nsa.gov/public_info/declass/ukusa.shtml (letöltve: 2013. október 11.)

6 Példa erre a második világháborút megelőzően mind a német (Würzburg és Freya eszközök), mind az brit oldalon (Robert Watson Watt nevéhez köthető) radar fejlesztések végrehajtása – forrás: Janusz Pielkiewicz: Kémek, ügynökök, katonák., Zrínyi Kiadó, Budapest

Felismerve az új technológiák nyújtotta előnyöket és lehetőségeket a bipoláris világrend COCOM listája jelezte a szocialista blokk országai fejlett technológiáktól való elzárásának szándékát, a nyugati technológiai előny megtartásának célját. Kihatásai megmutatkoztak a távközlési rendszerek ellenőrzésének képességében is, korlátozva az új megoldásokhoz hozzá nem férő országok titkosszolgálati rendszereinek fejlődését. A bipoláris szembenállás és gondolkodás légkörében így teret nyertek a nemzeti erőforrásokon, valamint a szövetségi rendszereken belüli technikai együttműködésekre alapuló fejlesztések, amelyekre mindkét fél esetében találhatunk példákat. A Szovjetunió széthullásával biztonsági környezetünk megváltozott és a korábbi katonai jellegű veszélyeken túl a biztonság egyéb tényezői is nagyobb jelentőséget kaptak, kihatva a helyüket kereső titkosszolgálati / nemzetbiztonsági szervezetek feladatrendszerére. 1994-ban megszűnt a keleti blokk tagországai ellen létrehozott alapvetően kereskedelmi célú COCOM lista, és ezzel megnyílt a fejlődés és a korszerűbb technológiákhoz való hozzáférés lehetősége a volt szocialista országok számára is. Átalakultak a szövetségi rendszerek, így például a NATO bővítéssel a közös értékek, érdekek és célok mentén új irányok nyíltak meg, lehetőségeket és kapcsolatokat teremtve a különböző technikai rendszerek és eszközök fejlesztése előtt is.

XXI. századi társadalmunkban a különböző technikai és infokommunikációs eszközök és rendszerek használata már a mindennapok egészét meghatározó tényező. Információk elképzelhetetlen mennyiségével találkozunk, amelyek észrevétlenül is befolyásolják biztonságunkat. A világ (kétoldalú kommunikációt lehetővé tevő) távközlési kapacitása például 1986-2007 között évente 28%-al nőtt, amit szorosan (évi 23%-os emelkedéssel) követett az adatok tárolási kapacitásának növekedése is. 1990 óta már világszerte a digitális technológia vette át a szerepet, amely arányaiban (2007-ben) 99,9%-ot képviselt7. Ugyanez, a formájában és mennyiségében változó információs tömeg éri a titkosszolgálati/nemzetbiztonsági szférát is, amelynek sajátos rendeltetéséből adódóan - szigorú törvényi szabályozással összhangban - kell a feladatai hatékony ellátásához szükséges információkat kiválasztani, értékelni és elemezni. Ezen információk többsége valamilyen technikai rendszerhez, megoldáshoz köthető, amely indukálja a vizsgált ágazat technikai területeinek fejlődését is. Talán a legismertebb, kiemelt szerepet betöltő technikai jellegű információszerző terület a SIGINT, amely a rádiós úton kisugárzott jelek felderítését célozza meg. Léte nem új keletű, a források és a technikai képességek változása azonban állandó megújításra készteti a SIGINT belső elemeit. A hagyományos értelemben vett rádiózás jelentősége átértékelődött és a korábbi, szűkebb felhasználói körhöz köthető megoldásokkal szemben globális kommunikációt biztosító új technológiák jelentek meg. Példaként a mobiltelefónia megjelenése említhető, amelyből 2012-ben becslések szerint már 6,83 milliárd üzemelt8, így joggal nevezhető alapvető technikai kommunikációs csatornának. Ha figyelembe

7 Martin Hilbert, Priscila López: The World's Technological Capacity to Store, Communicate, and Compute Information, Science 1 April 2011, Published online 10 February 2011

8 Key Global Telecom Indicators for the World Telecommunication Service Sector in 2012 - http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers (letöltve: 2013. október 10.)

vesszük, hogy tíz évvel ezelőtt még 1 milliárd alatti előfizető9 létezett, egyértelművé válik, hogy terjedésük fontos formáló tényező az információgyűjtő szervezetekre. A tömegesen megjelenő hírközlési, távközlési információk, a kapcsolódó technikai jelek és paraméterek értelmezése és feldolgozása azonban másfajta szakértelmet és képességeket is igényel. A másik jelentős változást az Internet elterjedése okozta (2012-ben már közel 2,5 milliárd felhasználó10), amely a kommunikációellenőrzés, az adatgyűjtő rendszerek, illetve az OSINT jellegű feladatok további fejlődését vetíti előre. Utóbbi tevékenység ma már alapjaiban épít azon informatikai képességekre, melyek a források tömegéhez kapcsolódóan biztosíthatják az adatok kutatását, továbbítását, tárolását és elemzését-értékelését. Itt érdemes megjegyezni, hogy egyes szakértői becslések szerint a titkosszolgálatok információs igényeinek jelentős (80-90%) része jelenik meg „nyílt forrásokban", amelyek célirányos feldolgozása segítheti a szakfeladatok végrehajtását, illetve orientálhatják az információgyűjtés további területeit is.

Tendenciák

Az egyre fejlettebb kommunikációs technológiák és a technikai területek sokrétűsége, valamint egyéb sajátosságai miatt jelen rövid tanulmánynak nem lehet célja, hogy azokat részleteiben vizsgálja, azonban néhány kapcsolódó gondolat talán tendenciaként jelezheti a titkosszolgálati szféra sajátosságait.

Globalizáció

A leghangsúlyosabb tényező a kommunikációs technológia fejlődésének folytatódása, amely határoktól függetlenül formálja a titkosszolgálatok működését és feladatrendszereiket. Ennek nyomai elsősorban a technikai vonatkozású elemeken (így például a technológiailag fejlettebb országok biztonsági szféráiban már alkalmazott technológiai szabványok és megoldások11 elterjedésén) keresztül láthatóak. A hírközlési piac megnyitásával, a multinacionális távközlési piaci szereplők megjelenésével, egyes rendszerek földrajzi „összekapcsolásával" a határok technikai értelemben vett szerepe is leértékelődött. A titkosszolgálatok számára ez a „biztonságos" távoli területről történő információ és adatgyűjtés lehetőségeit vetíti előre, amelyet az E. Snowden által kiszivárogtatott és nemzetközi visszhangot kapott adatgyűjtési ügy is jelez. A gazdasági - üzleti jellegű érdekek légkörében a nemzeti szintű kommunikációs rendszerek visszaszorultak, a társadalom széles rétegei számára is könnyedén elérhető Internet, vagy műholdas kommunikációs lehetőség pedig még a regionális szerepkört is elmossa. A 2030-ra szóló előrejelzések (Megatrends12) kitérnek a biztonság és kommunikáció közötti kapcsolatra is, amely alapján az előkövetkező tíz évben tovább fejlődésnek lehetünk tanúi. Az új kommunikációs technológiák „kétélű karddá" válnak és az IT világ kihat majd

9 A mobiltelefon előfizetők száma 1999-ben 490 millió, 2001-ben 955 millió volt. ITU-Key Global Telecom Indicators 2001.

10 2,405 milliárd felhasználó - Internet World Stats – Miniwatts MG. http://www.internetworldstats.com/stats.htm

11 Ide sorolhatóak a GSM rendszerek, vagy akár a nem tipikusan titkosszolgálati célú, hanem biztonsági - készenléti rádiórendszerek (TETRA, Tetrapol) és szabványok térnyerése és a régi elavult eszközrendszerek leváltása.

12 Global Trends 2030: Alternative Worlds, Office of the Director of National Intelligence, http://www.dni.gov/index.php/about/organization/global-trends-2030

mind az egyénekre, mind a rendszerekre, politikai struktúrákra. Amellett, hogy azok a kormányok rendelkezésére állnak (tekintélyelvű és demokratikus rendszerekben egyaránt), a „social network" adta lehetőségekkel a civil társadalom is élni fog (mint pl. a Közel-Keleten).

Kibertér szerepének további növekedése

A rendszerek globális összetettsége, alkalmazásuk mindennapi életünket szolgáló pozitív rendeltetése mellett a hozzájuk kapcsolódó biztonsági veszélyeket is magas szinten tartja. A tágan értelmezett szférát mindez az egyre inkább előtérbe kerülő számítógép–hálózati hadviselés (Computer Network Operations – CNO), az információs műveletek, vagy akár a szövetségi és nemzeti szintű stratégiákban és normákban megjelenő, nemzetbiztonságot érintő kérdések között kulcselemként megjelenő kiberbiztonság kérdése kapcsán érintheti. Az előtérbe kerülő veszélyek, számos esetben ismeretlen, más esetekben azonban már megvalósított kiberbiztonsági események, számítógépes támadások13 lépesre kényszerítik az egyes államok vezetését. Mindeközben tagadhatatlan, hogy maguk az egyes országok is rendszeresen élnek a kibertámadások lehetőségével (a médiákban megjelent hírek14 szerint például az Egyesült Államok 2011-ben 231 kibertámadást hajtott végre, amelyek nagy része Irán, Oroszország, Kína és Észak-Korea ellen irányult). Összességében a kibertér várható eseményei, nyitottsága újfajta gondolkodást fognak követelni a nemzetbiztonsági ágazat tagjaitól is. Az esetlegesen felmerülő veszélyek nemzetbiztonsági vonatkozású kezelése, a lehetséges reagálás megoldásainak kialakítása több országban már most is új struktúrák és szakmai képességek koncentrálását eredményezte.

Adatgyűjtési rendszerek térhódítása

A titkosszolgálatok számára - országoktól függetlenül - célként fogalmazódik meg, hogy pontos, aktuális információkkal rendelkezzenek környezetükről, szabályozott módon elérjék és megszerezzék a számukra szükséges információkat. Ezek megoldásai során felhasználják mind az információgyűjtés nyílt és nem nyílt (titkos) megoldásait. Az adatgyűjtő rendszerek térhódítása a távközlés és az információs társadalom fejlődésével párhuzamosan megfigyelhető kísérőjelenség. Habár létezésük nem új keletű, napjainkban képességeik földrajzi értelemben való bővülésének, globális szintű jelenlétüknek lehetünk tanúi. A múlt század közepére visszanyúló Echelon rendszert, majd az 1970-es években nyilvánosságra kerülő NSA-hoz köthető MINARET elnevezésű programot (amely telefonok lehallgatására irányult 1967-1973 között) kinőve, napjainkban az Internethez köthető megfigyelési technológiák és adatgyűjtések kerültek előtérbe. Ide sorolhatóak a külső cégek-

13 A 2013-as PCI Technológiai Konferencia adatait hivatkozó hír szerint a számítógépes biztonság kapcsán a támadások kb. 20 %-as tekinthető szervezett támadásnak. A rangsorban a leggyakoribb (32 százalék) támadások között az illetéktelen behatolások, a kémprogramok (30 százalék), és a trójai vírusok (27 százalék) vannak jelen. Forrás: A legegyszerűbb számítógépes fenyegetések egyben a legelterjedtebbek - 2013. október 3. http://www.biztositasiszeme.hu letöltve: 2013. október 6.

14 Barton Gellman, Ellen Nakashima: U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show, Aug. 30, 2013. The Washington Post, http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration (letöltve: 2013. október 06.)

hez kapcsolódó, infrastruktúrájukba beépítve működődő rendszerek (PRISM15), az upstream adatgyűjtés (pl. a brit Mastering az Internet16, kommunikáció ellenőrzésére irányuló projekt, vagy a Tempora-rendszer17, amely a Nagy-Britanniába belépő, illetve az országot elhagyó adatokat figyeli), vagy akár a feltételezett ún. GENIE program, amely keretében programokat telepíthetnek külföldi számítástechnikai eszközökre18.

Tagadhatatlan ugyanakkor, hogy a technikai rendszerekben keletkező adatok egy része értelemszerűen alapadatként jelenhet meg a titkosszolgálatok előtt is, amelyek megfelelő jogi keretek között értékesen szolgálhatják a társadalom és tagjainak biztonságát. Ezek leválogatása, szűrése, strukturálása és elemzése azonban speciális rendszereket és megoldásokat igényel. Fentiek is mutatják, hogy az adatgyűjtési képességek fizikai - technikai értelemben elsődlegesen az infokommunikációs rendszereket és szolgáltatásokat üzemeltetők szintjén állnak rendelkezésre, így a folyamatosan növekvő mennyiségű adatok gyűjtése, tárolása, majd felhasználása felerősítik a jogi korlátok és az adatvédelem kérdését. Anélkül, hogy az információgyűjtés korlátait (pl. jogi, gazdasági, stb.) jelen írásban vizsgálnánk, fontos hangsúlyozni, hogy mindezek kialakítása, működtetése és alkalmazása - egyedi nemzeti eltéréseket mutatva - szigorúan szabályozott keretek között kell, hogy történjen.

Civil kapcsolatok erősödése

A titkosszolgálatok tevékenysége nem elválasztható a társadalom nyílt színterén végbemenő technológiai- technikai változásoktól (lásd például az Internet térhódítását), így fontos területként jelenik meg a civil szférában kialakított megoldások átvétele és becsatornázása saját rendszereikbe. Megnőtt tehát a „civil" gazdasági szereplők, intézmények és vállalatok tudományos és mérnöki szerepvállalásának súlya. Az érintett vállalatok részére a titkosszolgálati szféra tagjai (valamint az erre alkalmas eszközök iránt érdeklődő egyéb nem állami szereplők) sajátos piacot jelentenek, amely pedig egyre inkább jelzi a nyílt, fejlesztési ismeretek és képességek becsatornázását. Habár a különböző tudományos-kutató intézetek és vállalatok sajátos módon korábban is megjelentek a szférában, a nyíltan szabályozott megjelenés lehetősége még több piaci szereplő becsatornázását tette lehetővé. Amíg korábban az új fejlesztések és megoldások a katonai és hadiipari fejlesztések irányából kerültek át a civil társadalom szintjére, addig napjainkra már ennek fordítottja is jelen van. Különösen igaz ez azon országokra, ahol korlátaik és képessége-

15 Az NSA tevékenységéhez kapcsolódó Internetes szolgáltatók (Microsoft, Yahoo, Google, Facebook, Skype, Youtube, stb.) rendszereihez kapcsolódó adatok gyűjtésére és elemzésére szolgáló rendszer. Forrás: Tom Murse: What is PRISM int he National Security Agency?, About.com, http://uspolitics.about.com/od/antiterrorism/a/What-Is-Prism-In-The-National-Security-Agency.htm (letöltve: 2013. október 10.)

16 Forrás:http://en.wikipedia.org/wiki/Mastering_the_Internet

17 Mike Wheatley: Project Tempora: How the British GCHQ Helps the NSA Spy on US Citizens, June 24.

http://siliconangle.com/blog/2013/06/24/project-tempora-how-the-british-gchq-helps-the-nsa-spy-on-us-citizens/

18 Barton Gellman, Ellen Nakashima: U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show, Aug. 30, 2013. The Washington Post, http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration (letöltve: 2013. október 06.)

ik nem teszik lehetővé a szükséges mértékű fejlesztői bázis fenntartását. A gyakran előre nem látható fejlődési irányok, a piacorientált technikai megoldások és alkalmazások megjelenése a kapcsolódó nemzetbiztonsági feladatok vonatkozásában mindenhol a világon a nemzetbiztonsági képességek folyamatos technikai megújítását igénylik.

Érdemes kiemelni az Egyesült Államok 1958 óta működő DARPA19 szervezetét és projektjeit, amely egyik fő célja az USA biztonsága érdekében a technológiai fölény megtartása. Habár az ügynökség kevesebb, mint 1%-át képviseli a nemzeti K + F területnek, a fejlett technológiákhoz kapcsolódó új tudományos eredmények létrehozásában szerepe a kutatásokba bevonásra kerülő civil szereplők, intézetetek, egyetemek kutatási, innovációs munkáján keresztül rendkívül meghatározó. A DARPA által felölelt főként rövidtávú 2-4 éves fejlesztésekre fókuszáló projektek számos területen voltak és vannak jelen (így a számítógép-hálózatok, a mesterséges intelligencia , a kommunikáció, a GPS, az UAV, stb).

Felgyorsuló fejlődés

Az utóbbi évtizedekben lerövidült az új tudományos eredmények felfedezése és gyakorlatban való megjelenése közötti idő, a legkorszerűbb technológiákra építve folyamatosan új és újabb technikai eszközök jelennek meg, bővül a szolgáltatások köre és ezzel párhuzamosan csökkennek (például a hírközlés) költségei.20 Talán ide sorolható a titkosszolgálatok oldaláról jelentkező „rendszerszintű" képességek megteremtésének irányába való még erőteljesebb elmozdulás is, hiszen a korábbi egyedi jellegű adat és információgyűjtő elemekkel szemben a külső technológia környezet, az adatok központosított feldolgozása ebbe az irányba mutat. A hírközlés szinte minden területén megfigyelhető az információk továbbítására szolgáló rendszerek és az informatika egymáshoz további közeledése és napjaik rendszerei (így titkosszolgálati technikai rendszerei is) már alapelvként a számítástechnikai megoldásokra építenek, elmosva a korábbi határokat. Olyan felhasználói igények kerülnek előtérbe mint a mobilitás, szélessávú IP alapú információtovábbítási igény, automatizáltság, biztonság. Adatainkat személyes eszközeinken túl már gyakran a „felhőben" tároljuk, amely a jövőre kitekintve módosulást fog eredményezni az információgyűjtő szervezetek oldaláról is. Amíg a felhasználók a függetlenség érzését, a mobilitást, az információk széles megjelenési formáját (pl. kép, hang, stb.) felhasználó megoldásokat értékelik, addig az információgyűjtés szempontjából a háttérben meghúzódó hálózati struktúrákhoz igazodó rendszerszintű gondolkodásra helyeződik a hangsúly.

Egyensúlytalanság

Az államok eltérő műszaki-technikai képességekkel rendelkeznek az új, tudományos technikai megoldások kifejlesztése és az eszközök rendszerbe állítása terén. A kutatás – fejlesztés földrajzi egyensúlytalanságot mutató további fejlődése ezt a folyamatot várhatóan még inkább felerősíti majd. Amíg a fejlett technológiák birtokában lévő országok (pl. Egyesült Államok, Nagy-Britannia, Németország,

19 Defense Advanced Research Projects Agency (költségvetése közel 3 milliárd USD) bővebben lásd: http://www.darpa.mil/ (letöltve: 2013.október 10)

20 Global Trends 2015 Report

Franciaország, Izrael, Kína, Oroszország) képesek a legújabb tudományos ismeretek és megoldások nemzetbiztonságuk szolgálatba állítására, addig a korlátozott képességekkel (és erőforrásokkal) rendelkező országoknál mindezek nem, vagy csak jelentős késéssel jelennek meg. Tagadhatatlan a fejlett országok technikai értelemben vett dominanciája is, így például az Egyesült Államok NSA szervezetének szerepe, amely a fejlett világban a legmeghatározóbb, technikai feladatrendszerrel rendelkező titkosszolgálati szervezet. Ide sorolható a brit GCHQ, vagy a jelentős high-tech exporttal rendelkező Izrael érintett szervezete is, amely a jelfelderítés, elfogás, elemzés, a kommunikáció, és az adatforgalom felderítése21 területeken fejlődik.

Módosuló hadviselés

A védelemre (biztonságra) fordított kiadások meghatározzák, más értelmezésében korlátozzák az érintett szféra működésének és fejlődésének kereteit. A hidegháború óta a védelmi kiadások ismét emelkednek, szinte valamennyi nagyhatalom, így az Egyesült Államok, Oroszország, vagy akár Kína tekintetében is növekedés volt megfigyelhető. A növekedés nagysága természetesen eltérő, így pl. Kína esetében 1998-2007 között több mint kétszeresére nőtt a védelmi kiadás. Az EU kiadásai az előző évtized közepén az USA ezirányú kiadásainak körülbelül egyötöde volt, ami mutatja a jelentős szakadékot az USA és az EU között.22 Mindennek jelzésértéke lehet a titkosszolgálati technikai területekre is, amelyek fejlesztési költségvonzatait, azok valós nagyságát nyílt adatok hiányában nem érdemes becsülni23. Több tanulmány is megjegyzi, hogy a változó gazdasági erőviszonyok mentén a hidegháború befejezését követően az erős technológiai fölénnyel rendelkező Egyesült Államok tovább növelte előnyét a technikai képességek megteremtése terén is. Ez azonban nem jelentheti a szétesõ Szovjetunió romjain formálódó új országok (főként Oroszország), vagy akár Kína titkosszolgálati képességének figyelmen kívül hagyását. Napjainkban, a fejlett országokban a kibertér erősödő szerepére fordítanak kiemelt figyelmet és jelentős összegeket költenek a kapcsolódó hadviselési elemek folyamatos bővítésére, illetve a védelemre, előrevetítve a hadsereg hagyományos erőinek és szerkezetének jövőbeli átalakulását.

Nemzeti érdekek felerősödése

Összességében a technikai lehetőségek már globális méretű titkosszolgálati tevékenységek megteremtését vetítik előre, érthető hát, ha ezen rejtett képességek vélt, vagy valós veszélyének kérdése egyre gyakrabban kerül elő a nemzetközi kapcsolatokban is. Az Edward Snowdenhez kapcsolódó NSA tevékenységét érintő

---

[21] Israel's secret intel unit spawnshigh-tech tycoons - UPI, TIMES, News Economia Società, 2013.09.10. http://times.altervista.org/israels-secret-intel-unit-spawns-high-tech-tycoons/ (letöltve: 2013.09.30)

[22] Joanna Spear, Neil Cooper: Trends in defence expenditure, In: Alan Colins (ed): Contemporary

Security Studies, Oxford University Press 2010. p. 402

23 A The Washington Postban közzétett adatok (FY 2013 Congressional Budget Justification 2012) mutatják az USA vonatkozó szolgálatai költségvetésének nagyságrendjét. E szerint 2013-ban 53 milliárd dollárból gazdálkodnak. http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/

2013 elején kirobbant botrány24 - amely szerint az NSA hétköznapi emberek telefonhívásainak, elektromos kommunikációjának adataihoz fért hozzá - az Európai Unió és az Egyesült Államok közötti kapcsolatokban is kérdéseket vetett fel. 2013. végén az Európai Parlament is vizsgálatot indított25 az NSA által végzett adatgyűjtés ügyében. Az európai államok bizalmának csökkenését jelzi:

- a biztonságosabbnak ítélt nemzeti hírközlési és adatátviteli rendszerekre való áttérés (például Franciaországban a Thales által kifejlesztett Teorem mobiltelefon alkalmazásának állami szektorban való kiterjesztése26);
- az új eszközök és megoldások elterjedését hátráltató jogi és adatvédelmi korlátok beépítése (például a Google Glass európai megjelenését érintő hírek27);
- a független nemzeti szintű rendszerek és adattárolási megoldások létrehozásának az igénye, a globális méretű rendszerektől való szeparációs kezdeményezések28.

Mindezek azonban a felhő-technológiával, adatközpontok működtetésével foglalkozó multinacionális cégek számára piaci veszteségként jelentkeznek, hiszen a nemzeti szintű „kommunikációs bezárkózás", a hardver és szoftver háttér nemzeti keretek között tartása jelentős bevételkiesést eredményezhet számukra. Az Internet szabadságának sérülését morális okokból felvető szakértői körökben29 egyre gyakrabban kap hangot a hálózat újrastrukturálásának és olyan megoldások kialakításának a gondolata, amelyek visszaszoríthatják az adatgyűjtő rendszerek alkalmazását. A nemzeti hatóságok (vagy akár nemzetközi szervezetek) számára nagy gondot okoznak az internetes társaságok magatartásának szabályozási kérdései is, amelyek az üzleti célokból történő adatgyűjtés előtt szabnának korlátokat30.

Jövő

A titkosszolgálatok technikai fejlődését, jövőbeli képességeit nem lehet megjósolni. Az azonban talán mindenki számára egyértelmű, hogy a feladatrendszerük-

24 Lásd többek között: http://www.usatoday.com/story/news/nation/2013/06/21/snowden-charged-espionage-hong-kong/2447665/, vagy http://uspolitics.about.com/od/antiterrorism/a/The-Criminal-Case-Against-Edward-Snowden.htm

25 NSA inquiry: MEPs hear US privacy experts, whistleblowers and Snowden statement. Press release, http://www.europarl.europa.eu/news/hu/news-room/content/20130930IPR21126/html/NSA-inquiry-MEPs-hear-US-privacy-experts-whistleblowers-and-Snowden-statement (letöltve: 2013. október 10.)

26 Biztonsági okokból tiltják a Gmail-t a francia hivatalnokoknak, 2013. szeptember 13. http://index.hu/

27 Európa évekig nem kaphat Google Glasst 2013. szeptember 19,

http://index.hu/

28 Leszakadna az internetről egy ország, 2013. szeptember 23., http://hvg.hu/

29 Take back the Internet September 17, 2013 by Bruce Schneier, Kurzweill accelerating intelligence, http://www.kurzweilai.net/take-back-the-internet (letöltve: 2013.október 10.)

30 A Google adatgyűjtésének, főként adatvédelmi szabályok megsértése miatti tevékenysége már több nemzetközi fórumon is felmerült, így például 2013-ban egy francia hatóság indít eljárást a cég ellen. Például a Google szabadalmi védettséget kapott „tekintetkövető rendszere" Forrás: Az érzelmeinket figyelné meg a Google, 2013. augusztus 29 http://index.hu, Adatvédelem miatt ütheti meg a bokáját a Google - http://index.hu/, 2013. szeptember 27.. letöltve: 2013.10.04.

ből adódóan mindig is a „technikai élvonalra” törekvő szolgálatok fejlődése nem elválasztható a külső környezet változásaitól.

Jelen rövid tanulmányt így, a talán nem túl távoli jövőre kitekintve a tudomány várható fejlődése kapcsán a szakemberek körét is megosztó technológiai szingularitás31 elméletére való figyelemfelhívással zárom. A Google fejlesztési igazgatója, Ray Kurzweil Szingularitás küszöbén című könyvében megfogalmazott gondolatok szerint a világ még mindig az igazi tudományos robbanás és a mesterséges szuperintelligencia megjelenése előtt áll. Mindez előrevetíti a technológiák és a biológiai létezés, gondolkodás összefonódását és átértékelését. A szerző technológiai fejlődésre építő alapvetése, az információtechnológia exponenciális ütemben, évente megduplázódó növekedésének gondolata, amely 2020 környékén válik meghatározóvá. A technológiai változás felgyorsulása az emberi létre olyan mély hatással lesz, hogy az, visszafordíthatatlanul átalakul.

Felhasznált irodalom:

[1] Budai Balázs Benjamin: E-government, avagy kormányzati és önkormányzati kihívások az on-line demokrácia korában, Aula Kiadó 2002

[2] Dobák Imre: Terrorizmus és kommunikáció, Új Honvédségi Szemle, LIX. Évfolyam 1. szám. 2005.

[3] Haig Zsolt: Számítógép–hálózati hadviselés rendszere az információs műveletekben, http://portal.zmne.hu/download/bjkmk/bsz/bszemle2006/1/06_Haig_Zsolt.pdf

[4] Fürjes János: A korszerű rádiófelderítés kihívásai az információs műveletekben, Hadmérnök, III. Évfolyam 2. szám - 2008. június

[5] Keegan, John: A háborús felderítés, Az ellenség megismerése Napóleontól az Al-kaidáig, Európa Könyvkiadó, Budapest, 2005.

[6] Shapiro, Car – Hal R. Varian: Az információ uralma, a digitális világ gazdaságtana, Geomédia Szakkönyvek, Budapest, 2000

[7] Szöllősi Sándor: Converging networks’s developmental trends, the questions of the technical adaptability in infocommunications systems of the Hungarian Army, ZMNE, Extract of Thesis, 2007, http://193.224.76.4/download/konyvtar/digitgy/phd/2008/szollosi_sandor_ten.pdf

[8] Writers, Staff: Researchers warn of 'hit and run' cyber attackers, Washington (AFP) http://www.spacedaily.com/reports/Researchers_warn_of_hit_and_run_cyber_attackers_999.html

[9] European Parliament Report, A5-0264/2001, 11 July 2001, http://cryptome.org/echelon-ep-fin.htm

[10] Hadsereg helyett hackerek, 2013. szeptember 27., http://nol.hu/

[11] Visszatért a netes kémhálózat, 2013. szeptember 27., http://www.hvg.hu

[12] Titkos adatgyűjtés - Vizsgálódnak az Európai Parlamentben, 2013. szeptember 05. http://ma.hu

[13] Felelnie kell a Google-nek az adatgyűjtésért 2013. szeptember 12., http://index.hu/

[14] Snowden urges EU parliament to protect whistleblowers, October 01, 2013 http://rt.com/news/snowden-eu-parliament-protect-whistleblowers-593/

31 Bővebben lásd a vonatkozó könyvet ajánló írásokat: http://index.hu/tudomany/raykurz/, valamint, http://ekultura.hu/olvasnivalo/ajanlok/cikk/2013-08-02+12%3A00%3A00/ray-kurzweil-a-szingularitas-kuszoben

NYIKES Zoltán[109]

AZ INFORMÁCIÓ FELHALMOZÓDÁSA A KIBERTÉRBEN

Rezümé

A szerző a kibertérben egy helyen előforduló nagy mennyiségű információ védelmével kapcsolatban gyűjtötte össze azokat az előfordulási helyeket, amelyek kritikusak lehetnek. Összegyűjtésre került a globális és a magyar kibertér biztonságát veszélyeztető és fenyegető kiberkémkedés, kibertámadás, kiberbűnözés, kiberhadviselés és a kiberterrorizmus, továbbá a kiberteret használó adatközpontok biztonsága, tervezési hibái, valamint a pénzügyi visszaélésekkel és csalásokkal kapcsolatos aktualitások, valamint az vállalati IT biztonságot érintő aktualitások. Ezzel kapcsolatban bemutatásra kerül az aktuális „kibervédelmi" törvény, valamint a Magyar Honvédség kibervédelmi koncepciója.

Kulcsszavak

információ felhalmozódás, globális kibertér, magyar kibertér, kibervédelem kiberhírszerzés, kiberbűnözés, kiberterrorizmus, kiberhadviselés, internet, IT biztonság, adatközpont, fizikai biztonság, személyi biztonság, Honvédelmi Minisztérium, Magyar Honvédség

Akkumuláció vagy aggregáció

Az információk nagymennyiségű felhalmozására jelenleg még nincs elfogadott megfelelő fogalom. Ennek a fogalom meghatározását természetesen nem vállalom magamra, ehelyett inkább megpróbálom a fenti fogalmak meghatározásának bemutatását, vizsgálatát.

Az **akkumuláció**, mint fogalom, latin eredetű szó, jelentése *felhalmozás, tartalékolás, lerakódás.*[19.] Más környezetben jelenthet *energiafelhalmozódást*, vagy *mechanikai fölhalmozódást.*[20.]

Az **aggregáció**, mint fogalom, szintén latin eredetű szó, jelentése *felhalmozás, összesítés*.[18.] Az *aggregálódik* ige jelentése *felgyülemlik, felhalmozódik, összegyűlik*.[21.]

Kijelenthető, hogy a két fogalom egymás szinonimája, viszont szakterületenként vagy tudományáganként eltérően használatos, egymással nem helyettesíthetőek. Például az akkumulációs réteget, amelyet más néven feldúsulási rétegnek is neveznek az elektronika világában, nem szokás „aggregációs rétegnek" hívni. Ezzel szemben az IT világban már létező kifejezés a közösségi oldal aggregáció, ami olyan alkalmazást jelent, amellyel egy online felületre gyűjthetjük össze a közösségi oldalak tartalmait.[17.] Ebben az esetben sem használatos a közösségi oldal akkumuláció kifejezés.

Az IT tudomány esetében viszont az információ akkumuláció, vagy az információ aggregáció szóösszetétel, mint fogalom még nem elterjedt. Ennek ellenére az információs technológiák mai szintű fejlettségének köszönhetően az információ koncentráltan, egy helyen, egyre nagyobb mennyiségben fordul elő, illetve a Cloud Computing technológiának köszönhetően az adataink egyszerre több szerve-

109 Magyar Honvédség 54. Veszprém Radarezred Információvédelmi központ, központparancsnok, nyikes.zoltan@mil.hu

ren valahol a felhőben tárolódnak, de virtuálisan egy nagy egységként mutatkoznak! Az, hogy a két változat közül az IT szakterület magyar képviselői a magyar nyelvben melyiket fogják meghonosítani, az majd annak lesz betudható, hogy az angol nyelvterületről, melyik változat fog megérkezni hazánkba, hogyha ez a téma valamikor vizsgálat tárgyát fogja képezni a szakma által. Ebből kifolyólag a voksomat nem teszem le egyik változat mellett sem. Ezért inkább továbbiakban az információ felhalmozás vagy felhalmozódás kifejezést fogom használni a jelenség leírására.

A kibertér

Az információ felhalmozódása a mai tudás alapú, más néven, információs társadalmunk egyik alapja. Kérdés az, hogy ez hol, mikor, milyen formában, milyen adatok esetében, mekkora mennyiségben történik. Ugyanis a feltett kérdések megválaszolása esetében lehet az adott felhalmozott információk védelméről beszélni, annak szükséges védelmi szintjét megállapítani.

Az információ felhalmozódásának egyik legnagyobb színtere maga a globális kibertér, ami globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint e rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese. Amely tartalmazza a magyar kiberteret, ami a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne. [13.]

A kibertér, ami az információ felhalmozódásának jelenleg a legnagyobb platformját jelenti, annak a védelmére régóta megindultak a különböző szintű védelmi kísérletek. Az tény hogy ennek a térnek a védelmét, úgy mint minden más fizikai értelemben létező térnek, úgymint szárazföld, tenger, levegő, világűr, ezt is elsősorban szabályzás révén lehet megalapozni. A Magyar Parlament 2013.-ban elfogadta és az adott év július 1.-i hatállyal életbe is léptette az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt, melyet a kiberbiztonság megteremtésének jegyében alkottak. Ennek a törvénynek az elkésztésénél a legjobb gyakorlatok, szabványok és ajánlások kerültek felhasználása. Ezt a jogalkotó a végrehajtási rendeletek elkészítésénél is folytatni szeretné. A törvény a COBIT informatikai szabályozási keretelvgyűjtemény, az ISO 2700x szabványcsalád, az NIST SP-800, IFIP 199/200 kockázatelemzési útmutató, valamint a KIB 25. és a KIB 28. ajánlásai alapján készült.

A törvény a hatálya alá tartozó szervezetek számára előírja a szervezet biztonsági szint besorolását, amely a COBIT 4.1 DS5 érettségi modell alapján került megállapításra. Két besorolás fog megszületni, a törvény által előírt, és az aktuális helyzetet tükröző, melyen 2 évente kell egy-egy szintet emelni a költségminimalizálás érdekében.

A törvény alapján az eszközök, a szoftverek, személyek és a szabályzó eljárásrendek együttesét tekintjük rendszernek. A rendszerek biztonsági osztályba sorolása a társadalomi-politikai, illetve a jog sérüléséből adódó hatások, a szemé-

lyek, csoportokat érintő károk, a közvetlen és a közvetett anyagi károk figyelembevételével kell elvégezni. Az elvégzett kockázat elemzés alapján kell a biztonsági osztályba sorolást külön-külön, a bizalmasság, a rendelkezésre állás és a sértetlenség alapján kell végrehajtani. Nagyság illetve a kár bekövetkezésének, gyakoriságának együttes figyelembe vételével kell a kockázati tényezőket megállapítani. A legfontosabb a megelőzés és a korai figyelmeztetés, az észlelés, a reagálás, valamint a biztonsági események kezelésének végig vitele zárt folyamatban ahol feldolgozásra kerül mindaz, ami miatt az esemény bekövetkezett, amely később és vissza kell, hogy hasson a későbbiekben.

A megelőzés érdekében a szervezet vezetése és annak felelőssége jelentős hangsúlyt kapott, úgy az outsourcing esetén is, ahol a vezető felelőssége megmarad. A képzések és továbbképzések jelentősége hangsúlyosabb, mint korábban, akár vezető, akár elektronikus információbiztonsági felelős, akár felhasználói szinten.

A STUXNET kapcsán, ma már nem csak a PC-k esetében kell félni igazán a vírusoktól, hanem az igazi pusztítás akkor következik be, amikor például egy olajfinomító nagyvállalat valamelyik telephelyén üzemelő elemében jelenik meg olyan vírus, ami robbanást idéz elő. Sajnos ma már ilyenekre is képesek azok akik rosszindulatú programokat gyártanak.[10.]

A kibertér és azontúl

A malverek, azaz rosszindulatú, kártékony szoftverek elleni harc egyféle fegyverkezési harc, olyan, mint az evolúció, ami a túlélésért folytatott küzdelem. Az evolúció nem csak a kibertérre vonatkozik, hanem valódi világban is. A szervezeteknek fejlődni kell az internet uralta világban azért, hogy életben tudjanak maradni. A cselekvések konzekvenciáinak elemzése a célok tudatában lehetséges.

A kiberbűnözés pénzügyi lopás, csalás, amelyek egyének ellen irányulhat, pl. banki adatok megszerzése adathalászás módszerével, vagy pedig cégek ellen, amelyek jelen vannak az interneten, vagy pedig maga az állam is célpont lehet olyan bűnözők által, akik pl. szociális segélyekkel akarnak visszaélni. Az ilyen fajta tevékenységekkel okozott kár több 10 vagy 100 milliárd dollár évente.

A kiberhírszerzés, a kémkedés keretében egyes országok más országok információit szeretnék megszerezni. A hírszerzési technikák és a módszerek szinte megegyeznek a kémkedés hőskorában használtakkal. Viszont a kiberkémkedés nagy előnye a hagyományos kémkedéshez képest, hogy óriási adatmennyiség, jelentős számú alternatív megoldás elérhető online. Például az összes személyes e-mail fiók, amit vizsgálni lehet. Hiszen nem egy irodai fiókot kell feltörni, hanem elegendő csak az e-mail fiókokat és a meglévő virtuális rejtőzködési technikák alkalmazásával lehetetlen bárkire is rábizonyítani a tettét. A motiváció azonban a konvencionális és a valódi kiberbűnözés mögött nagyjából ugyan az.

Egy nagyon fontos variánsa ennek manapság az ipari kémkedés, amikor is egy cégnek a kereskedelmi, üzletit titkait lopják el. Egy ország, aki mondjuk, szeretné ellopni az üzleti titkait egy másik országnak sokkal biztonságosabban teheti meg azt azáltal, hogy a „küszöb alatti online biztonságot” használja ki, vagy valakit lefizet. Bárki, aki a belső folyamatokat ismeri, hozzájárulhat a sebezhetőséghez.

Az állami kémkedés és az üzleti kémkedés jól elkülöníthető, azonban ezek átfedésbe kerülnek, ha a védelemiparról esik szó. Ha egy ország védelmi titkokat akar megszerezni sokkal könnyebben megteheti, ha a védelemiparban aktív cégeknek a hálózatain keresztül teszi azt és nem a másik ország honvédelmi minisztériumát célozza meg. Tisztában lehetünk azzal, hogy ezek a kémkedési problémák, legyenek azok üzleti, vagy állami teljesen tényszerűek.

A következő fenyegetés a hackernek vagy hacktivistának kategorizálnak, azok sorolhatók ebbe a kategóriákban, akik esetleg szórakozásból vagy politikai - ideológiai indíttatásból törnek fel oldalt, vagy lopnak adatot, információt, amivel kárt okoznak. Ezeknek a hackereknek, hacktivistáknak a motivációja ugyan eltérő, azonban a technikájuk, és az áldozatokra gyakorolt hatásuk ugyan az, vagy hasonló.

A világ ez idáig még megmenekül az igazán komoly kiberterrorizmustól, mert a terroristák az interneten keresztül fizikai hatást még nem nagyon értek el. Ez azonban elgondolkodtató, mert a terrorszervezetek jelentős informatikai ismeretekkel rendelkeznek, amelyet ki is használnak. Kifinomult műveleti technikákat alkalmaznak, jól alkalmazzák a kiberbiztonságot, de eddig úgy döntöttek, hogy offenzív célokra nem használják fel a tudásukat. A kiberterrorizmusra minden országnak az önvédelem szempontjából középtávon is valódi fenyegetéskén kell tekinteni.

A kiberhadviselés célja, az egyik állam által elkövetett cselekedet annak érdekében, hogy egy másik állam IT infrastruktúráját térdre kényszerítse vagy leállítsa békeidőben. Például a szolgáltatás elérésének meghiúsítása Észtországban. Ide tartozik az is hogy az egyik állam egy másik állam polgári, katonai rendszereit megbénítsa, annak érdekében, hogy utána támadást indítson. Például az orosz – grúz konfliktust megelőzően. Valamint megemlítendő a STUXNET, amely két valódi stratégiai jelentőséggel bír. Elsősorban egy tényleges valódi kibertámadás, amelyet egy ország indított egy a másik ellen. Másodsorban pedig olyan vezérlő rendszerek ellen irányuló támadás, amely vezérlő rendszereket nem csak nukleáris anyagok gyártásában használnak, hanem a kritikus infrastruktúrák vezérlésében is. Ilyen támadás első alkalommal volt tapasztalható.

Érdemes átgondolni, hogy kik az áldozatok, illetve kik azok, akik a védelmi oldalon vannak. Ilyen lehet maga az állampolgár, aki közvetlen célpontja lehet, vagy vétlen áldozat, egy ártatlan szemlélődő, akinek csak véletlenszerűen lopták el a hitelkártya adatait, amúgy egy vállalat elleni támadás során. Vagy pedig hacker áldozatai, akik csak szórakozásból támadták meg őket. A következő áldozati csoport a cégek, szervezetek, akik valamilyen okkal, céllal az internetet használják. Ide sorolandóak a vállalatok, a kormányzati hivatalok, kormány irodák, jótékonysági szervezetek. A harmadik csoport a védelmi szféra, az informatikai cégek, a rendőrség, a kormányzati hírszerző és biztonsági szervezetek, akik igyekeznek a legitim és biztonságos felhasználását elősegíteni az internetnek. Ezen szervezetek közvetlenül részt vesznek a kibertérben folyó küzdelemben. Szerepük és motivációjuk más és más. A viselkedésüket szűk motivációs körre le lehet szűkíteni.

A magánszemélyek az internetet mindennapi dolgaikhoz és szórakozáshoz használják. A védelem megteremtésében a cégek üzleti funkciók miatt, a kormány-

zatok a belső folyamatok és a szolgáltatások használata miatt motiváltak. Mivel a megfelelő egyensúly megtalálása a védelem és a költséghatékonyság között van.

A kommunikációs cégeket és szolgáltatókat, az internet és kormányzati hatóságokat, valamint a hírszerzést és az IT biztonsági ipart, az internet megvédésére irányuló egy fajta szakmai hit, mint motivációs tényező hajtja, működteti. A felelősség a nemzetbiztonság iránt, valamint a bűnmegelőzés és a kémelhárítás iránt, továbbá motivációként fellépnek még a kereskedelmi érdekek is. Ez az a kétféle motivációs faktor, ami a két oldalon jelentkezik és ami ebből levezethető, az a felismerés, hogy a kibertér technikai evolúciója, evolúciós változásokat indukál a szervezetekben.

A kiberbűnözők kifinomult szervezeti struktúrákkal rendelkeznek, hogy aztán ezekkel a struktúrákkal pénzt keressenek. Technológiát adnak-vesznek egymás között. Lopott hitelkártya adatokkal árulnak. Gyakorlatilag távol tartják a titkaiktól a bűnüldözést és saját megbízható közösségeket építenek. Elég furcsa a megbízhatóságról beszélni a bűnözés kapcsán, de létezik a „betyárbecsület" és ebben a „világban" eléggé kifinomult módszerekkel tudják menedzselni ezt a fajta bizalmat. Ezek a technikák és struktúrák nem kizárólag csak a bűnüldözés miatt fejlődtek, de a legitim ipar is sok szempontból is használja azokat.

A kiberkémkedéseket vizsgálva megállapítható, hogy nagyon nagy és komplex szervezetek állnak az egyes kibertámadások mögött. A támadás sikerességéhez nagyon nagyszámú ember együttműködésére van szükség, akik ismerik a célt, a célcsoportot és képesek levezényelni a ezt a fajta támadást.

A kibervédelem esetében fel kell tenni azt a kérdést, hogy vajon milyen kockázattal kell szembe néznie az egyes csoportoknak és hogyan lehet ezt a kockázatot kezelni? A magán személyek szempontjából a legnagyobb kockázat az adatlopás révén az áldozattá válás. Áldozatává válhatnak egy hackernek, aki csak úgy szórakozásból, vagy valamilyen sérelem miatt támadja meg őket. Józan emberi ésszel ezek a kockázatok csökkenthetők, de ezek nem fogják megvédeni őket a nagyobb elhatározású támadóktól. A kockázat csökkentése érdekében az egyéneknek nem csak technikai képességeket kell elsajátítani, hanem meg kell tanulni bizalmatlannak lenni, mindennel, ami az interneten van.

A kereskedelmi-kormányzati szervezetek esetében a támadás jelentős anyagi veszteségeket okozhat, ez lehet információvesztés, vagy a cégek szempontjából szellemi termék elvesztése, reputáció-, vagy az ügyféladatok vesztése. A kormányzat szempontjából lehet a minősített információk vesztése, elvesztése is. Az interneten szolgáltató vagy kereskedő cégeknél súlyos károkat okozhat, ha bebizonyosodik, hogy a cég IT biztonsága „küszöb alatti". A kormányzat számára a közvélemény bizalmának elvesztését jelentheti. Az online szolgáltatásokra manapság nem csak az emberek elvárása miatt van szükség, hanem a költséghatékonyság érdekében is indokolt. Kockázatos az is, hogy egy cégnek a belső folyamatait támadják és ez által működés képtelenné válik, elveszti a termelőképességét, ami üzletvesztéshez vezethet.

A cégeknek változtatni kell a viselkedésükön és a cégkultúrájukon, mert például a dolgozók bármilyen USB háttértára használnak, vagy kockázatos oldalak látogatnak, amivel az összes többi dolgozó szükségtelen kockázatnak van kitéve. Tehát nagyon fontos elem a dolgozók esetében a felhasználói tudatosság növelése,

a felhasználók oktatása, képzése. Ennél még talán minden szempontból kritikusabb a szervezet vezetésének az elkötelezettsége. A felső vezetőknek fel kell ismerni azt a tényt, hogy az informatikát felhasználva nem csak előnyök, hanem hátrányok is keletkeznek és ezekkel a kockázatokkal a vezetőknek maguknak is tisztában kell lenniük és tenniük kell ellene. Át kell gondolniuk az üzleti kockázatokat és megalapozott döntéseket kell hozniuk a kockázatok csökkentéséről. Széleskörű cselekvési tervet kell készíteni vészhelyzetre, és az adatmentésre. A vezetőknek minden esetben oda kell figyelni a saját viselkedésükre is, hogy megfeleljenek az vállalat politikájának. Ugyanis, ha az informatika használatához tartozó szabályokat maga a vezető nem tartja be, „lebéníthatja" a vállalati biztonságot. A cégek külső együttműködésének a területén hatékony védekezés lehet a fenyegetésekkel szemben a kollektív védelem, amely segíthet az információ megosztásában a cégek között. A kibertér transznacionális domain, ami nem tartja tiszteletben az országhatárokat. A nemzetek közötti adat megosztás területén attitűd és kultúraváltásra van szükség.

A kormányzatokkal szemben felvetődik a fokozottabb aktív szerepvállalás a közoktatásban, a polgárai kiberbiztonságának növelése érdekében.[12.]

Az adatközpontok és azok biztonsága

A kibertérben az információ felhalmozódása az adatközpontokban jelentkezik a legkoncentráltabban. Ezek az adatközpontok a kiberkémkedés, a kibertámadások és a kiberbűnözés első számú célpontja, mert ezeken a helyeken egyszerre nagy mennyiségben szerezhető be-, semmisíthető meg-, vagy rossz szándékkal változtató meg az információ.

Nagyon fontos, hogy mit tekintünk biztonságosnak egy adatközpont kapcsán. Az adat jelenleg nagyon fontos, tehát pénzt, bevételt jelent. Az adatközpontok nem újdonsültek, már az ókorban is voltak. Az adatokat nem csak lopni, hanem megsemmisíteni is megéri. Tehát az adatokra vigyázni kell, mert az a „tőkénk". A nagy kérdés, hogy milyen messzire kell „elmenni" a biztonság tekintetében. Ezt mindig a pénz dönti el. Ugyanis be kell tartani a szabályozásokat, be kell tartani bizonyos minőségbiztosítási minősítési szinteket, amiket az üzembiztonság kapcsán kell figyelembe venni. A megtérülési idő az, ami jelenleg számít a kivitelezési kényszerhatáridők és a spórolás miatt. Ezért az alapvető tervezési feltételekről rendszerint elfeledkeznek. Rengeteg olyan adatközpont létezik, ahol a megrendelő legfőbb elvárása az rendelkezésre állás. Az adatközpont védelmének tervezése szempontjából tisztában kell lenni azzal, hogy „kik" azok, akik támadhatják az adatainkat. Mindig lehet „egy fokkal" biztonságosabbnak lenni, viszont sokszor megfeledkeznek arról, hogy bármilyen eszköz lehet kiváló, azonban ha azt rosszul használják, az hatástalan lesz. Adatközpont tervezésénél és üzemeltetésénél figyelembe kell venni, hogy lehet olcsón üzemeltetni, lehet spórolni a képzésen, a rendezvényeken, csak nem biztos, hogy érdemes. Hiszem, amikor utólag kell az esetleges katasztrófa bekövetkeztét követően a hibát elhárítani az mindig sokkal drágább! Sokkal többe kerül az utólagos hibaelhárítás. Nem elehet önmagában biztonságot tervezni csak a szabályozások betartásával. Amiket végig kell gondolni az elektronikus információvédelemhez tartozó fizikai biztonság tekintetében az, hogy az adatközpontba nem juthat be bárki. Az adatközpontok, elhelyezkedésüket te-

kintve, távoli objektumokban vannak, ahova nehéz a bejutás és az engedélyköteles. Az adatközpontok egyrésze a szervezet saját maga által üzemeltett, viszont vannak, amelyek szolgáltatást nyújtanak. Ezeknek a biztonságáról gondoskodni kell. Ez viszonylag a már egyszerűbb, mert erre már vannak elfogadott és kialakult szabályok módszerek. A nagyobb kihívás az újonnan létesülő adatközpontok esetében jelentkezik, mert meg kell találni az egészséges egyensúlyt a fizikai biztonság és az anyagi lehetőségek között, pl. minél távolabbi helyszínre tervezik az adatközpontot, akkor annál többe fog kerülni az infrastruktúra kialakítása.

Az IT eszközök biztonságának a kialakítása jóval „egyszerűbb" a meglévő kialakított fizikai biztonság tekintetében. Ezzel szemben a humánfaktor, azaz a személyi biztonság a legkritikusabb, mert az informatikai rendszer és a tápellátás lehet redundáns, de az „egy ponton" megtámadható rendszer gyenge lánc szeme maga az ember. Ha van olyan „egy" ember aki, „mindent tud", akkor természetesen tőle lehet információt szerezni, és ez sokkal olcsóbb, mint a hackerek alkalmazása.

Nagyon fontos a tervezési fázis során az, ami szintén a humán faktorhoz tartozik, hogy a tervezés során nem mindig olyan tervező csapat tervezi a rendszert, aki minden szakterületen rendelkezik megfelelő ismeretekkel. Például az projekt kivitelezésének közepe táján veszik észre azt, hogy amiatt, hogy nem volt előre kellően megtervezve az amúgy „olcsónak" szánt rendszer, már jelentős a pénzügyi keret felhasználás, ami miatt folyamatos a költségek csökkentése. Nagyon fontos az üzemeltetés kérdése, az üzemeltetők tudása, képzése, továbbképzése, tesztelése, mert nagyon hajlamosak a mai adatközpont üzemeltetők egy egy gyártó termékeihez ragaszkodni. Főleg abban az esetben, hogyha az a termék olcsó is, és vezetés feltételezi, hogy amennyiben az üzemeltető szakállomány adott gyártó „script nyelvét" ismeri, akkor az majd a másik gyártó „script nyelvét" is fogja ismerni. De ezt tudjuk, hogy nem felel meg a valóságnak. A tesztelés fontossága is igen hangsúlyos, külső cégek és belsős munkatársak által el kell végeztetni. Nagyon fontos a rendszeres karbantartás, ami rendszeresen el szokott maradni.

A leggyakoribb információszerzési módszer a jóhiszeműséggel történő visszaélés és a kényszerrel történő módszer. Jóval olcsóbb az ilyen módszerek alkalmazása, mint a ritka és nagy tudású programozóké, aki távolról drága eszközökkel dolgoznak.

Nagyon fontos a hardver kérdése, ahol a következő szempontok nincsenek mérlegelve pénzügyi okokból, úgy, mint a „jövőállóság", a dokumentáció, a támogatás, a termék élettartama, továbbá nem a szigorúbban vett műszaki kérdések, mint a referenciák, és a minőség biztosítási minősítések, mások tapasztalatai, valamint a kompatibilitás más gyártók termékeivel. Az operációs rendszerek választása esetében is a fentiek érvényesek, kerülendő a „teszik-nem tesztik" alapon történő döntés.[2.]

A bankok információbiztonsága

Az egyik „legzsebbevágóbb" kérdés, kimondható, hogy a bankok információbiztonsága tekintetében jelentkezik. Ugyanis legyen szó az üzleti-, állami-, vagy magán szektorról, minden szektornak vannak pénz és a bank ügyei. A mai világban megállapítható, hogy bankszektor, ahogy a gazdasági életben, úgy az IT

biztonság területén is nélkülözhetetlen terület, ezen a területen jelentkezik legjobban az információ felhalmozódása, ha csak az ügyféladatokat vesszük alapul.

Egy a pénzügyi csalásokkal foglalkozó beszámoló szerint 2013 első félévében összességében kedvezőbb kép mutatkozott a bankokat és az ügyfeleiket érő csalásokkal kapcsolatban, mint az azt megelőző időszakokban. Nagy-Britanniában például a vizsgált időszakban a károk nagysága 21 százalékos csökkenést mutatott a 2012 első felében kimutatott veszteségekhez képest. Hasonló csökkenés volt a telefonos banki csalások vonatkozásában is. Szakértői vélemények a bankok közötti hatékony információmegosztást, a magasabb fokú online biztonsági eszközöket és az ügyfelek nagyfokú tudatosságát látják a javulásban. Az adathalász weboldalak esetében még nagyobb az előrelépés a biztonságot illetően, ugyanis a banki csalásokat segítő, phishing weblapok mennyisége egy év alatt 87 százalékkal csökkent. Ez nagyban volt köszönhető a szolgáltatók aktívabban és gyorsabb reagálásának a bizalmas banki adatokat gyűjtögető weboldalakkal szemben.

A bemutatott adatok azt sejtetik, hogy jó irányba halad ez a terület a biztonság tekintetében. Ez sajnos csak részben igaz, ugyanis van egy olyan terület, ahol a csalók egyre nagyobb aktivitást mutatnak. Ami nem más, mint a bank- és hitelkártyákkal, illetve az azokhoz tartozó adatokkal való visszaélések.

A bankkártya csalások a vizsgált időszakban 17 százalékos növekedést mutattak 2012 hasonló időszakához képest. A legnagyobb mértékben a külföldi kártyákkal történő csalások, a bank-automatákkal kapcsolatos visszaélések, valamint a kártyaadatok lopása miatt következtek be az anyagi veszteségek. A probléma azon tranzakciók során jelentkeznek, amikor fizikailag nincs szükség egy adott bankkártyára, kizárólag az ahhoz tartozó adatok megadása is elégséges.[7.]

Az információbiztonság hatékonysága

Az kibertérben szolgáltató cégek, bankok és a különböző adatbázisokat szolgáltatásait igénybe vevő felhasználók számára is egyértelmű hogy a megfelelő védelem súlyos költségeket emészt fel. Ezzel szemben az információ biztonságra áldozott erőforrások, nem az ablakon kidobottak. Az információ felhalmozódása esetében jelentős erőforrások vannak a biztonságra fordítva. Az, hogy ez mennyire hatékony, azt maga az „élet” bizonyítja. Ugyanis egy az információ biztonságát vizsgáló felmérés arra világított rá, hogy 2012-höz képest a helyzet rosszabbra fordult, legalábbis ami a kiadásokat, károkat illeti. A vizsgált cégek, szervezetek esetében a kiberbűnözés miatt felmerült költségek éves szinten átlagosan 26 százalékos növekedés mutatnak a 2012-es évhez képest. Megemlítendő mindenképp, hogy a költségek az elmúlt négy év során összesen 78 százalékkal emelkedtek. A támadások száma is növekvőben van. Idén már 122 támadást intéztek hetente átlagosan egy-egy szervezettel szembe, a tavalyi 102-val szemben. A probléma nagyságát növeli, hogy egy-egy incidens elhárítása átlagosan 32 nap volt, ameddig ez 2012-ben 24 napot vett igénybe egy-egy biztonsági esemény kezelése.

A felmérés szerint a legtöbb erőforrást a kiberbiztonsági eseményeknek, a szolgáltatásmegtagadási támadások, az alkalmazottak nemkívánatos tevékenységei, valamint a webalapú támadások voltak. Ez a három kockázati tényező a kiberbűnözéssel kapcsolatos költségek 55 százalékát teszik ki. Amennyiben a költségeket vizsgáljuk a külső és a belső kiadások alapján, akkor kiderül, hogy a külső

kiadások legnagyobb részét az adatlopási események, valamint az üzletmenet-folytonosságot sújtó támadások teszik ki. A belső források leginkább a biztonsági események detektálására, illetve az incidensreagálásra lett fordítva. A károk nagyságát befolyásoló tényező az adott szervezet mérete és tevékenységi köre is. A felmérés megállapítja, hogy a legjelentősebb veszteségek a pénzügyi, a védelmi és az energetikai szektorokban tevékenykedő vállalatokat érik, ezzel szemben alacsonyabb a kár mértéke a kereskedelemmel, a vendéglátással és a fogyasztási cikkek előállításával foglalkozó cégek körében. A vizsgálat tárgyát képezte, az hogy milyen hatást gyakorol a kiadásokra és a veszteségek méretére a korszerű biztonsági megoldások és a megfelelő szabályozások alkalmazása. Az eredmény, hogy hatékony védelmi megoldásokkal rendelkező vállalatok jobban és gyorsabban képesek fellépni a kibertámadásokkal szemben. Ezen szervezeteknél éves szinten átlagosan 4 millió dollárral kevesebb a kiberbiztonságra fordított költség. Amennyiben mindehhez jól megvalósított biztonságirányítás és megfelelően képzett szakembergárda is párosul, akkor évente további 1,5 millió dollárt tudnak még az említetteken felül megspórolni.[6.]

A Magyar Honvédség kibervédelmi koncepciója

A hatékony és korszerű kibervédelem, valamint annak finanszírozhatósága az állam számára azon belül is a védelmi szektor és a Magyar Honvédség számára sem közömbös. Az előttünk álló kihívások és a hozzá társuló erőforrásokkal való megfelelő gazdálkodás jelentős feladatot ró az azzal foglakozó szakállomány részére. Az életbe lépett „kibervédelmi" törvény kiemelten foglalkozik a Magyar Honvédség (MH) kezelésében lévő infokommunikációs rendszerek védelmével. Ennek kapcsán került kidolgozásra és lépett hatályba a Magyar Honvédség kibervédelmi szakmai koncepciójának kiadásáról szóló miniszteri utasítás, amely a honvédség kiberműveleti tevékenységének alapelveit, feladatait határozza meg. A Honvédelmi Minisztérium a Magyar Honvédség kommunikációs és információs rendszereinek védelméért, valamint az ehhez szükséges kibervédelmi képességek kialakításáért és fejlesztéséért felelős. Ezen koncepció célja, hogy a nemzeti és nemzetközi törekvésekkel összhangban szabályozzák a Magyar Honvédség katonai szervezeteinek vezetéséhez és irányításához szükséges katonai híradó és informatikai rendszer (MH Kormányzati Célú Elkülönült Hírközlő Hálózat) védelmi képességeinek megerősítését. A koncepció általános irányelveket fogalmaz meg a kibervédelem érdekében. Az új képességek tervezését és kialakítását segíti a szabályozási feladatok, az elektronikus adatkezelő hálózatok biztonsági szintjének emelése, a kibertámadás elleni képességek fejlesztése, a szaktudás növelése, a kutatás és a fejlesztés valamint az együttműködés területén. Ugyanis az elmúlt időszakban megnövekedett a magyar kiberkörnyezetet, köztük a kormányzati rendszereket is célzó különböző forrásokból indított kibertámadások száma és súlyossága.[9.]

Összegzés:

„A kibertérben lévő adatok, és az adataink védelme kiemelkedően fontos!" Hallhatjuk ezt a felhívást lassan már annyit, hogy szinte már a „csapból is ez folyik". Ezzel szemben az egyes emberek, a szervezetek, addig ezzel a felhívással nem foglalkoznak megfelelő képen, ameddig nem történik velük bármi nemű visszaélés, vagy be nem következik valamilyen szintű incidens. A magyar

„kibervédelmi" törvény egy régóta várt és nagy űrt lefedő jogszabály. A Magyar Honvédség, mint az ország védelmére hivatott egyetlen fegyveres erő, már korábban is rendelkezett a törvényben foglalt rendszer biztonsági szint besorolási kötelezettséggel. A törvény ezúttal csak megerősítette azt a tényt, hogy eddig is „jó úton" járt a „sereg". A törvény a kibervédelemnek fekteti le a törvényes alapjait. Láthattuk, hogy mennyi féle veszélyforrásnak vagyunk kitéve abban a társadalomban, világban, amit információs, vagy tudásalapú társadalomnak hívunk. A hatékony szabályzás, a jól alkalmazott technológiák, és a megfelelő színvonalú ismeretekkel rendelkező szakemberek együttese tudja csak biztosítani a szervezetek, de akár egy adott ország kiberterének a biztonságát. A nagy mennyiségben felhalmozott adataink védelmének megalapozásához elengedhetetlen a mindenre kiterjedő, alapos kockázatelemzés lefolytatása, és a kockázatelemzés eredményeként meghozott védelmi intézkedések alkalmazása. A fentiek arra is rávilágítottak, hogy egy rendszerben a leggyengébb „láncszem" maga az ember. Vagy azért mert az ember gyarló, és mindig többre vágyik, és ha kell a „lelkét is eladja", vagy pedig azért mert más kultúrához, más politikai, vallási közösséghez tartozik, ezáltal vélt vagy valós sérelmeiért a kibertérben elkövetett cselekménnyel vesz elégtétel. Akár így, akár úgy van, a végeredmény az áldozatra nézve ugyan az. Ezért tartom szükségesnek, hogy a kockázatelemzés a személyi biztonságra legalább annyira terjedjen ki, mint a fizikai, vagy adminisztratív biztonságra az elektronikus információbiztonság mellett.

Felhasznált irodalom:

[1] ÁGOTA András mk. őrnagy – Dr. KASSAI Károly mk. ezredes – TÓTH Gergely főhadnagy: A kiberkonfliktusok aktuális kérdései, nemzetközi kitekintésben, Sereg szemle, Az MH Összhaderőnemi Parancsnokság folyóirata, XI. évfolyam, 2-3. száma, 2013. április-szeptember, HU ISSN: 2060-3924

[2] BALKU Ferenc: Biztonságos? adatközpot biztonsága, Előadás, ITBN 2013. Budapest, 2013. szeptember 25.

[3] Jeff BARDIN: Kiber szellemmé akarsz válni? – Nyílt forrású információszerzés! Előadás, HACKTIVITY 2012. Budapest, 2012. október 12.

[4] BUCSAY Balázs: PayPass Sérülékenységek, Előadás, HACKTIVITY 2012. Budapest, 2012. október 12.

[5] Prof. Dr. KOVÁCS László: Kiberhadviselés, mint a jövő egyik legnagyobb kihívása, Előadás, ITBN 2012. Budapest, 2012. szeptember 25.

[6] KRISTÓF Csaba: Milliós kiadásokat úszhatunk meg korszerű védelemmel http://biztonsagportal.hu/millios-kiadasok-uszhatok-meg-korszeru-vedelemmel.html letöltve: 2013. október 11.

[7] KRISTÓF Csaba: Nincs megállás – egyre több a bankkártyás visszaélés, Biztonságportál http://biztonsagportal.hu/nincs-megallas-egyre-tobb-a-bankkartyas-visszaeles.html letöltve: 2013. október 11.

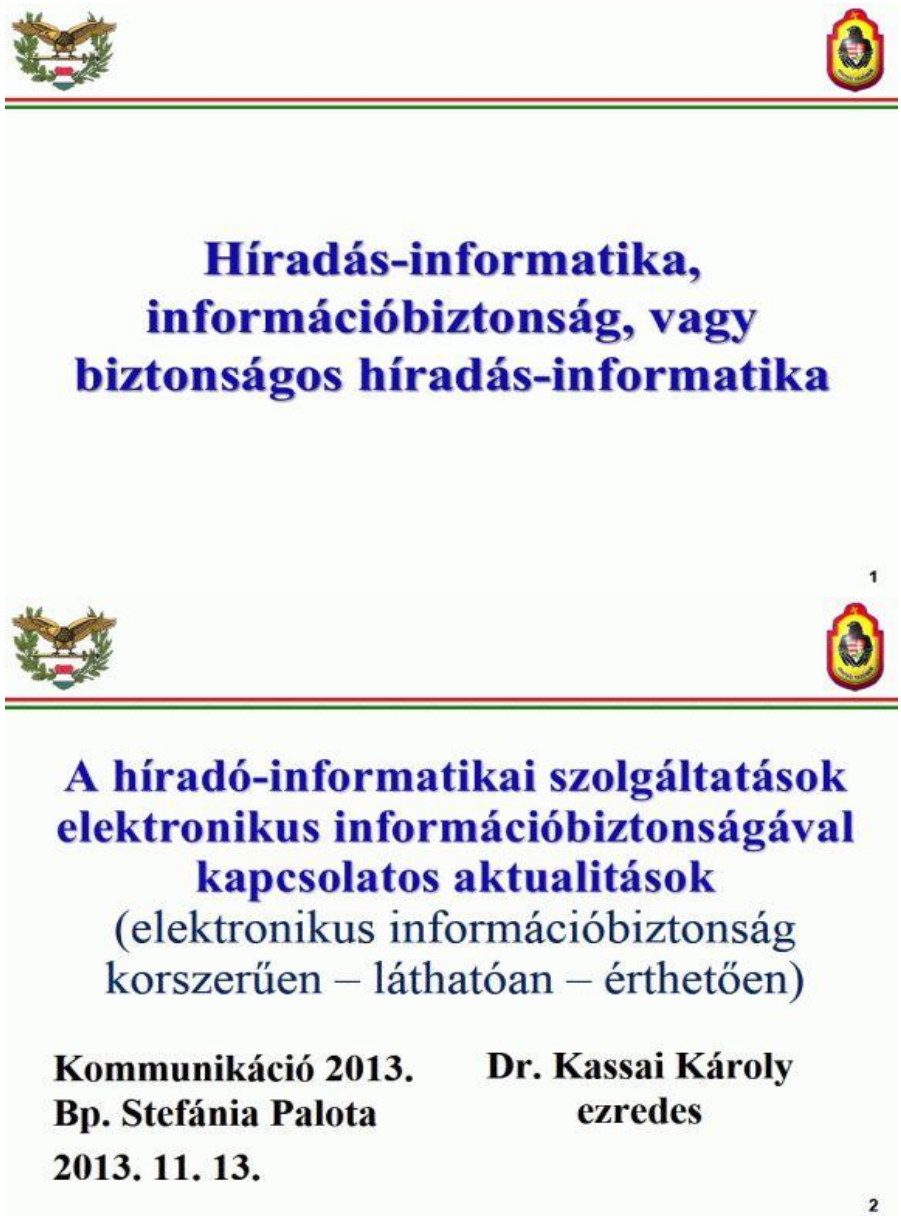
[8] ma.hu: MH Kormányzati Célú Elkülönült Hírközlő Hálózat, Honvédségi kibervédelem: miniszteri utasítás a koncepció kiadásáról http://www.ma.hu/belfold/188442/Honvedsegi_kibervedelem_miniszteri_utasitas_a_koncepcio_kiadasarol letöltve: 2013. október 8.

[9] Dr. MUHA Lajos: Törvény az elektronikus információbiztonságról, Előadás, ITBN 2012. Budapest, 2012. szeptember 25.

[10] Dr. MUHA Lajos: Törvény az elektronikus információbiztonságról: helyzet, teendők, Előadás, ITBN 2013. Budapest, 2013. szeptember 25.
[11] OTTI Csaba, ŐSZI Arnold: A biometria biztonsága és sérülékenysége, Előadás, HACKTIVITY 2012. Budapest, 2012. október 12.
[12] Sir David PEPPER: Kibertér és azon túl – folyamatban az evolúció, előadás HACTIVITY 2012. Budapest, 2012. október 12.
[13] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról,
[14] 301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról,
[15] 1035/2012. (II. 21) Korm. határozata Magyarország Nemzeti Biztonsági srtatégiájáról
[16] 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről
[17] H2Online, Közösségi oldalak aggregációja
http://www.h2online.hu/?post_type=fogalomtar&p=592 letöltve: 2013. szeptember 10.
[18] Idegen Szavak Gyűjteménye, Aggregáció
http://idegen-szavak.hu/aggreg%C3%A1ci%C3%B3 letöltve: 2013. szeptember 10.
[19] Idegen Szavak Gyűjteménye, Akkumuláció
http://idegen-szavak.hu/akkumul%C3%A1ci%C3%B3 letöltve: 2013. szeptember 10.
[20] Kislexikon, Akkumuláció
http://www.kislexikon.hu/index.php?f=Akkumul%E1ci%F3&all=1 letöltve: 2013. szeptember 10.
[21] Tinta Könyvikadó, Idegen szavak szótára, aggregáció
http://www.tintakiado.hu/dictionary_idegenszotar.php?entry=ef5db2fe7390f69737e04b75e2c014b24e3308b316eafe91aafa87582e093744 letöltve: 2013. szeptember 10.

KASSAI Károly

A HÍRADÓ-INFORMATIKAI SZOLGÁLTATÁSOK ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGÁVAL KAPCSOLATOS AKTUALITÁSOK



Tartalom

- Híradó-informatikai történések
- Üzemeltetés – alkalmazás – biztonság
- Teljes életút (életciklus) szemlélet
- Elektronikus információbiztonsági integráció

3

Megalapozás

- Magyar Honvédség elkülönült hálózat üzemeltetési szükséglet (346/2010. Korm. r.)
  - **Katonai sajátosságok**, hadműveleti követelmények
    - Állandó híradó-informatikai rendszer
    - Tábori híradó-informatikai rendszer
    - **Különleges jogrend feladatai**
  - Üzemeltetés szempontjából cél az önállóság, de:
    - **Külső szolgáltatók** igénybe vétele
    - Nem kritikus **szolgáltatások kihelyezése** (SLA-k fontossága)
  - Önálló biztonsági felügyeleti feladatok ☺☺

4

Stratégiai szintű felügyelet

- MH KCEHH üzemeltetés alapú szabályozása
  - **55/2013. (IX. 13.) HM utasítás** az MH KCEHH békeidejű üzemeltetési és felügyeleti rendje….
  - az **üzemeltetés technikai alapú szabályozása** (keretrendszer)
    - központi üzemeltetési szabályozási követelmények
    - helyi üzemeltetés szabályozás követelménye
    - igénybevételi rend és ügyfélszolgálat kérdései
    - elektronikus információbiztonsági szabályzatokra vonatkozó felülvizsgálati követelmény

5

HI szakmai irányítás

- **Híradó – Informatikai Szabályzat** (HISZ) kidolgozása
  - MH **általános keretrendszer kialakítása**, az Ált/210 szabályzat (a „kis zöld”) kiváltása
  - A híradás és informatika nézőpontjainak közelítése
  - **Szolgáltatás központú szemlélet**, folyamatok megalapozása
  - „LEGYEN BENNE BIZTONSÁG!” ☺☺
    - **Megfontoltan, óvatosan**, ez már egy másik szakterület…

6

Következő csapás

- **Híradó - Informatikai Stratégia kialakítása**
  - Korábbi – hatályon kívüli – jogszabály alapján már ismert feladatkör
  - **Védelmi Tervező Rendszerbe** illeszkedő, stratégiai szintű tervezési dokumentum
  - Szoros elektronikus információvédelmi kapcsolat és **összehangolási szükséglet**

7

Állítás

- **Meghatározható egy olyan áttekinthető szabályozási keretrendszer**, mely **alkalmas** a Magyar Honvédség szervezeteinél az **elektronikus információvédelmi képességek szabályozására.**

8

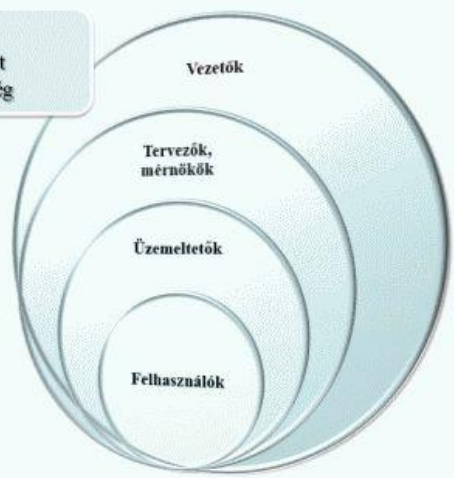
Fejlődés-alkalmazkodás?

- Kezdetben volt az ügyvitel…

9

Felismerések – testreszabás

- Mindenkinek feladata szerinti,
- Szolgáltatás-specifikus, testreszabott védelmi rendszabályokra van szükség



10

Változások

- **Szabvány alapú megközelítés**
  - Nem kell mindig feltalálni valamit
  - Bevált gyakorlat előnyeinek kihasználása
- **Szabályozók strukturálása**
  - Nem lehet mindent egyszerre, egy helyen „megmondani”
- A **felhasználói és az üzemeltetői sík** szétválasztása
  - „A cipész maradjon a kaptafánál” – az SZVSZ végnapjai…

11

Változások 2

- **Biztonsági követelményekre** és **védelmi rendszabályokra** való tagolás
  - Általános követelmények alapján specializálható, részletezett feladat meghatározás lehetősége
  - Tartalmi pontosság
- Egységes ellenőrzési szempontrendszer kialakulása
  - Objektivitás
  - **Elmozdulás a mérhetőség felé**

12

Életciklus szemlélet

- **Híradó - Informatikai Szabályzat** (2014)
  - Az elektronikus információbiztonsági szabályozórendszert nem lehet integrálni egy másik szakterület szabályozásába, mert:
    - Túl sok, túl bonyolult…
    - Rugalmatlan, gigantikus szabályzat keletkezik = tanulni kell a múltból
  - **Életciklus állomások szerint** a **feladatok átfogó jellegű megfogalmazására** van szükség

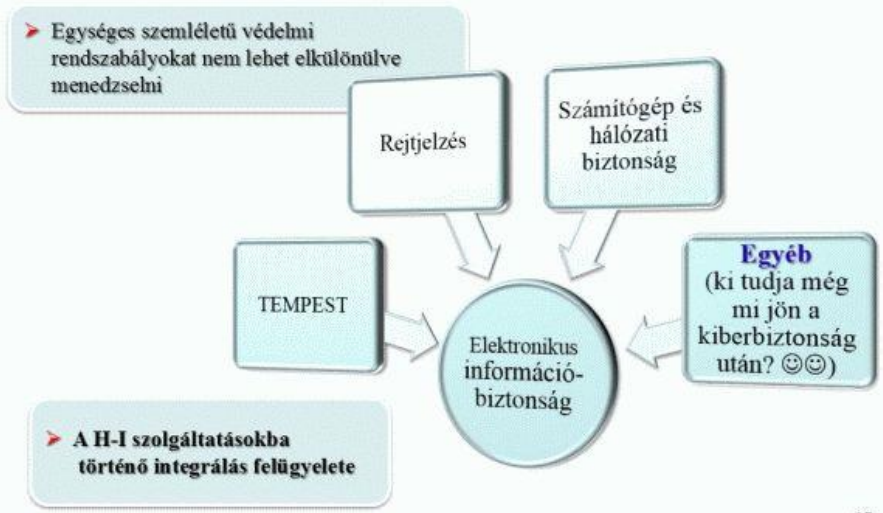
13

Nem csak üzemeltetünk…

- A **hadműveleti követelmények**, **felhasználói igények** biztonsági szempontjai
- A „biztonság” megjelenése **a tervezés, kialakítás** során
- **Engedélyezés**
- Az **üzemeltetés** biztonsági szempontjai és feladatai
- A **rendszerből történő kivonás** biztonsági szempontjai és feladatai

14

Integráció



15

Tisztelettel köszönöm a figyelmet!

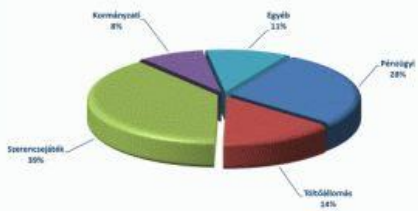
…És ne csak akkor gondoljanak az információbiztonságra, mikor már baj van!

16

TÓTH Ferenc

MOBIL MŰHOLDAS MEGOLDÁSOK

Főbb referenciák



Pénzügyi:
OTP Bank, Takarékszövetkezetek

Töltőállomás hálózatok
Agip, Lukoil, MOL, OMV, Shell Hungary, Shell Bulgaria

Kormányzati:
Külügyminisztérium, Miniszterelnöki Hivatal, Magyar Honvédség, Országos Katasztrófavédelmi Főigazgatóság

Szerencsejáték:
Szerencsejáték Zrt.

Egyéb:
SCADA (EDF, MOL FGSZ, MOL Olaj, vízművek), KKV-k, Ideiglenes szolgáltatások, Ásványi anyag kutató cégek

Telepített végpontok száma: 4 000

3

HTD – főbb műszaki és üzemeltetési paraméterek

Minősítések

- NATO beszállítói minősítés
- Nemzetbiztonsági minősítés
- Telephely Biztonsági Engedély (Nemzeti Szigorúan Titkos/NATO Titkos/EU Titkos szintig)
- ISO 9001-2008 minősítés

Infrastruktúra

- Közvetlen kapcsolat a Nemzeti Távközlési Gerinchálózattal;
- Redundáns backhaul infrastruktúra (különböző optikai összeköttetések, mikró összeköttetések, műholdas kapcsolatok)
- Gerinchálózati ponttal a magyarországi legnagyobb Internet adatcserélő központ a SZTAKI épületében
- Redundáns elektromos infrastruktúra (duplikált áramellátás, szünetmentes tápegysége és generátor)

Műszaki üzemeltetés

- 24/7 proaktív hálózatfelügyelet (helpdesk, level 1 és level 2 rendszermérnökök)

4

Mobil műholdas megoldások előnyei

- Magyarország és a Közép-Európai régió teljes lefedése,
- Gyenge infrastruktúrával rendelkező, nehezen megközelíthető helyszínek ellátása,
- Földi hálózatoktól függetlenül mindenhol elérhető,
- Internet független, zárt hálózat,
- Folyamatosan (24/7) menedzselt és felügyelt hálózat;
- Magas rendelkezésre állás,
- Rugalmas hálózat felépítés, gyors telepíthetőség,
- Automata rendszerek esetén a műholdra állás gyors és automatikus - 1 gombnyomásra (kb. 5 perc) üzemképes,
- Egyes típusok esetében menetközbeni adat és video átvitel,
- Nem igényel külön oktatást, speciális szakértelmet, fizikai munkát,
- Könnyen szervizelhető.

5

Felhasználási példák

- Mobil hálózat helyreállítása;
- TETRA rendszer tartalékolás, kihosszabbítás;
- Video jel/hang továbbítása helyszínről/helyszínekre;
- Mobil okmányirodák összeköttetése;
- Katasztrófavédelmi feladatok helyszíni szervezése;
- Mobil ellenőrzési pont felállítása (mélységi határ ellenőrzés, e-útDíj ellenőrző pontok);
- Veszélyes anyagok szállításának ellenőrzése;
- Kritikus infrastruktúrák adatátviteli tartalékolása;
- Központi adatbázisok elérése változó helyszínekről;
- Helyszíni sajtótájékoztatók;
- Menet közben működő (valódi) mobilitás.

6

Mobil megoldás – Gépjárműre szerelt

- Elegáns, könnyű felépítés, opcióként áramvonalas megoldásokkal,
- Bármilyen járműre telepíthető,
- Ideiglenes, vagy végleges tetőrögzítés,
- Szélessávú adatátvitel,
- Működőképesség 5 perc alatt,
- Polgári, katonai és védelmi célokra,
- Szélsőséges körülmények között tesztelt, masszív kivitel.

Mobil megoldás – Menet közben

- Használat mozgás közben,
- Szélessávú adatkommunikáció akár 4 Mbps sávszélességgel,
- Video és hang szolgáltatások,
- Akár 11 cm-es magasságú antenna,
- 100 km/h sebesség felett is működik,
- Azonnali kommunikáció-helyreállás a kilátás blokkolásának megszűnése után (akár 1 másodperc).

Műholdas telefon megoldások - Főbb jellemzők

- Inmarsat (BGAN, ISatPhone), Iridium, Thuraya, Globalstar rendszerek,
- Mobil telefon-, és/vagy szélessávú adatkapcsolat kiépítése szinte bárhol a világon, perceken belül,
- Egyszerűség és könnyű használhatóság,
- Kisméretű készülékek (akár 1 kg),
- Kompatibilitás a földi telekommunikációs hálózatokkal,
- IP és vonal-kapcsolt hálózati kompatibilitás,
- Garantált sávszélesség opció (Inmarsat BGAN streaming),
- Biztonságos kommunikáció.

9

Műholdas telefon megoldások – Új készülékek I.

Cobham Explorer 710 (Inmarsat BGAN)

- Egyidejű hang- és adatkommunikáció,
- Az első készülék, amely az Inmarsat új BGAN HDR (Higher Data Rates) technológiáját alkalmazza,
- Streaming akár 650 kbps sávszélességgel,
- Internet hozzáférés 492 kbps sávszélességgel,
- Sávszélesség aggregációval több, mint 1 Mbps-os streaming,
- Okostelefon alkalmazások,
- Wi-Fi hotspot funkció 100 méterig.

10

Műholdas telefon megoldások – Új készülékek II.

Iridium Extreme műholdas telefon

- Különleges strapabírósággal rendelkező, por- és vízálló készülék (IP 65 és MIL-STD 810F szabványoknak megfelelő kivitelezés),
- Beépített GPS helyzetmeghatározó,
- Vészhelyzeti (SOS) funkció,
- Könnyű és könnyen kezelhető készülék.

11

Műholdas telefon megoldások – Új készülékek III.

Cobham Explorer 325 (Inmarsat BGAN)

- Mozgás közbeni kommunikáció, automatikus műholdkeresés
- Egyidejű hang- és adatkommunikáció
- Adatátvitel: 384/384 kbps le- és feltöltés
- Streaming adatátvitel 128 kbps-ig
- Könnyű telepíthetőség és felhasználóbarát kezelhetőség
- Egyszerre több felhasználó általi hozzáférés
- IP kézibeszélő
- Gépjárműre mágneses módon rögzíthető

12

Műholdas telefon megoldások - Titkosítás

- Nagysebességű IP/Ethernet hálózati titkosító megoldások,
- Beépített TCP/IP gyorsítás,
- Soros kialakítású berendezések védelmi, stratégiai és egyéb kormányzati alkalmazások számára,
- Biztonságos Iridium és Inmarsat BGAN műholdas hálózati szolgáltatások egyéb perifériák bevonása nélkül,
- Helyi és távoli menedzsment.

13

Inmarsat L-TAC

Az L-TAC technológia az Inmarsat új megoldása az ún. Beyond Line of Sight (közvetlen rálátás nélküli) műveleti kommunikációra

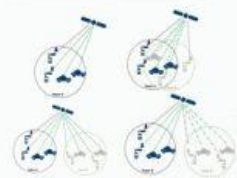
Főbb jellemzők:

- L-sávos TACSAT rendszer az Inmarsat műholdas hálózatára alapozva,
- Alacsony késleltetési idők,
- Mozgás közbeni kommunikáció,
- Költséghatékonyság: alacsony egyszeri és üzemeltetési díjak,
- A már meglévő UHF rádiók és titkosító berendezések használata,
- Minimális betanulási folyamat,
- Rugalmas kapacitás bérlet,
- Felhasználóra szabható, egyéni lefedettségi opciók.

14

Inmarsat L-TAC – Műszaki paraméterek

- 25 kHz standard csatorna allokáció,
- Osztott csatorna opció (5db 5 kHz alcsatorna),
- Moduláció:
  - FM – hang és/vagy alacsony sávszélességű adat
  - ANDVT – hang és/vagy alacsony sávszélességű adat
- Lefedettségi opciók:
  - korlátozott kiterjedésű spot (kb. 800 km átmérő)
  - regionális spot (kb. 3 200 km átmérő)
  - felhasználóra szabott spot
- Konfigurációs opciók:
  - egy vagy több hálózat – egy vagy több lefedettség alatt.



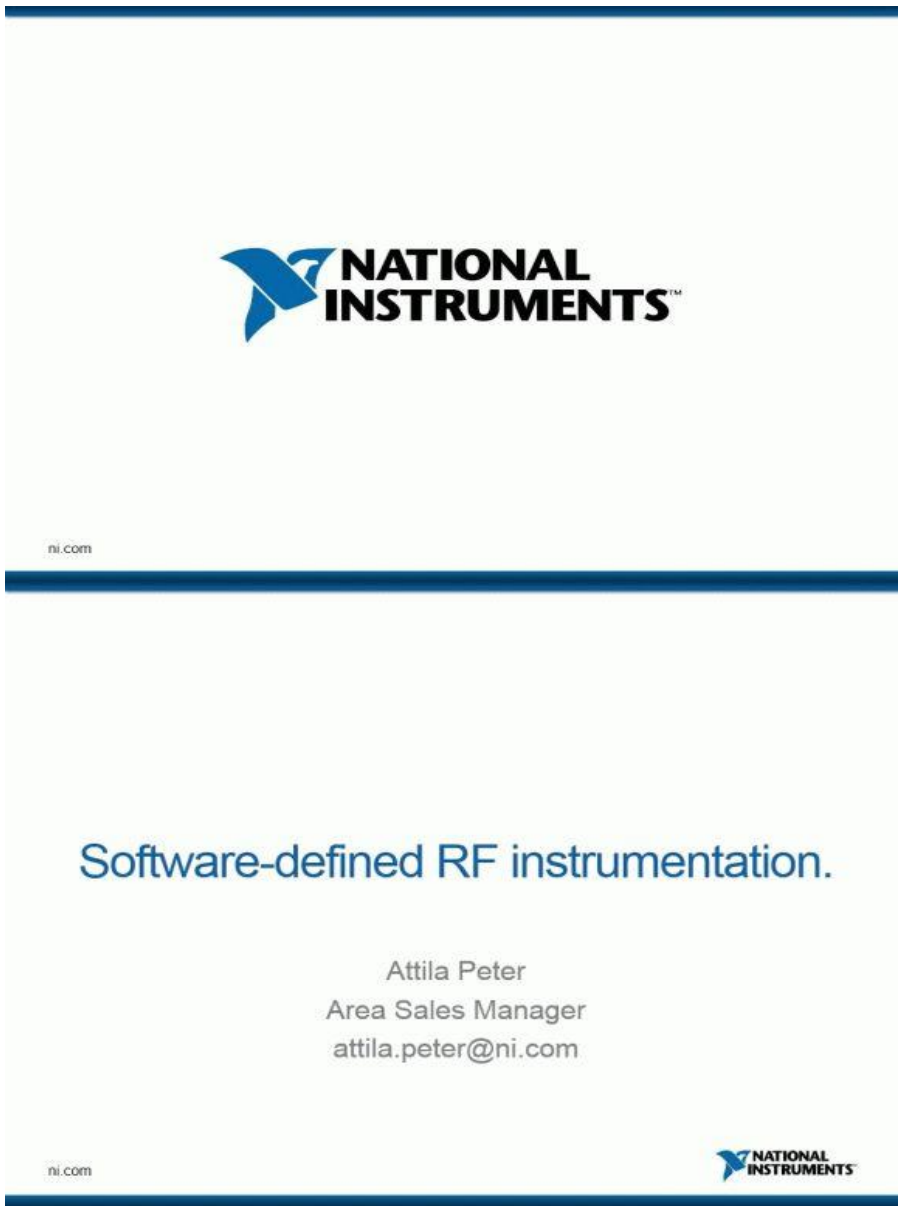
Kapcsolat

Hungaro DigiTel Kft.
2310 - Szigetszentmiklós-Lakihegy
Komp u. 2.

Tel: +36 1 4888 500
Fax: +36 1 4888 501
www.hdt.hu

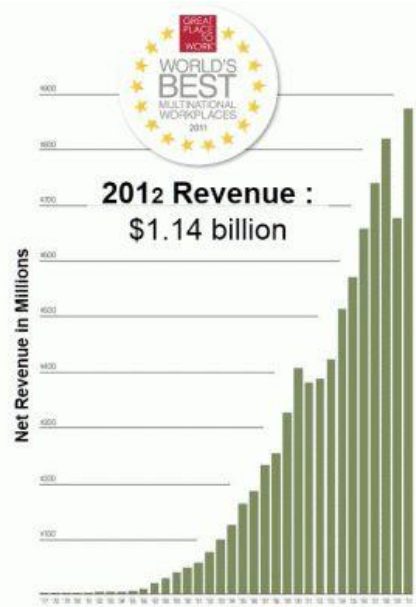
PÉTER Attila

SZOFTVERESEN DEFINIÁLT MŰSZEREZÉS KOMMUNIKÁCIÓ RENDSZEREK FEJLESZTÉSÉBEN ÉS TESZTELÉSÉBEN

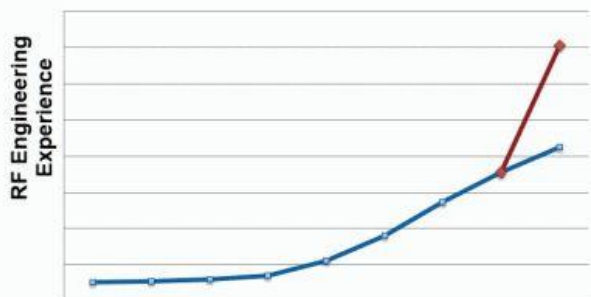


National Instruments

- Corporate headquarters in Austin, Texas
- Leaders in computer based measurement and automation, **graphical system design**
- Innovators with **16% of annual revenue invested in in R&D**
- **6500** Employer WorldWide
- More than 600 Alliance Partners
- Production in **Debrecen**
- Fortune's 100 **Best Companies to Work** For 12 Consecutive Years



NI's Investments in RF



SIGNALION

Phase Matrix

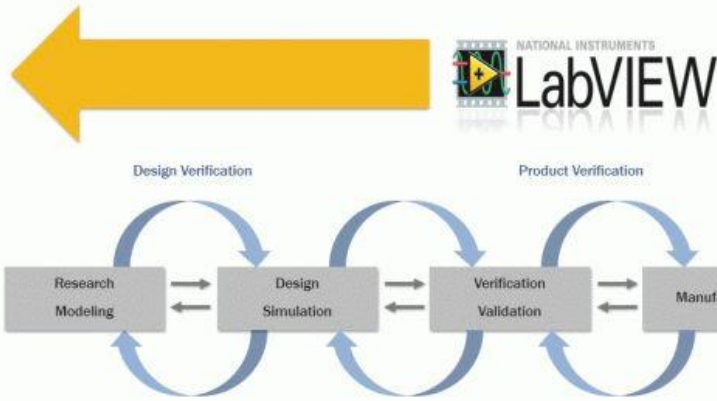
AWR

Ettus Research

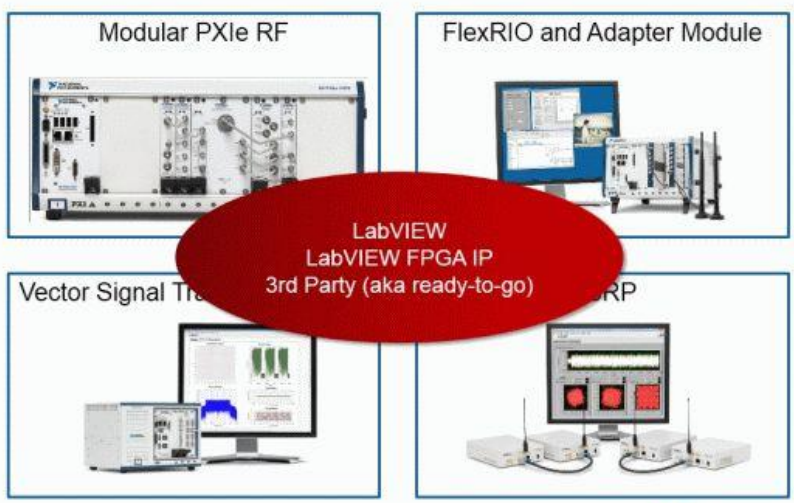
AWR

RF Systems Design R&D Validation Phase Matrix, Inc. Production Tests

Expanding LabVIEW into System Design



Outline – Hardware & Software

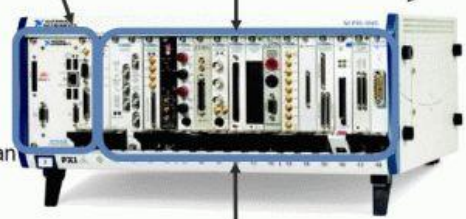


PXI(e) Combines Standard Technologies

Controller
- Embedded PC or remote PC / laptop interface
- Runs all standard software
- Up to 4 cores
- Up to 8GB RAM
- SSD Option (front panel accessible)
- Real-Time OS as an option

Chassis:
- Option for redundant cooling fans
- Up to 925 W total power, no derating 0-55° C

PXI Backplane
- PCI(e) bus
- Timing and Synchronization
- Up to 12GB/s total BW
- Peer-to-peer streaming (module to module)



1500+ Peripheral Modules

PXI Products. . .Over 1,500 and Counting

Data Acquisition and Control
Multifunction I/O
Analog Input/Output
Digital I/O
Counter/Timer
FPGA/Reconfigurable I/O
Machine Vision
Motion Control
Signal Conditioning
Temperature
Strain/Pressure/Force/Load
Synchro/Resolver
LVDT/RVDT
Many More. . .

Modular Instrumentation
Digital Waveform Generator
Digital Waveform Analyzer
Multimeter/LCR Meter
Oscilloscope/Digitizer
Source/Signal Generator
Switching
RF Signal Generator
RF Signal Analyzer
Vector Network Transceivers
Vector Network Analyzer
RF Power Meter
RF Preamplifiers & Attenuators
IF Conditioning
Programmable Power Supply
Many More. . .

Bus Interfaces
Ethernet, USB, FireWire
SATA, ATA/IDE, SCSI
GPIB
CAN, DeviceNet
Serial RS-232, RS-485
VXI/VME
Boundary Scan/JTAG
MIL-STD-1553, ARINC
PCMCIA/CardBus
PMC
Profibus

Others
IRIG-B, GPS
Direct-to-Disk
Reflective Memory
DSP
Optical
Resistance Simulator
Fault Insertion
Prototyping/Breadboard
Graphics
Audio
Many More. . .

Configure the system by yourself at: ni.com/advisor =>PXI Advisor

Example 2. Vector Analyzer - NI PXIe-5665

- **Specifications**
  - Bandwidth: 20 Hz to 3.6 / 14 GHz
  - RTBW: 25 or 50 MHz with DDC
  - Noise: < -154 dBm/Hz (<-165 dBm/Hz) for 1 GHz
  - IP3: > +24 dBm (700 MHz to 3.6 GHz)
  - Phase Noise: -129 dBc/Hz (1 GHz @ 10 kHz)

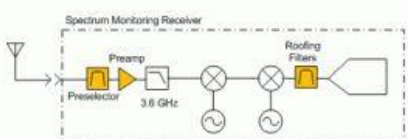
- **Top Features**
  - Great noise and phase parameters
  - RF „List Mode" – fast tuning
  - Multichannel receiver architecture
  - Fast data transfer to CPU and P2P

Applications
- Replacement for any traditional, box instrument
- GNSS, WLAN, ZigBee, LTE, …
- Record and playback

Example 3. Spectrum Monitoring - NI PXIe-5667

- **Specifications – like in NI PXIe-5665 plus:**
  - Pre-selection Filter (NI PXIe-5693):
    - 20 MHz to 7 GHz Preselection
    - DC to 30 MHz Bypass path
    - Integrated preamplifier
    - 16 sub-octave pre-selection Filters
    - 4 notch filters for FM & TV frequencies

  - IF Conditioning Module (NI PXIe-5694):
    - 7 IF Roofing Filters (30 kHz to 50 MHz)
    - IF Outputs: 193.6 MHz,187.5 MHz, 21.4 MHz



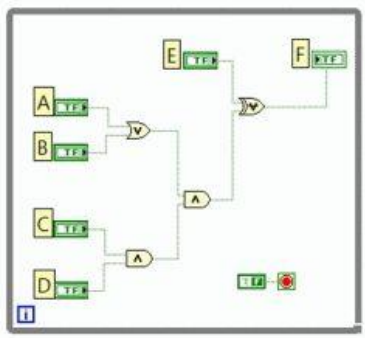
Applications
- Interference detection and identification
- Surveillance (incl. record&playback)
- Jamming / Deception

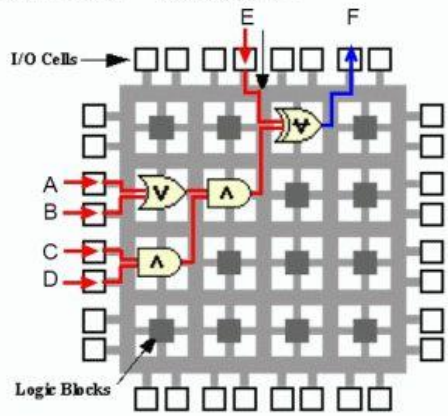
10

LabVIEW Logic in FPGA Implementation

Implementing Logic on an FPGA: F = {(A+B)CD} ⊕ E

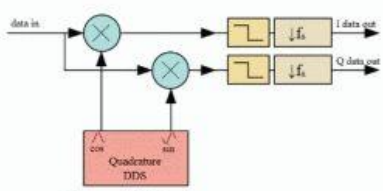
LabVIEW FPGA Code





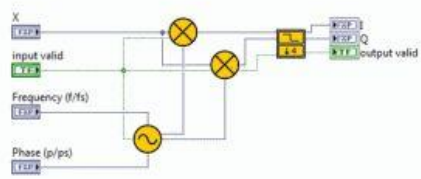
FPGA Circuits Graphical Programming

Think that way:



Source: Wikipedia

Program that way:



Effect – FPGA programming becomes accessible for RF specialists, without in-deep knowledge of FPGA specifics (i.e. VHDL, Verilog, etc.)

NI FlexRIO System Architecture

NI FlexRIO Adapter Module

- Interchangeable I/O
- Analog and digital, RF In/Out or RF In&Out
- NI FlexRIO Adapter Module Development Kit (MDK) for custom adapters

NI FlexRIO FPGA

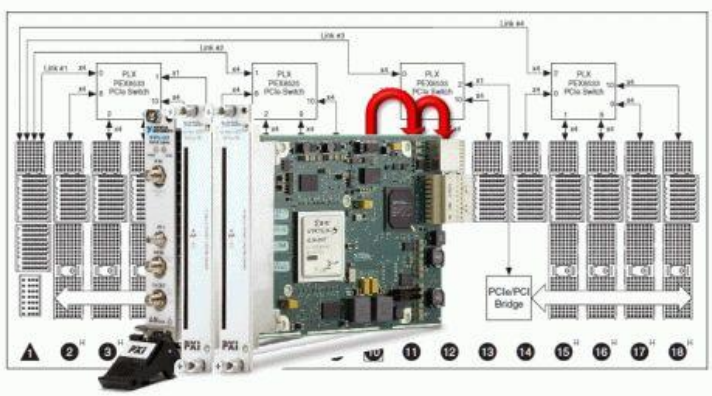
- Virtex-5 or Kintex-7 FPGA
- 132 digital I/O lines (up to 1Gb/s)
- Up to 2GB DDR3 DRAM
- Up to 1540 DSP Slices
- LabVIEW FPGA Cloud Compile Service for faster compilations

PXI Platform

- Synchronization
- Clocks\triggers
- Power Supply\Cooling
- Data Streaming

FlexRIO/RAID P2P Streaming

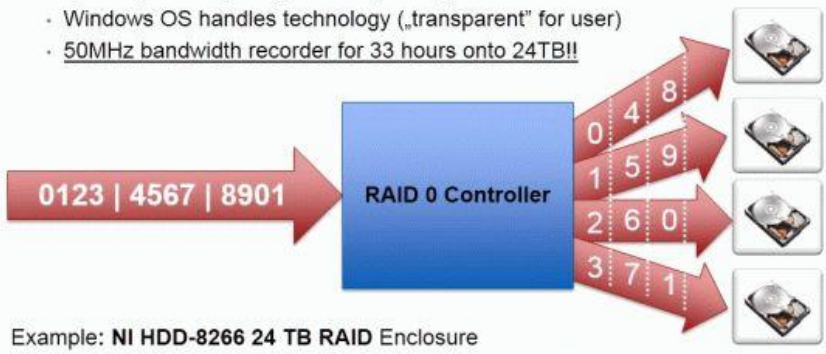
- >800 MB/s unidirectional
- >700 MB/s bidirectional
- ~10 us latency
- Up to 16 streams for 1 FPGA



Usage of RAID technology

„**R**edundant **A**rray of **I**ndependent **D**isks"
RAID 0 → Seperation of data stream without redundancy

- Speed gain comparing to saving to single HDD
- Windows OS handles technology („transparent" for user)
- 50MHz bandwidth recorder for 33 hours onto 24TB!!



Example: **NI HDD-8266 24 TB RAID** Enclosure
Up to **3.6 GB/s** sustained read and write speeds

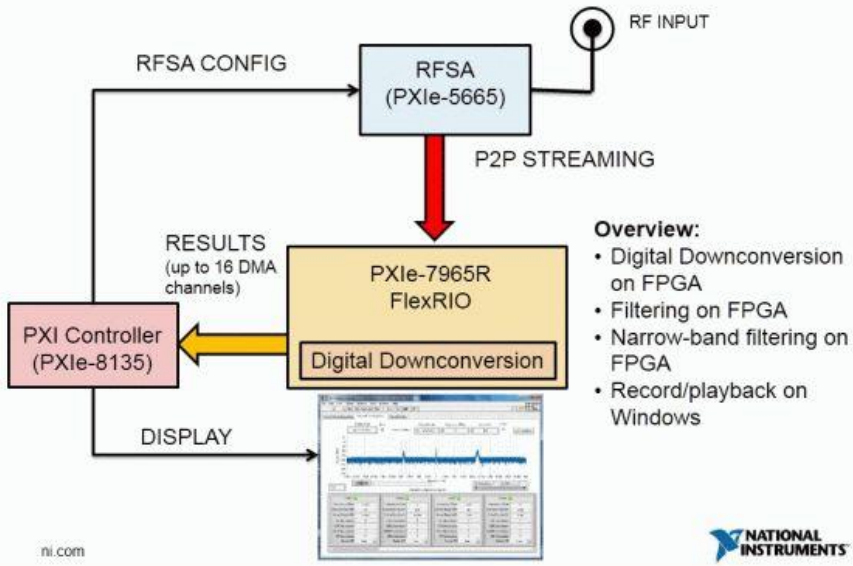
User Solution: IAV Automotive Engineering Inc.

About IAV Automotive Engineering:
IAV Automotive Engineering is one of the leading engineering and design providers for the automotive industry, working for automakers and suppliers like **Audi**, **Bentley**, **BMW**, **Chrysler**, **Daimler**, **Ford**, **GM**, **Porsche** and **Volkswagen**. One of the company's recent projects involved testing and validating in-vehicle radio and navigation systems for one of Germany's leading car manufacturers.

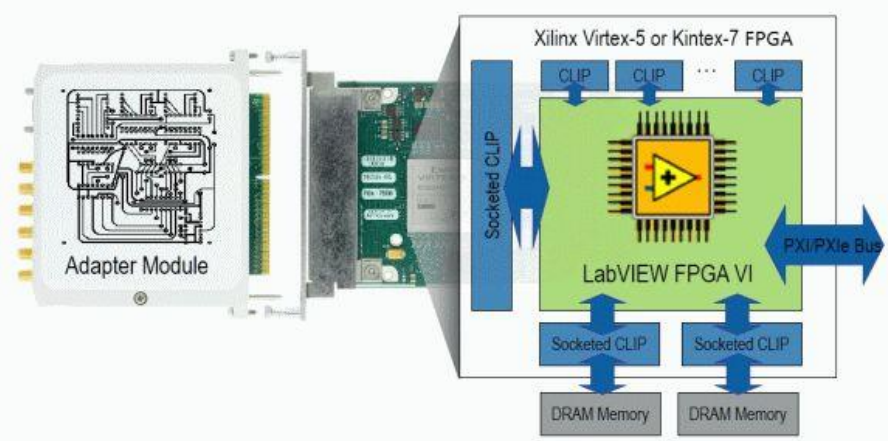
- RF signal testing (AM/FM, RDS, TMC, DAB/DMB, GPS, and HD Radio (IBOC))
- Must ensure top-notch quality during thousands of possible test cases
- Needed repeatability to make their test and validation operations as efficient as possible – record and playback solution based on PXI

"When you're dealing with the most prestigious automakers in the world, quality is of the utmost concern; the high-throughput RF streaming capabilities of NI PXI technology has made it efficient for us to record and play back all common analog and broadcast signals in use today".
- Hans-Joachim Tepper, a test engineer at IAV

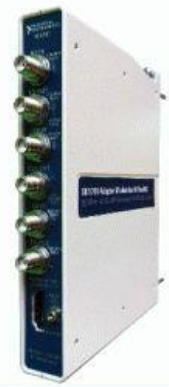
FPGA Coprocessing - Multichannel DDC



NI FlexRIO & FAM (Front Adapter Module) Modules



FlexRIO RF Transceiver – NI 5791



- Specifications
  - Frequency: 200 MHz to 4.4 GHz
  - I/O: (1) Rx, (1) Tx
  - Duplex Mode: FDD, TDD
  - RF RTB: 100MHz (FDD)
  - Dynamic range: > 80 dB
  - Phase noise: -90 dBc/Hz @ 10 kHz (2.44 GHz)
  - ADCs: 14b, 130 MS/s
  - DACs: 16b, 640 MS/s
- Features
  - LabVIEW FPGA
  - 12 lines DIO
  - External LO architecture

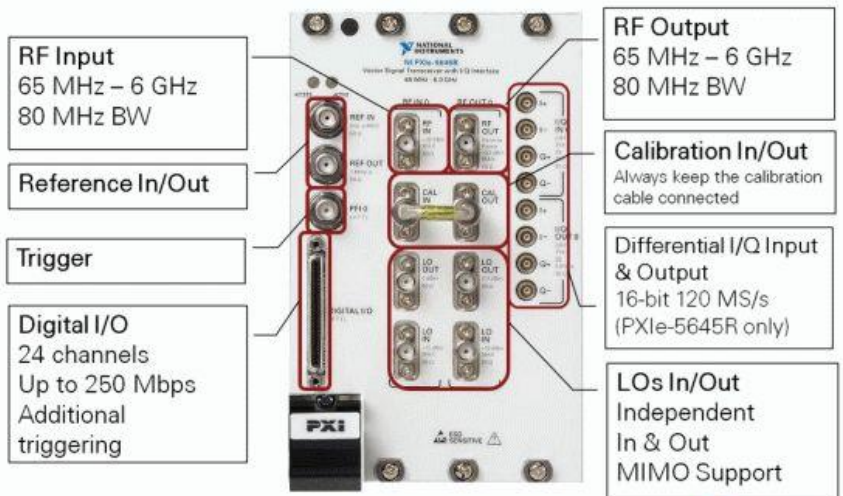
Applications
- Coherent MIMO
- Software Defined Radio
- On-line spectrum analysis
- Research and prototyping communication protocols

FlexRIO RF High Bandwidth RF In/Out – NI 5792/3

- Specifications
  - Frequency: 200 MHz to 4.4 GHz
  - I/O: (1) Rx or (1) Tx
  - RF RTB: 200MHz (FDD)
  - Dynamic range:> 105 dB
  - Phase noise: -94 dBc/Hz @ 10 kHz (2.4 GHz)
  - ADC (5792): 14b, 250 MS/s
  - DAC (5793): 16b, 250 MS/s
- Features
  - LabVIEW FPGA
  - 12 lines DIO
  - External LO architecture

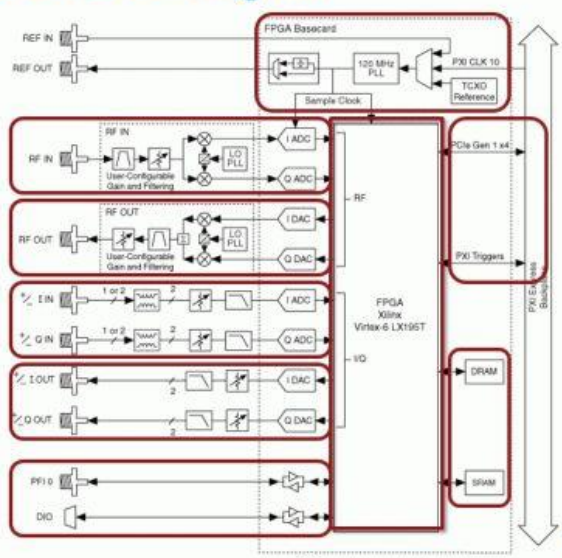
Applications
- Coherent MIMO
- Software Defined Radio
- On-line spectrum analysis
- Beamforming
- Signal intelligence (SIGINT)

RFSA + RFSG + Digital I/O + FPGA ≈ VST



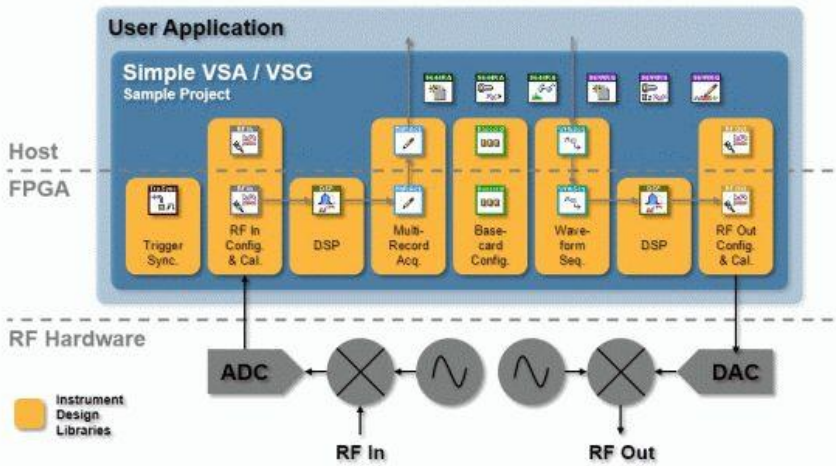
NATIONAL INSTRUMENTS

PXIe-5645R Block Diagram

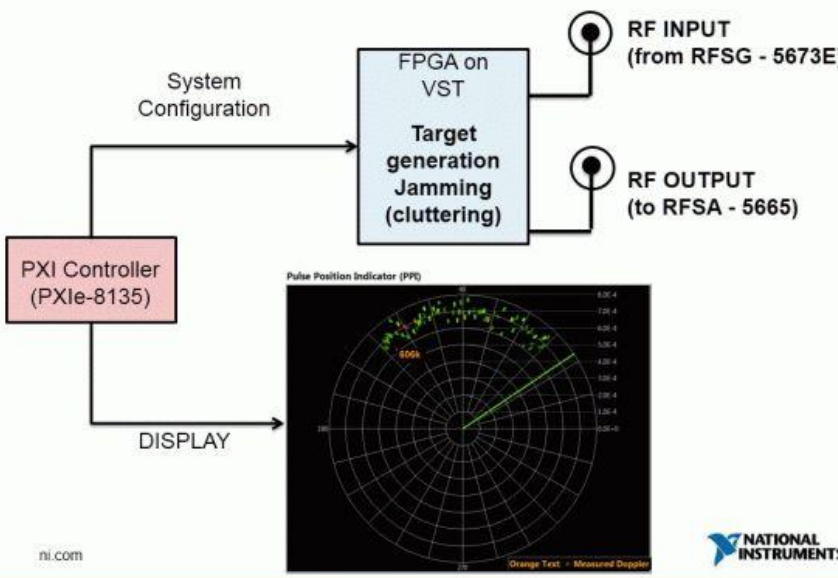


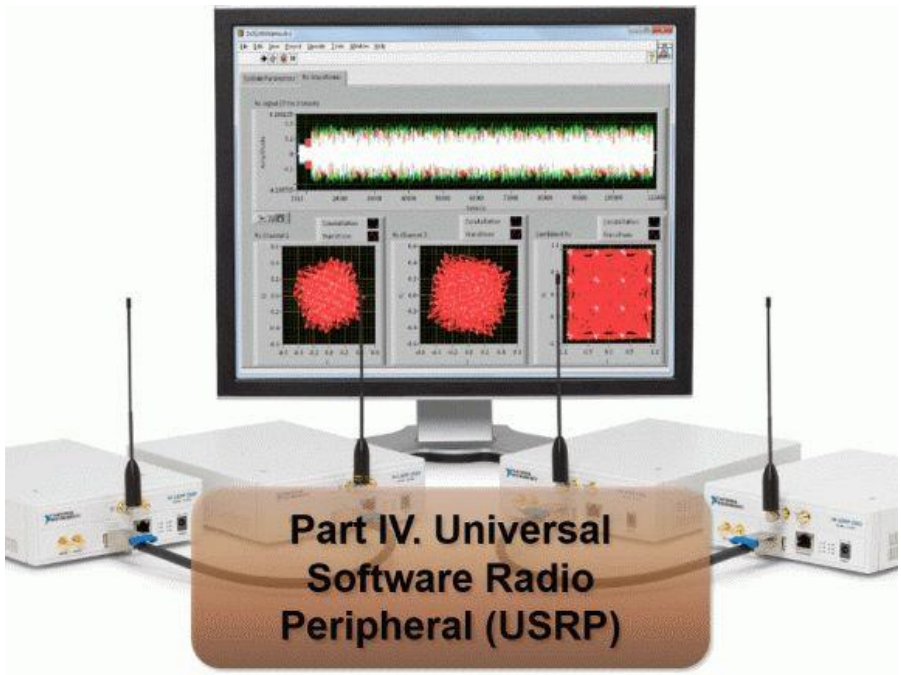
NATIONAL INSTRUMENTS

Simple VSA / VSG Sample Project

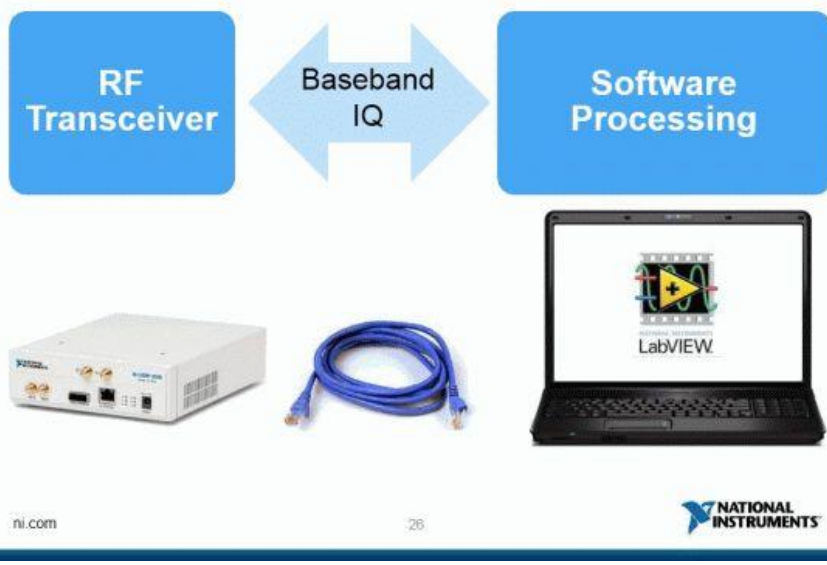


Radar Demo – With VST

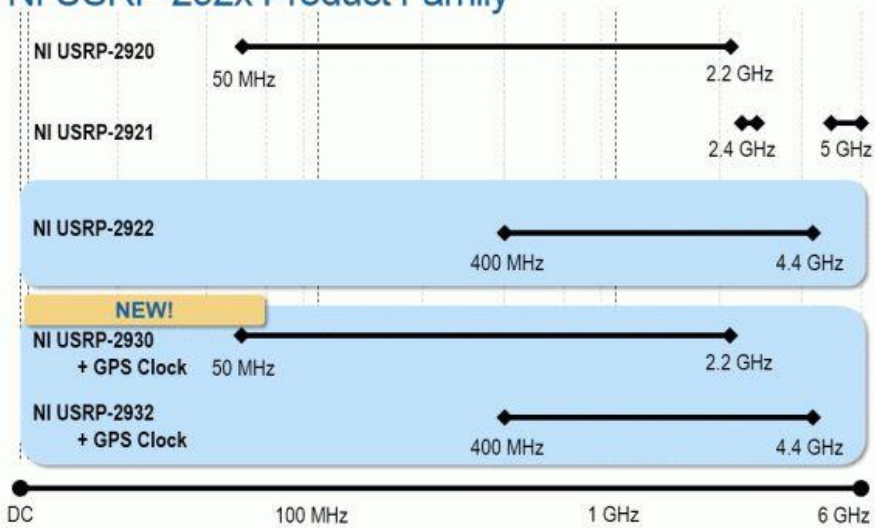




NI USRP Software Defined Radio



NI USRP-292x Product Family



GPS-Disciplined Clock Enabled Applications

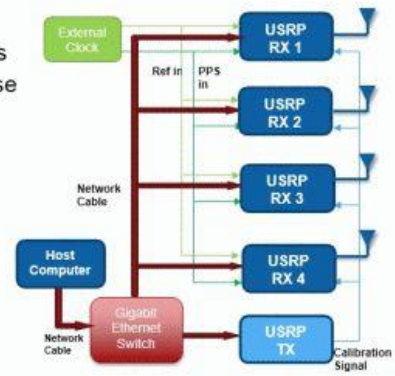
- Distributed MIMO
- Spectrum Monitoring
- Triangulation
- Cognitive Radio
- Adaptive beam forming

NI USRP Research Case Study: Position Detection & Localization

Prof. Athanassios Manikas
Comm & Array Processing Chair
Imperial College, London
Imperial College London

- Testing MUSIC direction finding algorithm
- Rapid prototyping in LabVIEW with MathScript RT
- Synchronized up to12 USRP devices
- Reference provides continuous phase alignment compensation

Direction Finding (uniform linear array)



NATIONAL INSTRUMENTS

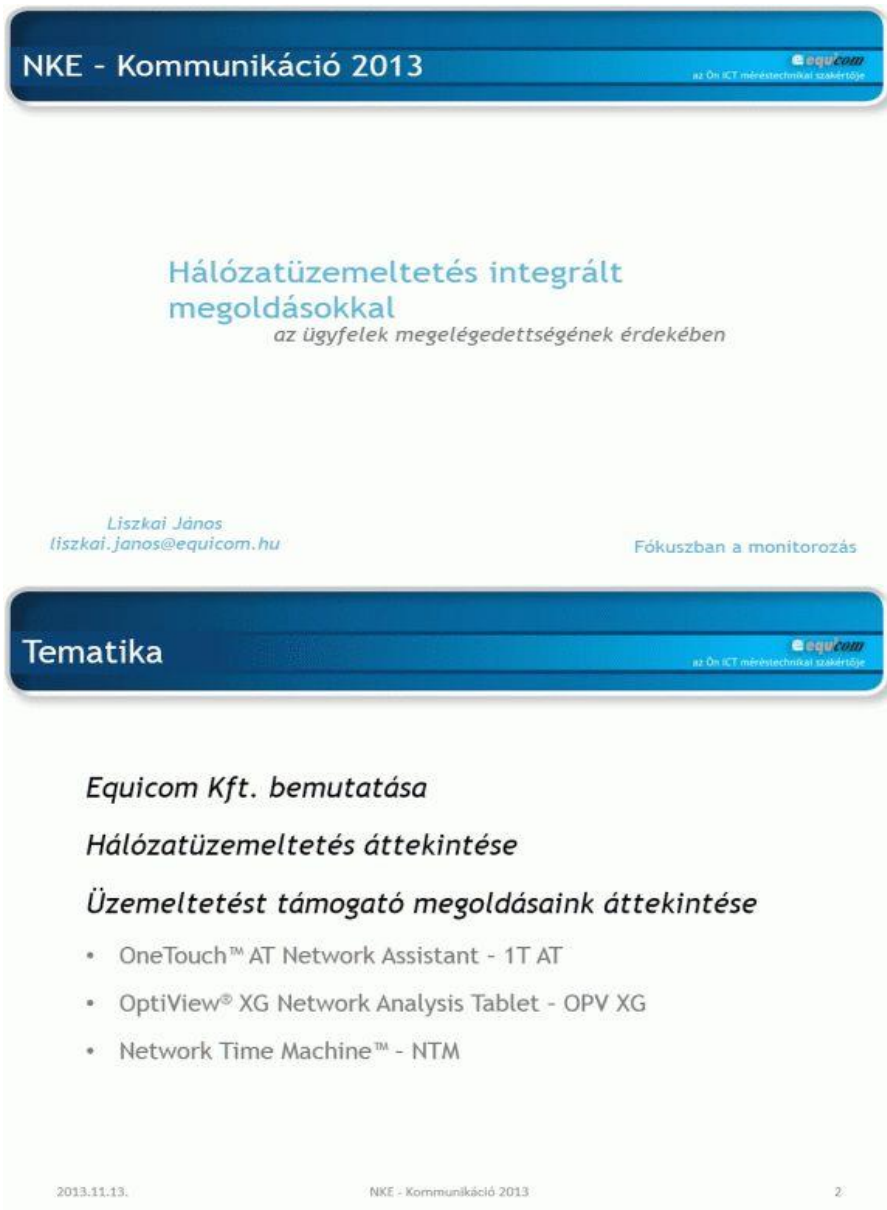
Summary

- PXI RF Instruments as a replacement for traditional, box instruments
  - Added FPGA for very fast DSP
  - Record and playback capabilities
  - Configure your system by yourself at: **ni.com/advisor** =>**PXI Advisor**
- PXI FlexRIO Adapter Modules as a mid-cost, FPGA-based solutions for SigInt, beamforming and SDR
- Vector Signal Transceiver as a generator, analyzer, digital I/O and FPGA processing unit in 3-slot device (4 with IQ I/O)
  - Ready-to-go software for typical applications (streaming, etc.)
  - Open firmware for custom applications
- USRP as a low-cost, SDR solution
- All of the above supported by powerful LabVIEW Software or 3rd party solutions from NI's Partners (ni.com/partners)

NATIONAL INSTRUMENTS

LISZKAI János

HÁLÓZATÜZEMELTETÉS INTEGRÁLT MEGOLDÁSOKKAL



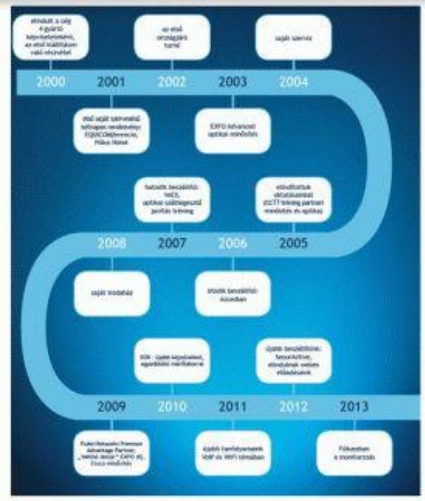
Equicom Kft. bemutatása

equicom
az Ön ICT méréstechnikai szakértője

- Kizárólag ICT méréstechnikai megoldásokra szakosodva
- Több mint 15 éves szakmai múlt
- Világviszonylatban vezető beszállítók kizárólagos magyarországi képviselete

EXFO, Fluke Networks, AIRMAGNET, FITEL, SUNRISE TELECOM, VeEX, ACCEDIAN, SecureActive

- Piaci jelenlét: szolgáltatók és vállalati szegmens
- Közvetlen kapcsolat a felhasználó és a gyártó között
- Szakértelem, tanácsadás, támogatás, szakmai oktatások (9 tematikus EOK tanfolyam)



Hálózatüzemeltetés

equicom
az Ön ICT méréstechnikai szakértője

Csak egy dolog állandó: a VÁLTOZÁS!

- Expanzió
- Konszolidáció
- Új alkalmazások és szolgáltatások

Szigorú rendelkezésre állás

- Teljesítményproblémák gyors elhárítása kiemelt fontosságú!

Hálózatüzemeltetés

equ'com
az Ön ICT méréstechnikai szakértője

Jól definiált projekt terv a változások követéséhez

Hálózatüzemeltetés

equ'com
az Ön ICT méréstechnikai szakértője

	Felmérés	Telepítés/Érvényesítés	Hibakeresés/Üzemeltetés
Feltételek	• Jelenlegi környezet felmérése • Infrastruktúra skálázódása, flexibilitása • Változáshoz szükséges erőforrások feltárása • Mik lesznek a változások hatásai?	• Az új rendszer telepítése, konfigurálása • Teljesítményvizsgálat • Személyzet felkészítése, oktatása	• Hibakeresés, bizonyítani az igazunkat • Változtatások elvégzése • Optimalizálás
Feladat	• Leltár • Topológia • Teljesítmény küszöbök • Dokumentálás	• Portok, kábelek ellenőrzése • Throughput vizsgálat • Válaszidők mérése • Link teljesítménymérése • Dokumentálás	• Probléma vizsgálat • Sávszélesség kihasználtság mérése • Útvonal vizsgálat • Infrastruktúra állapotvizsgálata • Csomaganalízis • Dokumentálás

Üzemeltetést támogató megoldásaink áttekintése

equ'com
az Ön ICT méréstechnikai szakértője

Felmérés | Telepítés/Érvényesítés | Hibakeresés/Üzemeltetés

- Hálózat és szerver teljesítmény felmérés
  - *Kulcs eszközök és linkek*
- Eszközleltár és topológia
- Sávszélesség teszt
- Kihasználtság vizsgálata
- Forgalomanalízis
  - *Összetétel, mennyiség, szereplők*



Üzemeltetést támogató megoldásaink áttekintése

equ'com
az Ön ICT méréstechnikai szakértője

Felmérés | **Telepítés/Érvényesítés** | Hibakeresés/Üzemeltetés

- Hálózati teljesítmény teszt
  - *Throughput, Latency, Jitter, Frame Loss, QoS*
- Alkalmazás teljesítmény
  - *TCP válaszidő*
  - *3Play paraméterek (MOS, R-faktor, stb.)*
- Alkalmazás infrastruktúra
  - *Állapot, válaszidő*
- 10/100/1000M, 10G linkek minősítése



Üzemeltetést támogató megoldásaink áttekintése

Felmérés | Telepítés/Érvényesítés | Hibakeresés/Üzemeltetés

- SLA paraméterek vizsgálata
- Monitorozás
- Problémakezelés, riasztás
- 1 klikk/OneTouch teszt
- Kulcs eszköz monitorozás
- Flow és csomaganalízis
- Riportok készítése, dokumentálás



2013.11.13. NKE - Kommunikáció 2013 9

OneTouch™ AT Network Assistant

Egy érintés a vezetékes és vezeték nélküli hálózat vizsgálatához klienstől a felhőig.

- **Hordozható hibakereső** *réz, optikai és Wi-Fi hálózatokra*
- **Beépített teszteljárások**
- **AutoTest** *egy perc alatt*
- **Alkalmazás és hálózati teljesítmény tesztek**
- **Wi-Fi teljesítményvizsgálat** *a Veri-Fi™ eljárással*
- **Capture** a beépített és filterezhető in-line/végponti TAP segítségével
- **Remote Control** *a táveléréshez és együttműködéshez*

2013.11.13. NKE - Kommunikáció 2013 10

OptiView® XG Network Analysis Tablet

equ'com
az Ön ICT méréstechnikai szakértője

Dedikált eszköz automatizált hálózati és alkalmazás analízisre és a hiba gyökerének gyors feltárására

- **Kapcsolódás, generálás, és capture** *akár 10G-s linken*
- **Alkalmazás centrikus analízis** *akár csomagdekódolás nélkül*
- **Eszközleltár** és képességek felderítése
- **Wi-Fi hálózatok vizsgálata** - *biztonság, lefedettség és interferencia kérdések*
- **Beépített dokumentáció a problémamegoldáshoz**
- **Útvonal analízis** *a hálózati teljesítmény problémák feltárásához*
- **Hálózati teljesítmény teszt** *az SLA paraméterek ellenőrzéséhez*

2013.11.13. NKE - Kommunikáció 2013 11

Network Time Machine™

equ'com
az Ön ICT méréstechnikai szakértője

Minden az egyben megoldás, csomagvesztés nélküli diszkre írás közben azonosítja a hibás hálózati tartományt vagy szervert

- **Nagy teljesítményű capture** akár 20Gbps sebességgel
- **Folyamatos teljesítményanalízis** *a problémás terület izolálására (kliens, szerver vagy hálózat)*
- **Alkalmazás centrikus analízis** *akár csomagdekódolás nélkül*
- **Szerver alapú appliance** *adatrögzítés, tárolás, utólagos analízis és dokumentálás céljára*

2013.11.13. NKE - Kommunikáció 2013 12

Témakörrel kapcsolatos oldalak

equicom
az Ön ICT méréstechnikai szakértője

http://www.equicom.hu/onetouch_at

http://www.equicom.hu/optiviewxg

http://www.equicom.hu/ntm

info@equicom.hu

equicom
az Ön ICT méréstechnikai szakértője

Köszönöm a figyelmet!

?

TRENCSÁNSZKY Imre

A DIGITÁLIS KATONA ALAPFELSZERELÉSE: IP ALAPÚ, TAKTIKAI ADATTOVÁBBÍTÓ RENDSZER

VTQ ORCA II SD COFDM alapú képi, hang és adattovábbító hírközlési rendszer jellemzői

A kombinált adat-hang átviteli rendszer több mint egy okos rádió, mivel harctéri körülmények között képes kép, kétirányú hangkapcsolat és kis sebességű telemetriai (RS232<128 kbps 868 MHz-en) adatkapcsolat egyidejű kiszolgálására.

Jellemező alkalmazási területei:

- harctéri robotvezérlés (pl. UAV, aknamentesítő...)
- személyi (POV) kamerakép közvetítése pl. sisakkamera vagy fegyvertávcső kameraképe (katonai vagy rendőri erők használhatják)—az NKE számára szállított rendszer ilyen
- álcázott fix telepítésű PTZ kameraállomások rádiós adattovábbítási igényeinek kiszolgálása (pl. tábori területvédelem vagy határvédelem)

SCI-Network

VTQ ORCA II SD kép és hangtovábbító rádió-adórendszer főbb műszaki paraméterei

- COFDM moduláció a kép felirányú továbbítására (QPSK, 16 QAM, 64 QAM), GFSK a kétirányú telemetria és WiFi a 2. tartalék video-jelfolyam(stream) átvitelére
- sávszélesség: 6,7 vagy 8 MHz
- kódolás-hibajavítás: ½, 2/3, ¾, 5/6, 7/8
- video-jelfolyam tömörítés codec: MPEG2
- titkosítás: 256 AES
- késleltetés: 200 ms
- felbontás: max. 576iPAL/ 30 framerate
- 1 db full-duplex audio csatorna (MP3 128 kbps) az élőbeszédre
- interfészek: analóg PAL kép + 1 db RCA a hang részére
  1 db RS232 és 2,4 Ghz WiFi a mellényben
- frekvencia: tetszőlegesen rendelhető a 200 MHz-6 GHz-es tartományban; a szállított ZMNE eszköze COFDM (képátvitel) modulációval 340-400 MHz-es sávban működik; a telemetria GFSK modulációval 868 MHz-en, az IP alapú 2. videostream 2,4 GHz-en
- adóteljesítmény: 200mW COFDM és 500 mW GFSK (max 10W-os rendelési opció)

SCI-Network


A valósidejű adattovábbító-rendszer katonái ruházaton viselhető változata a 2 db mobil-eszközzel (ZMNE Híradó tanszék Demonstrációs eszköz)
Feladata: kétirányú hang és adatkommunikáció + képi és hanginformáció továbbítás
sisakkamera
Fejbeszélő+hallgató
Taktikai mellény a beépített eszközökkel (interfészillesztők, digitalizálás,adófokozatok, akkumulátor és antennák)
2 db IP67-es védettségű érintőképernyős mobileszköz a szöveges üzenetek és a 2. videostream kétirányú továbbítására
SCI-Network

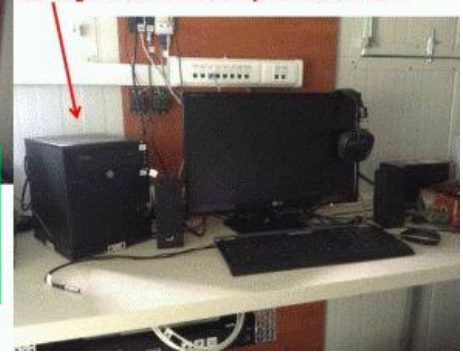

A valósidejű adattovábbító-rendszer katonai ruházaton viselhető változata a (ZMNE Híradó tanszék Demonstrációs eszköz)
Feladata: kétirányú hang és adatkommunikáció + képi és hanginformáció továbbítás
SCI-Network

Az adattovábbító rendszer parancsnoki-operátori bázisállomása az antennarendszerrel egy zárt, vontatható, kitolható árbóccal ellátott utánfutóra szerelve; (antennarendszer és álcázott konténer külső kép, ZMNE Híradó tanszék Demonstrációs eszköz)
Feladata: 350 és 868 valamint 2400 MHz-es bázisállomási működés

Az adattovábbító rendszer parancsnoki-operátori bázisállomása egy zárt vontatható utánfutóba szerelve (konténerbelső kép, ZMNE Híradó tanszék Demonstrációs eszköz)
Feladata: 350 és 868 valamint 2400 MHz-es bázisállomási működés

Analóg és digitális képi források vétele és megjelenítése, 2 irányú kihangosított hangkapcsolat, 2 irányú RS232 telemetria, PoE WiFi bázisállomás vezérlése (VTQ adó-vevőegység, PoE switch, WiFi AP)

Központi irányítópult a HP miniszerveren futó IP alapú alkalmazásokkal: hang, kép-digitalizálás és rögzítés valamint a 2-irányú szöveges üzenetküldés operátorállomása




A MESH alapú kommunikációs rendszereké a jövő
AgileMesh™
A Digitális katona továbbfejlesztési irányai
A sokoldalúság és szinte korlátlan fejlesztési lehetőségek miatt áttérés az IP-re
Elosztott MESH hálózati modell-alig sebezhető
Minél többen használják, annál stabilabb, nagyobb biztonságú
Néhány már megvalósult kiegészítő: pl. kézen viselhető vagy sisakkijelzőn megjeleníthető érintőképernyős bevetés-támogató eszköz; személyi fej, infra és fegyvertávcső kamerák képének átküldése a bevetésben résztvevők számára, drón(ok) képének közvetlen átvitele a földi taktikai csoportnak, közvetlen drónirányítás
A különféle egyéb, külső (vegyi, biológiai) szenzorok csatlakoztathatósága és az egyéni fizikai állapot monitorozás előtt megnyílik az út
A rádiós MESH IP hálózat csak a keretet, hordozóközeget adja a felhasználási lehetőségek és jövőbeni kiegészítő eszközök, szoftverek könnyen integrálhatóak
SCI-Network

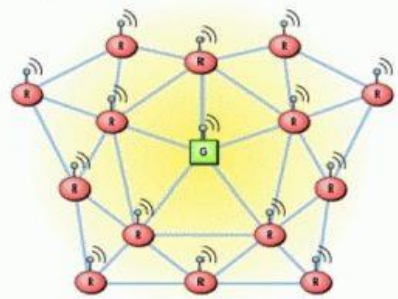

A MESH alapú kommunikációs rendszereké a jövő
AgileMesh™
Miért használjunk rádiós MESH hálózatokat?
A kommunikációs hálózatok jövője: elosztott hálózati modell nagy hibatűréssel
A hagyományos centrális és sebezhető struktúrával szemben jóval kevésbé sebezhető: multipont-multipont alapú
A hálózat tetszőleges két végpontja között közvetlen kapcsolatot nyújt
Többszörös adatbetáplálási és többszörös fogadási pontok
Szükségtelenné teszi az infrastruktúra tervezést
Automatikusan, önállóan formálódik, konfigurációt nem igényel
Sérülés esetén öngyógyuló, újrakonfigárólódó
Optimalizált terhelésmegosztással az információ mindig a legrövidebb útvonalon terjed
Nincs LOS működési korlát (NLOS esetén is működik)
SCI-Network

Az AgileMesh G2 szériájú MESH rendszer jellemzői

AgileMesh™

A MESH egy olyan kommunikációs technológia ahol a pókhálószerű topológia minden egyes csomópontja (node) a saját adatát betáplálja (elterjeszti) a hálózat többi tagja felé és más node-ok adatait pedig relézi (továbbítja). Így minden node adatot vesz és ad (továbbít) multipont-multipont módon. Ezért is lehet az elosztott hálózat nagy hibatűrésű, mivel nincsenek kitüntetett és sebezhető centrális csomópontjai.

Source: Penton Media, Inc. and Machine Design Magazine. Copyright 2007

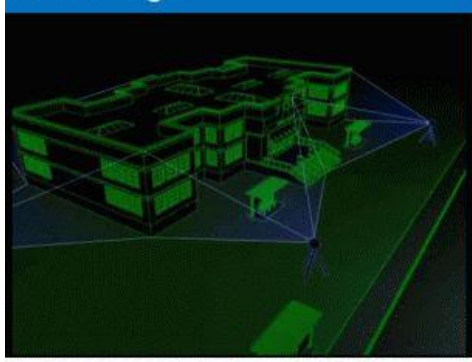


In mesh networks, each wireless node acts like a router, sending and receiving data from other nodes. Self-configuring networks automatically determine the best path for data to take across the network. Data, such as video, automatically bypasses failed or out-of-range nodes.

SCI-NetWork

Az AgileMesh G2 szériájú MESH rendszer alkalmazási lehetőségei

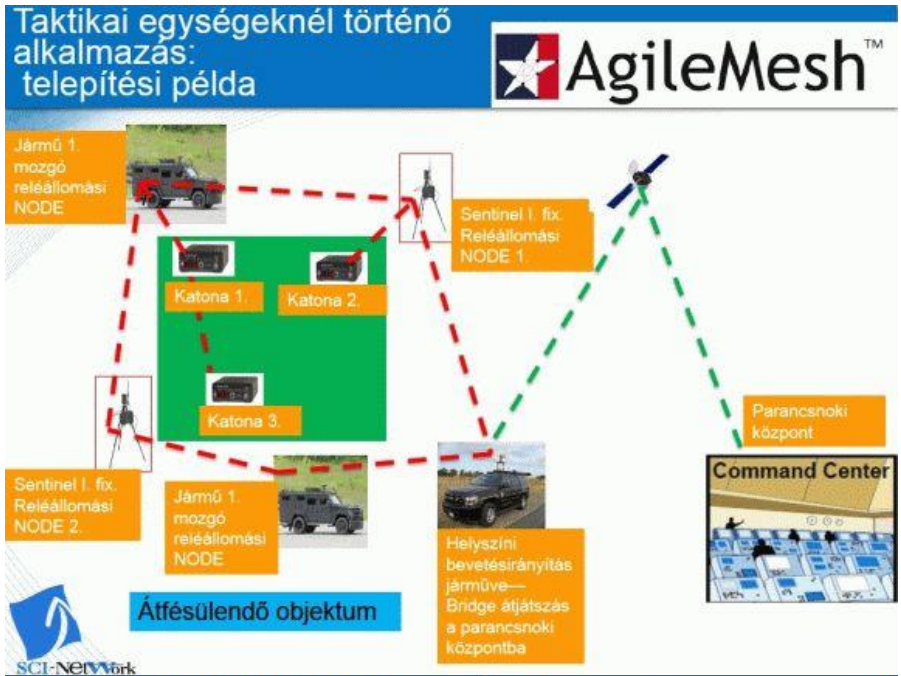
AgileMesh™



Mindig javasolt több betáplálási és kicsatolási pontot használni az adatbiztonság miatt!

- Ismeretlen objektum rajtaütés és objektum átfésülése
- tűszejtési szituációk
- Tüntető, garázda tömeg vagy zárt területek megfigyelése gyorsan telepíthető pontokról
- Periméter (virtuális kerítés) védelem pl. az ideiglenes éjszakai tábor körül—ekkor mozgás, hang, rezgés érzékelők, belövésirány-határoló mikrofonhálózat, gyalogsági felszíni radar (élőerő felderítésére) és infrakamerák telepítése a Sentinel I. 3 lábú mobil állványára
- Drónok és más távirányított járművek kép/hang és adat leirányú sugárzása a taktikai egységeknek

SCI-NetWork


Taktikai egységeknél történő alkalmazás: telepítési példa
AgileMesh™
Jármű 1. mozgó reléállomási NODE
Sentinel I. fix. Reléállomási NODE 1.
Katona 1.
Katona 2.
Katona 3.
Parancsnoki központ
Command Center
Sentinel I. fix. Reléállomási NODE 2.
Jármű 1. mozgó reléállomási NODE
Helyszíni bevetésirányítás járműve— Bridge átjátszás a parancsnoki központba
Átfésülendő objektum
SCI-Network


Az AgileMesh G2 szériájú MESH rendszer felépítése
AgileMesh™
Standard Camera
Thermal Imager
Thermal Imager
Infra-Red Camera
AgileMesh Sentinel
Pole Camera
AgileMesh Watchtower
IP Camera
AgileMesh Scout
Audio
Covert Cameras
Bio-Chem, Alarm and Other Sensors
Bomb Robot
IP Phones
COMMANDO MESH
SCI-Network

Az AgileMesh G2 szériájú MESH rendszer felépítése

AgileMesh™

Személyen viselhető változat

Kisméretű, járóautóba építhető változat

Működés közben átkonfigurálható

- IT tudás nélkül, a feladatot végző személy bevetés közben átállíthatja
- Az RF környezethez automatikusan alkalmazkodik
- Társszervek vagy szervezetek együttműködését is lehetővé tesz (interoperabilitás)

Csatorna és Node azonosító választó (forgató) kapcsoló

- frekvencia
- MeshID
- titkosítás (SAE, AES-256)
- NodeID (IP cím)

Mesh Szomszéd kijelzés

- telepítési segédlet
- Szabad csatorna segéd

SCI-NetWork

Mi a CommandMesh? I.

AgileMesh™

- Esemény, incidens, bevetés-területet lefedő taktikai rádiós MESH hálózat
  - Minden bejövő adatforrás(hang, kép, szenzorok és kommunikáció) adatait egy gyorstelepítésű, területlefedő hálózatba integrálja
  - Valósidejű taktikai információkat továbbít minden egység felé/között
  - Valósidejű, az egységek közötti taktikai kommunikációt továbbít, minden egység felé/között
- Egységes CommandMESH környezet minden a csoportban résztvevő node számára (interoperabilitás más egységekkel)

Járműbe telepíthető AgileMESH készlet

SCI-NetWork

Mi a CommandMesh? II.

AgileMesh™

- A bevetési környezet azonnali átlátása→taktikai tudatosság, előrelátás
- így az első vonalbeli egységek biztonságát javítja
- 360-fokos kamerás megfigyelést tesz lehetővé
- Könnyen kiterjeszthető újabb átjátszó node-ok telepítésével
- Biztonságos átvitel
- Nagyon, gyors, technikai tudást nem igénylő néhány percen belüli telepítés
- Beépített akkumulátor, külső infrastruktúrától független működés (6-8 óra)

SCI-Network

Az AgileMesh G2 szériájú MESH rendszer felépítése

AgileMesh™

- FastEth interfészcsatlakozás a MESH hálózat 25 Mbps -es cellaforgalmához (pl. IP-s HD kamera csatlakoztatásához és a video-stream vételéhez)
- Analóg video input (1 db vagy 2 db)
- Analóg video output
- 1. Audió csatorna – felirányú
- 2. Audió csatorna – kétirányú (csapatkommunkáció– PTT)
- Biztonságos átvitel (AES kódolással)
- Helyszíni felvétel is rendelkezésre áll
- A szigetszerűen működő taktikai MESH hálózatot a központi parancsoksághoz PP link, bérelt vonallal vagy műholdas összeköttetéssel és egy NetworkBridge-Router alkalmazásával csatlakoztatjuk
- Tetszőlegesen választható 2,4, 4,9 és 5,2-5,8 Ghz-es működés (mindet tudja az eszköz); javasolt az EU-ban is használt, 4,9 GHz-es NATO és rendvédelmi szervek számára fenntartott sávban üzemeltetni

SCI-Network

Az AgileMesh célhardver előnyei

AgileMesh™

- Kizárólag erre az célra (elosztott-hálózati rádiós MESH modell) fejlesztett HW és SW
- A videó és audió processzor integrálva van a HW-ben (nem SW-es megoldású)
- Szabadalmaztatott egyedi és titkosított rádiós MESH protokoll
- Egyszerűen kezelhető, szabadalmaztatott felhasználói interfész hogy ne csak a technikai-kiszolgáló személyzet tudja kezelni/telepíteni

- Elsődlegesen taktikai, előretolt, tűzvonalban lévő egységek, terepi adatkommunikációs igényeire fejlesztett, ezért is telepíthető fél órán belül egy MESH node (a viselhető változat azonnal üzemkész)

SCI-Network

Ruházaton Viselhető Digitális katona modell készlet

AgileMesh™

- Az univerzális CommandMesh hálózat egy NODE-ja (mellényzsebben elfér)
- sisakkamera
- Headset (fejhallgató és beszélő)
- 2 db akkumulátor
- akkumulátor-töltő
- Omni-antennák
- kábelek
- csatlakozó-adapterek
- Minden tartozék és a berendezés egy ütés és vízálló kézitáskában kap helyet

SCI-Network

Sentinel I. node—a mobil megfigyelőrendszer

AgileMesh™

- Az univerzális CommandMesh hálózat egy NODE-ja a bőröndbe beépítve
- PTZ kamera Infra képességgel
- könnyen összeállítható és telepíthető 3 lábú felépítés
- Az összes tartozék, Omni-antenna és szerelvény belefér egy ütésálló bőröndbe
- beépített akkumulátor és töltő
- Ütés és vízálló kivitel

SCI-Network

Járműbe építhető változat

AgileMesh™

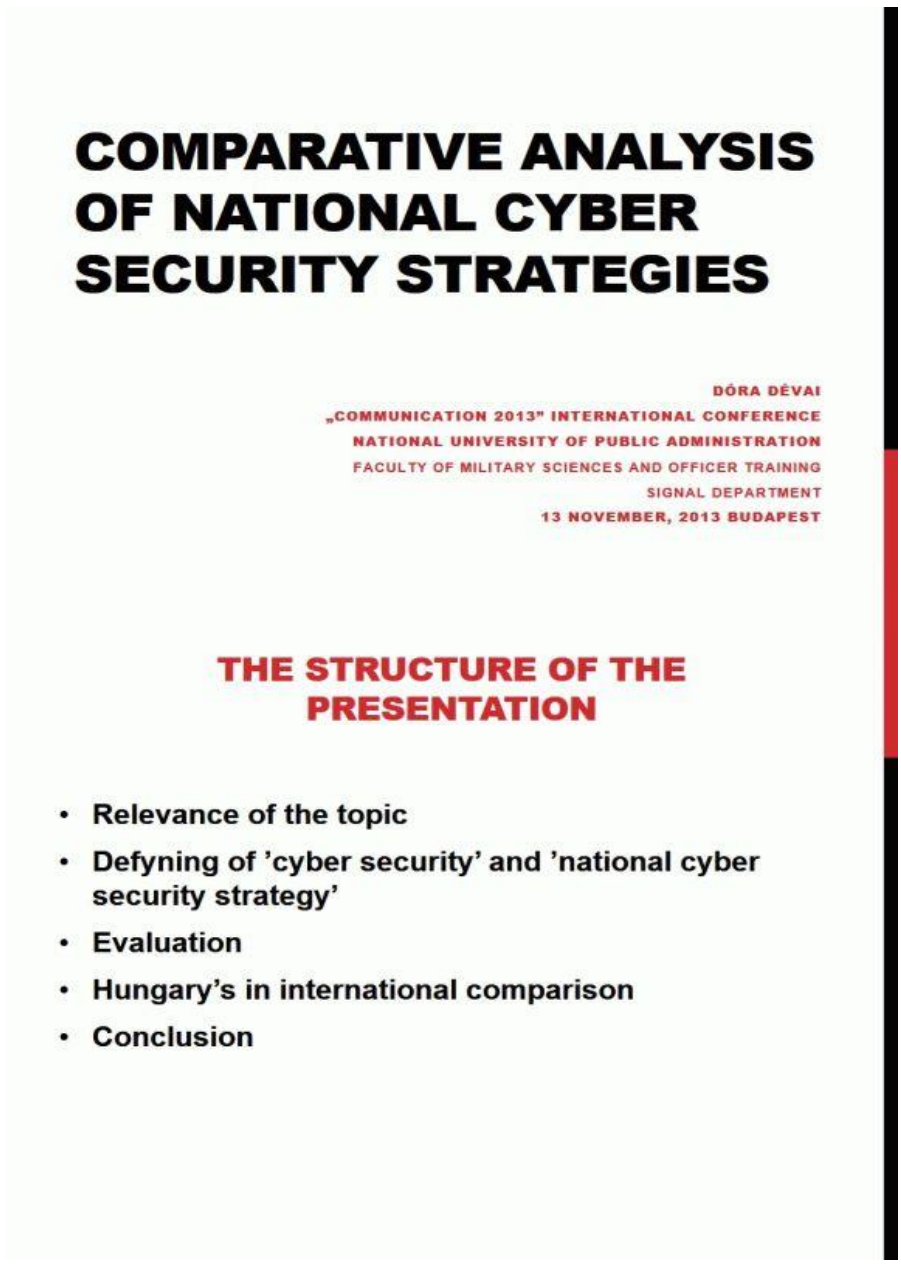
- Az univerzális CommandMesh hálózat egy NODE-ja
- Rackbe (nagy méretű, megfigyelő vagy parancsnoki rádiós kocsira) szerelhető változat—létezik kisméretű járőrautóba való is
- Egyidejűleg Network Bridge is lehet (opció)
- Nagynyereségű omni antennák
- Az osztott rádiós kültéri (ODU) eszköz a jármű tetején lévő árbócra van szerelve az RF veszteségek minimalizálása érdekében (PoE táplálás)

SCI-Network


Köszönöm a figyelmüket!
timre@scinetwork.hu
SCI-NetWork
Távközlési és Hálózatintegrációs zRt. ▪ 1142 Budapest, Erzsébet királyné útja 125. ▪ telefon: 06 1 467-7030

Dóra DÉVAI

A COMPARATIVE ANALYSIS OF NATIONAL CYBER STRATEGIES



THE INCREASING RELEVANCE OF CYBER SECURITY AND NATIONAL CYBER SECURITY STRATEGIES

Evolutionary trends in cyberspace have accelarated since the mid 1990s.

First well-publicised major incidents incidents appear, e.g.:

- First wave in 2000, the year of the millenium software bug and „Love Letter" software worm.
- DDoS attack on Estonia in 2007.
- Cyber attack on Georgia in 2008.
- Stuxnet in 2010.

DEFYNING OF 'CYBER SECURITY' AND 'NATIONAL CYBER SECURITY STRATEGY

No universally accepted definition.

- **ISO**
- **ITU**
- **ENISA**
- **EDA**
- **NATO**

Huge diversity at the national level. What transpires is more a reflection of general trends.

EVALUATION

Standards set by the Europan RAND Corporation studies

Cyber Power Index (by Booz Allen Hamilton)

ENISA

HUNGARY'S IN INTERNATIONAL COMPARISON

Hungary's National Cyber Security Strategy (21 March, 2013)

Act 50 of 2013 about the Electronic Information Security of the Governmantal and Municipal Entities (25 April, 2013)

CONCLUSION

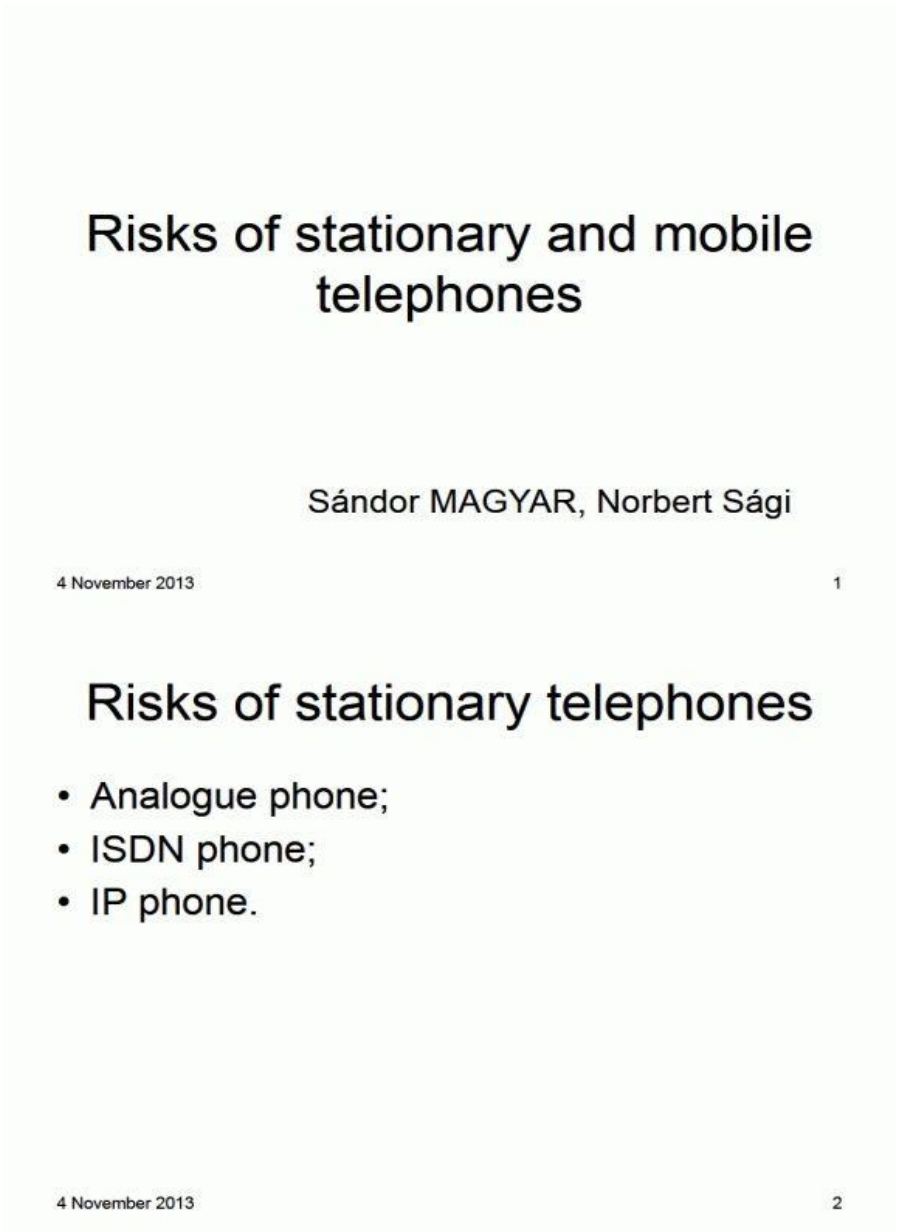
-Current results

-Future trends

-Hungary on the right track (?)

Sándor MAGYAR – Norbert SÁGI

RISK OF STATIONARY AND MOBILE TELEPHONES



Stored call information

- Source telephone number;
- Destination telephone number;
- Call time;
- The length of a call;
- Routing information;
- Etc.

Risks of PBX

- Default login and password;
- No password policy;
- No different level of passwords;
- Open communication port;
- Remote access to the PBX;
- Lost or unmanaged analogue extensions;
- Telephones with modem tones;

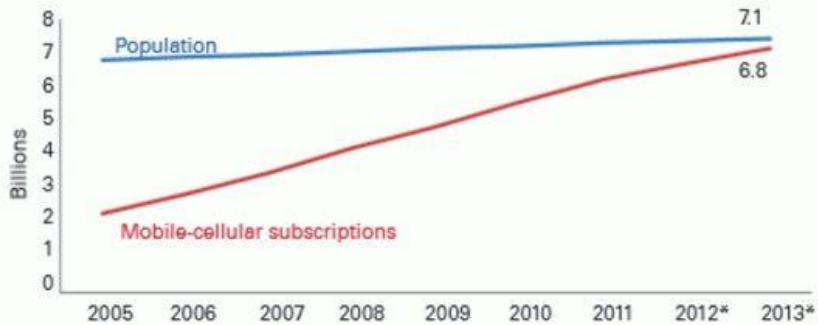
Risks of stationary IP telephones

- IT endpoint;
- Reconnaissance;
- Spoofing;
- Eavesdropping;

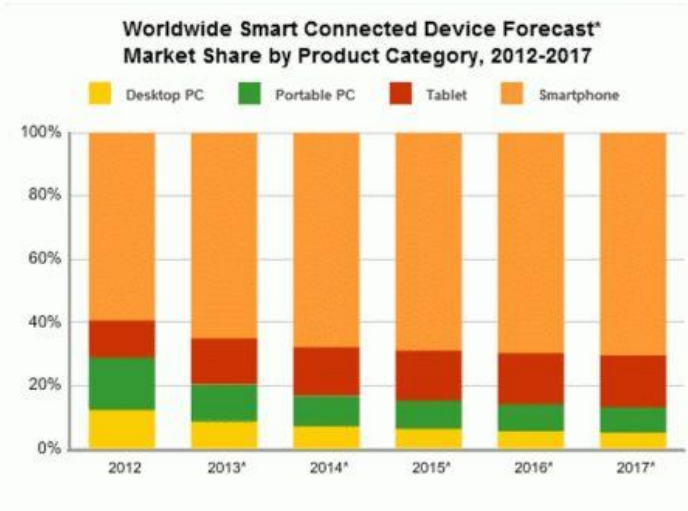
Risks of stationary IP telephones

- Signalling and media manipulation
- Service theft/fraud
- DoS/Distributed DoS (DDoS) attacks
- Fuzzing and buffer overflow exploits
- VoIP spam
- VoIP phishing

Global mobile-cellular penetration a

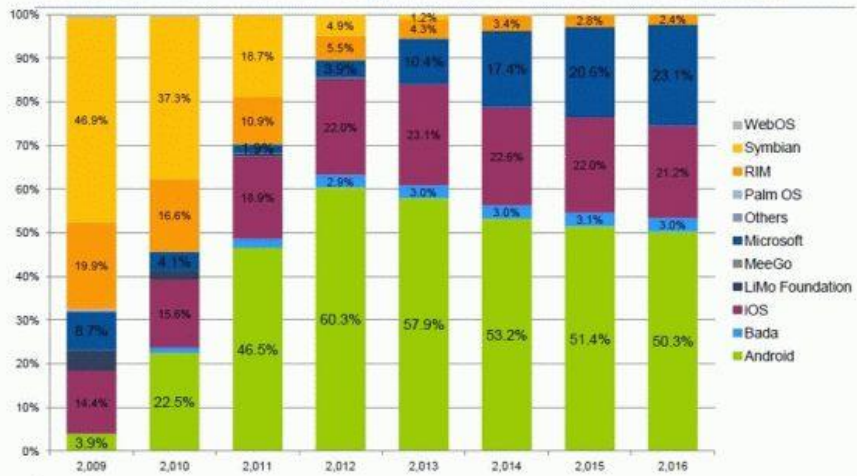


Source: ITU World Telecommunication /ICT Indicators database
Note: * Estimate



Source: IDC Worldwide Quarterly Smart Connected Device Tracker, September 11, 2013.

Gartner Forecast Estimates Mobile OS Sales by Market Share (2009-2016)



Source: Gartner

Forecast: Mobile Devices by Open Operating System, Worldwide, 2009-2016, 2Q12 Update

Risks of mobile telephones

First time installation

For example on a Samsung Android device:

- Create a samsung account and enjoy a variety of services with a single account
- Do you have a Goggle Account?
- Use WIFI and mobile network location.
- Let Google apps access your location.
- This phones belongs to…

4 November 2013 11

Location

Password protection.

- PIN;
- Screen lock;
- Using the same passwords.

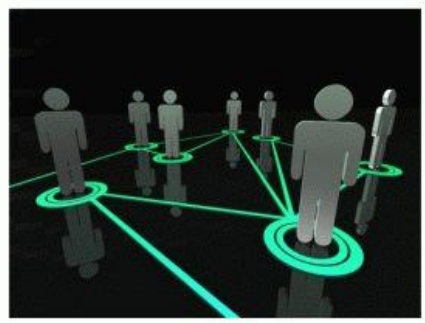
Bluetooth and WI-FI

- Open ports;
- WIFI hotspots;
- Rogue access point;
- VPN tunnel.

Bluetooth®

Social network

- Part of everyday life;
- To be always connected;
- Strong addiction.



Effects of downloading apps

- From unknown or untrusted place
- Malwares that:
  - Generate premium SMS
  - Steal information
  - Record the phone calls
  - Etc.

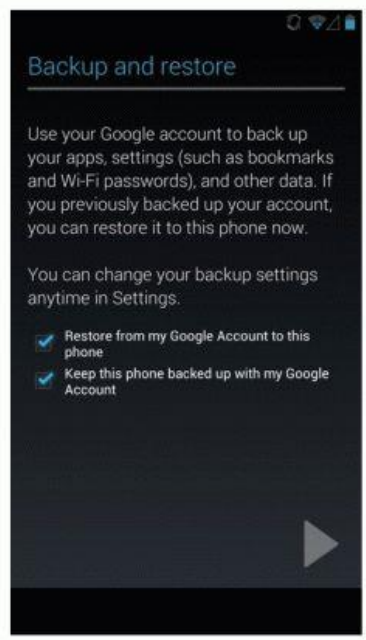
Anti-virus software

- Scanning,
- Updating virus definition,
- Uninstalling apps,
- Deleting files;
- Managing stolen device.

Clouds

Sensitive data in the cloud:

- passwords;
- email accounts;
- backups;
- etc.



Jailbreaking or rooting

- Jailbreaking iPhone;
- Rooting Android;
- Third-party device firmware;

User behaviour

- Use - where?
- Leave - where?

Secondhand phones

- Who has used the IMEI.
- What kind of apps are on the mobile.

Hostile operator network

- Open BTS technology available.
- The mobile connecting the strongest sign.
- Eavesdropping with man-in-the-middle.

NFC

- NFC-enabled phones with mobile wallets

SPOOFING

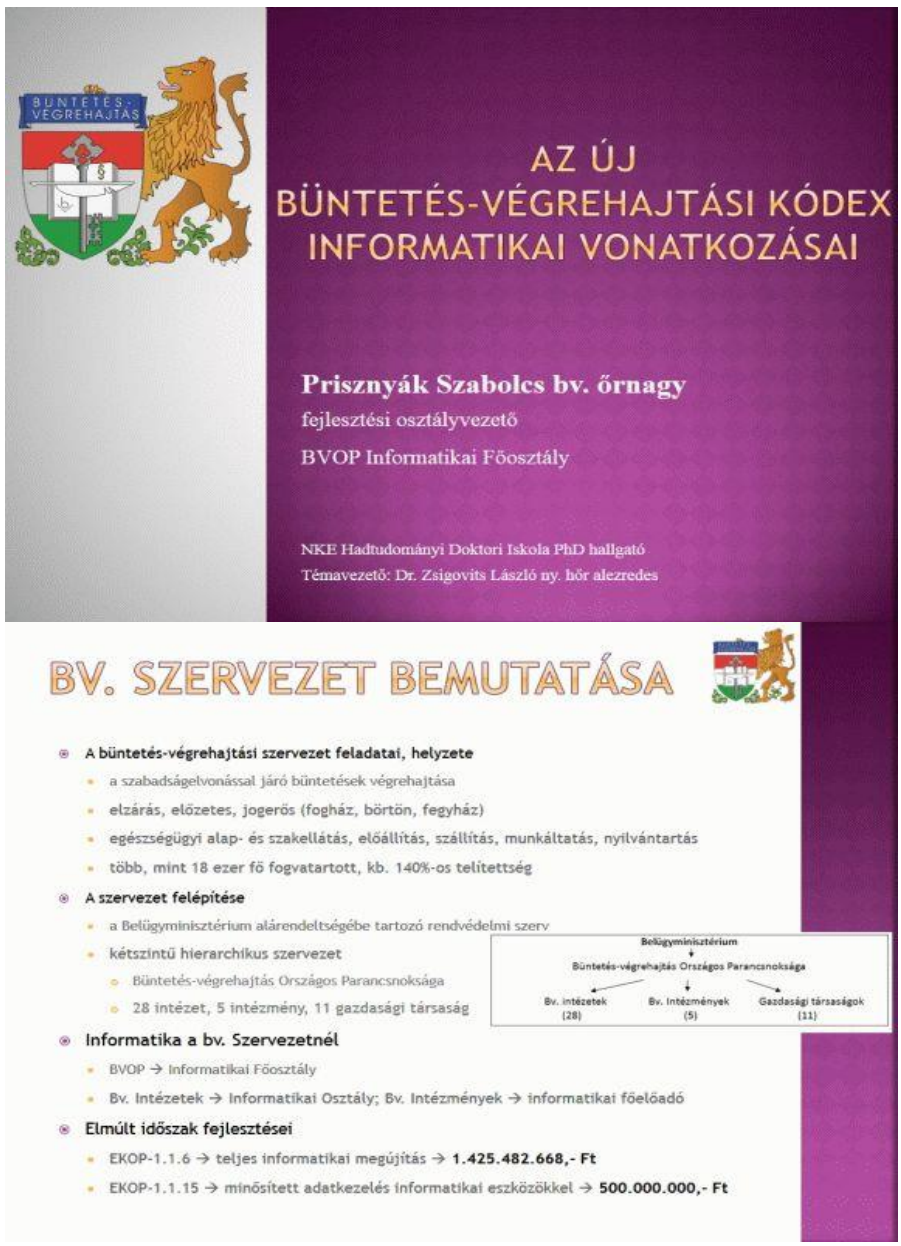
- Caller ID spoofing;
- Caller voice spoofing.
- Background noise;
- SPOOFAPP.

Thank you for your attention!

4 November 2013 25

PRISZNYÁK Szabolcs

AZ ÚJ BÜNTETÉS-VÉGREHAJTÁSI KÓDEX INFORMATIKAI VONATKOZÁSAI



VÁLTOZÁSOK AZ ÚJ BV KÓDEXBEN

- Jelenlegi jogszabályok
  - 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről
  - 1979. évi 11. törvényerejű rendelet a büntetések és az intézkedések végrehajtásáról
  - 6/1996. (VII. 12.) IM rendelet a szabadságvesztés és az előzetes letartóztatás végrehajtásának szabályairól
- Informatikai vonatkozású változások a Bv. Kódexben
  - Kapcsolattartás új formái
  - Reintegrációs őrizet

1979. évi 11. tvr.
kapcsolattartási formák

- látogató fogadása
- levelezés
- telefonálás
- csomagküldés

Bv. Kódex
180.§. Az elítélt kapcsolattartási formái:

a) ~~levelezés,~~
b) elektronikus levelezés,
c) telefonbeszélgetés a bv. intézet által biztosított vezetékes, illetve fogvatartotti mobiltelefonnal,
d) internet alapú telefonhívás, illetve internet alapú video telefonálás,
e) ~~csomag küldése és fogadása,~~
f) ~~látogató fogadása,~~
g) ~~látogató bv. intézeten kívüli fogadása,~~
h) ~~kimaradás,~~
i) ~~eltávozás.~~

ELEKTRONIKUS KAPCSOLATTARTÁS

- Milyen hálózaton?
- Milyen eszközökön?
- Milyen technológiával?
- Milyen szoftverekkel?
- Milyen rendszerlogikával?
- Ki, mit, mikor, hogyan ellenőriz?
- Kik a szereplői a folyamatnak?
- Milyen jogosultsággal?
- Milyen azonosítási módszer (eszköz) alkalmazásával?
- Informatikai biztonság?
- Erőforrások?



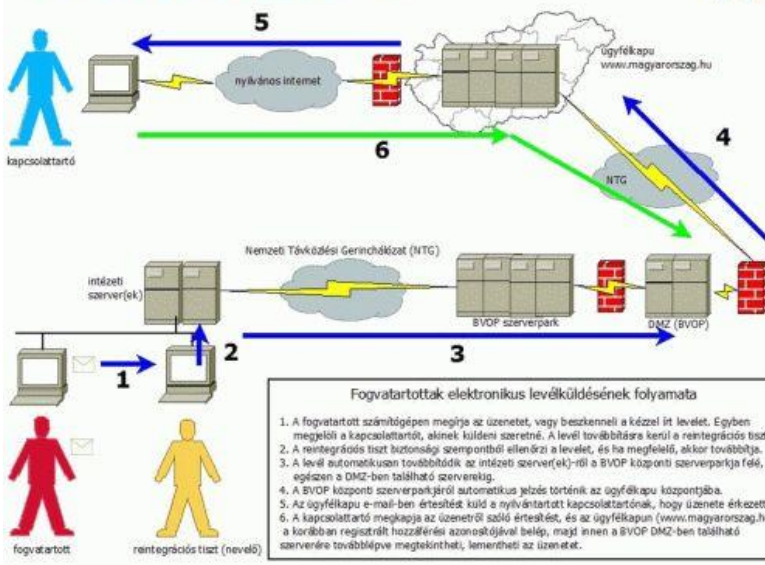



ELEKTRONIKUS KAPCSOLATTARTÁS

- **Bv. szervezet zárt célú hálózata → szolgálati feladatok végrehajtása**
  - Logikailag és fizikailag elkülönül helyi hálózat (LAN)
  - Táv-adatátviteli hálózat (WAN) a NISZ Zrt. Üzemeltetésében.
  - Egykapus megoldás: egy központi ki- és bejárat a BVOP-n keresztül.
- **Eszközök**
  - Speciális számítógépek: ipari kivitel, „vandál biztos" megoldás (IP65, IP67)
- **Szoftverek, technológia**
  - Levelezés esetében nem az elterjedt szabványok (SMTP, POP3, IMAP)
  - Egyedi célalkalmazás, ami file megosztáson alapul
  - Telefon és videotelefon esetében javasolt a Microsoft Lync program használata
- **Szereplők**
  - Fogvatartottak, reintegrációs tiszt, kapcsolattartó
- **Ellenőrzés**
  - Azonos módon a hagyományos levelezéssel, csak más platformon
- **Azonosítás**
  - Célszerű a bv. szervezetnél már ismert Active Directory technológiát alkalmazni
  - Fogvatartottak azonosítására célszerű másodlagos eszközt is alkalmazni
    pl.: PIN-kód, vonalkód, QR-kód, ujjlenyomat, írisz, tenyérvéna
    Fenti megoldások közül a tenyérvéna azonosítás
    a legmodernebb és egyben a legnagyobb biztonságú.
- **Rendszerlogika**

Microsoft® Lync™

RENDSZERLOGIKA



Fogvatartottak elektronikus levélküldésének folyamata

1. A fogvatartott számítógépen megírja az üzenetet, vagy beszkenneli a kézzel írt levelet. Egyben megjelöli a kapcsolattartót, akinek küldeni szeretné. A levél továbbításra kerül a reintegrációs tiszthez.
2. A reintegrációs tiszt biztonsági szempontból ellenőrzi a levelet, és ha megfelelő, akkor továbbítja.
3. A levél automatikusan továbbítódik az intézeti szerver(ek)-ről a BVOP központi szerverparkja felé, egészen a DMZ-ben található szerverekig.
4. A BVOP központi szerverparkjáról automatikus jelzés történik az ügyfélkapu központjába.
5. Az ügyfélkapu e-mail-ben értesítést küld a nyilvántartott kapcsolattartónak, hogy üzenete érkezett.
6. A kapcsolattartó megkapja az üzenetről szóló értesítést, és az ügyfélkapun (www.magyarország.hu) a korábban regisztrált hozzáférési azonosítójával belép, majd innen a BVOP DMZ-ben található szerverére továbblépve megtekintheti, lementheti az üzenetet.

REINTEGRÁCIÓS ŐRIZET

- A jelenlegi jogszabályokban ismeretlen ez a fogalom
- Az új Bv. Kódexben önálló cím 234-238.§
  - Az **első alkalommal** szabadságvesztésre ítélt, aki **öt évnél nem hosszabb** tartamú szabadságvesztését **fogház vagy börtön** fokozatban tölti ..... a **szabadulás előtt legfeljebb hat hónappal** reintegrációs őrizetbe helyezhető.
  - A bv. bíró által kijelölt lakás és az ahhoz tartozó bekerített hely.
  - Elhagyni csak meghatározott célból lehet (munkavégzés, eü. ok, stb.)
  - A büntetés-végrehajtási szervezet a rendőrséggel együttműködve ellenőrzi.
  - A reintegrációs őrizet megszüntethető ha: Az elítélt a **távfelügyeleti eszközök** vállalt alkalmazási szabályait megszegi, a távfelügyeleti eszközt megrongálja vagy használhatatlanná teszi.

RENDŐRSÉGI HÁZIŐRIZET

- Lokális őrizet és engedélyezett napirend szerinti mozgást lehetővé tevő kombinált személykövető.
- Mobil cella (LBS) és RF jeladóval (Beacon) megerősített helymeghatározás
- Egészségügyi szempontból biztonságos, vízálló.
- Újrahasznosítása költségtakarékos (Csak szíjkészlet cseréjét és gyors átkonfigurálást igényel más terhelten történő alkalmazás)
- A rendszer korrekt működése a fogvatartott együttműködésére épül.
- Normál háztartási eszközökkel az eltávolítás nehézkes, szabotázs egyértelmű detektálása optikai szenzorral biztosított.

Telepítési készlet

- 1 darabos (1nyomos) egység
- Adapter
- 1 x szíj
- 2 x dugó
- 2 x szögestálca
- Szíjvágó
- Kijárási-tilalmi egység

- A jogbiztonság érdekében terhelttel (fogvatartottal) csak hivatásos állomány érintkezhet.
- Kulcs kérdés a közrend (bv-nél biztonsági) és műszaki (informatikai) szakterület együttműködése.

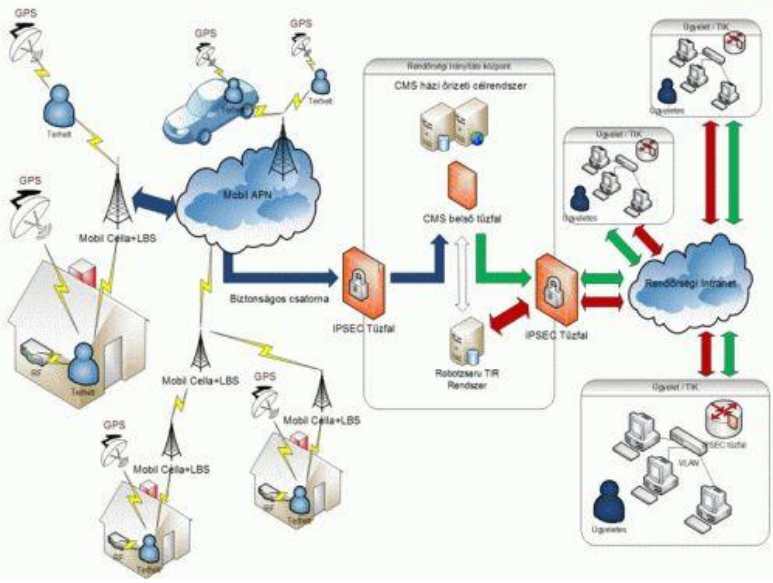
ZÓNA LEHETŐSÉGEK

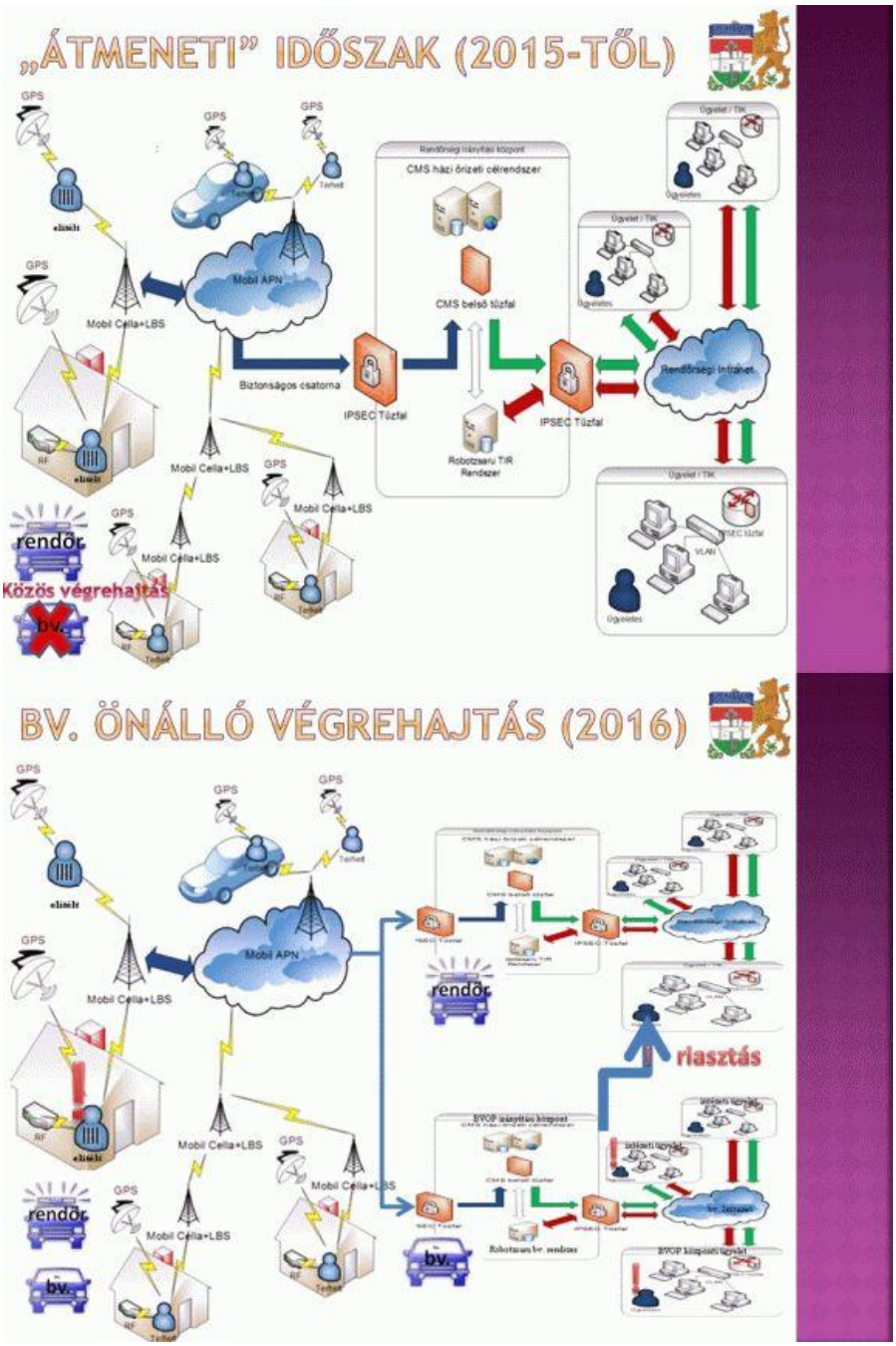
- A fogvatartottnak a számára kötelező lakhelyen túl több zóna szabható meg, melyekhez eseti,vagy ismétlődő napi/heti rend kapcsolható.
- Megfelelő engedély esetén a fogvatartott számára előírt tevékenységet, valamint munkát végezhet.
- A kizárási, tartózkodási idő szerinti definiálás lehetővé teszi a kitiltás, eltiltás, lakhely elhagyás stb. feladatokban történő alkalmazást.

Zóna alakok
- körkörös
- Sokszög

Zóna típusok
- integrációs
- kizárási

JELENLEGI RENDŐRSÉGI RENDSZER




„ÁTMENETI" IDŐSZAK (2015-TŐL)
GPS
Mobil APN
Mobil Cella+LBS
Biztonságos csatorna
IPSEC Tűzfal
CMS házi őrizeti célrendszer
CMS belső tűzfal
Robotszaru TIR Rendszer
Rendőrségi Intranet
Ügyelet / TIK
Ügyeletes
VLAN
rendőr
Közös végrehajtás
bv.
BV. ÖNÁLLÓ VÉGREHAJTÁS (2016)
riasztás


BÜNTETÉS-
VÉGREHAJTÁS
KÖSZÖNÖM A FIGYELMET !
e-mail: prisznyak.szabolcs@bv.gov.hu

KALÓ József

AZ EGYESÜLT ÁLLAMOK HADEREJÉNEK HARCTÉRI KOMMUNIKÁCIÓJA A II. VILÁGHÁBORÚ ALATT

Az Egyesült Államok haderejének harctéri kommunikációja a II. világháború alatt

„Kommunikáció 2013”
Nemzetközi tudományos-szakmai konferencia 2013. nov. 13.

Általános jellemzők

- Nagyon vegyes a kép → megtalálhatók a kor legfejlettebb kommunikációs eszközei (rádiók) és XIX. századiak ugyanúgy (fénytávíró)
- A legfontosabb eszközök: rádió, tábori telefon, távíró- és telexgépek, futárok, jelzőrakéták, füstjelek, jelzőzászlók és jelzőtáblák (panelek), kar- és kézjelek, stb.
- A kommunikációs tevékenységet végrehajtó egységek (híradók) feladatai is széles skálán mozogtak:

- üzemeltetés
- a felszerelés fejlesztése, fenntartása, javítása
- a hírközlési eszközök, felszerelések, a híradó-kiszolgálás biztosítása
- a telefon- és távíróvezetékek telepítése és javítása
- rejtjelzés és rejtjelmegfejtés
- rádiófrekvenciák, hívójelek és kódok kiosztása és kezelése
- az ellenséges zavaró- és lehallgató-tevékenység akadályozása
- az ellenséges hírközlési forgalom elfogása, megfigyelése és zavarása

- a saját hírközlés figyelemmel kísérése az üzembiztonság érdekében, a biztonsági intézkedések kidolgozása és végrehajtása
- radar működtetése, rádió-iránymérés biztosítása, repülőgépek számára rádió-jeladók és földi navigációs irányító rendszerek létrehozása és működtetése
- (néhány haderőben álló- és mozgóképek, valamint kiképző-, motiváló- és propagandafilmek készítése)

- A rádiók nagy technikai fejlődése a két háború közötti időszakban, különösen a ‘30-as években
- A tömegtermelés megindulása

→

- Ezredszinten és az alatt is jelentős számú hordozható rádió ↔
- számuk még így is kevés: még az amerikai haderő is csak 1944-re tudta kielégíteni a meglévő igényeket
- A tengelyhatalmak haderői a háború előre haladtával még a veszteségeket sem tudták pótolni!

A harctéri kommunikáció eszközei

- Minden nagyhatalom haderejében a **tábori telefonok**, és a vezetékes hírközlési eszközök voltak az elsődlegesek
- **Előnyük** a rádiókhoz képest:

- nagyobb hatótávolság és megbízhatóság,
- jó hangminőség (erősítőket lehetett integrálni a rendszerbe, hogy nagyobb távolságokra növeljék a jelerősséget)
- jelezhetőek a „bejövő hívások” (a kapcsolótábla kezelője meg tudta szakítani a vonalat)

- a telefonforgalmat sokkal bonyolultabb volt lehallgatni („beszivárgás és megcsapolás"), mint a rádióadásokat
- számottevően nem zavarták a légköri körülmények vagy az időjárás
- [szükség esetén a meglévő civil vonalak is felhasználhatók voltak katonai célokra]

Hátrányuk:

- sok időre és kábelre volt szükség a rendszer kiépítéséhez
- fenntartása szakadatlan munkát igényelt (ellenséges tűz, beszivárgás, időjárás, saját járműforgalom)

- gyakran jelentkezett anyaghiány is
- csak védelemben voltak ideálisak, támadáskor „csak" a támogató egységek és a tüzérség maradtak a hálózatban, az előrenyomulók nem → újra kellett telepíteni; vagy ún. könnyű „támadóvezeték"-et fektettek előrenyomulás közben (nem volt képes több egyidejű üzenet továbbítására, rövid hatótávolság)

A korabeli **rádiók** már hordozhatóak (egy vagy több ember, állatok, járművek) voltak, de még mindig viszonylag nehezek

- Ebben az időszakban két fő típus létezett: az AM és az FM rádiók
- A japán hadseregben csak AM rádiók (máshol is ebből volt a legtöbb):

- nagy hatótávolságra hangokat (beszéd), ill. még nagyobb hatótávolságra folyamatos hullámokat (Morze-típusú kód) továbbított

Hátránya:

- nem lehetett használni mozgás közben
- időigényes volt a beüzemelése
- a beszédátviteleknek távolsági korlátai voltak és nem voltak mindig tiszták, sok statikusságot vettek fel, a fogadóállomás nem tudta fogadni az adást a más állomások vagy a légköri körülmények okozta interferencia következtében

- nem tudtak idomulni a gyorsan változó helyzetekhez
- még kevésbé voltak hatékonyak, amikor járműre szerelték őket → a jármű elektromos rendszere interferenciát hozott létre és le is árnyékolta
- az FM-rádiókhoz képest nagyobbak és nehezebbek voltak

Előnye:

- finomhangolással a kezelők a fő frekvencia mellett a közelben lévő frekvenciákat is figyelték → több adást tudtak fogni ugyanazon a hullámsávon

Amerikai híradócsapatok speciális jellemzői

Az amerikai harctéri kommunikáció eszközei

SCR-300 hordozható rádió adó-vevő

EE-8 tábori telefon

Kulturális specifikumok

- A ABLE J JIG S SUGAR
- B BAKER K KING T TARE
- C CHARLIE L LOVE U UNCLE
- D DOG M MIKE V VICTOR
- E EASY N NAN W WILLIAM
- F FOX O OBOE X X-RAY
- G GEORGE P PETER Y YOKE
- H HOW Q QUEEN Z ZEBRA
- I ITEM R ROGER

Amerikai kód-abc 1941-ből

Köszönöm a figyelmet!

SZÖLLŐSI Sándor

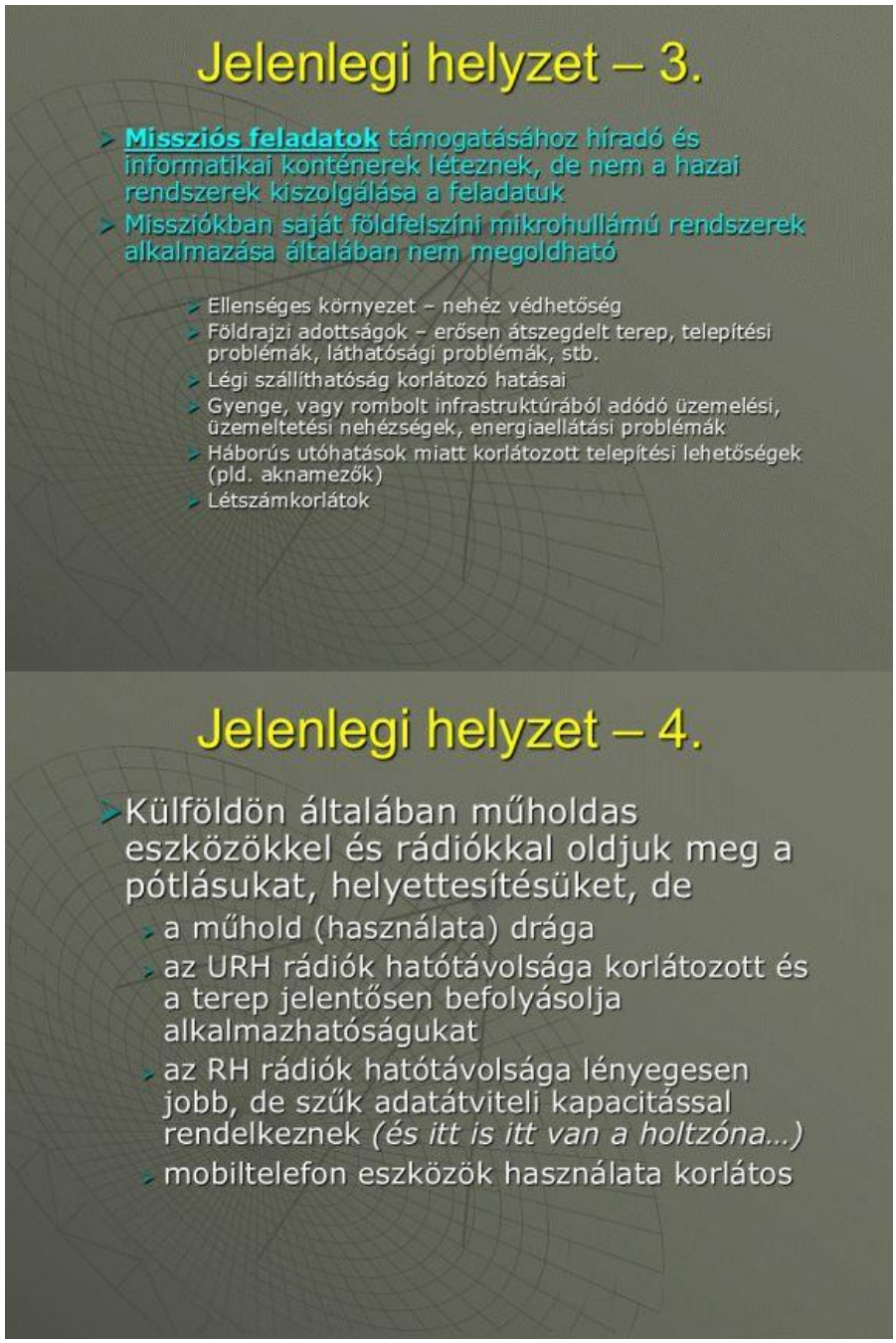
TÁBORI MIKROHULLÁMÚ RENDSZEREK TÚLÉLŐKÉPESSÉGÉNEK JAVÍTÁSA

Jelenlegi helyzet – 1.

- **Honi üzemelésű** mikrohullámú **tábori** rendszer jelenleg analóg technikán alapul (R-1406/G)
  - Műszakilag és erkölcsileg elavult, logisztikai problémák (javítóanyagok, stb.)
  - Nagy méretek, nagy létszámigény (telepítés)
  - Kevés a hozzáértő szakember, bonyolult kezelés
  - Nagy időigény (telepítés, beüzemelés, bontás, áttelepülés)
  - Az állandó, digitális alapú rendszereinkhez való bekötés nehézkes – szűk keresztmetszet probléma
  - Adatátvitelre korlátozottan alkalmas (modem)
  - Mai elvárásoknak már nem felel meg

Jelenlegi helyzet – 2.

- Hatótávolságuk legfeljebb 40-50 km (néhány speciális telepítési/alkalmazási helyzettől eltekintve)
- Fejlesztési szándék mellett is nehéz perspektivikus és megfizethető megoldást találni


Jelenlegi helyzet – 3.
Missziós feladatok támogatásához híradó és informatikai konténerek léteznek, de nem a hazai rendszerek kiszolgálása a feladatuk
Missziókban saját földfelszíni mikrohullámú rendszerek alkalmazása általában nem megoldható
Ellenséges környezet – nehéz védhetőség
Földrajzi adottságok – erősen átszegdelt terep, telepítési problémák, láthatósági problémák, stb.
Légi szállíthatóság korlátozó hatásai
Gyenge, vagy rombolt infrastruktúrából adódó üzemelési, üzemeltetési nehézségek, energiaellátási problémák
Háborús utóhatások miatt korlátozott telepítési lehetőségek (pld. aknamezők)
Létszámkorlátok
Jelenlegi helyzet – 4.
Külföldön általában műholdas eszközökkel és rádiókkal oldjuk meg a pótlásukat, helyettesítésüket, de
a műhold (használata) drága
az URH rádiók hatótávolsága korlátozott és a terep jelentősen befolyásolja alkalmazhatóságukat
az RH rádiók hatótávolsága lényegesen jobb, de szűk adatátviteli kapacitással rendelkeznek (és itt is itt van a holtzóna…)
mobiltelefon eszközök használata korlátos

Ergo: semmi sem elég jó!

Van egyáltalán valami megoldás?

Kiútkeresés a zöld úton 1.

- Meg kell válaszolni a következő kérdéseket:

1. Szükség van-e földi mikrohullámú tábori rendszerekre?
2. Ha igen, van-e lehetőség jó minőségű adatátvitelt megvalósító, nagytávolságú kapcsolatokat biztosító megoldásokra, átjátszóállomások lehetőség szerinti minimalizálása mellett?
3. Ha nem, akkor a képességek biztosíthatók-e más módon, de az eddigi műholdas rendszerek kihagyása mellett?
4. Ha műholdas technika nem kikerülhető, lehet-e saját Magyar Műhold, azt anyagilag és műszakilag képesek vagyunk-e üzemeltetni, olcsóbb-e, mint a bérlés?
5. A Magyar Műhold áttelepíthető más pályára is? (azaz használható-e Magyarországon és külföldön egyaránt)

Kiútkeresés a zöld úton – 2.

- Kérdés:
  1. Szükség van-e földi mikrohullámú tábori rendszerekre?
  2. Ha igen, van-e lehetőség jó minőségű adatátvitelt megvalósító, nagytávolságú kapcsolatokat biztosító megoldásokra, átjátszóállomások lehetőség szerinti minimalizálása mellett?
- Válasz:
  1. Nincs! „Csak” az előnyös képességekre van szükség, nem ragaszkodunk sem a jó öreg R-1406/G-hez, sem bármilyen más digitális tábori (harcászati) reléhez.
  2. Sajnos jelenleg nincs olyan földfelszíni digitális adatátviteli rendszer, mely biztosítja akár a 80-100 km-es hatótávolságok mellett a nagysebességű adatátvitelt, átjátszóállomások nélkül (ráadásul a területlefedés lenne az optimális a számunkra)

Kiútkeresés a zöld úton – 3.

- Kérdés:
  3. Ha nem, akkor a képességek biztosíthatók-e más módon, de az eddigi műholdas rendszerek kihagyása mellett?
  4. Ha műholdas technika nem kikerülhető, lehet-e saját Magyar Műhold, azt anyagilag és műszakilag képesek vagyunk-e üzemeltetni, olcsóbb-e, mint a bérlés?
- Válasz:
  3. Műholdas megoldások nélkül a hatótávolság-korlátok jelenleg nem leküzdhetők.
  4. Egy tisztán hazai rendszer kiépítése és üzemeltetése valószínűleg sokszorosan meghaladja az ország gazdasági lehetőségeit, bár a komplett műholdas rendszerek árai számomra nem ismertek. Ettől függetlenül belátható, hogy csak az igen jó gazdasági helyzetben lévő, gazdag országok (vagy még inkább nemzetközi cégek) képesek ilyen rendszereket építeni és üzemeltetni. A válaszom mégis az, hogy lehet Magyar „Műhold”! És az ára? Nézzük…

Kiútkeresés a zöld úton – 4.

- Újabb kérdések:

1. Mi ez a Magyar „Műhold”?
2. Miért kell a „zöld” úton haladni?

Valaki tudja a választ…

Kiútkeresés a zöld úton – 5

- A valóság:

1. Ez az eszköz nem is magyar és nem is műhold, de mindkettő lehet. Tulajdon szempontjából magyarrá válhat, mi üzemeltethetjük, és műszakilag műholdas jellegű szolgáltatásokat biztosíthat megfelelő felszerelés után, olcsó üzemeltetés mellett, minimális földi támogatással, autonóm módon.
2. Mitől „zöld”? Nem a terepszínűre festés miatt, hanem a felhasznált energia alapján, mert a Napból „táplálkozik”.

Nem, nem! Ez most nem matek …

Kiútkeresés a zöld úton – 6.

- Az ötlet:

1. Kell egy olyan eszköz, ami magasan repül, hogy egyszerű módszerekkel ne lehessen a működését megzavarni, valamint ne lehessen könnyen tönkretenni, megsemmisíteni
2. Nagy terület lefedését biztosítsa bármilyen információ vonatkozásában
3. Ne kelljen rakétával, vagy más hordozóeszközzel pályára állítani, hanem tudjon saját maga le, és felszállni
4. Legyen annyira teherbíró, hogy képes legyen egy mikrohullámú átjátszó berendezést magával vinni (ez nem jelent extra elvárást, hiszen a mai ilyen jellegű berendezések nagyjából egy átlagos felnőtt ember tömegével mérhetőek össze, az eszköz bonyolultságának függvényében)
5. Rendelkezzen olyan energiaforrással, mely hosszútávú, leszállás nélküli üzemet biztosít, akár éjszaka is
6. Ne legyen szükség emberi személyzetre az eszközön
7. Működési ideje legyen összemérhető egy átlagos kommunikációs műhold életciklusával, de lehetőleg utána is legyen újrahasznosítható
8. Egyszerű és minimalista földi kiszolgálást igényeljen a repülési ciklusa alatt

Kiútkeresés a zöld úton – 7.

- Lehetőségek:

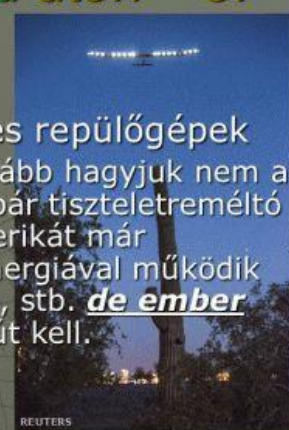
1. Drón eszközök – amerikai ember nélküli elektromos mini napelemes repülőgép
   - 9 órán keresztül folyamatosan repült. (nagy kapacitású akkumulátor és napelem együttes alkalmazásával)
   - A repülőgép 6 kg
   - Teljesen vízálló
   - Kézben hordozható, percek alatt összeállítható
   - Kézből indítható
   - Használható vízen és szárazföldön
   - Két ember elegendő a működtetéséhez
   - Semmilyen egyéb infrastruktúrát (kifutópálya, indító állomás…) nem igényel
   - A működtetése csendes, önállóan működik és folyamatos megfigyelést tesz lehetővé.

Majdnem jó!

De mi egy kicsit nagyobbra vágyunk...

Kiútkeresés a zöld úton – 8.

- Lehetőségek:
  2. Nagyméretű napelemes repülőgépek
     1. Solar Impulse - ezt inkább hagyjuk nem a számunkra járható út, bár tiszteletreméltó rekordokat állít fel, Amerikát már átrepülte, tisztán napenergiával működik éjszaka is, alig 1600 kg, stb. ***de ember vezeti***. Nekünk másik út kell.



Kiútkeresés a zöld úton – 9-a.

- Lehetőségek:
  2. Nagyméretű napelemes repülőgépek
     1. Solara drón
        - A gyártó az 5 éves folyamatos működés miatt a drónt **légköri műholdnak** nevezi.
        - A repülési magassága majdnem 20.000 méter. (Ez messze a hagyományos repülőgépek repülési magassága felett van)
        - Feladata lehet jelenleg:
          - Térképészet
          - Termés monitorozás
          - Időjárás megfigyelés
          - Katasztrófa felmérés
          - vagy bármi más, ami alacsony magasságú műholdat igényelt

Kiútkeresés a zöld úton – 9-b.

- Lehetőségek:
  2. Nagyméretű napelemes repülőgépek
     1. Solara drón
        - Saját akkumulátorait napelemek segítségével tölti fel. (a nagy repülési magasságban a légkör nem csökkenti a napsugárzás energiáját)
        - A gép 60 méter széles és kb. 113 kg szállítására képes.
        - Repülési sebessége 97 km/h
        - Hatótávolsága 4,5 millió km

Kiútkeresés a zöld úton – 9-c.

- Lehetőségek:
  2. Nagyméretű napelemes repülőgépek
     1. Solara drón
        - Költsége csak töredéke egy hagyományos műholdnak (kevesebb, mint 2 millió dollárba kerül, de a gyártó célja az egy millió dolláros repülőgép platform megteremtése)
        - Működtetési költség szinte nincs, csak néhány ember figyeli időnként a monitorokat, hogy a gép ne csináljon semmi szokatlant
        - Ez napi árfolyamon 413 millió Ft körül van, árcsökkenés esetén pedig természetesen a fele.
        - Összevetve azzal, hogy nincs szükség mobil földfelszíni mikrohullámú rendszerekre, csak a hordozható eszközök képességeit kell megteremteni, ez a beruházás gyors és hatékony, arányait tekintve olcsó beruházásnak minősül, harcászati képességeket tekintve pedig nagyságrendi ugrást a jövőbe, miközben „zöld energiát" használunk céljaink eléréséhez

Kiútkeresés a zöld úton – 9-d.

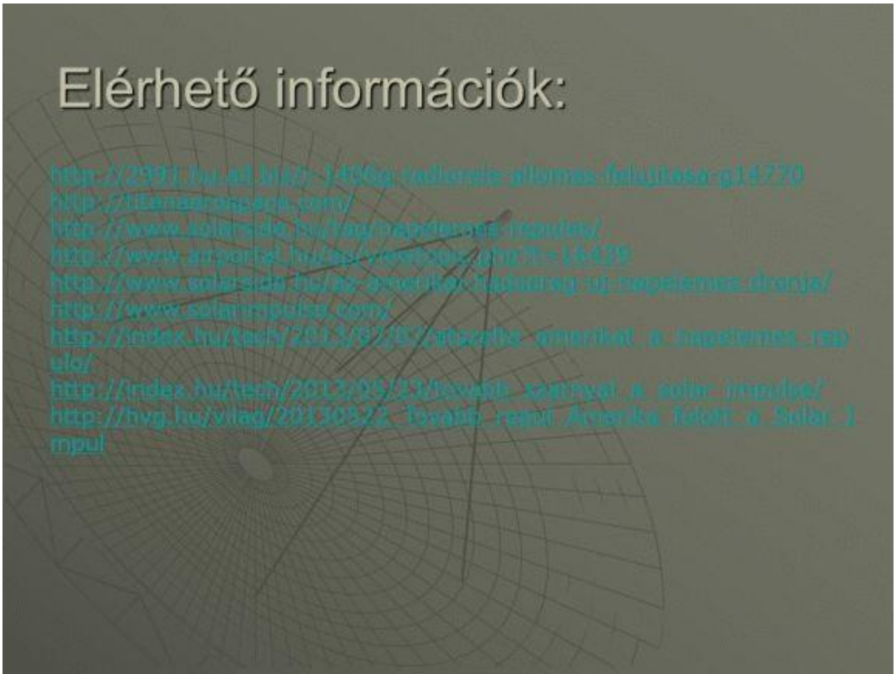
- Lehetőségek:
  2. Nagyméretű napelemes repülőgépek
     1. Solara drón
        - A megfigyelés mellett az egyik várható feladata a rendszernek, hogy katasztrófák esetén nagy területen biztosítsa a **mobiltelefonok számára a 4G lefedettséget.**
        - Ez utóbbi azt is jelenti, hogy természetesen más (katonai) rendszer kiszolgálása is megoldható ilyen módon!!!

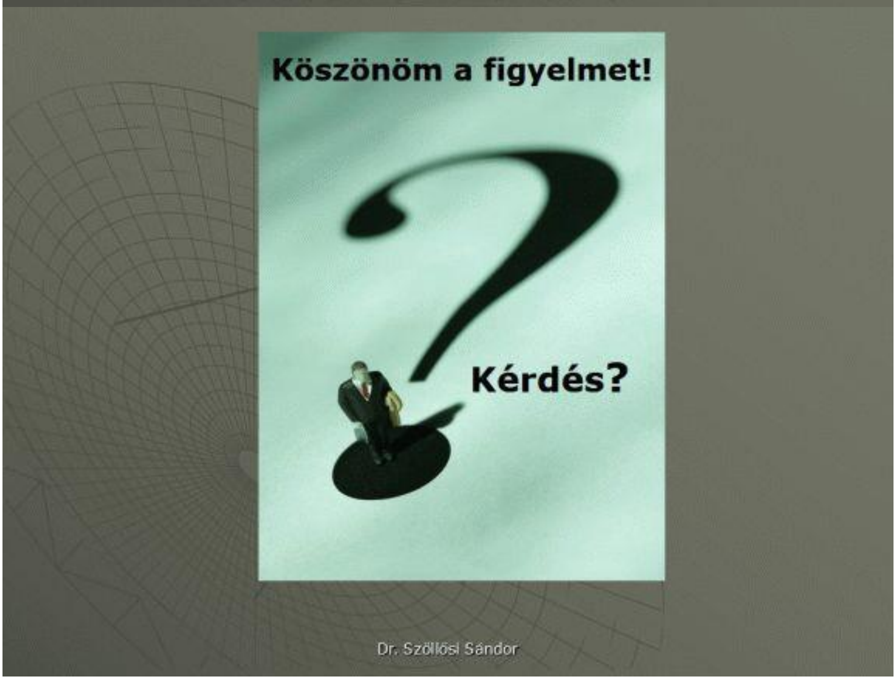
Kiútkeresés a zöld úton – 10.

- Az utolsó kérdés:
  5. A Magyar „Műhold” áttelepíthető más pályára is? (azaz használható-e Magyarországon és külföldön egyaránt)
- Válasz:
  5. Az előzőekből következően igen, bár nem túl gyorsan (kb. 97 km/h–val egy ideig eltart az út pld. Afganisztánig…). Ennél jobb, ha a kiszolgálási terület közelében egy biztonságos területről szállunk fel és onnan már hamar elérhető a célterület. Persze ekkor több ilyen eszközre van szükség.

Összességében:

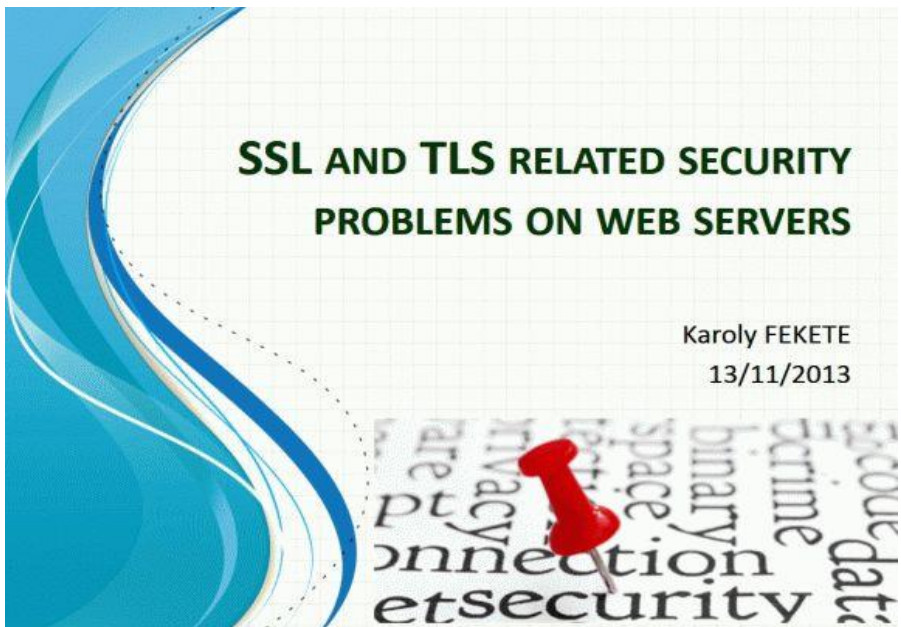
- Van kiút, de pénzbe kerül.
- A bemutatott lehetőségek olyan stádiumban vannak, hogy 1-2 éven belül tömegesen elérhetőek lesznek (a javasolt megoldás már most is megvehető!).
- Érdemes lenne újra elővenni a tábori rendszerek fejlesztését és meggyőződésem, hogy a felvázolt irányban történő elmozdulás az egyedüli helyes út a harcászati rendszereink terén meglévő több évtizedes (!) elmaradás minél olcsóbb és gyorsabb megoldására.

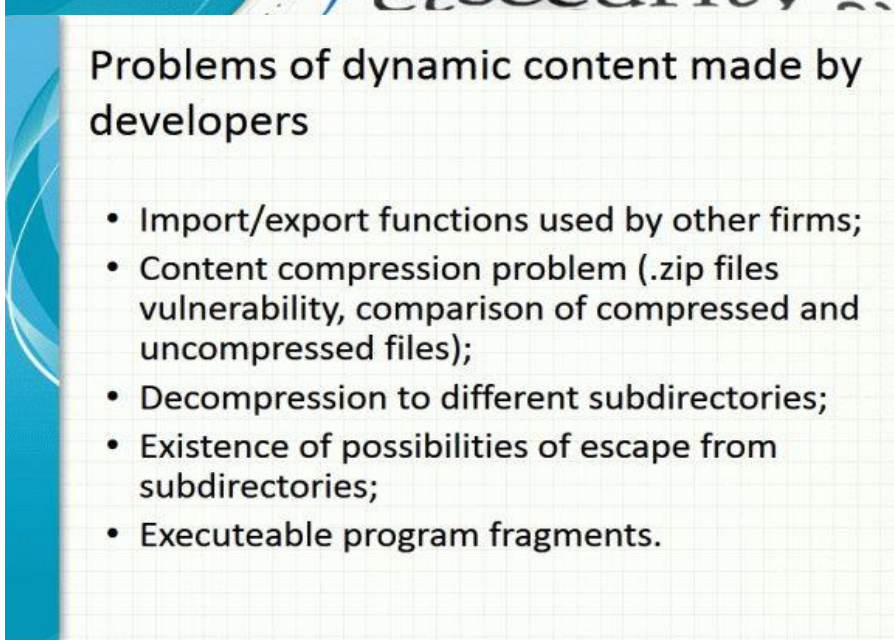

Elérhető információk:
http://www.solarimpulse.com/


Köszönöm a figyelmet!
Kérdés?
Dr. Szöllősi Sándor

Karoly FEKETE

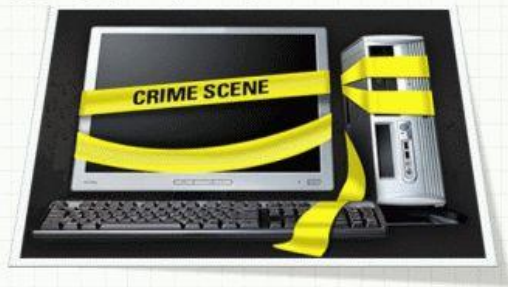
SSL AND TLS RELATED SECURITY PROBLEMS ON WEB SERVERS





Problems caused by third parties, external causes

- Connecting companies;
- Test servers;
- Export-import functions;
- Log handling and logging (script tags, crossite scripts).

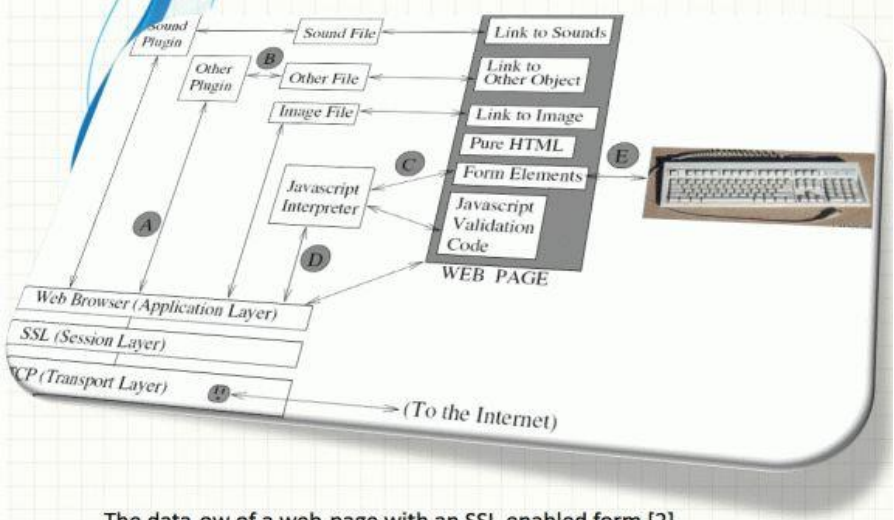


Problems of configuration

- firewalling;
- session handling;
- default password;
- no isolation of web pages.

Protocol problems

- Secure Socket Layer and Transport Layer Security;
- Chosen-plaintext cryptographic attack;
- Compression Ratio Info-leak Made Easy- CRIME [1];
- Browser exploit against SSL/TLS – BEAST (adaptive chosen plaintext attack with predictable initialization vectors) [2];



The data-ow of a web-page with an SSL-enabled form [2]

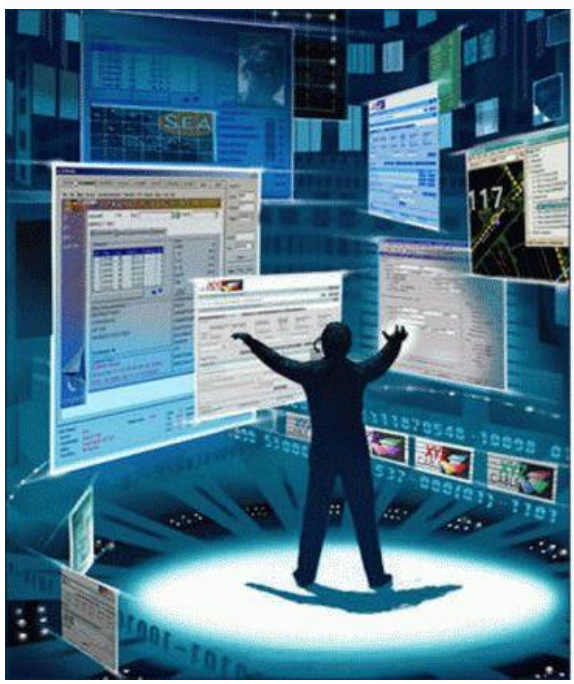
BEAST, CRIME, BREACH
SSL/TLS Attacks Timeline

BEAST
"Browser Exploit Against SSL/TLS" - decryption of secure cookies in minutes.

BREACH
leverages HTTP compression attacking HTTP responses.

2011 | 2012 | 2013

CRIME
a side-channel attack against compression in HTTPS implementations.



Other problems

- Problems of frameworks;
- Problems of Server (linux, java, PHP vulnerabilities);
- Browser related problems;
- Others (backup, cloud).

References:

- *[1] Pratik Guha Sarkar - Shawn Fitzgerald :* Attacks on SSL - A comprehensive study of BEAST, CRIME, TIME, BREACH, LUCKY 13 & Rc4 biases, iSEC Partners, Inc 123 Mission Street, Suite 1020, San Francisco, CA 94105, August 15, 2013, https://www.isecpartners.com;
- *[2] Gregory V. Bard:* Vulnerability of SSL to Chosen-Plaintext Attack, University of Maryland, May 11, 2004, http://eprint.iacr.org/2004/111.pdf;
- *[3] M. Bellare - A. Desai - E. Jokipii - P. Rogaway:* A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation, Foundations of Computer Science, 1997;
- *[4] H. Krawczyk:* The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?)." Crypto 2001.
- *[5] Omar SHANTOS:* BREACH, CRIME and Black Hat, http://blogs.cisco.com/security/breach-crime-and-blackhat/

QUESTIONS?

SZABÓ András

EGY LÉPÉS AZ URH ALAPÚ IP ADATHÁLÓZATOK FELÉ

NEMZETI
KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR

Egy lépés az URH alapú IP adathálózatok felé

Készítette:
Szabó András mk. fhdgy.
NKE HHK KÜI
Informatikai és Elektronikai hadviselés Tanszék
Tanársegéd

NEMZETI
KÖZSZOLGÁLATI EGYETEM

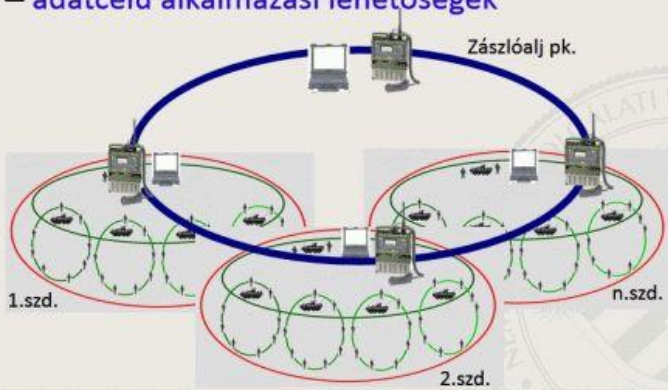
Felépítés

- Bevezetés
- Problémafelvetés
- MRR URH rádió adatátviteli képességei
- Hiányosságok
- Megoldási lehetőségek
- Összegzés

NEMZETI KÖZSZOLGÁLATI EGYETEM

Bevezetés

- URH rádiók
  - beszédcélú alkalmazási lehetőségek
  - adatcélú alkalmazási lehetőségek



NEMZETI KÖZSZOLGÁLATI EGYETEM

Problémafelvetés

URH rádió hálók illesztése a tábori híradó ás informatikai rendszerekhez

Interfészek, szabványok?

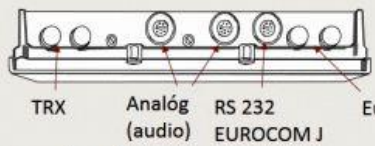
Tervezés, paraméterezés?

Szolgáltatások?

NEMZETI KÖZSZOLGÁLATI EGYETEM

Az MRR 300 URH rádiócsalád adatátviteli képességei

- MRR MP300, MV300 RCT interfészei



Buszsebességek

X.25

- Sebesség: 2400, 9600, 16000 bit/s (szinkron)

Transzparens szinkron/aszinkron adatok

- 300 – 16000 bps szinkron

- 300- 19200 bps aszinkron

- Relé üzemmódban max. 4800 bit/s

NEMZETI KÖZSZOLGÁLATI EGYETEM

Adatátviteli igények

- Szöveges üzenetek

  pl.:harcparancsok,

  veszélyfigyelmeztetés

- Képi információ

  pl.:Térkép

http://alfred.maleczki.free.fr/geo/zdrv/zador.gif

NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR

Hiányosságok

- jelenleg nincs X.25 interfész a tábori informatikai végpontokon
- Nincs olyan szoftver ami a soros adatátvitelt támogatná natívan (kiv. C2)
- szeparált adat háló létesítésének hiánya
- adat replikáció problémák az alárendelt-elöljáró rádióháló között

NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR

MEGOLDÁSI LEHETŐSÉGEK?

NEMZETI KÖZSZOLGÁLATI EGYETEM

1.) Eszközcsere

MR500 IP képes rádió

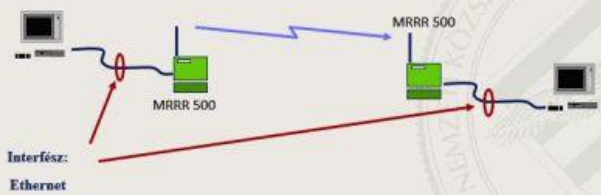
•RCT csere, TRX fireware update

+ Natív IPv4 képes

+ Routing

- Ár

- Új logisztikai és kiképzési rendszer



Ábra:dr. Németh András okl. mk. szds. MRR oktatási segédlet

NEMZETI KÖZSZOLGÁLATI EGYETEM

2.) PAD funkció

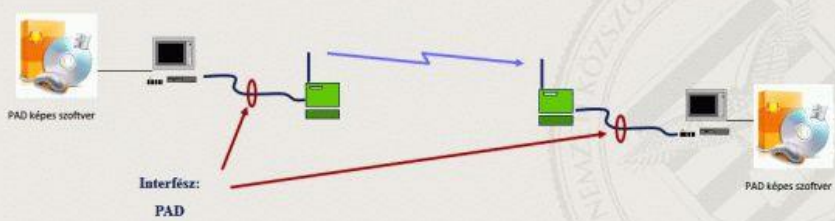
• RCT firmware csere

+ Működne a saját eszközökön

+ Minimális kiegészítés a képzési anyagokban

- Ár

- PAD képes szoftver igénye



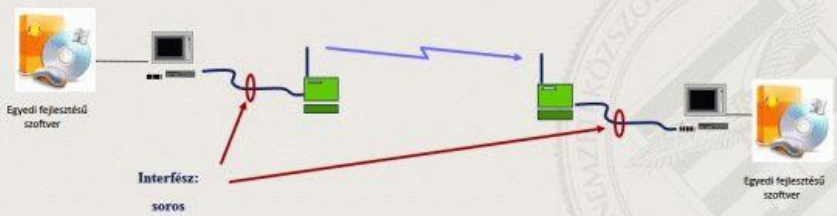
NEMZETI KÖZSZOLGÁLATI EGYETEM

3.) Egyedi K+F

Pl.:Németh Szabolcs TOPCIS hierarchikus adatátviteli implementációja

\+ „Testreszabott”

\- nem „univerzális” megoldás



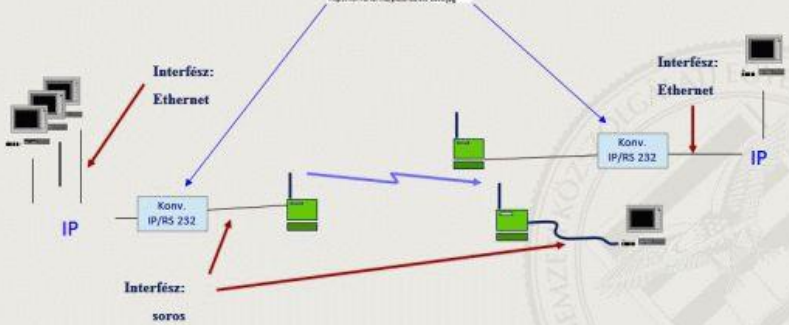
NEMZETI KÖZSZOLGÁLATI EGYETEM

4.) soros – Eth. konverzió

+egyszerű

+olcsó

\- nincs egyedi címzés




NEMZETI KÖZSZOLGÁLATI EGYETEM
Megoldási lehetőségek összehasonlítása
Eszköz csere
PAD funkció
Egyedi K+F
Soros – Eth. konverzió
Pro
+ Natív IPv4 képes
+ Routing
+ Működne a saját eszközökön
+ Minimális kiegészítés a képzési anyagokban
+„Testreszabott"
+ Egyszerű
+ Olcsó
Kontra
- Magas ár
- Új logisztikai és kiképzési rendszer
- Magas ár
- PAD képes szoftver igénye
- Nem „univerzális" megoldás
- Nincs egyedi címzés
NEMZETI KÖZSZOLGÁLATI EGYETEM
Soros- Ethernet konverter...
DEMO


NEMZETI
KÖZSZOLGÁLATI EGYETEM
Kérdések + Válaszok

BENEDEK Andor

MAGYAR FEJLESZTÉSŰ MIKROHULLÁMÚ BERENDEZÉSEK AZ MH HÁLÓZATÁBAN

KOMMUNIKÁCIÓ 2013

2013. november 13.

MAGYAR FEJLESZTÉSŰ MIKROHULLÁMÚ BERENDEZÉSEK AZ MH HÁLÓZATÁBAN

dr. Benedek Andor
TOTALTEL Kft.

Mikrohullámú átviteltechnika

Lokátor-technika: mikrohullámú áramköri technika és eszközök fejlődése

1950-es évektől: analóg sokcsatornás nagytávolságú mikrohullámú összeköttetések

Nyalábolás és moduláció: FDM-FM

Rádióátvitel a mikrohullámú sávokban

- erős nyalábolás: energetikailag hatékony
- nagy sávszélesség: nagy csatornaszám
- gyors telepítés kedvezőtlen földrajzi környezetben is

TOTALTEL 2

Mikrohullámú berendezés-gyártás Magyarországon

1960-tól: FMV, ORION

Fejlesztő központ: TKI

Jelentős elméleti eredményekre épülő gyakorlati fejlesztés

Jelentős volumenű berendezés-gyártás hazai és export területekre

80-as évektől áttérés digitális technikára

- regenerálás szerepe
- átviteli kapacitás és sávszélesség

TOTALTEL 3

A mikrohullámú átvitel reneszánsza

90-es évek: a mobil kommunikáció igényei

Hasonló infrastruktúra

Városi hálózatok, fokozatos kiépítés

Hiányos távközlési infrastruktúra gyors pótlása nyilvános és magánhálózatokban

- kis- és közepes kapacitású, rövid távú átvitel
- magasabb frekvenciasávok

TOTALTEL 4

Az MH mikrohullámú hálózata

1986-ig kiépült digitális RP rendszer

1993: várpalotai lőtéri hálózat Totaltel TDR berendezésekkel

2000: az 1,5 GHz-es sáv kiürítése miatt a teljes hálózat átalakítása

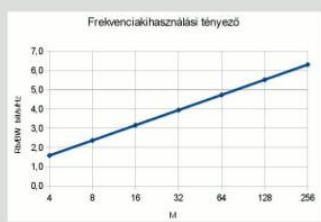
2002-től: az átviteli kapacitások növelése, az informatika átviteli igényeinek kielégítése, az MH szervezeti átalakulás követése

2009-től kapacitás-bővítés új, jobb frekvenciahatékonyságú berendezések alkalmazásával

Sebesség-sávszélesség-moduláció

Magas szintű (nagy állapotszámú) moduláció

$$R_b \leq \frac{k.BW}{n(1+\alpha)} \log_2 M$$



Magas szintű moduláció

A nagy állapotszámú modulációs rendszerek érzékenyek a zajra és torzításra (nagy jel-zaj viszony igény, kisebb teljesítmény): csökkenő rendszerérték

Megoldás: a rádiócsatorna pillanatnyi állapotához illeszkedő moduláció automatikus beállítása = adaptív moduláció

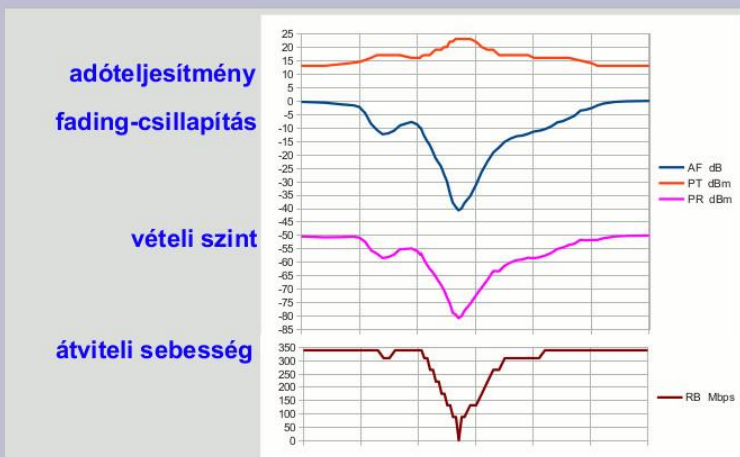
A lehetőséget a csomag-átvitel és az SDR modem biztosítja

A moduláció-váltást a hibajavító dekóder vezérli

Az átkapcsolás bitvesztés- és hibamentes

További adaptív technika: vételi szint által vezérelt adóteljesímény-szabályozás (ATPC)

Az ADM működése



ADM összeköttetés méretezése

Méretezés referencia módra: tipikusan M_{ref}=16 vagy 32

R_b előírt valószínűséggel garantált R_{bref} értékét M_{ref} határozza meg:

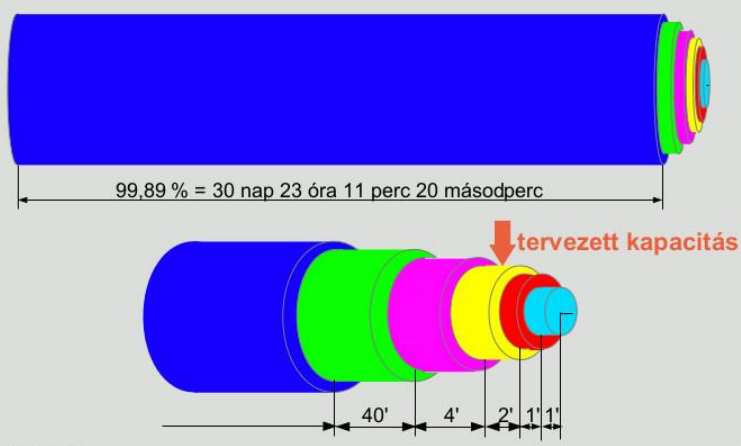
$Prob(R_b>R_{bref})=Prob(F<FM_{Mref})=P_{Mref} < P_o$ (előírt érték, pl. 0,005 %)

M_{min}	<	M_{ref}	<	M_{max}
R_{bmin}	<	R_{bref}	<	R_{bmax}
$P_{rth,Mmin}$	<	$P_{rth,Mref}$	<	$P_{rth,Mmax}$
FM_{Mmin}	>	FM_{Mref}	>	FM_{Mmax}
P_{Mmin}	<<	$P_{Mref} < Po$	<	P_{Mmax}

Az idő nagy hányadában: $R_b=R_{bmax}>R_{bref}$

A csatorna megszakadási valószínűsége: $Prob(R_b<R_{bmin})<<P_o$

Az ADM nyeresége



TDR-F-W digitális mikrohullámú berendezések

Fix vagy adaptív moduláció 4-8-16-32-64-128-256 QAM

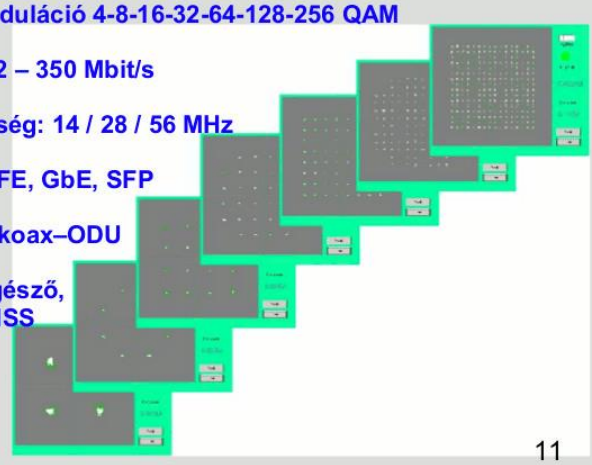
Átviteli kapacitás: 22 – 350 Mbit/s

Csatorna-sávszélesség: 14 / 28 / 56 MHz

Interfészek: E1, E3, FE, GbE, SFP

Osztott kivitel: IDU–koax–ODU

Menedzsment: böngésző, LCT, SNMP, MXMSS



TOTALTEL 11

TDR-F-W ODU

Frekvenciasávok: 5-13-15-18-23-26-38 GHz

Adóteljesítmény: 20 – 30 dBm

ATPC: 0 - 20 dBr

Csatorna-sávszélesség: 14 / 28 / 56 MHz

Max. kábelhossz: 100 / 300 m

TOTALTEL 12

TDR-F-W IDU

Alapkiépítés
10/100/1000Base-T/opt.

Bővített kiépítés
1-17 E1 + 10/100Base-T + 10/100/1000Base-T/opt.
SNMP menedzsment
szolg. távbeszélő

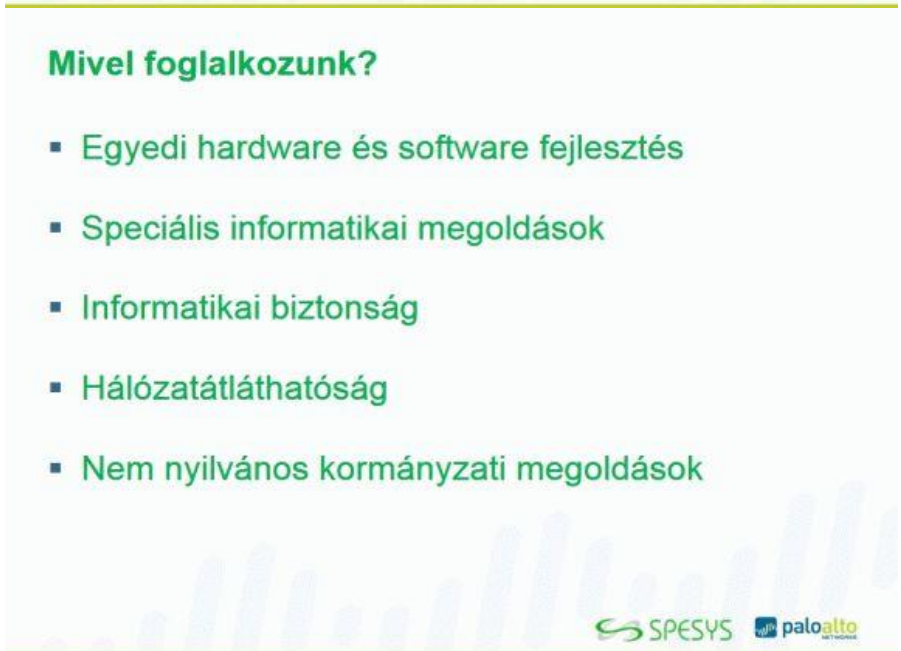
VLAN (802.1q), QoS: 802.1p, Q-in-Q, IPv4 ToS

TOTALTEL 13

Köszönöm a figyelmet!

ZAUTASVILI Péter

PAOLO ALTO NETWORKS TERMÉKEI A BIZTONSÁG SZOLGÁLATÁBAN



SpeSys - Palo Alto Networks

- A SpeSys Kft. a prémium IT biztonsági megoldásokkal foglalkozik
- Új biztonság szemlélet szükséges a hagyományos mellett

A SpeSys a Palo Alto Networks Platinum partnere

SPESYS paloalto

Palo Alto Networks termékei a biztonság szolgálatában

SPESYS

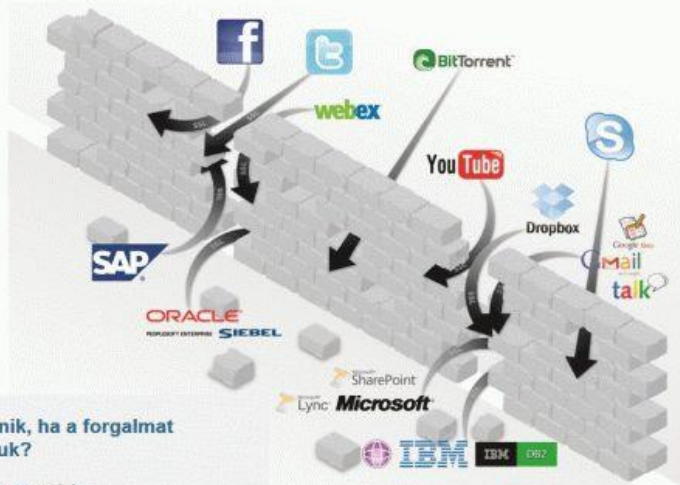
paloalto NETWORKS

the network security company™


Hálózatok-tapasztalatok
Alkalmazások, melyeket senki sem kedvel...
Alkalmazások, melyekre kevésbé figyelünk
Alkalmazások, melyekre mindenkinek szüksége van
custom tcp
telnet
PENVPN
LogMeIn
custom udp
ftp
SSL
VNC
LDAP
VPN
RDP
encrypted tunnel
SMB
snmp
DB2
Active Directory
Siebel
SPESYS
paloalto


Alkalmazások átengedése a tűzfalon
BitTorrent
webex
YouTube
Dropbox
SAP
ORACLE
SIEBEL
SharePoint
Microsoft
IBM
A hálózat biztonsági policy érvényesítése a tűzfalon
Rálát a teljes forgalomra
Kijelöli a határvonalakat
Engedélyezi a hozzáférést
A hagyományos tűzfalak nem jelentenek többé megoldást
SPESYS
paloalto

Alkalmazások átengedése a tűzfalon: Titkosítás

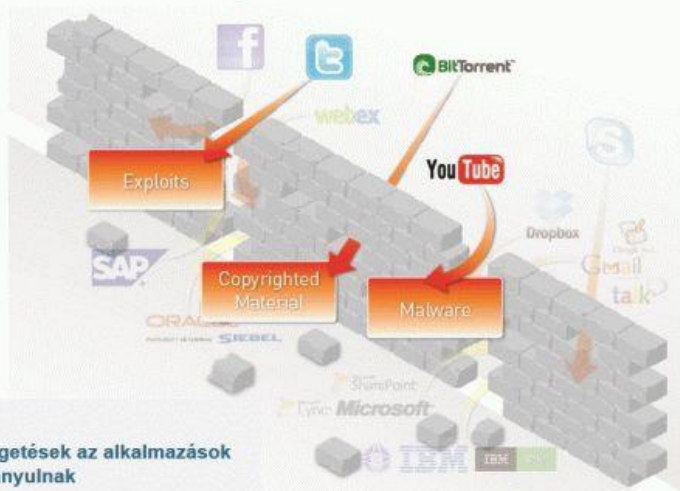


Mi történik, ha a forgalmat titkosítjuk?

- **SSL**
- **Egyéb titkosítás**

SPESYS paloalto

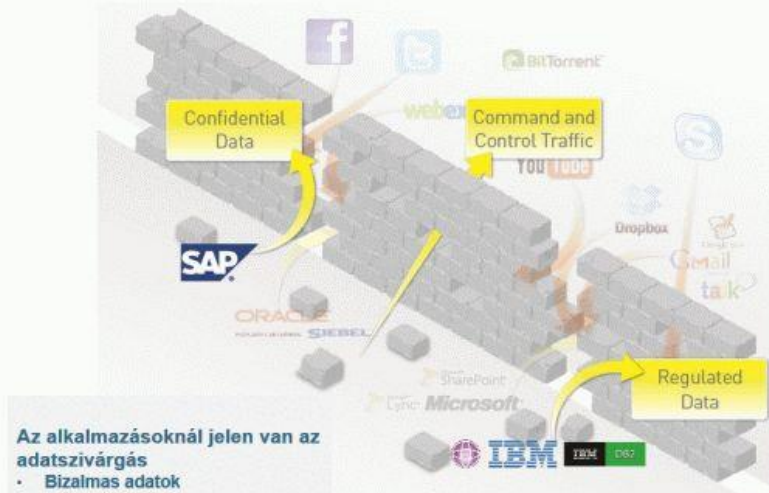
Alkalmazások átengedése a tűzfalon:



A fenyegetések az alkalmazások ellen irányulnak

SPESYS paloalto

Alkalmazások átengedése a tűzfalon: Adatszivárgás



Az alkalmazásoknál jelen van az adatszivárgás

- **Bizalmas adatok**

SPESYS paloalto

Ismerős?

Nem rossz, de nem elég!

Több modul nem megoldás a problémára

Kevesebb rálátás a forgalomra

Bonyolult és költséges bevezetni és fenntartani

Nem alkalmazás központú

SPESYS paloalto

Az új generációs tűzfal (NGFW) nem egy extra modul

Si Stateful Inspection **+ X ≠ NGFW**

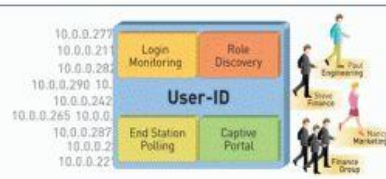
UTM	NGFW
Moduláris felépítés, tartalomszűrés, policy, logging, reporting, és gyakran a menedzsment felületen keresztül nem nyerhetők ki döntéshozatalt igénylő információk.	Egyszerű felépítés, tartalomszűrés, policy, logging, reporting, és a menedzsment felület összefüggő, döntéshozatalt igénylő információkat biztosít.

SPESYS paloalto

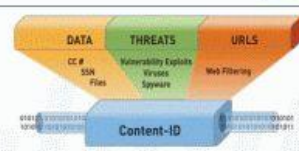
A azonosítási technológiák átalakítják a tűzfalat

App-ID™
Alkalmazás azonosítás

User-ID™
Felhasználó azonosítás

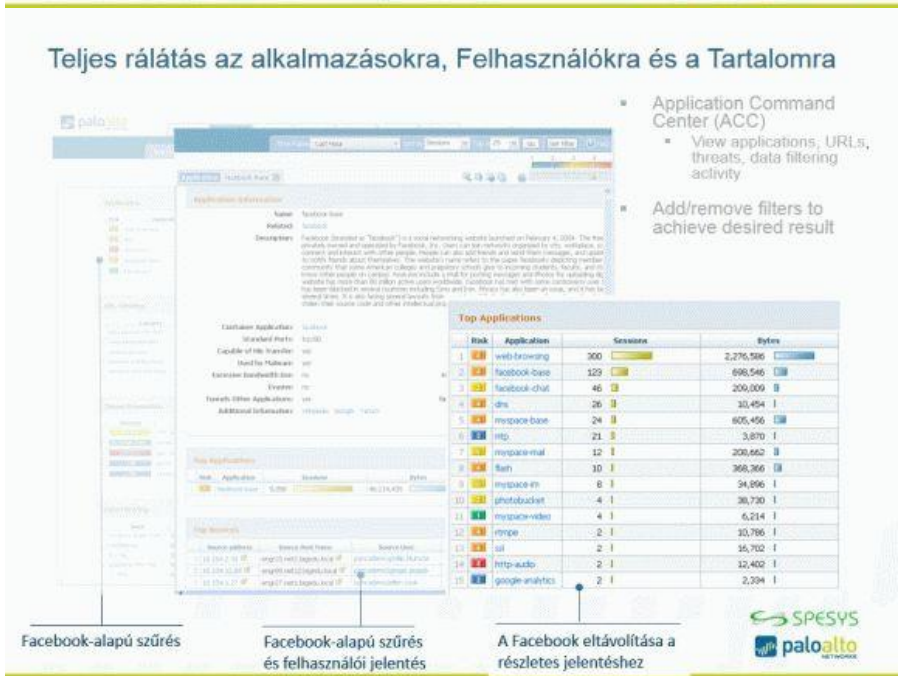


Content-ID™
Tartalomszűrés



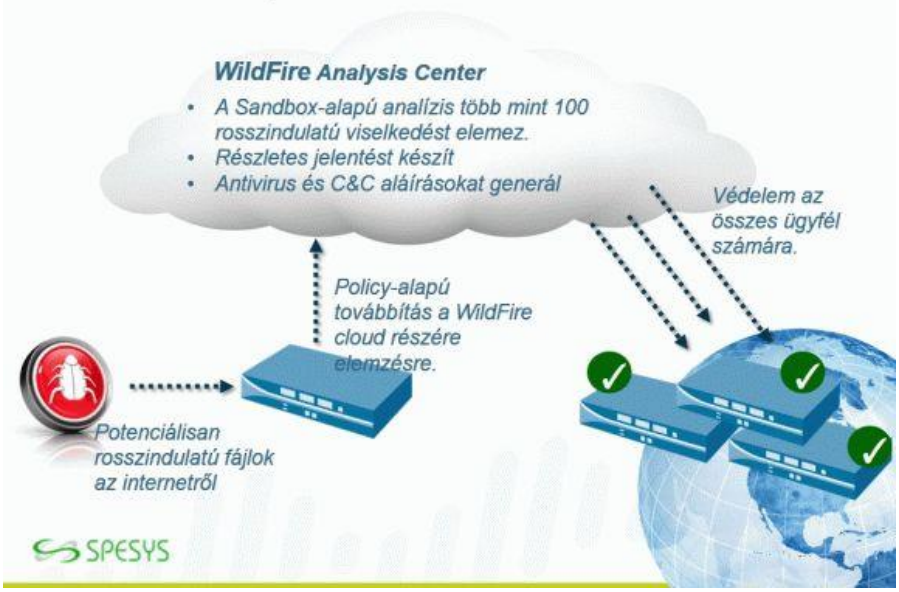
SPESYS paloalto

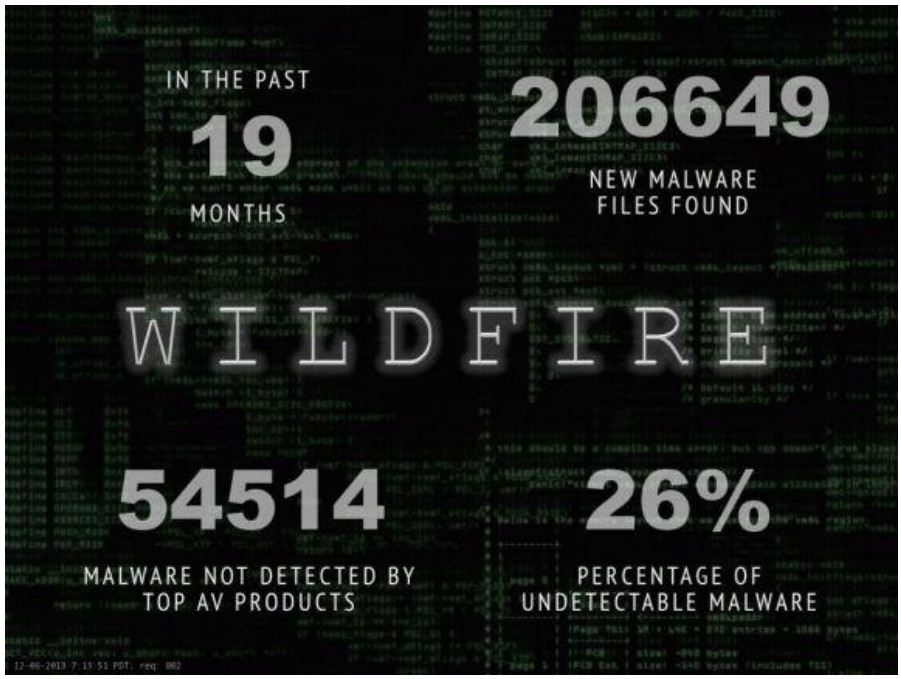

Egyetlen Biztonsági Policy Konzol
Security Rules
Name
Source Zone
Destination Zone
Source Address
Source User
Destination Address
Application
Service
Action
Profile
Allow Business Applications
12-lan-trust
12-lan-untrust
any
Exec Staff
IT Admin
finance
marketing
any
business-application
networking
any
Add Rule
Clone Rule
Delete Rule
Disable Rule
Move Rule
-- Select --
• A policy meghatározza az engedélyezett alkalmazásokat.
• A profilok által aktiválható tartalomszűrési funkció, mint az AV, IPS, anti-malware, URL and QoS.
Security Profiles
Antivirus
Anti-Spyware
Vulnerability Protection
URL Filtering
File Blocking
Log Forwarding
Data Filtering
SPESYS
paloalto

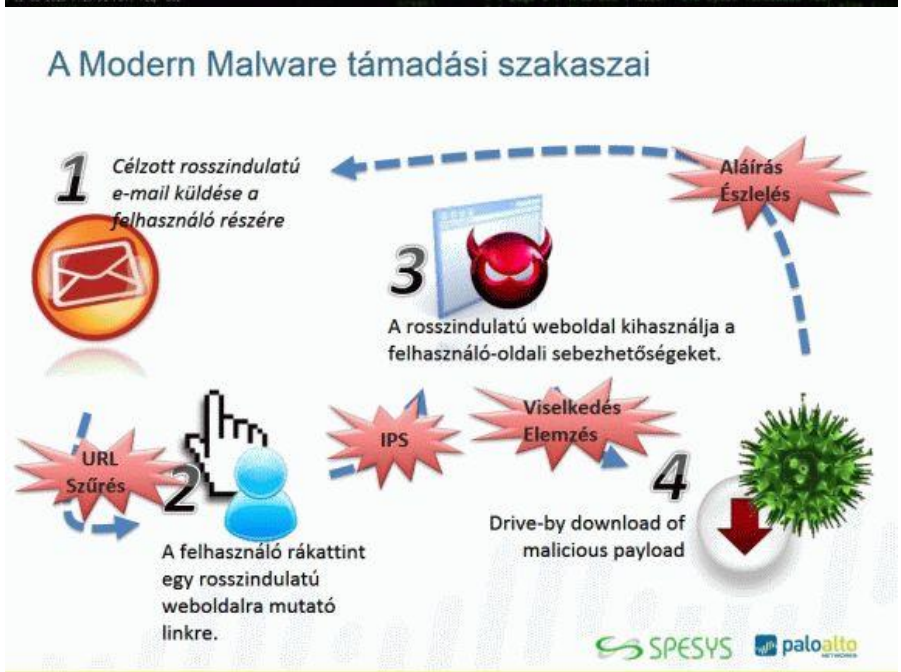

Teljes rálátás az alkalmazásokra, Felhasználókra és a Tartalomra
Application Command Center (ACC)
View applications, URLs, threats, data filtering activity
Add/remove filters to achieve desired result
Top Applications
Rank
Application
Sessions
Bytes
1 web-browsing 300 2,276,586
2 facebook-base 129 698,546
3 facebook-chat 46 209,009
4 dns 26 10,454
5 myspace-base 24 605,456
6 ntp 21 3,870
7 myspace-mail 12 208,662
8 flash 10 368,366
9 myspace-im 8 34,896
10 photobucket 4 38,730
11 myspace-video 4 6,214
12 rtmpe 2 10,786
13 ssl 2 16,702
14 http-audio 2 12,402
15 google-analytics 2 2,334
Facebook-alapú szűrés
Facebook-alapú szűrés és felhasználói jelentés
A Facebook eltávolítása a részletes jelentéshez
SPESYS
paloalto

A Malware lehetőségek tárháza

A WildFire felépítése

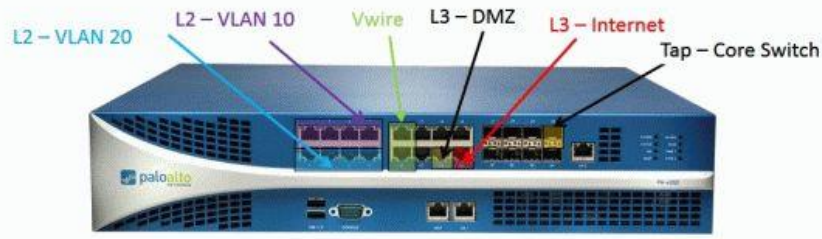



IN THE PAST
19
MONTHS
206649
NEW MALWARE
FILES FOUND
WILDFIRE
54514
MALWARE NOT DETECTED BY
TOP AV PRODUCTS
26%
PERCENTAGE OF
UNDETECTABLE MALWARE


A Modern Malware támadási szakaszai
1
Célzott rosszindulatú e-mail küldése a felhasználó részére
Aláírás Észlelés
3
A rosszindulatú weboldal kihasználja a felhasználó-oldali sebezhetőségeket.
URL Szűrés
2
IPS
Viselkedés Elemzés
4
Drive-by download of malicious payload
A felhasználó rákattint egy rosszindulatú weboldalra mutató linkre.
SPESYS
paloalto

Rugalmas alkalmazási lehetőségek

Ugyanannak a doboznak különböző hálózati módokban történő egyidejű használata.



- Számos működési mód: Tap Mode, Virtual Wire, Layer 2, Layer 3 with dynamic routing support (RIP, OSPF, BGP)
- Felhasználó által állítható működési módok – egyetlen doboz több port mód egyidejű használatát is támogatja
- Virtualizáció – VLAN interfészek L2-es és L3-as, virtuális routerekhez és virtuális rendszerekhez

SPESYS paloalto