Balog Károly

Digitális PMR-ek támadási és védelmi lehetőségei

Napjainkban az engedélyhez kötött és engedély nélkül is üzemeltethető PMR[1] rádiótechnológia a mobiltelefonoknál már megtapasztalt paradigmaváltáson megy keresztül. Újfajta digitális PMR rendszerek és egyedi készülékek kezdenek elterjedni a gyakorlatban, melyek frekvenciaengedélyhez nem kötött változatai ráadásul olcsók, bárki számára hozzáférhetők, és mozgásuk sem korlátozott. Mivel ezek az eszközök a hagyományos távközlési infrastruktúrákat kikerülhetik, ebben az esetben felderítésük, ellenőrzésük kizárólag a rádiófelderítés eszközrendszerével történhet. Természetesen a más kommunikációs infrastruktúrához is kapcsolódó rendszerek nem csak a rádiócsatornán keresztül támadhatók. Cikkemben áttekintem és összefoglalom mind az egyedi készülékek, mind a rendszerek támadási vektorait, valamint a PMR készülékekben és rendszerekben alkalmazható védelmi megoldásokat is.

Kulcsszavak: digitális professzionális/magán mobilrádió, rádiófelderítés, rejtjelzés, titkosítás, elektronikai védelem, információbiztonság

Bevezető

Kutatási témámban a nemzetbiztonsági rádiófelderítésen belül annak viszonylag új célterületével, az engedélyhez kötött és engedély nélkül is használható PMR eszközök digitális változatainak felderítési ellenőrzési kérdéseivel foglalkozom. Annak eredményeként, hogy az analóg PMR rádiótechnológia a mobiltelefonoknál már megtapasztalt paradigmaváltáson megy keresztül, neves európai, amerikai és japán gyártók szabványos digitális rendszerei és készülékei egyre jobban kezdenek elterjedni a gyakorlatban. Emellett azonban jelentős népszerűségnek örvendenek a kínai cégek olcsó, de a szabványok kereteit gyakran átlépő készülékei is.

Mivel az ilyen eszközök teljes mértékben kikerülhetik a hagyományos távközlési infrastruktúrákat, ebben az esetben felderítésük és ellenőrzésük kizárólag rádiós úton, a rádiófelderítés eszközrendszerével történhet. Másrészt viszont az engedélyhez kötött rendszerek esetében egyre elterjedtebb, a trönkölt rendszerek esetében pedig általános, hogy

1 PMR: Professional/Private Mobile Radio – professzionális/magán mobilrádió. A felhasználók által saját maguknak nyújtott, zárt körű rádióalkalmazások gyűjtőneve.

ezek valamilyen egyéb távközlési infrastruktúrához is kapcsolódnak, a legtöbb esetben valamilyen IP alapú hálózathoz történő csatlakozással. Ebben az esetben viszont a hálózati oldalról is támadhatóvá válnak a rendszerek.

Ezek az új típusú digitális eszközök a professzionális rendszerekhez hasonló megoldásokat tartalmaznak, azonban ezeket többféle eltérő szabvány formájában valósítják meg. [1] Ezért a hagyományos analóg felderítő berendezésekkel felderítésük csak részben, azonban ellenőrzésük (dekódolásuk) egyáltalán nem valósítható meg. Ehhez egyfajta paradigmaváltás szükséges az ellenőrző eszközök megoldásaiban is. A célom, hogy megvizsgáljam a rendszerek rádióspektrumon keresztüli sebezhetőségét, másrészt a hálózati infrastruktúra felőli támadásának lehetőségeit is. Ehhez szükséges a készülékek és rendszerek biztonsági fenyegetéseit, sérülékenységeit, és ezek kockázatát is feltérképezni (Risk Management) az ilyen rendszerek evolúciója során. A védelmük lehetséges megoldásait is célszerű körüljárni az elektronikai védelem, valamint az információbiztonság (Information Assurance) szemszögéből is, melyek rendkívül fontosak a kritikus infrastruktúrákban (repülőterek, erőművek stb.) alkalmazott PMR-eknél, vagy kiemelten fontos pl. kiscsoportos taktikai kommunikációra történő alkalmazásánál.

Az információbiztonság több mint titkosítás

Ebben a részben megvizsgálom, hogy az IP-hálózatokhoz is kapcsolódó, de alapvetően rádiós, tehát összességében hibrid rendszerek milyen biztonsági kockázatokkal rendelkeznek a korábbi hagyományos rádiós rendszerekhez képest. Ez utóbbinál kézenfekvő kockázatot egyedül a rádiócsatornán keresztüli lehallgatás (zavarás – elektromágneses sugárzás révén megvalósuló információszerzés vagy az információtovábbítás korlátozása, akadályozása), továbbá a fizikai pusztítás jelent. Az ezek elleni védekezés az *elektronikai védelem*[2] módszereivel lehetséges. Ehhez járul még hozzá a berendezések fizikai védelme, valamint esetlegesen a redundáns kialakítás a folyamatos működés biztosítására. Azonban a hibrid rendszereknél gyakorlatilag az infokommunikációs, így több más között az informatikai komplex rendszerekre jellemző (külső és belső) fenyegetésekkel és az ezeket lehetővé tevő sérülékenységekkel is foglalkozni kell. Mivel a hibrid rendszerek műveleti tartománya az RF spektrum mellett a vezetékes hálózati infrastruktúrát is magába foglalja, így a hibrid PMR rendszerek a kibertérben működnek, azaz a támadásukra a kibertéri műveletek, védelmük során pedig a komplex kibervédelmi vagyis elektronikai- és számítógéphálózat-védelmi eljárások alkalmazhatók. [2] Ez utóbbi komplex megvalósítására a civil rendszerek esetében napjainkban az információbiztonság (IA –Information Assurance) ad választ. Vizsgáljuk meg a következőben a két összetevőt külön-külön.

2 EPM: Electronic Protective Measures. Elektronikai védelem, amelyik biztosítja az elektromágneses spektrum saját részről történő hatékony használatát.

Az elsődleges kérdés az RF spektrumon keresztüli támadás lehetősége, azaz a *rádiófelderítés:* a technikai, tartalmi és geolokációs adatok megszerzése, illetve az *elektronikai támogatás*[3]*:* az elektronikai helyzet feltérképezése a zavarás vagy megsemmisítés szempontjából. Mindkét típusú felderítésnél, mind analóg és digitális átvitelnél egyaránt lényeges a használt elektromágneses spektrum, átviteli eljárás és protokoll ismerete, azonban lehallgatásnál az alkalmazott titkosítás ismerete, és ennek visszafejtési módszere is lényeges, hiszen a tartalmi hozzáféréshez ez a meghatározó kulcstényező. A zavarás szempontjából a frekvenciatartományok, a teljesítmények, és a fizikai elhelyezkedés a fontosabbak. Természetesen ezek a tartalom megszerzéséhez szintén fontos adatok, melyek alapvetően befolyásolják az adatszerzés sikerességét. A fenti szándékos tevékenységek elleni védekezésre az *elektronikai védelem* adja meg a választ.

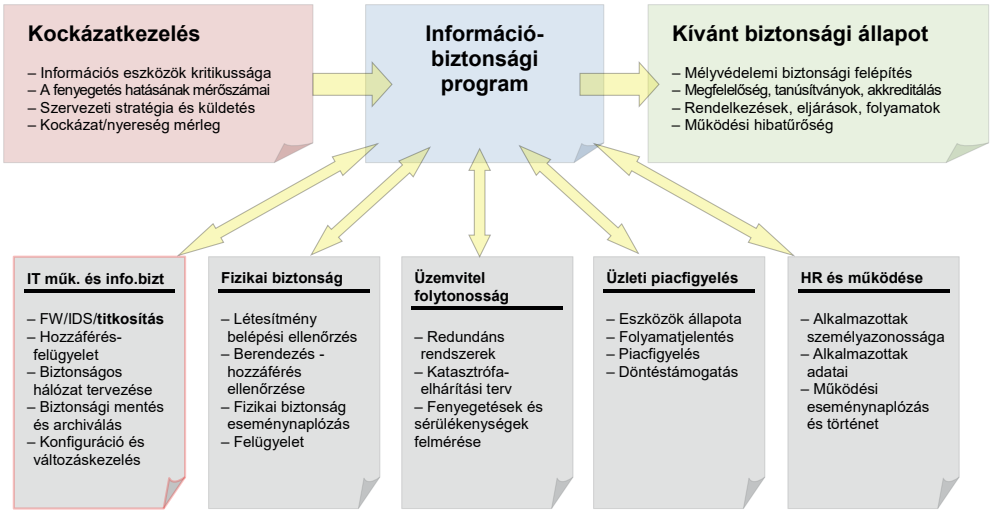
A második kérdés az információbiztonság, melynek alapvető objektumait elsősorban a *biztonságot fenyegető veszélyeztetések*, másodsorban a védelmi megoldások, rendszabályok képezik. A biztonságot fenyegető veszélyeket itt alapvetően a kiberműveleteken belüli *számítógép-hálózati műveletek* támadó részei jelentik. Azaz hardveres vagy szoftveres úton történő behatolás a PMR rendszerek kapcsolódó hálózataiba. Ez a hálózat struktúrájának feltérképezését, a hierarchikus működési sajátosságok feltárását, a hálózati adatáramlás tartalmának regisztrálását, a hálózatokban folyó megtévesztő, zavaró tevékenységet, a célobjektumok program- és adattartalmának megváltoztatását, megsemmisítését jelentik. [2] Természetesen ezek hibrid PMR rendszerek esetében konkrét hálózati elemekhez, objektumokhoz, és adott rendszerekben megvalósuló konkrét folyamatokhoz köthetőek.

Az információvédelem az információbiztonság kialakítására és fenntartására – a biztonság összetevőinek érvényesülésére – irányuló tevékenységek és rendszabályok összessége. Egy adott objektum biztonsága elleni fenyegetések csökkenthetők, elháríthatók az objektumot fenyegető szereplőkre, jelenségekre, továbbá a védendő rendszer elemeire irányuló tevékenységekkel is. Védelmi intézkedések közé tartozik mindenekelőtt a biztonságot fenyegető szereplőkre, jelenségekre vonatkozó információk megszerzése, valamint a képességeiket, lehetőségeiket csökkentő, célzottan „rájuk irányuló" ellentevékenység is. [3]

A PMR/LMR[4] rendszerek esetében is az általánosan elfogadott kockázatalapú üzleti és információbiztonsági elméletek szerint a kockázatelemzésnek megfelelően kialakított információbiztonsági program, azaz a komplex védelmi intézkedések együttesének alkalmazásával érhető el a kívánt biztonsági állapot. [4] Ennek döntési folyamatát és a szervezetre gyakorolt hatásait mutatja be az 1. ábra.

3 ESM: Electronic Support Measures. Elektronikai támogatás.

4 LMR: Land Mobile Radio, a PMR fogalmának amerikai megfelelője, de fogalmilag ugyanazt a kategóriát jelenti.



1. ábra: Az információbiztonság döntési folyamata és hatása a szervezetre (Forrás: [4])

A biztonság kockázatalapú megközelítése abból indul ki, hogy a biztonság egy dinamikusan változó, kedvező állapot, azonban tökéletes biztonság a gyakorlatban szinte sohasem érhető el, mindig számolni kell valamilyen kockázattal. A védelmi intézkedéseket a kockázatok elemzésére kell építeni. A kockázat egy ismert negatív hatású, adott valószínűségű jövőbeli esemény, melynek bekövetkezése függ a sebezhetőségtől is. A kockázatmenedzsment feladata, hogy a fenyegetések azonosítására és kiküszöbölésére – hatásuk felmérésére alapozva – költséghatékony megoldásokat alkalmazzon. Ehhez tisztában kell lenni a sebezhetőségekkel, a fenyegetésekkel, valamint azzal, hogy ezeket milyen védelmi intézkedésekkel lehet mérsékelni. [5]

Az 1. ábrából látható, hogy általánosságban az információbiztonságnak a PMR rendszerek esetében, az informatikai biztonság mellett számos aspektusa van, így a fizikai biztonság mellett az üzemvitel-folytonosság, az üzleti piacfigyelés, valamint az emberi erőforrásokkal történő gazdálkodás szempontjait is figyelembe kell venni. Az egyes területeknek önmagában is jelentős szakirodalmuk van, így a jelen cikk kereteiben csak a kutatási témámhoz szorosabban kapcsolódó, technikai úton történő adatszerzés lehetőségeivel foglalkozom leginkább.

Ennek kérdései az információbiztonság területén belül az informatikai biztonság témaköréhez kapcsolódnak alapvetően, és a sérülékenységekhez kötötten általában szándékosságot feltételeznek a támadó részéről (lásd a számítógép-hálózati műveletek támadó jellegét fentebb). Tehát a nem rádiós úton történő technikai hozzáférés aspektusát az informatikai hálózatokon keresztüli (távoli) hozzáférés veszélyei jelentik. Így elsődlegesen az informatikai rendszer határvédelmét biztosító tűzfal (FW – Firewall), behatolásdetektáló rendszerek (IDS – Intrusion Detection Sytem) védelme mellett a biztonságos háló-

zattervezés és ehhez történő hozzáférés-felügyelet játszik kiemelkedő szerepet. Mindezek mellett pedig adminisztratív feladatok is vannak, melyek az adatbiztonság témakörébe tartoznak, úgymint a rendszeres archiválás, és a rendszerváltozások folyamatos nyomon követése, felügyelete.

Természetesen a bevezetett rendszabályok és folyamatok érvényesülését folyamatosan ellenőrizni kell, amire a különféle minőségbiztosítási szabványok (pl. ISO/IEC 27001,[5] NIST 800) szolgálnak, melyek alapján elvégezhető az információs rendszer tanúsítása. Ha ezeket megfelelő módon alkalmazzák a gyakorlatban, akkor elérhető az elvárt biztonsági állapot, ami egy tervezett mértékű kockázatot tartalmaz.

A következő részekben áttekintem a PMR rendszerek típusait, és megvizsgálom, hogy ezek rendszerfelépítésük okán alapvetően hogyan különböznek támadási lehetőségek és a szükséges védelmi megoldások tekintetében is.

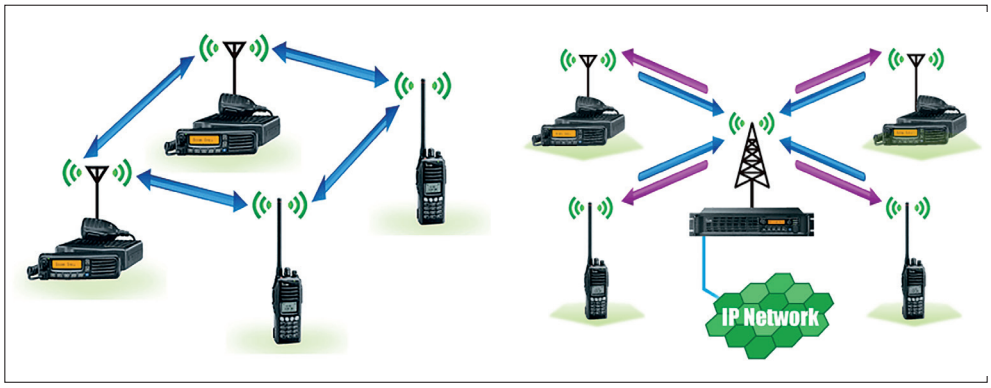
A PMR rendszerek támadási és védelmi szempontú csoportjai

Az ilyen típusú rendszerek támadási és védelmi lehetőségeinek vizsgálatakor a biztonság alanyából, azaz a védendő információból és az azt továbbító PMR/LMR rendszerek típusaiból kell kiindulnunk. [5]

Így a legegyszerűbb direkt kommunikációt alkalmazó rendszerek (2. ábra bal oldala) támadhatók a legkisebb felületen, kizárólag a rádiócsatornán keresztül, mivel ezek nem rendelkeznek semmilyen infrastruktúrával, egyedül a kommunikációban részt vevő készülékekkel. A rádióknak saját tápellátásuk van, így ha ezekből még tartalékkal is rendelkezünk, az egyik leghibatűrőbb kommunikációs módozatot kapjuk, melyet egyedül véletlen vagy szándékos zavarással tudunk hatástalanítani. A felderítésük, ellenőrzésük pedig kizárólag a rádiófelderítés eszközrendszerével lehetséges. Ezeket felfoghatjuk katonai terminológiában egyfajta harcászati hálózatnak is, mivel nem helyhez kötöttek, bárhol bevethetők, nincs infrastruktúra-igényük, így ha a rádió-össze-köttetés nem akadályozott és a rádiók működnek, összehangoltak, létrejöhet az összeköttetés. Az egyedüli probléma a korlátozott földrajzi lefedettség, amely azonban a rádiók teljesítményének növelésével jelentősen kiterjeszthető. A védendő eszközök köre egyedül a kommunikációban részt vevő rádiókat jelenti. A védendő információk köre ezeknél a rádióknál az átvitt beszédinformáció mellett valamilyen jelzésinformáció. Ezek analóg rendszernél valamilyen szelektív hívásjelzés, digitális esetben pedig ezeken felül valamilyen szabványfüggő formátumú lassú

5 Az ISO/IEC:27001 szabvány alapvető célja az Információbiztonsági Irányítási Rendszer létrehozása és működtetése. A szabvány felhasználóinak a biztonsági követelményeket, intézkedéseket a szervezet üzleti céljaiból és stratégiájából kell levezetniük. A szabvány megfelelőségi és ellenőrzési követelményei alapján elvégezhető az informatikai (információs) rendszer tanúsítása.

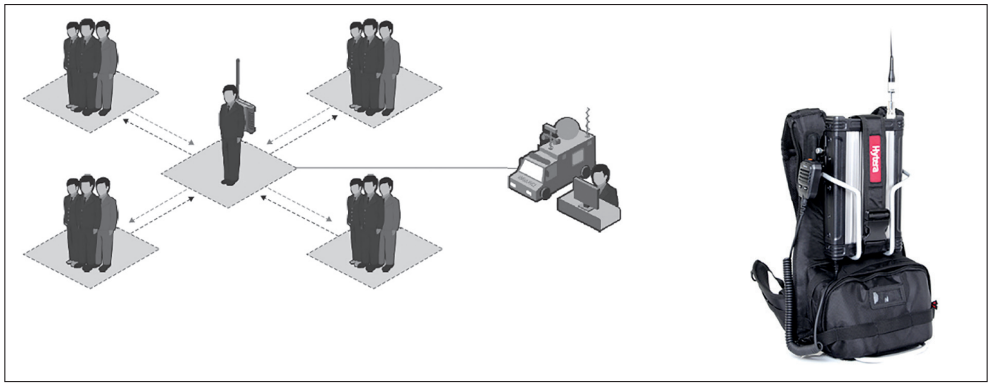
adat, amelyik általában valamilyen státusz- vagy rendszer-, illetve rövid szöveges üzenet, pozícióinformáció, valamint egyéb jelzést és azonosító információkat hordozhat. [1]



2. ábra: Direkt kommunikáció és helyszíni, vagy diszpécser típusú rendszer (Forrás: [6])

Ha nagyobb területi lefedettség szükséges, átjátszót alkalmaznak a hatótávolság növelésére. Ekkor a kommunikáció a PMR terminálok között nem direkt módon, hanem egy átjátszó állomáson keresztül jön létre (2. ábra jobb oldala) ezek az ún. helyszíni vagy diszpécser típusú rendszerek, melyek nagyon elterjedtek a gyakorlatban, a kiskereskedelemben, üzletekben, raktárakban, gyárakban, építkezéseken, kikötőkben, tömegközlekedésben, repülőtereken, taxi-, biztonsági és futárszolgálatok kommunikációja biztosítására.

A technológiai fejlődés eredményeként már rendelkezésre állnak olyan különleges hibrid taktikai megoldások is, amelyek egy hátizsákban hordozható kisméretű átjátszó alkalmazásával, komplex módon terjesztik ki egy korlátozott területen a lefedettséget pl. épületen belül, vagy egyéb infrastruktúra-hiányos területeken (3. ábra). Egy ilyen rendszer bár nem direkt kommunikációt alkalmaz, de a mobilitásával taktikai körülmények között biztosíthatja a diszpécser rendszerek kiterjesztett hatótávolságát és menedzselhetőségét.

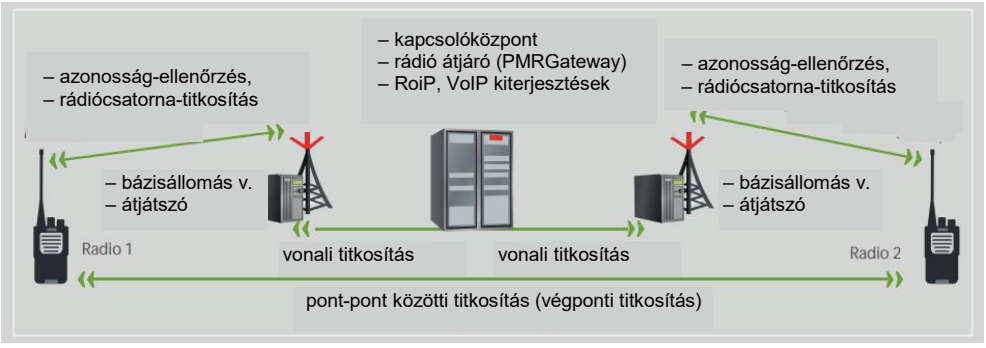


3. ábra: Hordozható taktikai diszpécser típusú rendszer (Forrás: [7])

A harmadik típus a dedikált trönkölt rendszerek csoportja, melyek a mobilhálózatokhoz hasonlóan bázisállomás-rendszert, kapcsolóközpontokat és központi adminisztrációt alkalmaznak, akár egy országot is átfogó területi lefedettség és a szolgáltatások biztosítására.

Látható, hogy a diszpécser, a hibrid taktikai és a trönkölt rendszereknél a rádiókészüléken kívül a rendszerek nagyságától és komplexitásától függő járulékos infrastruktúrával is számolni kell. Ezekben a modern rendszerekben szükség szerint integrálhatnak több kommunikációhordozót, így létrehozva egy olyan kommunikációs hálózatot, amely megfelelően összekapcsolja a területet és a háttér irodai hálózatot a nagyobb hatékonyság és a zökkenőmentes felhasználói élmény érdekében. [8] A helyszíni/diszpécser típusú és trönkölt rendszerek, valamint az IP-alapú vezetékes és vezeték nélküli hálózati technológiák kombinálásával eltérő nagyságú és topológiájú hálózatok építhetők, melyek a VoIP[6] és RoiP[7] megoldások alkalmazásával változatos, az igényeknek megfelelő rendszerek létrehozását teszik elérhetővé.

Ezek további sérülékenységeket, és egyben komplexebb támadási lehetőségeket jelentenek. A védendők köre ezeknél kiterjed az átjátszó vagy bázisállomásokra, kapcsolóközpontokra, diszpécser állomásokra, az ezek elhelyezésére, valamint a rendszer felügyeletére-vezérlésére kiépített objektumokra, továbbá az ezekhez kapcsolódó hálózatképző elemekre, informatikai eszközökre, vezetékes vagy vezeték nélküli átviteli utakra egyaránt. A védendő információk köre tekintetében pedig a rádiócsatornán átvitt információkon felül az összekötő felhordó hálózatokon átvitt beszéd és jelzés információkra is kiterjed az adatok védelme, ahogyan ez a következő ábrán látható.



4. ábra: Átviteli utak lehetséges védelme PMR rendszereknél (Forrás: [9])

A 4. ábra az átviteli utak összes lehetséges védelmi és azonosítási eljárását ábrázolja, de ezek adott rendszerekben skálázva vannak, azaz a teljesen titkosítatlan és azonosság-ellenőrzés nélküli esettől (többnyire analóg) egészen a végponti titkosításig, ami a legnagyobb biztonságot jelenti.

6 VoIP: Voice over Internet Protocoll: beszédátvitel internetprotokoll segítségével.
7 RoIP: Radio over Internet Protocoll.

A fentiekből következik, hogy napjainkban a legegyszerűbb rádiókommunikációs technológia is összetettebb, mint az elődei, így sokkal sérülékenyebb is azoknál. Ez a tény azonban nem mindig tükröződik az egyes alkalmazók rendszer-felügyeleti gyakorlatában. [4] Napjaink internethez kapcsolódó rendszerei nem csak a rádiós alrendszer, de a hálózati infrastruktúra oldaláról is támadási felületet nyújtanak, így adott esetben sokkal sérülékenyebbek, mint az ezektől elszigetelt rendszerek.

Ezt a tényt már számos gyakorlati példa is bizonyította, hiszen akár szándékos háborús pusztítás vagy természeti katasztrófa sújtotta térségekben nemegyszer az infrastruktúra-független direkt kommunikációs rádiórendszerek maradtak az egyetlen működőképes kommunikációt biztosító megoldások, ahogyan ez a legutóbbi nepáli földrengésnél [10], de más korábbi katasztrófák vagy háborúk (pl. délszláv, iraki, afganisztáni) során is bekövetkezett. Az egyedi készülékekből álló, hagyományos infrastruktúrát nem használó készülékek autonóm csoportjai biztosítják az egyetlen működőképes és viszonylag jól használható kommunikációs módot, a hagyományos infrastruktúrák kiesése és működésképtelenné válása esetében (ha nem számolunk a meglehetősen drága, tehát a polgári lakosság számára elérhetetlen műholdas globális megoldásokkal).

Az átvitt információ fontosságát azonban nem a rendszer felépítése határozza meg, így a direkt kommunikációt alkalmazó (adott esetben taktikai célú) rendszereknél is lehet kiemelt fontosságú az átvitt közlésinformációk védelme. Természetesen itt is mérlegelni kell a kockázatot, és ennek megfelelően lehet döntést hozni az alkalmazott titkosítás erősségéről illetve szükségességéről. Az átvitt információk érvényességi ideje alapján történő szelektálás is szempont lehet a védendő információk meghatározásának körében, ahogyan ez a következő NATO-dokumentumból is kiderül. [11, 5–2. o.] Ebben megállapítják, hogy városi körülmények között, a harcászati kommunikáció legalacsonyabb szintjén az információk érvényessége olyan rövid idejű, hogy nem szükséges titkosítás alkalmazása, mivel ez jelentősen kisebb előnnyel járna, mint az igen magas bekerülési költsége. Ezenfelül annak a veszélye is reálisan fennáll, hogy egy végpont elfogásával esetleg az egész titkosítási rendszer kompromittálódik. Továbbá indokként hozza fel a dokumentum a nemzetközi együttműködés nehézségeit is az együttműködő koalíciós partnerek között, a titkosításból adódó inkompatibilitások elkerülése érdekében. Látható módon a katonai harcászati rendszereknél is alkalmazzák a kockázatelemzés módszerét és az anyagi szempontok, és a kockázatok együttes figyelembevételével állapítják meg a titkosítás szükséges mértékét adott esetben.

Összességében megállapítható, hogy a direkt kommunikációt alkalmazó rendszerek kizárólag a rádiócsatornán keresztül támadhatók. A helyi/diszpécser típusú és a trönkölt rendszerek ezen felül a hálózati infrastruktúra felől is sérülékenyek. Ez utóbbiaknál ezek fizikai objektumainak és az ezekben elhelyezett berendezéseknek, továbbá a hálózatok további más hálózatok irányába kiterjesztett kapcsolódásainak és ezek hálózatképző elemeinek sérülékenységével is számolni kell. Megállapítható, hogy minél nagyobb és bo-

nyolultabb rendszerről beszélünk, annál több a támadási lehetőség, azonban ezzel párhuzamosan nőhet a rendszerekben alkalmazott védelmi, azonosítási és titkosítási eljárások száma, és vélhetőleg hatékonysága is. A konkrét rendszerek általában mind egyedi, személyre szabott megoldásokat tartalmaznak, így a sérülékenységük a támadó számítógép-hálózati műveleteken belül a hálózat struktúrájának feltérképezésével, a hierarchikus működési sajátosságaik felderítésével tárható fel (távoli technikai adatszerzések esetén).

PMR rendszerekkel kapcsolatos sérülékenységek, támadások áttekintése

Az általam vizsgált rendszereknél a támadásokat 4 fő kategóriába sorolhatjuk, úgymint passzív, aktív, külső és belső támadások. A passzív támadás lehet a rádiófelderítés ezen belül az információ lehallgatása, dekódolása, rögzítése, a kommunikációban részt vevő felek azonosítása, a kisugárzás irányának valamint helyének meghatározása, a kommunikáció forgalmi analízise, annak eloszlása, továbbá az egyes készülékek RF újlenyomatának azonosítása is ide sorolandó. Ez utóbbi a digitális rendszerek esetében veszített jelentőségéből, mivel ha az információtartalmat vissza tudjuk fejteni, akkor az [1]-ben leírtak szerint a digitális rendszerekben az egyes eszközök azonosítóit, egyedi címeit még titkosított esetben is ismerjük egy rádióhálózaton belül, ami adott környezetben azonosítja őket. Aktív tevékenységek közé tartozik a kommunikáció zavarása, és a fizikai pusztítás, továbbá a rádiós út speciális aktív támadási formája a közbeékelődéses (MitM[8]) támadás, ami a rádiótelefonok esetében alkalmazott támadási eljárás, a titkosítás eliminálása érdekében, de megfelelő feltételek esetén szerintem PMR hálózatok esetében is alkalmazható. A hálózati infrastruktúrán keresztüli támadás szintén aktív tevékenység.

A rádiófelderítés, zavarás, fizikai pusztítás és a hálózati oldalról történő hozzáférés egyaránt külső támadásnak minősül, azonban egy hálózat belülről is támadható, viszont itt már jelentős szerepet játszik a fizikai biztonság is, amivel azonban nem foglalkozom, de megemlítem a fontosságát. Összességében a továbbiakban a külső támadásokra koncentrálok, ami lehet passzív és aktív is. Így tulajdonképpen két részre osztható a vizsgálat, ami nagyjából az ilyen rendszerek főbb részeit is jelenti. Az egyes LMR/PMR rendszereknél a biztonsági fenyegetések és sebezhetőségek vizsgálata szempontjából egy mai rendszert a következők kombinációja jellemzi:

– rádiós alrendszer és sérülékenységei;
– Voice-over-IP (VoIP) alrendszer és sérülékenységei.

Korábban az analóg rádiórendszerek esetében általában elszigetelt hagyományos rádióhálózatokkal álltunk szemben, ahol ha valami zavar volt az egyik csatornán, ideig-

8 MiTM: Man in the Middle, azaz közbeékelődéses támadás, amikor az adatforgalom rajtunk keresztül bonyolódik a hálózatban a rádiócsatornán vagy a csatlakozó hálózati infrastruktúra vezetékes részén.

lenesen áthangoltak egy tartalékra. A modern helyszíni/diszpécser típusú vagy trönkölt rendszerek esetében azonban a rendszer meghibásodása már nem korlátozódik egyetlen csatorna elvesztésére, hanem akár a teljes rendszer üzemképtelenségével is járhat. Amerikai tapasztalatok alapján több száz, de akár több ezer felhasználóra is kihatással lehetnek pl. a természeti katasztrófák, ahogyan a közelmúltban Detroitban ez bekövetkezett. Másodszor, a hardveralapú platformok erősen függenek a számítógépektől és a rajtuk futó szoftverektől. Az instabil operációs rendszerek rendszerhibákat okozhatnak az esetleges lefagyásokkal, a helytelen paraméterbeállításokkal, és így tovább.

Harmadszor, a helyi vagy diszpécser, illetve a trönkölt típusoknál a legnagyobb erőfeszítések ellenére sem beszélhetünk teljesen elszigetelt rendszerekről. Így a modern rádiós rendszerek a következő (többnyire) szándékosságot feltételező sérülékenységekkel rendelkeznek:

- A rádiós alrendszer (RF site) problémája (fizikai és informatikai egyaránt):
  - helyi hozzáférés a RF vezérléshez, az IP-címének elfogása vagy behatolás a hálózatba;
  - távoli hozzáférés az RF vezérléshez, belépési ponton keresztüli támadás a hálózati kapcsolókon vagy vezérlőkön keresztül;
  - rádiófrekvenciás interferencia nem szándékos előidézése/kialakulása, szándékos interferencia okozása, azaz zavarás;
  - hamis/lopott készülékazonosítóval hozzáférés a rendszerhez, támadás a vezérlőcsatorna jelzésátvitelén keresztül;
  - készülékbe integrált beszéd- és adatátviteli képességek felhasználása belépő pontként a hálózat vagy programok elleni támadásra;
  - az információk szándékos lehallgatása a rádiócsatornán, azaz a rádiófelderítés;
  - titkosítás esetén a kulcskezelő rendszer biztonsági problémái.
- IT biztonság problémája (megosztott kapcsolatokkal és szolgáltatásokkal):
  - szoftverfüggő hibák: vírusok, kompatibilitási problémák, szoftverfrissítések;
  - hálózati elemeken keresztüli távoli támadás lehetősége a vezérlő és menedzsment platformokhoz, a diszpécser állomások hardver- és szoftver- (többnyire Windows-alapúak) sérülékenységeinek távoli támadása;
  - a felhasználói fegyelem problémája (a számítógép-terminálok illegális/nem megfelelő felhasználása), saját programok futtatása, fertőzött adathordozók csatlakoztatása;
  - egyre nagyobb függőség a rendszeren kívüli összeköttetésektől (adatbázisok, és egyéb adatátviteli alkalmazások, illetve perifériák).
- A fizikai biztonság problémája (közös helyiségek):
  - szándékos behatolás a rendszerbe, helyi eléréssel;
  - lopás/elvesztés (számos modern rádiórendszerben a készülékek lehetővé teszik a használat megkezdése előtti felhasználói azonosítás lehetőségét, amely lehet akár egy kódsorozat beütése, de manapság akár biometrikus azonosítás is; a rádió ello-

pása/elvesztése esetén a digitális eszközöknél az egyedi azonosítók miatt lehetőség van a diszpécserállomáson keresztül a készülékek tiltására a rendszerben, mely később újra aktiválható);
– a fenti rádiós, illetve IT-infrastruktúra elemei és ezek elhelyezésére szolgáló objektumok elleni fizikai támadások.

További nem szándékos kockázati tényezők PMR hálózatok esetében a következők:
– áramellátás zavarai, környezeti tényezők hatása;
– berendezéshibák, antennarendszer hibái;
– az emberi erőforrás vétlen biztonsági kockázatai.

A rádiós alrendszer támadási lehetőségei

A rádiókommunikáció kezdeti formáinak kialakulása óta alapvető igényként jelent meg az átvitt üzenethez (kommunikáció tartalmához) való hozzáférés, azaz a *rádiófelderítés*, megvalósítása. A lehetőség kézenfekvő volt, hiszen egy rádióadás elektromágneses jeleit tetszőleges számú rádiókészülékkel vehetjük anélkül, hogy az eredeti jelre az bármilyen hatással lenne, azaz gyakorlatilag észrevétlenül, passzív módon. A jelek vétele mellett a kisugárzás irányának és fizikai helyének megállapítása is ide tartozik. A modern digitális rádióknál ezt akár maguk a rádiók is közölhetik, a beépített GPS-ek adatait továbbítva, amit vissza lehet fejteni. A lehallgatás megvalósítása a különféle rádióvevőkkel, vevőrendszerekkel és a hozzákapcsolt antennákkal lehetséges. Az aktív megoldások tekintetében számításba vehető a rádiók és rendszerek *zavarása*, melyet ezeknél az eszközöknél célzottan keskeny sávon, de akár egy adott szélesebb tartományt lefogva is el lehet végezni. A rádiós alrendszer hálózati elemei (melyek a rádiós alrendszer távvezérlésére szolgálnak) az IT-sérülékenységeken keresztül támadhatók, hasonlóan más hálózati elemekhez.

A *titkosított információk visszafejtésére*, tehát az analóg scrambling eljárások és a digitális titkosítások támadására, törésére, eliminálására irányuló megoldások ismertetése, azok titkosítási eljárásainak bemutatása előtt értelmetlen lenne, ezért analóg esetben ennek bemutatása az analóg beszédtitkosítási eljárások (scrambling) után, a védelem résznél közvetlenül azokhoz kapcsolódva kerül ismertetésre. A digitális rádiók titkosításáról mégis itt kell néhány szót ejteni előzetesen, mert az egyik *legújabb támadási vektor ezek kulcsainak megszerzésére vagy eliminálására irányul*.

A digitális kódolások visszafejtésének napjainkban külön tudománya van, a kódtörés. Ahhoz azonban, hogy feltörjünk egy kódolást, be kell azonosítani, hogy milyen módszerrel készült a titkosítás. Ezután lehet kipróbálni a kulcsokat. A PMR rádiók titkosítására napjainkban elterjedt AES,[9] egy szimmetrikus kulcsú rendszer, azaz ugyanaz a kód szükséges

9 AES: Advanced Encryption Standard. Fejlett titkosítási szabvány, 2001-ben szabványosították az USA-ban.

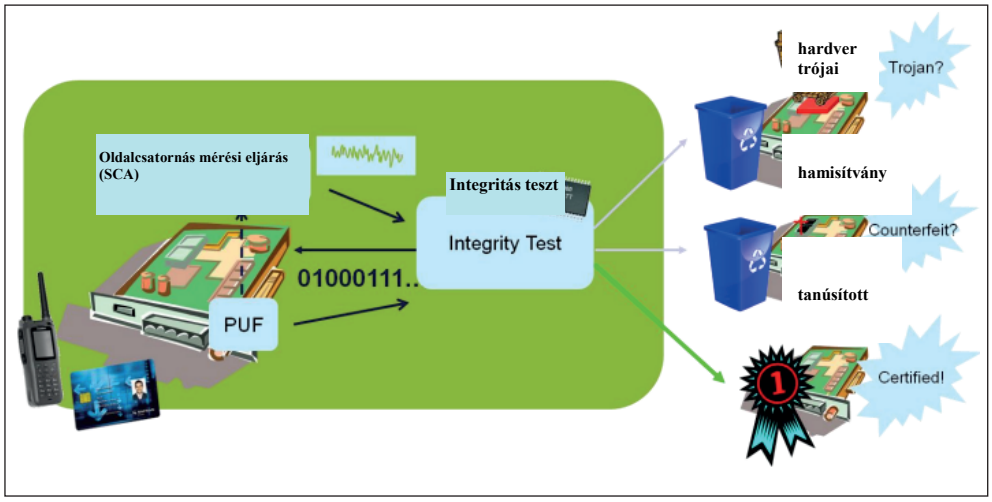
az üzenet titkosításához, mint a dekódoláshoz. Itt a kulcsok nem nyilvánosak, ellentétben az ún. aszimmetrikus vagy nyilvános kulcsú rendszerekkel, mint az RSA,[10] aminél két eltérő kulcs van. A titkosító kulcs nyilvános, de a dekódoláshoz szükséges második kulcs csak az üzenet vevőjénél áll rendelkezésre, megfelelően biztonságosan tárolva. Azaz bárki küldhet nekem titkosított üzenetet, de csak én tudom visszafejteni. A legjobb módszer az üzenet megfejtésére, ha azt számítógépen rögzítjük, és valamilyen matematikai elmélet és az eljárás valamilyen gyengeségének kihasználásával igen erős hardvertámogatás mellett próbálkozunk a lehetséges kulcsok kiszámolásával. Az erős titkosítások esetén azonban ez véges, tehát műveletileg használható időn belül általában nem vezet eredményre. Azonban ha a titkosítási eljárásba mesterségesen hibát visznek, a kulcs feltörhető. Természetesen a legkézenfekvőbb megoldás a nem nyilvános kulcsok megszerzése lenne mindkét fenti esetben, amivel bármilyen kommunikáció visszaállítható eredeti formájában.

A titkosítási rendszernek alapvetően 3 eleme van. A kódolás és dekódolás algoritmusa (a mód, ahogyan az információból kódolt üzenet lesz, majd megint információ), a titkosító kulcs, valamint a rendszer kulcskezelési megoldása. Mivel egy adott eszköz esetében a titkosítási rendszer és az algoritmus nem változik, ezért az integritás megőrzése érdekében a titkosító kulcsokat kell változtatni adott időnként. A kulcskezelési (key management) megoldások erre szolgálnak, azaz előállítják, tárolják, szétosztják, kiválasztják, továbbá megsemmisítik vagy archiválják az egyes kulcsokat. A probléma általában a kulcsmenedzsment kivitelezése, azaz hogyan juttassuk el a kulcsokat a felhasználókhoz. Ez a kérdés már a korai katonai célú digitális harcászati rendszerek esetében is felmerült [12], mivel ellenséges környezetben nagyobb a veszélye egy kulcs kompromittálódásának. Ekkor dolgozták ki a rádiócsatornán keresztüli kulcscsere eljárását, az OTAR[11] technológiát, amelyet azóta számos vezeték nélküli rendszerben alkalmaznak, így pl. trönkölt, de akár helyi vagy diszpécser típusú PMR rádiórendszerek esetében is. Így ezzel már meglehetősen nagy biztonság érhető el a kulcsok kompromittálódásának megelőzése terén.

Napjainkban azonban a fentiek miatt megjelent egy új lehetőség, amelyik a rendszerben lévő *biztonsági áramkörök hardverelemeken keresztüli fertőzésével* (hardver trójai – HT[12]), próbálja meg a kommunikáció visszafejtéséhez szükséges kulcsokat megszerezni, vagy azokat gyengíteni. Ezek pl. a később említett AES blokktitkosító modulokat (8. ábra) támadják. Egyre növekvő az aggodalom, hogy a hardverelemek hamisítása drámaian növekszik. Napjainkban a piacokon kapható alkatrészek mintegy 5-20%-a hamisított alkatrészként kerül forgalomba. Továbbá a fenyegető „trójai" programok, vagy az integrált áramkörök (IC) rejtett funkciói az elméletből egyre inkább a gyakorlati megvalósítás mezejére léptek.

10 RSA: Rivest, Shamir, Adleman, azaz a kifejlesztőinek kezdőbetűiből elnevezett, nyílt kulcsú titkosítási eljárás.
11 OTAR: Over The Air Rekeying, azaz rádiócsatornán keresztül kivitelezett kulcscsere eljárás.
12 HT: Hardware Trojan. Hardver trójai program, ami az eszközökben már gyári állapotban is megtalálható a hamisított alkatrészek miatt, így gyárilag hordozza az ilyen alkatrészekből összeszerelt rádiók sérülékenységét.

A probléma annyira valós, hogy az EU kutatási projektet indított a fentiek megoldására a hetedik keretprogramon belül, több mint 5 millió euró támogatással. [13] A HINT projekt 2013. májusban megjelent publikációjában [14] smart ID card és PMR kézi készülékeken demonstrálják a HT detektálását az általuk kidolgozott módszer segítségével, ahogyan ez az 5. ábrán látható.



5. ábra: A HINT projekt hardverintegritás-tesztje (Forrás: [14])

A HINT projekt a fenti új kihívásokkal foglalkozik, innovatív technológiák kifejlesztését kutatja annak ellenőrzésére, hogy a vizsgált rendszer eredeti és nem módosították. E technológiák támogatják egy adott rendszerben használt hardverelemek (integrált áramkörök, amelyek lehetnek ASICS[13] áramkörök, hagyományos COTS[14] alkatrészek csakúgy, mint a legmodernebb átprogramozható eszközök, CPLD[15]/FPGA[16] áramkörök egyaránt) biztonságának, hitelességének és integritásának megállapítását. Erre az ún. PUF[17] alapú aláírást és azonosság-ellenőrzést valamint az SCA[18] eljárást alkalmazzák, amelyek lehetővé teszik a fenti hardverelemek hatékony és biztonságos ujjlenyomatának megállapítását és az ezekhez képesti eltérések detektálását. A fenti projekt kutatói a [15] bevezető publikációjukban a HT által egy PMR készülékben előidézhető eseményeket a következőkben aposztrofálták:

13 ASICS: Application Specific Integrated Circuits. Alkalmazásorientált integrált áramkörök, amelyek adott speciális célra, adott feladatra készülnek.
14 COTS: Commercial Off-The-Shelf. Hagyományos, általános célra készült kereskedelmi forgalmú alkatrészek.
15 CPLD: Complex Programmable Logic Device. Komplex átprogramozható logikai eszköz.
16 FPGA: Field Programmable Gate Array. Átprogramozható kapuáramkörtömbök adott, pl. rádiós funkciók hardveres végrehajtására.
17 PUF: Physically Unclonable Function. Fizikai másolásvédelmi funkció.
18 SCA: Side Channel Analysis. Oldalcsatorna alapú azonosság-ellenőrzés; egy hardverkomponens viselkedésének elemzésén alapuló eljárás, amellyel megállapítható az eredeti specifikációtól való eltérés.

1. Szolgáltatás-megtagadás előidézése: a készülékben alkalmazott cryptoASIC és a hardver kriptoprocesszor között. A cryptoASIC-ba implementált HT képes a két eszköz közötti busz kommunikációját gátolni, továbbá képes ún. kill switch állapotba kapcsolni a kriptoprocesszort, ami ezután csak újraindítással hozható ismét működésbe. Ezután két lehetőség van: a HT csak ideiglenesen működött és visszaáll a normál működésre a HT következő betöltődéséig, vagy a HT hatása folyamatos, és az eszköz nem működik többé, azaz tönkremegy.

2. Információszivárgás: érzékeny információk kiszivárgása, pl. a titkosító kulcs. Ezzel lehetőség van az érzékeny védendő információk megszerzésére, lehallgatására csakúgy, mint a PMR hálózat 4. ábrán jelölt rádiócsatornán keresztüli azonosság-ellenőrzésének (authentication) kijátszására. Erre kétféle lehetőséget látnak.

Direkt szivárgás esetén a fertőzött terminál közvetlenül elküldi a titkosító kulcsokat a készülék I/O kimenetén vagy a rádiócsatornán, vagy áltitkosító algoritmus számolása mellett a titkosítandó üzenetet (plain text) titkosítatlanul küldi a rádiócsatornán, azaz eliminálja a titkosítást. Ez könnyen észrevehető, ezért a következő eljárás sokkal kifinomultabb.

Indirekt szivárgás esetén a titkosító kulcs visszanyerésére alkalmas információkat szivárogtat ki az eszköz ideiglenesen vagy véglegesen, Pl. órajelváltozás, áramfelvétel, feldolgozási idő változtatása formájában, mintegy titkos jelzésátviteli csatornaként. Ez az ún. SC vagy oldalcsatorna, melynek a megmérésére dolgozott ki eljárásokat a projekt, mind az eszköz elektromágneses kisugárzásának megmérésével, mind az eszközhöz közvetlen hozzáféréssel kivitelezve. Ezeken felül elképzelhető, hogy a HT egy hibát injektál a ciphertextbe, ami a titkosított adat. Egy hibás és egy jó ciphertext közötti különbségből matematikai módszerrel: különbségi hibaanalízissel (DFA – Differential Fault Analysis) akár egyetlen hibás ciphertext injektálásával is megtörhető az AES, vagy az RSA algoritmus. Az ilyen támadások könnyen kivitelezhetők a criptoASIC módosításával, pl. minden OTAR kulcscsere során újra elküldve az oldalcsatornán az új kulcsot, amint a HT érzékeli annak megjelenését a criptoASIC bemenetén.

3. Áramköri meghibásodás: Eltérően az első pontban leírtaktól, a fertőzött eszköz tovább működik, csak hibásan. Ekkor pl. a HT bizonyos belső kapcsolatokat, vagy a memóriatartalmat változtatja meg, amely nem okoz információszivárgást, de működési problémát idéz elő egy rendszerben. A hatás itt is lehet átmeneti és állandó egyaránt. Egy másik módszernél a HT nem engedi alvó (energiatakarékos) üzemmódba a készüléket, miáltal az igen hamar lemerül. A terminál használója nem gondol HT-ra, csak az akkumulátor hibájára. Egy harmadik módszernél egy rejtett vezetékes kapcsolatot hoznak létre pl. egy CPLD és egy cryptoASIC között. Ezt szinte lehetetlen észrevenni, de fizikai hibát képes előidézni, pl. egy vezeték túlterhelődésével. Ez szikrákat idézhet elő, ami adott környezetben robbanást okozhat. A hiba csak a HT betöltésével aktiválja a kapcsolatot, így pl. ATEX[19] robbanásbiztos minősítésű rádiók tanúsítása során sem derül rá fény, így idézve

19 ATEX: Az EU-ban és Magyarországon is érvényes robbanásbiztonsági direktíva francia nevéből: utilisés an Atmosphéres Explosives.

elő akár valódi robbanásokat is a később ilyen körülmények között fokozottabban használt rádiók esetében.

4. Szabotázs előidézése: A támadó a HT segítségével módosítja a PMR biztonsági funkcióit. Pl. a készülékben alkalmazott véletlenszám-generátor (RNG – Random Number Generator) kimenetét állandóan nullára állítja, ami jóval kisebb biztonsági szintet eredményez, mint a véletlen adatokból generáltak. Az RNG kimenetét általában egy online teszterrel folyamatosan ellenőrzik, pl. FIPS 140-2 vagy AIS-31 tesztekkel, azonban egy kifinomult HT a teszt eredményét is képes módosítani, vagy annak hatását eliminálni. És végül lehetséges olyan módosítás alkalmazása a HT segítségével a készülékben, hogy egy lejárt titkosító kulcs esetében az új megküldött érvényes kulcs nem kerül alkalmazásra, ahelyett a régi marad érvényben.

5. Érzékeny adatok megváltoztatása: A fenti 4 veszélyt a [14]-ben kiegészítették egy ötödikkel is. Ennél a HT megváltoztathatja a belső csomópontok és egyes áramkörök memóriatartalmát, ahol azok tárolódnak vagy feldolgozzák őket. Az összes ilyen érzékeny adat (pl. kulcsok, jelszavak, PIN kódok, vagy egyéb felhasználói adatok) megváltoztatása jelentős hatással van a készülék által nyújtott szolgáltatásra.

A VoIP alrendszer támadási lehetőségei

Az IP-hálózatok jól ismert előnyei mellett az IP-protokollok, -platformok és -szolgáltatások nyitottsága, révén ez egyben jelentős új biztonsági réseket jelent az ezeket alkalmazó PMR hálózatok működésére és a kritikus infrastruktúrák környezetében. Az IP-hálózatok robbanásszerűn megnövekedett aszimmetrikus fenyegetettségei nem kezelhetők a hagyományos biztonsági és kockázati megközelítésekkel. A hagyományos fenyegetési modellek szimmetrikusak, és jól definiált határok mentén mozognak. Azonban napjainkban a fizikai és a kiberhadviselés határai elmosódottak a globális társadalompolitikai fenyegetések fejlődése és a nagymértékben szerteágazó vállalati számítástechnikai modellek eredményeként.

Az aszimmetrikus fenyegetések esetén nem beszélhetünk határozott peremvonalakról és feltételekről, amik mentén a támadások zajlanak. Ezek a következőket jelentik:

– külső és belső védelmi vonalak támadása;
– kifinomult automatikus támadási módszerek alkalmazása a technology stack (pl. OSI 7 rétegű modell) alsóbb vagy felsőbb rétegeiben;
– kevert támadások alkalmazása a fizikai és a kibertámadások szabad kombinálásával;
– a hálózati rendszerek és a kritikus infrastruktúrák kapcsolódásának kihasználása;
– az emberi tervezés és a bennfentes részvétel lehetőségeinek kiaknázása.

Az új típusú, IP-alapú PMR hálózatok a számos előnyük mellett jól ismert protokollokat, szolgáltatásokat és felületeket alkalmaznak a hálózati és IT-infrastruktúra különböző szintjein, amelyek a sebezhetőségek gazdag tárházát kínálják.

A fenyegetések matematikája, azaz a fenyegetettség + sérülékenység = kockázat képlete szerint, a fentebb leírt fenyegetésvektorok viszonylag ártalmatlanok lennének, ha nem lennének jelentős emberi és technológiai hiányosságok az IT-függő szervezetekben. A tapasztalt biztonsági mérnökök szerint azonban a legtöbb kereskedelmi és kormányzati IT-infrastruktúrákban találhatók súlyos sérülékenységek. Ezek a következők lehetnek: Hiányzó megfelelő határvédelem és forgalom-ellenőrzés. A fizikai hozzáférés hiányos ellenőrzése. Frissítetlen és rosszul beállított eszközök. Gyenge vagy hiányzó jelszavak. Nem megfelelő biztonsági jelentések. Gyenge antivírus-védelem a rosszindulatú programok ellen. Emberi hibák a rossz képzés és szakmai fejlődés hiányosságai következtében. Adatszivárgás, az információk nem szándékos közzététele.

De ha a fentiek mind rendben lennének, akkor is elmondható, hogy szinte naponta fedeznek fel eddig ismeretlen sérülékenységeket, melyekkel az eddig biztonságosnak hitt rendszerek is kompromittálhatóak (lásd példaként az alkatrészeket fertőző hardver trójai esetét). Az emberi és rendszerhibák ajtót nyitnak a jogosulatlan hozzáférések, szolgáltatás-megszakítások és adatszivárgások széles skálájának. Átfogó információbiztonsági megközelítés nélkül a támadók, terroristák és bűnözők válnak egyre sikeresebbé.

A PMR hálózatok, készülékek védelmi lehetőségei

A rádiós alrendszer esetében a védelem bizonyos részmegoldását az elektronikai védelem biztosíthatja, ezen belül is főleg az *elektronikai felderítés elleni tevékenység* megoldásai, amelyek nem csak az elektronikai támogatás, de a rádiófelderítés ellen is segítséget nyújthatnak. A másik az *elektronikai ellentevékenységgel szembeni védelem*, amelyik gyakorlatilag a szándékos vagy véletlen zavarok, illetve az elektronikai pusztítás ellen is biztosíthat megoldásokat. [2] Mindezek kivitelezése esetében természetesen figyelembe kell venni az ellenfél felderítő és elektronikai hadviselési képességeit, eszközeinek színvonalát.

Az *elektronikai ellentevékenységgel szembeni védelem* esetében a nem szándékos interferenciák – rádiózavarok – megszüntetésére adminisztratív és mérőszolgálati módszerek alkalmazhatók, melyekre hazánkban a polgári rendszerek esetében az NMHH[20] jogosult. Ez a hatóság rendelkezik az ilyen rendszerek zavarásának megmérésére alkalmas országos rendszerrel, és hatáskörrel a bemért zavarások megszüntetésére.

A *felderítés elleni tevékenység* magában foglalja az elektromágneses kisugárzások korlátozását (passzív rendszabályok) és a felderítés előli kitérés különböző módozatait (aktív, az adóberendezések paramétereit megváltoztató, észlelhető rendszabályokat), amelyek úgymond elrejtik az elektromágneses jeleket és eszközöket az ellenséges felderítés, helymeghatározás és azonosítás elől. Ide tartozik továbbá a felderítő berendezések és adataikat

20 NMHH: Nemzeti Média és Hírközlési Hatóság.

továbbító híradó eszközök megsemmisítése, megrongálása vagy zavarása is (békeidőben ezek nem alkalmazhatók). A kisugárzások korlátozása jelentheti a szükséges legrövidebb kommunikáció alkalmazását, a terjengősség mellőzését az információcserénél, de a szándékos rádiócsend alkalmazását is a lehallgatás felmerülő veszélye esetén. Ezek PMR-ek esetében szerintem jól alkalmazhatók. Az aktív rendszabályok azonban már az adófrekvencia és üzemmód változtatását, a kisugárzott teljesítmények minimalizálását jelenthetik például. Megjegyzem, hogy ez az eljárás szerintem polgári rendszerek esetében korlátozottan alkalmazható, hiszen ezek engedélyhez kötött frekvenciákon és üzemmódokban, meghatározott teljesítménnyel működhetnek. Azonban a direkt kommunikációt alkalmazó frekvenciaengedélyhez nem kötött eszközök, vagy az engedély nélkül illegálisan használt rádiók esetében ezek a célnak megfelelően alkalmazhatók, és a bűnözők és terroristák vélhetőleg alkalmazzák is ezeket a felderíthetőség csökkentésére.

A fentiek ellenére azonban a rádióadások megfelelő módszerekkel békeidőben legtöbbször felderíthetők, így a *híradó-biztonsági előírások* segítségével magát az információt is védeni kell a felderítés ellen. Ez lehet csoportos vagy egyéni védelem. Ennek nyílt adások esetén kézenfekvő megoldása a rövidítések, kulcsszavak alkalmazása, azonosítás, hitelesítés kérése az eszköz alkalmazásakor. Azonban a legkézenfekvőbb megoldás a titkosítás alkalmazása, melynek napjainkban elterjedt megoldásait az alábbiakban tekintem át.

Titkosítási eljárások

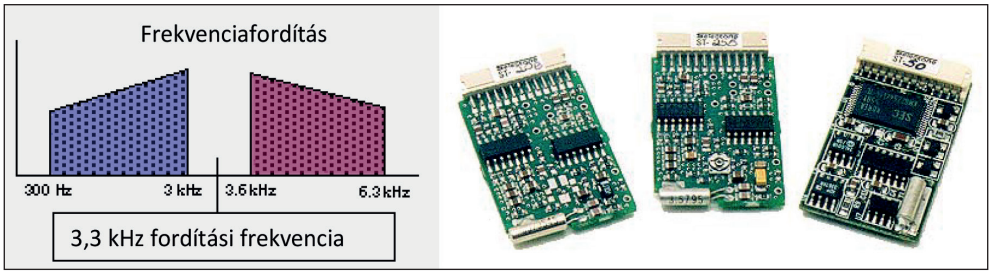
Már a rádiózás hőskorában is felmerült az információ védelmét biztosító eljárások kidolgozása. A kezdeti jelzésátviteleknél erre megfeleltek az offline módú eljárások, pl. morzeátvitelnél, különféle kulcskönyvek, sifre táblázatok stb., azonban az élő beszédkommunikáció megjelenésével online, valós idejű eljárások kidolgozása vált szükségessé az azonnali információátvitel megvalósításához. A beszédátvitelre alkalmazott kommunikációvédelmi megoldásokra eltérő eljárásokat dolgoztak ki analóg és digitális rádiók esetében. Természetesen a digitális rádiórendszereknél megjelenik a natív adatátvitel lehetősége is, azonban ezeknél a hagyományos adatátviteli eljárásokra jellemző jeltitkosítások alkalmazhatóak. A szakirodalomban általában szinonimaként használják a rejtjelzés (scrambling) és a titkosítás (encryption) fogalmát, azonban ezek kivitelezése technikailag jelentősen eltér egymástól. A rejtjelzés analóg jeleknél használt szűréssel, vágással, keveréssel módosított frekvenciaspektrumú jelátvitelt jelent, amely relatíve kisebb biztonsági szinttel és még rosszabb hangminőséggel párosul. Ezzel szemben a digitális titkosítás az alkalmazott algoritmus szerint megváltoztatja az átvitt jel információ- vagy adattartalmát. Ez normál esetben digitális jelekkel működik, tehát digitális PMR-ek esetében, illetve analóg esetben is, ha előtte digitalizáljuk a beszédet.

A gyakorlatban ez azt jelenti, hogy el kell döntenünk, hogy egy adott feladatra adott konfigurációban használandó rádiós rendszer esetében milyen kommunikációvédelmi eljárást alkalmazunk a rádiócsatornán, ha egyáltalán alkalmazunk bármilyet.

Analóg eljárások

Az analóg rádiós rendszerekben a védelem alkalmazására az eredeti hang néhány paraméterét bizonyos algoritmus szerint megváltoztatják, így az eredetitől eltérő hanginformáció továbbítódik a rádiófrekvencián. Ezt a folyamatot angolul „scrambling"-nek nevezik, amire a legjobb magyar megfelelő talán a rejtjelzés kifejezés. A vevő oldalán csak a descrambling algoritmus ismeretében dekódolható az eredeti jel. Az analóg jelkódolás két csoportra osztható: (egyszerű) frekvenciafordítás és dinamikus frekvenciafordítás.

A frekvenciafordítás nagyon egyszerű, a bemeneti jelet egy előre meghatározott frekvenciára tükrözik (6. ábra). Az emberi hang spektruma 300 és 3000 Hz közé esik, elegendő csak ennek a sávnak a változását figyelemmel kísérni. A tükrözött hang 3,6 és 6,3 kHz között, az eredeti frekvenciákhoz tartozó jelerősség fordított sorrendjével kerül átvitelre, ezáltal érthetetlen lesz az átvitt beszéd.

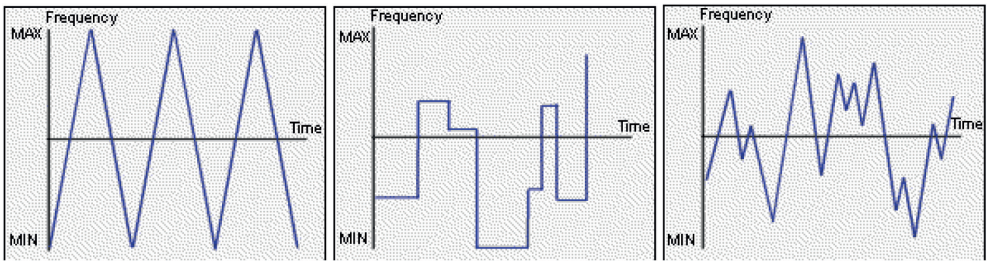


6. ábra: Egyszerű frekvenciafordítás elve és titkosító modulok (Forrás: [16])

Ehhez az átviteli módhoz gyártanak scrambling modulokat erre szakosodott cégek, pl. Selectone [16], Norcomm [17], MX-Com (jelenleg CML Microcircuits USA) [18], Transcript Ltd., Motorola, Kenwood stb., ahol az egyes gyártók általában szabványos fordító frekvenciákat alkalmaznak, de a modernebb titkosítók tükrözési frekvenciája, pl. a CML programozható. A PMR készülékeket gyártó cégek a felsoroltakon kívül még számos gyártó cégtől, illetve saját fejlesztésből is szerezhetnek be készülékeikbe titkosító modulokat.

A dinamikus frekvenciafordítással végzett titkosítás alapelve megegyezik az egyszerű (előzőekben részletezett) frekvenciafordítással, azonban a fordító frekvenciát időnként vagy folyamatosan megváltoztatják, ahogyan ezt a 7. ábra szemlélteti. A dinamikus eljárásnál alapvetően 3-féle változatot különböztetünk meg az algoritmusaik szerint. Ezek a következők:

– *Pásztázó frekvenciás rendszer (7/a. ábra):* A fordító frekvencia előre meghatározott minimum- és maximumérték között változik. A frekvencia emelkedésének és esésének mértéke állandó.
– *Ugró frekvenciás rendszer (7/b. ábra):* Az algoritmus a fordító frekvenciát lépteti változó időközönként. Itt a visszafejtésnél segítség lehet a hosszabb ideig folyamatosan egy frekvencián álló fordító frekvencia.
– *Álvéletlen pásztázó frekvenciás rendszer (7/c. ábra):* Az előző két módszer előnyös tulajdonságait használja fel, ez a típus a legnehezebben visszakódolható.



a) pásztázó frekvenciás *b) ugró frekvenciás* *c) álvéletlen pásztázó frekvenciás*

7. ábra: Dinamikus frekvenciafordítás változatai (Forrás: [19])

Mindhárom dinamikus frekvenciafordítású módszerre jellemző, hogy szükségük van szabályos időközönként szinkronizáló jelre, amit az adás mellett továbbítanak. Az ugró frekvenciás és az álvéletlen pásztázó frekvenciás kódolásnál a váltások tulajdonságait egy szoftveresen felprogramozott kód segítségével lehet beállítani. A komolyabb scrambling szinthez kötődő bonyolultabb elektronika meglehetősen drágává teszi az ilyen scrambling modulokat, ezért a telekommunikáció ezen árérzékeny szegmensében, a PMR rádiókban nem terjedt el az utóbbi módszer alkalmazása. A különböző gyártók készülékei, az eltérő scrambling módszerek és alkalmazott frekvenciák miatt nem kompatibilisek egymással. Azonban egy adott gyártó különböző típusú készülékei általában egyforma scrambling eljárást alkalmaznak.

Az ilyen módon megváltoztatott hanganyagok dekódolására az interneten is találhatunk segítséget. Az itt megtalálható programokkal lehetőség van a frekvenciafordítással kódolt adások azonnali vagy utólagos visszafejtésére. A programban a fordító frekvencia folyamatosan állítható, ezzel megkereshető az éppen használt tükrözési frekvencia. Az ilyen programok szabadon letölthetők az internetről, pl. a következő oldalról [20]. Egy ilyen program gyakorlatilag az inverz műveletét végzi el a scrambling folyamatának, azaz a frekvenciatükrözésnek, a sávfordításnak, az amplitúdóváltoztatásnak vagy az időbeli jelszétosztásnak. Itt nem beszélhetünk kulcsokról, hanem a scrambling paramétereiről, pl. a tükrözési frekvencia értékéről. A paraméterek megtalálása a kulcsa a descramblingnek.

A dinamikus frekvenciafordítással kódolt adások visszafejtésére a fenti program nem használható. Kézi állítással nem kereshető meg és nem követhető a gyorsan változtatott tükrözésifrekvencia-érték. A mai modern DSP jelfeldolgozási algoritmusokkal azonban ezek paramétereinek gyors visszafejtésére is lehetőség van, megfelelő szakértelemmel kiegészítve.

Digitális eljárások

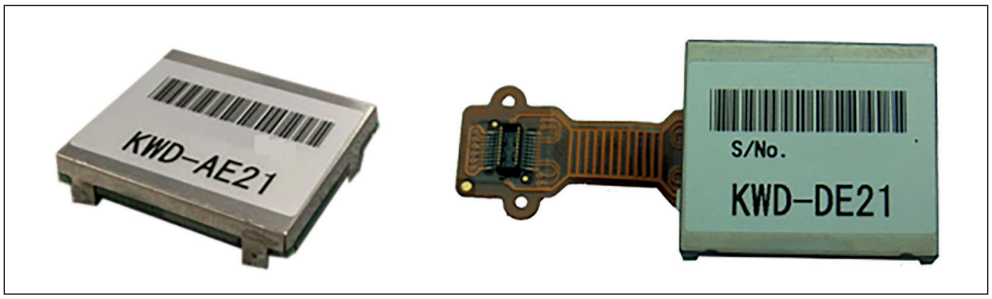
Az analóg rádiós rendszerekben is alkalmazható digitális titkosítási eljárás, azonban ez gyakorlatilag az analóg hanginformáció digitalizálásával jár, ami ezután már mint digitális jelfolyam titkosítható. Ezek az ún. időtartományú titkosító modulok, ahol az analóg mikrofon jelet 100–600 ms-os időszeletekre szegmentálják, majd ezeket további blokkokra osztják. A blokkokat ezután pl. a Selectone esetében egy 72 bites algoritmussal blokkonként titkosítják [16].

Manapság a digitális rendszerek esetében a kérdés szintén felmerül, annak ellenére, hogy maga a digitális átvitel már önmagában egy alap biztonságot jelent, a hagyományos rádiós eszközökkel történő hozzáférés ellen. Ez azonban a hamis biztonság érzetét keltheti a döntéshozókban, akik hagyományosan a biztonsági kérdésekre úgy tekintenek, mint egy költségnövelő és a működés szempontjából célszerűtlen tevékenységre, mely megköti a kezeit a felhasználóknak és a folyamatok kezelőinek egyaránt. [4] A fenti kijelentés alátámasztja, miért alkalmazzák a döntéshozók gyakrabban az olcsóbb megoldásokat. Miért tekintenek el egy egyébként is digitális átvitelű megoldásnál pl. a kiegészítő titkosítás alkalmazásától a különféle kisebb méretű helyszíni és diszpécser típusú rendszereknél.

A gyakorlatban a digitális PMR rádiók tekintetében kvázi szabványként terjedt el a AES[21]/DES[22] titkosító modulok alkalmazása, melyek azonban jelentősen megnövelik a készülékek árát, mivel ezek kb. 300–700 $-ba kerülnek, az analóg modulok 100 $ körüli árával szemben. Ilyen modulokat is több cég kínálatában találhatunk, ilyenek pl. a Kenwood cég saját Nexedge rádióiba szánt típusai. A 256 bites AES/DES algoritmusú KWD-AE21, illetve egy gyengébb, 56 bites DES algoritmusú KWD-DE21 panelba illeszthető titkosító modul (8. ábra).

21 AES: Advanced Encryption Standard. Fejlett titkosítási szabvány, az 2001-ben szabványosították az USA-ban.

22 DES: Data Encryption Standard. Adattitkosítási szabvány, az AES elődje, 1976-ben hagyták jóvá az amerikai kormányzati szervek nem minősített kommunikációjának titkosítására a számítógépes és kommunikációs rendszereknél. 1997-ben internetes összekapcsolású gépekkel 84 nap alatt törték fel a kódot, brute force módszerével, majd 1998-ban egy 250 000 dollárból épített célhardveren mindez már csupán 3 napig tartott.



8. ábra: Kenwood cég KWD-AE21 és KWD-DE21 AES/DES titkosító moduljai (Forrás: [21])

Mind a 256 bites, mind az 56 bites modul 1024 kulcs tárolására képes, melyek kulcsfeltöltő szoftverrel változtathatók. Az ilyen titkosító modulok hivatalos beszerzés során exportengedély-kötelesek adott országokban, így csak a megfelelő engedélyek alapján lehet megvásárolni és kivinni őket. Mint a lábjegyzetből látható, a DES kód már a 2000 körüli számítástechnika szintjén is sérülékeny volt, mivel akkortájt már brute force[23] módszerrel is törhető volt. Az AES viszont napjainkban is erősnek számít (brute force ellen).

Az analóg rendszerekhez képest a digitális átvitel már önmagában egy alap biztonságot nyújt a vétlen behallgatás ellen. De természetesen a védendő információk kritikussága függvényében célszerű mind az analóg mind digitális átvitelnél, a kockázattal arányosan alkalmazott titkosítást választani. Az is elképzelhető hogy ennek alkalmazásától el is lehet tekinteni, a kockázatok (pl. az információ érvényességi ideje) [11] és anyagi szempontok függvényében.

A támadás résznél leírtakból látható, hogy a titkosítás alkalmazása esetében a kulcskezelés eljárásai is védendő körbe tartoznak, mivel itt is elképzelhető a hamisított alkatrészeken keresztüli kompromittálódás.

Az iránymérés és helymeghatározás passzív eljárásai ellen a digitális átvitel önmagában nem véd jobban, mint az analóg jelek esetében, azonban a mért adó beazonosítása jóval nehezebb. A két időréses DMR jelek esetében az időosztásos átvitel miatt az iránymérés is gondot jelent, mivel hasonlóan a GSM-hez, az egyes időrések más fizikai helyzetű felhasználókhoz tartoznak, így az egyes időrések méréséhez időbeli szinkronizálás szükséges.

Az olyan új típusú fenyegetés ellen, mint a hardver trójai, csak a [14]-ben kifejtett utólagos módszerekkel, pl. SDA mérésekkel, illetve a megelőzés szintjén az ezeknek megfelelő szervezeti biztonsági szabályok betartásával védekezhetünk, pl. a biztonságos programozással:

– a cryptoASIC, CPLD, FPGA saját programozásával majd ezek megfelelő integritásának biztosításával;
– a rádiók biztonságos megszemélyesítésével: azaz a saját felhasználói algoritmusok, saját adatok belső felprogramozásával;

23 Brute force: a nyers erő módszere, azaz a fizikailag lehetséges összes kulcskód végigpróbálása egyenként egy adott üzenet megfejtésére.

– az érzékeny adatok, szoftver, firmware és kódok védelmével, integritásuk és megbízhatóságuk együttes biztosításával;
– a kriptográfiai algoritmusok olyan módszerű kidolgozásával, hogy az védett legyen az eljárás gyakorlati kipróbálásától és egyéb információszivárgástól egy rosszindulatú támadó számára.

A VoiP alrendszer esetében a védelem megoldása az információbiztonság (IA), rendszabályok, eljárások és folyamatok bevezetésével és betartatásával történik. Ennek alkalmazásával megvédhetjük az információkat és az információs rendszert egyaránt. Ennek során az IA a következők elérését igyekszik megvalósítani:

– rendelkezésre állást (a jogosult felhasználók részére);
– integritást (az adatok védelmét a jogosulatlan módosítástól és a pusztítástól);
– azonosítás- és hozzáférés-ellenőrzést (a hálózathoz és rendszerelemekhez hozzáférő felhasználók egyedi azonosítása valamilyen eljárással: pl. jelszó, PIN kód, biometrikus azonosítás stb.);
– megbízhatóságot (jogosulatlan személy védett folyamatokhoz és eszközökhöz történő hozzáférésének megakadályozása);
– letagadhatatlanságot (az információközlésben részt vevő felek elismerik egymás azonosságát, így bármely tranzakció [átvitel] letagadhatatlan).

Az IA ezenfelül biztosítja a helyreállítást egy sérült vagy kompromittálódott rendszernél, a felderítési, megelőzési és reagálási képességek beépítésével.

A fentiek betartásával megvédhető a hálózaton mozgó, az alkalmazások által kezelt, valamint a digitális formában bármely médiumon tárolt adatok együttese. Azaz a digitális információk bármely állapotú reprezentációja, nem csak az IP-hálózatokon, de bármely hozzá kapcsolódó IT-infrastruktúrán. Ebből következik, hogy az IA meglehetősen adatcentrikus, de érvényessége nem korlátozódik a digitális formájú adatokra, hanem bármilyen tágabb értelmű vállalaton, rendszeren belüli adatokra vonatkozik.

Ha biztonságos PMR rendszert akarunk üzemeltetni, akkor néhány kulcsfontosságú terület együttese által meghatározott szabályokat is be kell tartani. Ezek a területek a következők: szabályozási irányelveknek való megfelelés, IT- és hálózatbiztonság, fizikai biztonság, üzleti folytonosság és katasztrófa utáni helyreállítás, azonosság- és hozzáférés-kezelés, IT életciklus és projektmenedzsment, információgyűjtés és -elemzés.

Az IA által megkövetelt rendszabályok bevezetése alapját képezheti egy akkreditált szabályrendszer bevezetésének, mellyel tanúsítani lehet a rendszabályok megfelelő betartását. Az IA szabályrendszer kidolgozását a működő rendszerhez kell igazítani, tehát a szervezeten belül kell kidolgozni, de számos helyi szabályozásnak és vonatkozó jogszabálynak kell megfelelni. Ehhez egy IA menedzsernek szerteágazó ismertekkel kell rendelkeznie számos területen, pl. az IT kockázatmenedzsment, biztonsági szabványok, hálózati és peremvédelmi biztonsági szabványok, titkosítási szabványok stb., hogy csak a fontosabbakat említsem.

Összegzés, következtetések

A PMR rendszerek, rádiók alkalmazása ideális megoldás a kiscsoportos pont-többpont kommunikációra, így a szervezett bűnözés és a terrorizmus ilyen típusú kommunikációs igényeinek megvalósítására is. A direkt módú (átjátszó nélküli), de akár az egyedi, pl. hordozható átjátszón keresztüli (taktikai) megoldások egyaránt kikerülhetik a hagyományos távközlési infrastruktúrákat, így ellenőrzésük kizárólag passzív rádiófelderítéssel valósítható meg. A hibrid rendszerek esetében azonban a megjelenő új támadási felületek a hálózati oldalról is sebezhetővé teszik a rendszereket. Az ilyen komplex rendszerek a védelem szempontjából is komplex szemléletmódot igényelnek, az aszimmetrikus fenyegetések mentén, hiszen a támadások esetében is eddig nem látott újfajta aktív támadási eljárások megjelenésére is számítani kell. Így a hagyományos rádiófelderítés mellett előtérbe került a számítógép-hálózati aktív támadások lehetősége is, valamint olyan új eljárások is megjelentek, amelyekkel még az erősnek mondott AES titkosítást is képesek eliminálni a támadók, a cikkben említett hardver trójai segítségével. További lehetőségként pedig a készülékek elleni szabotázs kivitelezése is valósággá válhat segítségével.

A gyakorlati tapasztalatom szerint már most jelentős növekedés figyelhető meg (kutatásaim kezdetén a 3 évvel ezelőtti állapothoz képest) a digitális rádiók hazai és nemzetközi elterjedésében és alkalmazásában egyaránt. Az olcsó kínai készülékek tömeges megjelenése ezt a tendenciát csak tovább fogja erősíteni, főleg az engedélyhez nem kötött eszközök vonatkozásában, de akár az ennél magasabb PMR kategóriákban is. Egy professzionális titkosító modul jóval többe kerül, mint a legolcsóbb rádiók ára, így az alsóbb szegmensben nem valószínű ezek alkalmazása, de a felsőbb kategóriákban is meggondolásra készteti a döntéshozókat.

Az alkalmazott titkosítás mértékének meghatározásakor a magasabb biztonság ára, valamint az interoperabilitás megtartása közötti ellentmondást kell leküzdeni. A titkosító modulok 300, de akár 700 dollárral is megnövelhetik egy készülék árát, ami jelentős anyagi megterhelést ró a szervezetekre. Ennek ellenére a [22] szerint az amerikai felhasználók részére a titkosság sokkal fontosabb, mint az interoperabilitás, azonban a [11]-ben leírtak szerint ez nincs mindig így, még a katonai kommunikációban sem. Azonban a digitális átvitel miatt a hagyományos felderítő eszközökkel még titkosítás alkalmazása nélkül sem nyerhető vissza az átvitt beszédinformáció, ahogyan ezt a [1] cikkben elméleti síkon kifejtettem. A viszonylag korlátos frekvenciatartományokban működő digitális PMR rádiók felderíthetőek, és akár iránymérés is végezhető rajtuk a hagyományos eszközökkel, azonban hovatartozásuk ezekkel nem határozható meg. Egy olyan eszköz megalkotása és alkalmazási feltételeinek, körülményeinek kidolgozása szükséges, amely a fenti rendszerekből a digitális átvitelű beszéd, valamint az egyéb járulékos adatátviteli (műveleti) információkat is megfelelően képes kinyerni és felderítési adatokká konvertálni. Ehhez a megfelelő technikai megoldások kidolgozása vagy adaptálása szükséges a berendezésekben, azonban az emberi közreműködés sem nélkülözhető a jobb eredmény elérése érdekében.

Irodalomjegyzék

[1] Balog Károly: Digitális PMR rendszerek összehasonlítása I. *Hadmérnök*, 9 (2014. szept.)/3. www.hadmernok.hu/143_08_balogk.pdf (a letöltés ideje: 2014. 09. 30.)

[2] Haig Zsolt – Kovács László – Ványa László – Vass Sándor: *Elektronikai hadviselés.* NKE HHK Katonai Műszaki Doktori Iskola, Budapest, 2014. (ISBN 978-615-5305-87-0)

[3] Munk Sándor: Az informatikai biztonság rendszertanához. *Bolyai Szemle,* 18 (2009)/4, 157–174., portal.zmne.hu/download/bjkmk/bsz/bszemle2009/4/13_munksandor.pdf (a letöltés ideje: 2015. 05. 20.)

[4] Information Assurance for Private Radio Networks (Motorola White Paper), www.motorolasolutions.com/content/dam/msi/docs/business/product_lines/astro_25_network/encryption/_documents/astro25_information_assurancewhitepaper.pdf (a letöltés ideje: 2015. 05. 23.)

[5] Munk Sándor: Információbiztonság vs. informatikai biztonság. *Hadmérnök,* Robothadviselés 7. Tudományos Szakmai Konferencia különszáma, 2007. november 27., hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.html (a letöltés ideje: 2015. 05. 20.)

[6] Icom IDAS, What is dPMR, why digital? www.icom.co.jp/world/support/download/brochure/pdf/IDAS_dPMR.pdf/ (a letöltés ideje: 2013. 01. 15.)

[7] The world's thinnest & smallest full power digital portable radio, www.hytera.com/productResources.htm?columnId=416&proId=259&resourceType=2#page-index (a letöltés ideje: 2013. 01. 20.)

[8] Tait Communications (whitepaper): Tougher LMR systems, 10 ways to protect and strengthen your LMR system, www.taitradio.com/__data/assets/pdf_file/0014/123503/Tait_Tougher_LMR_Systems_Guide.pdf (a letöltés ideje: 2015. 05. 25.)

[9] Hytera DMR Trunking Products and Solutions, www.dmr-applications.com/15938 (a letöltés ideje: 2015. 05. 25.)

[10] John Ribeiro: *Ham radio attempts to fill communication gaps in Nepal rescue effort,* www.networkworld.com/article/2916374/ham-radio-attempts-to-fill-communication-gaps-in-nepal-rescue-effort.html (a letöltés ideje: 2015. 05. 25.)

[11] NATO Research and Technology Organisation: *Technical Communications In Urban Operations.* RTO Technical Report TR-IST-067, 2010. szeptember, ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-IST-067//$$TR-IST-067-ALL.pdf (a letöltés ideje: 2015. 05. 25.)

[12] Information Assurance for the Tactical Environment, 2002. szeptember, http://trygstad.rice.iit.edu:8000/Policies%20&%20Tools/InformationAssuranceTechnicalFramework3.1/ch09InformationAssuranceForTheTacticalEnvironment.doc (a letöltés ideje: 2015. 06. 05.)

[13] HINT Project, www.hint-project.eu/ (a letöltés ideje: 2015. 06. 05.)

[14] D1.2 Report on Specifications and overall architecture (Holistic Approaches for Integrity of ICT Systems) EU Seventh Framework Programme, www.cspforum.eu/HINT-D1.2-Report_on_specifications_and_overall_architecture-PU-M08.pdf (a letöltés ideje: 2015. 06. 05.)

[15] D1.1 Report on use case and architecture requirements (Holistic Approaches for Integrity of ICT Systems) EU Seventh Framework Programme, www.cspforum.eu/HINT-D1.1-Report_on_use_case_and_architecture_requirements-PU-M05.pdf (a letöltés ideje: 2015. 06. 05.)

[16] Selectone New Product Bulletin, A Private Collection Affordable Voice Encryption, www.comspec.com/selectone/npb/private/private.htm (a letöltés ideje: 2015. 05. 25.)

[17] Norcomm Voice Encryption, www.norcommcorp.com/VoiceEncryption.html (a letöltés ideje: 2015. 05. 25.)

[18] CML Microcircuits: Audio Band Frequency Inversion Scrambler FX/MX 128, www.cmlmicro.com/products/FX/MX128/ (a letöltés ideje: 2015. 05. 25.)

[19] Scrambling and Frequency Inversion, www.cescomm.co.nz/about/scrambling.html (a letöltés ideje: 2015. 05. 25.)

[20] Nino Porchino: Voice descrambler software for windows and soundcard, antoninoporcino.xoom.it/VoiceDescrambler/index.htm (a letöltés ideje: 2015. 05. 25.)

[21] Kenwood Europe: Optional Modules, Units, Brackets and Kits, www.kenwood.eu/comm/accessories/optional/ (a letöltés ideje: 2015. 05. 25.)

[22] Candy Phelps (Hendon Publishing): *Establishing secure, reliable LMR communications.* Public Safety IT, Jan/Feb 2010, www.hendonpub.com/resources/article_archive/results/details?id=1890 (a letöltés ideje: 2015. 05. 31.)

Digital PMRs Attack and Defence Possibilities

Balog Károly

In these days, both the licensed and license-free PMR radio technology is going through a massive paradigm shift as formerly seen at mobile phone technologies. In fact, the new digital PMR systems and individual devices are spreading, the license-free versions of which are cheap, easily accessible for everyone and not limited in their movements. Since these devices completely bypass the traditional telecommunications infrastructure, their detection and control is only possible by communication intelligence. Of course, the systems related to other communication infrastructures may be vulnerable not only through radio channels. In my paper I intend to overview and summarize the attack vectors of unique devices and systems, as well as the security solutions used in PMR devices and systems.

Keywords: digital Professional/Private Mobile Radio, Communication Intelligence, scrambling, encryption, electronic protection, information assurance