RFID és biztonság – 2010

Biztonságtechnikai azonosítás-technika terén az RFID a 90-es évek második felétől piacvezetővé vált, mellette csak a biometrikus azonosítás nagyléptékű fejlődése említhető.

Az RFID az automatikus azonosítási (AUTO ID) technológiák széles családjába sorolható. Olyan megoldások gyűjtő fogalma, amely tárgyak, vagy élőlények azonosítóját továbbítja vezeték nélkül, rádióhullámok segítségével. Az RFID technológiával lehetővé válik az adatok – emberi beavatkozás nélküli – teljesen automatikus beolvasása és feldolgozó számítógépre vezérlése. ***A szerk.***

A biztonságtechnika és más alkalmazások gyakran találkoztak és integrálódtak, így a beléptető és jegyrendszer, zártechnika és RFID technika, ellenőrzés és azonosítás az élet minden területén.

Szinte törvényszerű, hogy az RFID azonosító eszközök elterjedésével és széles körű alkalmazásával a hamisítás, a másolás terén új problémák merültek fel, gyakran hatalmas vihart kavarva, nem ritkán akár hatalmas vállalkozások cégek létét is veszélyeztetve.

Sajnos Magyarországon ezen a területen is érvényes, hogy az információ lassan és későn jut el a döntéshozókhoz. Sokaknak a Proximity vagy RFID egyfajta biztonsági minősítést is jelent, pedig nem feltétlen az. Önmagában a Proximity technológia nem jelent mindenek feletti biztonságot, hamisíthatatlanságot, másolás elleni védelmet. A nem megfelelően kiválasztott eszköz óriási veszélyeket rejthet. Másik oldalról a gyártók nem „reklámozzák" a problémákat, hiszen nem mindig érdekük a felvilágosítás, gyakran ugyanazon cég forgalmaz gagyi és megbízható eszközt is, vagyis számára mindegy, csak menjen a bolt. Persze azt is látni kell, hogy ami korszerű volt 15 éve, az ma már nem az.

■ Ha párhuzamot kell vonni, akkor a kontakt Smart Chip technológia és RFID technológia sok tekintetben hasonló utat jár be, hasonló biztonsági kérdéseket vet fel. Tudomásul kell venni, hogy a 80-as végének technikájára alapozott vagy később kifejlesztett egyszerű fix kódos RFID eszközök másolása, hamisítása ma már nem gond. Már léteznek a magas biztonságú, védett kódolású RFID eszközök, amelyek árban is elfogadhatóak, sokan mégis a gagyit alkalmazzák magas biztonságú helyeken is, mert az is Proximity, de olcsó. Az elmúlt években a nagyvilágban megjelentek a hamisítók, profi rendszerfeltörők, és nem csak az egyszerű fix kódos RFID azonosítókat, de az első generációs titkosított megoldással rendelkező RFID azonosítókat is feltörték, hatalmas botrányt okozva.

Nézzünk ezekre példát, mielőtt röviden összefoglalnánk az RFID és Proximity eszközök biztonságára vonatkozó kitételeket.

■ Az egyszerű fix kódos kártyák hordozható olvasóval könnyen kiolvashatók, akár táskából, zsebből, a megoldást YouTube-on is látható filmekkel demonstrálják (vagy oktatják?!). Ezekkel nem is érdemes foglalkozni, annyira egyszerű a technika, biztonsági szempontból nem megfelelőek, inkább ipari alkalmazásokban van helyük (mosodákban ruhaazonosítás, reptereken csomagazonosítás, gépkocsigyártásban folyamatellenőrzés, stb.) Ma már magasabb biztonságú fokozatot igénylő rendszerekben nagy kockázatot jelentenek.

A Berlinben tartott 26-dik Káosz Kommunikációs Kongresszuson („26th Chaos Communication Congress") jelentették be (2009. december 28-án), hogy az egyik legbiztonságosabbnak tartott LEGIC Prime kártya másolása és hamisítása nem jelent gondot. Filmet mutattak be, hogyan másolják le egy nagy reptér óvatlan alkalmazottjának kártyáját, amivel aztán szabadon tudtak közlekedni. Mivel a reptér biztonsága szempontjából a beléptető kulcsfeladatokat lát el, nyilvánvalóan nőtt a biztonsági kockázat. Pedig ez a kártya, 13,56 MHz-es, adatvédelemmel ellátott technológiát használ, úttörőnek számított a nagybiztonságú RFID technikában.

De a bűnözők nem kíméltek másokat sem, sőt korábban tört ki a botrány, a világ legelterjedtebb kártyájának a MIFARE Classic feltörése miatt. Az ISO 14 443 A/B szabványra épülő MIFARE Classic kártya első generációja széles körben használatos a közlekedési rendszerekben is, milliárdos nagyságrendben értékesített kártya. A Londoni Metro kártya feltörése és a feltört algoritmusok publikálása után gyakorlatilag utcasarkon lehetett bérletet venni. A gyártó cég elnöke nyilvánosan volt kénytelen elismerni a feltörés tényét és kijelenteni, a MIFARE Classic nem biztonságos. A gyártó cég védelmére azt lehet elmondani, hogy nagy fejlesztési erőket összpontosítva 2009-ben bejelentették a MIFARE PLUS X/S technológiát, amely gyakorlatilag feltörhetetlen, a ma ismert legkorszerűbb védelmi eljárásokat alkalmazza hacker támadásokkal szemben. A Mifare Plus chip megkapta a Common Criteria EAL 4+ tanúsítványt.

http://www.contactlessnews.com/2010/01/27/nxps-mifare-plus-granted-common-criteria-certification

■ Fenti tények nem jelentik azt, hogy a fix kódolású RFID technikának nincs meg a helye, vagy a MIFARE Classic használhatatlan, csak tudni kell, minek hol van létjogosultsága, melyik RFID megoldásnak mekkora a biztonsága. A Proximity nem minőséget jelent, nem szavatol automatikusan biztonságot, hiszen az csak RF technika, a mögöttes kódolás technika minősíti a biztonsági szintet.

■ Magyarországon elterjedt és alkalmazott ismert kártyatípusok egyszerű minősítése röviden, biztonsági fokozat szerint:

- ***Fix kódolású védelem nélküli RFID eszközök*** – EM 4100, ASK típusok, HID 125 KHZ, INDALA 125 KHz, TIRIS 134 KHz, iCODE 13,56 MHz, ISO 18000 UHF azonosítók
- ***125 KHz-es kódolás védett eszközök*** – Hitag2, HitagS
- ***Első generációs 13,56 MHz-es kódolás védett eszközök*** – MIFARE Classic ISO 144443 A/B, LEGIC prime
- ***Második generációs 13,56 MHz-es kódolás védett eszközök*** – MIFARE Plus X, HID iClass, Legic Advant, DesFire

■ Amennyiben a beléptető rendszer vagy más RFID alkalmazás biztonsági szintjének egyenszilárdsága követelmény, akkor az RFID technológiát is a követelmény szinthez kell igazítani. Meglévő rendszerek esetén elégséges az olvasó és kártya technológia megújítása, amennyiben indokolt.

Pálffy Zoltán