RFID tagek elleni támadás és a védekezés lehetőségei

Attack against the RFID tags and possibilities of the defense

Dr. Radványi Tibor, Biro Csaba, Dr Király Sándor

Dr Radványi Tibor publikációt megalapozó kutatása a TÁMOP 4.2.4.A/2-11-1-2012-0001 azonosító számú Nemzeti Kiválóság Program – Hazai hallgatói, illetve kutatói személyi támogatást biztosító rendszer kidolgozása és működtetése országos program című kiemelt projekt keretében zajlott. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.
Biro Csaba és Dr. Király Sándor publikációt megalapozó kutatása a TÁMOP-4.2.2.C-11/1/KONV-2012-0014 azonosító számú, FutureRFID - Az RFID/NFC technológia továbbfejlesztési lehetőségei az "Internet of Things" koncepció mentén című projekt keretében zajlott.

Abstract

Ebben a cikkben a napjainkban legdinamikusabban fejlődő, az automatikus azonosítás témaköréhez tartozó RFID technológiával és kriptográfiai algoritmusok kapcsolatával foglalkozunk. Kiemelten a kommunikációs folyamat végén lévő transzponderek támadását és lehetséges védekezéseket vizsgáljuk. Kitérünk rá, hogy az ismert és széles körben alkalmazott kriptográfiai algoritmusok közül melyek azok, melyek használhatók és melyek azok, melyek a technológia korlátai miatt nem. Az RFID transzponderek sokfélesége miatt nagyobb csoportokban vizsgáljuk ezeket. Figyelembe vesszük, hogy a védekezés sok esetben az elhárítást, míg más esetekben az adatok megfelelő védettségének biztosítását jelenti. Lehetőség van a tisztán RFID technológiát használó megoldások kiegészítése más azonosítási lehetőségekkel, pl. az egyéb biometrikus azonosítási lehetőségek integrálására. Esetenként más kommunikációs csatorna felhasználásával a viszontellenőrzések elvégzésére.

Bevezetés

Napjainkban széles körben megtalálhatóak az azonosítási rendszerek különböző formái. Egy olyan kódrendszert értünk ez alatt, amely például személyeket, tárgyakat, eseményeket, stb. egyedileg azonosít. Számtalan felhasználási mód hatására, megannyi új rendszert kellett létrehozni, amelyek ki tudták szolgálni a folyamatosan bővülő igényeket.
A legfiatalabb és legdinamikusabban fejlődő azonosítási módszer az RFID. [1]
A rádió frekvenciás azonosítás napjaink egyik legelterjedtebb azonosítási rendszere. Különböző típusú szenzorokkal párosítva széles felhasználási területen alkalmazható.
A technológia azonosítási- és biztonsági lehetőségeit egyre inkább kihasználják a modern útlevelek, a digitális azonosítók és nem utolsó sorban még a legújabb fizetési megoldások is.
Az RFID transzpondereket úgy tervezték, hogy bármilyen olvasó számára kiadja a tárolt információkat. Az első felhasználások során ez nem jelentett problémát, de manapság olyan esetekben használjuk, ahol ez problémákat vethet fel. Ezalatt elsősorban a személy azonosításra kell gondolni, például beléptető rendszerek, elektronikus útlevelek esetén. Alapértelmezés szerint az átviteli közeg, a rádióhullámok, titkosítatlan formában továbbítják az információt. Az olvasás nem kerül naplózásra a transzponderen, így az egyes olvasások illetéktelen olvasók által megismételhetőek. Helyzet meghatározó rendszerek esetén illetéktelen személyek kezébe is kerülhet az információ az azonosítandó objektum helyzetéről.

Támadási lehetőségek

Az RFID rendszerekre irányuló támadások két nagy csoportját különböztethetjük meg. E támadások egy része magára a transzponderre, más része az RF interface-re irányul. Ezen kívül természetesen lehetséges még az azonosítókat és kulcsokat tároló adatbázist is megtámadni, de az már inkább az informatikai rendszer elleni támadás témakörébe tartozik.

Támadás a transzponder ellen

Fizikai megsemmisítés

Fizikai megsemmisítésről abban az esetben beszélhetünk, ha az RFID tag-et fizikai vagy kémiai sérülés éri, amely által lehetetlenné válik a transzponder olvasása. Ez történik például egy antenna levágásakor, vagy a chip összetörésénél. Ettől kissé eltérő, de szintén a transzponder fizikai megsemmisítésének körébe tartozik a túl erős mező által történő megsemmisülés is. Az ISO/IEC 14443 vagy ISO/IEC 15693 szabványban megtalálható a mező maximális erőssége, mely a 13.56 MHz-es frekvenciánál 12 A/m. [7, 8]

Transponder klónozása

Ha az RFID kártya nincs védve titkosítással és ismert a kártya utasításkészlete, a funkcionalitása és a memória terület felosztása. Ekkor egyszerű az ilyen kártya lemásolása és a másolattal való helyettesítése. Problémát akkor okoz, amennyiben a rendszer nem figyel a duplikált kártyák jelenlétére.
A komolyabb és összetettebb rendszereknél, ahol szükséges a biztonság, kerülni kell a „csak olvasható" transzpondereket és a titkosítatlan adattárolást.
Ha egyszer rendelkezünk a tag-en tárolt adattal, akkor azt írható transzponderre visszaírva klónozhatjuk az egységet. Először az IOActive munkatársai hívták fel a figyelmet a problémára, de a gyártók már korábban is tudtak a veszély jelentőségéről. Természetesen az adatátviteli kommunikációs csatorna titkosítható, ismert titkosító eljárásokkal (DES, AES, RSA). A transzponderen tárolható kis adatmennyiség miatt a kulcs általában nem túl nagy, ezért elég adat esetén a kulcs megfejthető.

Elrejtés az olvasó elől (Faraday kalitka)

Egy másik rendkívül hatékony támadás az elrejtés, mikor fémes anyaggal burkoljuk be a transpondert, így meggátolhatjuk, hogy az olvasó mágneses vagy elektromágneses tere elérje a tag-et. A legegyszerűbb mód erre, ha alufóliába csomagoljuk a transzpondert, majd annak eltávolításakor újra működőképes lesz. Ez a támadási lehetőség bizonyos esetben a védelem eszközévé is válhat. Jó védelmet nyújt a később is említett Relay-attack támadással szemben. A tag-et tartalmazó kártyánkat, eszközünket egy fémtok, egy Faraday kalitka védi az illetéktelen olvasással szemben, amikor használaton kívül van.

Támadás RF interfészen keresztül

Az RFID rendszerek elleni másik támadási módszerek az RF interfészen keresztül érkeznek. Az RFID rendszerek rádió rendszerek és elektromágneses hullámok segítségével kommunikálnak közelre és távolra egyaránt. Így a támadónak lehetősége van a rádiófrekvenciás interfészen keresztül is támadást indítani.

Induktív csatolás

Ha a transzpondert a normál olvasási távolságon kívül helyezzük, a kommunikáció két különböző ok miatt is megszakadhat. Az egyik lehetséges ok, hogy a transzponder működéséhez nem kap elég

áramot az antennából, a másik pedig, ha a transzponder elég áramot kap ugyan, de a generált terhelés moduláció amplitudója nem elég nagy ahhoz, hogy az olvasó detektálni tudja. Az elérhető legnagyobb energiaellátást, a rendszer energiatartományának is nevezzük. Ha az olvasó olvasási távolságát növeljük, meg kell növelnünk az olvasó energiatartományát is. Ezt úgy tudjuk elérni, ha növeljük az olvasó antennájának az átmérőjét és az adó antennájában az áramot. Felmerül a probléma, hogy az olvasó megnövelt átmérője miatt a mágneses indukció csökken, így a terhelés moduláció jelének ereje is csökken, illetve a megnövelt energia miatt a zajszint is emelkedik.
Kfir és Wool (2005) megállapították, hogy azokat a transzpondereket, amelyek megfelelnek az ISO/IEC 14443-as szabványnak, maximum 40 cm-es távolságról lehet olvasni, még akkor is ha az összes paramétere optimálisan van beállítva.

Visszaszórásos csatolás

Nagy hatótávolságú RFID rendszernek nevezzük azt, melyben a két eszköz közötti távolság nagyobb, mint 1 méter. Általában UHF (868 vagy 915 MHz) vagy mikrohullámú frekvenciatartományban (2,5 vagy 5,8 GHz) működnek. Ha a transzponder kikerül a rendszer olvasási tartományából, szintén két lehetőség merül fel az adás megszakítására. Az egyik ok, hogy a transzponder nem kap elég áramot az antennából a működéshez. A másik lehetőség pedig, ha a visszavert teljesítmény kevés ahhoz, hogy az olvasó érzékelni tudja. A távolság növeléséhez emelni kell az olvasó átviteli teljesítményét. Ahhoz, hogy az olvasási távolság a kétszeresére nőjön az olvasó teljesítményét a négyszeresére kell emelni. Ha szeretnénk megtartani a visszaszórás teljesítményének mértékét kétszeres olvasási távolságon, akkor az olvasót teljesítményét már tizenhatszorosára kellene növelni. 2005-ben sikerült a Yagi-Uda antennával 21 méterről sikeres támadást végrehajtani.[8]

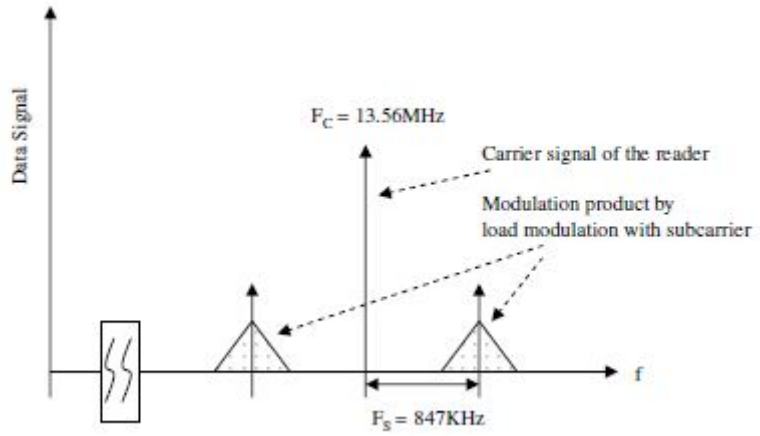
Kommunikáció lehallgatása (eavesdropping)

A kommunikáció lehallgatása az olvasó és a transzponder között történik. Az RFID rendszerek hatótávolsága pár centimétertől (pl.: 13.56 MHz) több méterig terjedhet (pl: 868 MHz). Rádió antennájának nagyságrendekkel alacsonyabb kimeneti feszültség szükséges ahhoz, hogy használható jeleket fogjon, így sokkal nagyobb távolságból lehallgatható a kommunikáció.
Finke és Kelter megállapították, hogy 13.56 MHz-es induktív csatolású rendszer, akár 3 méterről is lehallgatható, holott ezen a frekvencián a hivatalos működési távolság mindössze maximum 10 cm. A HF rendszereken kívül ezt a sávot használják az újabban egyre jobban elterjedő NFC rendszerek is. [8]
A vevő pár kHz-es sávszélességen az olvasó modulálatlan jelét több 100 méterről is érzékelheti. Nagyobb távolságnál a jelet zavarhatják fém tárgyak, mint például kerítések, alumínium tárgyak, de akár nagyobb épületek is torzíthatják.

Zavarás (Jamming)

Másik egyszerű megoldás a jel zavarása a transzponder és az olvasó között. Nagyon hatékony módszer, mely képes meggátolni a jelátvitelt. Passzív RFID rendszereknél az olvasó által generált nagyon erős hordozó jel (carrier signal) látja el energiával a transzpondert. Ilyenkor két gyenge modulált jel keletkezik a hordozó jel két oldalán (1. ábra), melyet a transzponder terhelésmodulációja (induktív csatolás esetében) vagy a modulált visszaszórás (visszaszórásos rendszerek esetében) generál.
Annak érdekében, hogy képes legyen az olvasó erős jelét megzavarni, és így interferálni az adatfolyamot az olvasó és a transzponder között (Down-link), legalább a távolságnak, az átviteli erőnek, és az antenna tulajdonságainak hasonlítania kell az olvasóra, amit használunk. A transzponder

és az olvasó közötti adatfolyamnál (Up-link) egyszerűbb dolga van a támadónak, mert ott a válasz jel sokkal gyengébb.
Ha a zavaró eszköz ugyanolyan távolságra helyezkedik el az olvasótól, mint amennyire a transzpondertől és ugyanolyan frekvenciatartományban működik, mint a transzponder által modulált oldalsávok, akkor csak pár mW átviteli teljesítmény szükséges a jelentős kár okozásához.



1. ábra Vivő jel és modulált csatornák

Hasonló kapcsolat vonatkozik az induktív csatolásos rendszerekre is. Meg kell jegyezni, hogy az induktív csatolást alkalmazó alacsony frekvenciás rendszerek (LF 125KHz, és HF 13,5MHz) az olvasási hatásos távolsága csak pár cm. A mágneses mező erősségét is figyelembe kell venni, mely szintén hozzájárulhat a zavaráshoz. Mindegyik zavaró eszköznek közel kell tartózkodnia az olvasóhoz, vagy elég nagy antennát vagy átviteli teljesítményt kell használnia.

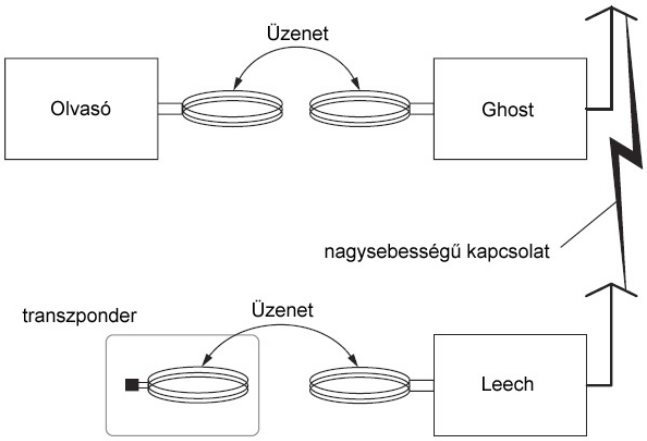
DoS – Denied of Service

Modern RFID olvasók könnyen tudnak nagyobb számú transzponderrel kommunikálni. Az olvasó ütközéselkerülő algoritmust használ az egyes címkék kiválasztására. EPC tagek esetében ezt még nehezíti, hogy csak azonosítókat tartalmaznak, így részleteket kell lekérni az adatbázisból. Jellemzően a következő két algoritmust szokták használni az ütközések elkerüléséhez: Bináris kereső fát és az ALOHA-t. Általában ezeknek az algoritmusoknak a gyengeségét kihasználva szokták indítania a DOS támadásokat. Megfelelő azonosítókat szimulálva a bináris keresőt teljes mértékben ki lehet akasztani. Minden egyes iterációban végig kell járni a teljes fát, ahhoz hogy megtalálja a keresett elemet.[8] Az RFID transzponderek működése szándékosan megszakítható a hozzáférés megakadályozásával. A szolgáltatás megtagadása a LOCK parancsok meg nem engedett használatával is elérhető. A LOCK parancs számos RFID előírásban szerepel annak érdekében, hogy megakadályozzák az engedély nélküli írást a transzponderek memóriájában. Attól függően, hogy milyen előírást alkalmazunk a LOCK parancs egy előre meghatározott jelszóval használható és tartós vagy ideiglenes hatást eredményezhet. Amennyiben a rendszer tartalmaz hálózati eszközöket, a támadó szolgáltatás megtagadást érhet el a middleware-n. Például az adatfolyam kiküldése esetén a rendszer túlterhelődhet, így az megtagadhatja a hozzáférést a normális felhasználóktól.

Jelfogó támadás (Relay Attack)

A jelfogó támadás az RF interfész elleni támadások különleges fajtája, ahol a támadó szándékosan kiterjeszti a tartományt két speciális eszköz (ghost, leech) segítségével az olvasó és a transzponder között. A *ghost*, transzpondernek szimulálja magát az olvasónál, míg a leech, olvasónak a kártyánál. A

két eszköz nagysebességű digitális vonalon van összekötve, így a távolság kiterjesztésének mérete gyakorlatilag végtelen. Az olvasó és a transzponder között a kommunikáció zavartalan és nem szükséges fizikai kontaktus, így a felhasználó csak később értesül a támadásról.
A kommunikáció egy üzenetküldéssel kezdődik, melyet az olvasó küld a *ghost*-nak, ami valójában a transzponder szimulációja. A *ghost* fogadja az üzenetet, majd nagysebességű rendszeren keresztül, minimális késéssel továbbítja a *leech* irányába adatmódosítás nélkül. A *leech* olvasót szimulálva továbbküldi az üzenetet az igazi transzpondernek. Az ellenkező irányú kommunikáció, ennek egyszerűen az ellentétje.



2. ábra Jelfogó támadás felépítése (RFID Handbook, 2010)

A módszer azonban néhány korlátba ütközik. A transzponder és a *leech*, illetve a *ghost* és az olvasó között maximum 10 cm távolság lehet. Ez a távolság a támadót könnyen leleplezheti, miközben próbálja elhelyezni az eszközöket az áldozatnál és az olvasónál. A RFID rendszerekben szabványtól függően maximális időlimitet is meg szoktak határozni, mely alatt a kommunikációnak le kell zajlania. Esetünkben a *leech* és a *ghost* közötti kommunikáció ideje bizonyos szabványokat használva akár 5 milliszekundum is lehet, míg az RFID rendszerekben a time-out akár az 5 másodpercet is elérheti. Modern eszközöket használva ez a limit könnyen betartható.[4]

Malware

A fenyegetések teljesen másik fajtája merül fel, amikor hackerek vagy bűnözők az RFID tag-ek kiszámíthatatlan (és általában rosszindulatú) módon való viselkedését okozzák. Általában a számítógép összeköttetésű illetve mobil RFID olvasók lekérdezésénél az RFID tag-ek egyedi azonosítójáért vagy a tag-en lévő adatért, amely gyakran szolgál adatbázis kulcsként, vagy amely valós tevékenységet indít el.
Mostanáig mindenki, aki az RFID technológián dolgozott hallgatólagosan azt állította, hogy pusztán egy RFID tag szkennelése nem tudja módosítani a háttérprogramot, és főképpen nem rosszindulatú módon. Sajnos tévedtek. Kutatásban bebizonyosodott, hogy létezik az RFID szoftvernek bizonyos sebezhetősége. Egy RFID tag (szándékosan) megfertőzhető egy vírussal és a vírus meg tudja fertőzni a háttér adatbázist, amelyet az RFID szoftver használ. Onnan pedig könnyedén továbbterjedhet másik RFID tag-ekre. Ez idáig senki sem gondolta, hogy ez lehetséges.
Az elkövetőnek elég vásárolnia egy olcsó terméket a szupermarketben, amelyhez RFID tag van rögzítve ahhoz, hogy megfertőzze a rendszert. Miután kifizette az árát a terméknek, otthon eltávolítja vagy megsemmisíti az RFID tag-et. Majd ez után elhelyezi rajta az általa írt „fertőző” RFID tag-et. Ezután visszamegy a szupermarketbe, és egyből a pénztár pulthoz megy és újra kifizeti a termék árát. De ekkor, amikor a termék szkennelve lesz a tag-en lévő vírus megfertőzi a szupermarket termék

adatbázisát, potenciálisan szabadjára engedve mindenféle pusztítást, úgy, mint az árak megváltoztatása.
De ugyan ilyen alapon az elkövető újra tudja írni például egy macska szub-dermális állat azonosító tag-jét. Majd elmegy vele egy állatorvoshoz és azt állítja, hogy ez egy kóbor macska és a macska megvizsgálását kéri. Amint ez megtörténik az adatbázis meg lesz fertőzve. Mivel az állatorvos ezt az adatbázist használja a tag-ek létrehozására az újonnan megcímkézett állatoknál, ezek az új tag-ek szintén fertőzöttek lesznek. Az RFID vírus jelen esetben, úgy terjed, hogy először az állatról terjed az adatbázisra, majd onnan ismét egy másik állatra.
De ennél is nagyobb fenyegetést jelent repülőterek esetén. A vírus segítheti a drog csempészeket vagy a terroristákat, azzal, hogy elrejthetik vele a csomagjukat. De a vírus miatt megfertőződött adatbázis, majd ez által megfertőzött csomagok, szintén képesek megfertőzni más repterek adatbázisait. A fertőzés eredményeként a csomagok elkerülhetnek teljesen más célállomásra, mint ahova eredetileg kellet volna.
Mostanra a probléma általános felépítése világossá vált. Amikor egy gyanútlan olvasó szkennel egy fertőzött tag-et, fenn áll a veszélye annak, hogy a tag kihasználja a sebezhetőséget a middleware-ben, hogy nem kívánt tevékenységet idézzen elő, amely tartalmazhatja az adatbázis megfertőzését is.
Az RFID Malware osztályai:
A Malware a rosszindulatú szoftver (malicious software) rövidítése, amelynek fő célja, hogy betörjön és megzavarjon számítógépes rendszereket. Kiszélesítve, az RFID malware egy olyan malware, amely RFID tag-en keresztül van továbbítva és végrehajtva.

1. Az RFID kihasználó (RFID exploit) egy rosszindulatú RFID tag adat, amely felhasználja némely részét az RFID rendszernek, amellyel kapcsolatba lép. Az RFID rendszerek fogékonyak a hackertámadásokra csak úgy, mint a hagyományos számítási rendszerek.
2. Az RFID féreg (RFID worm) egy RFID alapú kihasználás, ami visszaél a hálózati kapcsolattal, hogy ön-replikációt tudjon elérni. Az RFID férgek azzal szaporodhatnak, hogy kihasználják az online RFID szolgáltatásokat, de RFID tag-eken keresztül is képesek terjeszkedni. Az RFID féreg kód azt okozza a gyanútlan RFID szervereknél, hogy távoli helyekről letöltsön és végrehajtson néhány fájlt. Ennek a fájlnak az a célja, hogy kompromittálja az RFID middleware szervert azonos stílusban, mint a legtöbb Internet alapú malware. A féreg által megfertőzött RFID szoftver tovább tud fertőzni újabb RFID tag-eket azzal, hogy felülírja az adataikat az RFID féreg kód egy másolatával.
3. Az RFID vírus egy olyan RFID alapú kihasználás, amely önállóan sokszorosítja a saját kódját újabb RFID tag-ekre anélkül, hogy szüksége lenne hálózati kapcsolatra.

Támadások kivédésének egyéb lehetőségei

RFID rendszerek különböző támadási lehetőségeknek vannak kitéve. Sok esetben magát a címkét kell megvédenünk, máskor pedig az illetéktelen leolvasást, módosítást kell megakadályoznunk. Néhány országban, ahol már használnak e-útlevelet, semmilyen másolás elleni védelmet nem kínálnak. Klónozással vagy hozzáféréssel kapcsolatos támadásoknak jó ellenszere lehet a másodszintű azonosítás, mint például a PIN kód, biometrikus azonosítás. A kommunikációra irányuló támadásokat viszonylag egyszerű kivédeni kriptográfiai módszerekkel, az üzenetet különböző algoritmusokkal van lehetőségünk titkosítani.

Nyomtatott master-kulcs

A termék belsejébe nyomtatott mester-kulcs teljes körű működést biztosít a vásárlóknak. Visszahozhatják a tag-et a hash-lock módból, feloldhatják azt. A kulcsot a termék belsejében helyezik

el, így a vásárlás során nem látható. A módszer leszűkíthető kizárólag fizikai kontaktusra is, kiküszöbölve ezzel az RF csatorna sajátságaiból adódó biztonsági kockázatokat. [14, 15]

Észlelő egységek használata

Az RFID rendszerek felszerelhetőek olyan berendezésekkel, melyek alkalmasak a jogosulatlan leolvasások észlelésére is. Az erős *downlink* jel miatt más olvasók észlelése is egyszerű. A polcokba szerelt speciális detektáló egység segítségével a szolgáltatás-megtagadással járó támadások (DoS) idejében észlelhetőek.

Titkosítási protokollok

Hitelesítés passzív transzpondereken

Az alacsony költségű RFID rendszereken a biztonság megteremtése nagy kihívást jelent. Korlátozott erőforrások miatt erős titkosításokat lehetetlen implementálni, így különlegesen egyszerű algoritmusokat és protokollokat kell tervezni, melyek figyelembe veszik a passzív rendszerek korlátait. A passzív tagek tárolási kapacitása néhány száz bit és háttérszámításokat sem lehet rajta végezni, mert a címke csak akkor közvetít adatot, amikor az olvasó indukálja. A drágább és saját erőforrással rendelkező transzpondereknél használatos algoritmusok helyett primitívebb megoldásokat kell használni. Alapvető hash függvényeket használata sem támogatott, mint például az MD5 vagy az SHA-1. Általában az alacsony költségű címkék csak egy egyedi azonosítót tárolnak, így a legegyszerűbb támadási felület a klónozás. A protokoll hatékonyságának fokozásához, egyensúlyba kell hozni a protokoll komplexitását és a támadások elleni ellenálló képességet.
A CrySys (Laboratory of Cryptography and Systems Security) publikációjából ismerve kidolgoztak 5 olyan módszert (XOR, Subset, Squaring, RSA, knapsack), mely alkalmas passzív transzpondereken is titkosítást végezni. Az alap koncepció a következőből indult ki:

$$R \rightarrow T : x \oplus k = a$$
$$T \rightarrow R : f(x) \oplus k = b$$

ahol az R az olvasó, T pedig a transzponder. k a titkos kulcs, mely meg van osztva R-el és T-vel. x egy n bit hosszú random szám, és f egy n bit-ről n bitre leképezés [3]

XOR

A XOR protokollnak hasonló felépítése van, mint a korábbi példának, de ez különböző kulcsokat használ, különböző irányban. [6]

$$R \rightarrow T : x \oplus k_1$$
$$T \rightarrow R : x \oplus k_2$$

Biztonságos megoldás lenne, ha a k_1 és k_2 kulcsokat véletlenszerűen választanánk minden egyes futtatáskor. A rendszer korlátozott kapacitása miatt, előbb vagy utóbb problémába ütköznénk. Az egyik lehetőség ennek megvalósítására a XOR kulcsgenerálás, melyben *i* változó alapján R véletlenszerűen választ új $k^{(i)}$ kulcsot és XOR titkosítást hajt végre a $k^{(i-1)}$ kulccsal. Ezáltal a következő protokollt kapjuk:

$$R \rightarrow T : a^{(i)} = x^{(i)} \oplus k^{(i)},\ k^{(i)} \oplus k^{(i-1)}$$
$$T \rightarrow R : b^{(i)} = x^{(i)} \oplus k^{(0)}$$

ahol i = 2,3,… egy számláló, minden futásnál egyel növelve. $x^{(i)}$ az i-edik véletlenszám és $k^{(0)}$ és $k^{(1)}$ előre beállított osztott kulcsok. $k^{(1)}$, $k^{(2)}$, … sorozat nem változik véletlenszerűen, csak az értéküket nem tudja követni a támadó. [3, 13]

RSA

Az *E* függvény az RSA titkosítást végzi, mely *n* hosszú, tartalmazza a publikus *e* és a titkos *d* hatványt is. A protokoll a következőkép épül fel:

$$R \text{ --> } T : x$$
$$T \text{ --> } R : E\ (x \wedge k)$$

ahol *x* a maszk vektor, $0 < m < n$ bitek véletlenszerűen 1-re állítva. $x \wedge k$ az ÉS műveletet jelenti *x* és *k* között, mely maszkolja a *k* vektort, megtartva azokat az értékeket, ahol az $x=1$ és minden más bitet 0-ra állít *k*-ban. Az RSA titkosítás műveleteinek a szám függ a kitevő és a nyers szöveg bináris méretétől. A második lépésben meg kell győződni arról, hogy a nyers szöveg bináris mérete legfeljebb *m*. Továbbá fontos, hogy kisméretű publikus kitevőt használjunk *(pl.:* $2^{16} + 1$*)*. [3, 11]

LMAP – Lightweight Mutual Authentication Protocol

A másik híres protokoll az LMAP, mely álneveket használ, ezen belül is ál-indexeket. Az indexek 96-bit hosszúak és a tábla sorát azonosítják, melyben a címkéről tárolt információk találhatók. Minden tag egy kulcshoz van rendelve, melyben a 96-bit négy részre van osztva *(K = K1 || K2 || K3 || K4)*. Miközben az álindexeket és a kulcsokat frissítjük szükségünk van további 480 bit újraírható memóriára (EEPROM vagy FRAM). A szűkős kapacitások miatt, mely akár kevesebb is lehet, mint 1000 bit, csak a következő műveletek érhetők el: *XOR, OR, AND, mod* 2^m. A szorzás már túl költséges művelet lenne, ahhoz hogy használni lehessen. [15, 16]

Első lépésként egy hello üzenetet küld az olvasó a transzpondernek, melyre az álnevével válaszol. Második lépésben az olvasó két véletlen számot generál *n1*-t és *n2*-t. *n1*-ből és a két kulcsrészletből *(K1, K2)*, két részüzenetet generál *A*-t és *B*-t. Majd *n2* és *K3* párosból egy *C* részüzenetet. A transzponder a kapott üzeneteket feldolgozza, majd kinyeri belőlük az *n1*-t és az *n2*-t. A két kapott véletlen számot felhasználva generál egy *D* válaszüzenetet, melyben authentikálja magát az olvasónál. [2, 12]

Hitelesítés

Kölcsönös szimmetrikus hitelesítés

Ahogy Dr. Imre Sándor és Kis Zoltán által készített RFID Kutatási Projekt [5] is bemutatja, a kölcsönös szimmetrikus hitelesítés egy háromlépéses eljárás az olvasó és a transzponder között, mely kölcsönös szimmetrikus hitelesítésen alapszik, s mely egyszerre ellenőrzi mindkét fél tudását a titkos kriptografikus kulcsról.

Származtatott kulcsokon alapuló hitelesítés

A korábbiakban tárgyalt hitelesítő nagy hátránya, hogy minden transzponder ugyanazt a k titkosító kulcsot használja. Ez a tulajdonság potenciális veszélyt hordoz minden hasonló alkalmazás számára – mely nagyon nagyszámú transzpondert használ. Mivel ezek a transzponderek gyakorlatilag mindenki számára hozzáférhetőek, számolni kell a kulcs kompromittálódásának veszélyével. Amennyiben ez megtörténik, az eljárás teljesen használhatatlanná válik. Ezt megelőzendő, ha minden transzpondert egyedi kulccsal látunk el, a biztonság nagymértékben megnő. Ennek előállításához először a transzponder szériaszámát olvassák ki. [9]

Titkosított adatkapcsolat

Az előző fejezetben megismert felállást ez esetben egy potenciális támadóval egészítjük ki. Itt meg kell különböztetnünk két támadótípust. Az első –Támadó1-nek nevezik – megpróbál a háttérben maradni és lehallgatásos módszerekkel, passzív módon, értékes információkat nyerni az adatárból. Ezzel ellentétben Támadó2 aktívan részt vesz a kommunikációban, és saját (vagy más) hasznára módosítja is annak tartalmát. A kriptográfiai módszerek mindkét támadó ellen megoldást nyújtanak.

Az átviendő adatot (nyílt szöveg) titkosításnak vetik alá, így a támadó nem ismerheti meg annak eredeti tartalmát. [10]

Hash-alapú hozzáférés-vezérlés

Az olcsó smart címkéket tekintve szükséges egy egyszerű – egyirányú hash függvényeken alapuló – biztonsági sémát is bemutatni. Az eljárás megvalósítása hardverrel történik, mely során a zárolt és feloldott állapotban is működő tag-ek egy kis szeletet különítenek el memóriájából ún. metaID-k tárolás céljából. Az algoritmus viszonylag egyszerű: a transzponderekben implementálni kell a hash függvényeket, és szélesebb körű nyilvántartást igényel a back-end adatbázisokban. A séma rugalmas, bővíthető pl. többszörös hozzáféréssel, vagy éppen írásfelügyelettel. A metaID-ket egyszerű lekérdezni így pedig könnyű háttéradatbázis építési lehetőséget kínál third-party gyártók részére. Ugyanakkor a metaID-k egyedisége könnyű azonosítási lehetőséget is nyújthat.

Aszimmetrikus kulcsegyeztetés

A titkosítási lehetőségek közül végül ki kell emelni az aszimmetrikus kulcsegyeztetés módszerét is. E folyamatban, a lehallgatásra érzékeny adatok átvitele során, haa egy olvasó üzenni akar 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 kiszámolja v⊕r-t, majd elküldi a tag-nek. A visszairányú csatorna hatósugarán kívül tartózkodó lehallgató csak ezt a v ⊕ r-t hallja, amiből nem következtethet az eredeti v értékére.

Az NFC kommunikáció védelme

Használjuk ki az okos-telefonok rendelkezésre álló számítási kapacitását. A nagy processzor teljesítmény és a hagyományos RFID tag-ekhez képest nagy memória lehetővé teszi, hogy összetett kriptográfiai algoritmusokat használjunk. Megvalósíthatóvá válik akár az RSA algoritmus nagy prímszámok felhasználásával.

A kommunikációs folyamat teljes titkosítására használjuk az AES-128 algoritmust. Ezt egyedivé, kommunikációnként változóvá teheti, ha a közösen használt kulcsot a véletlenszerűen határozza meg az olvasó és az aszimmetrikus kulcsegyeztetés módszerével tudatja a tag-gel. Így a folyamat titkosítása egyedivé válik akár ugyanazon olvasó és tag két különböző üzenetváltása esetén is.

A relay-attack jellegű támadás elleni védekezés esetében az AES kulcs meghatározásában szerepet kaphat a rendelkezésre álló egyéb helyfüggő vagy tulajdonos függő információ is. Pl az okos-telefonban meglévő mozgás és irányszenzorok adatai, GPS adatok, telefon vagy SIM kártya azonosítók bizonyos részei.

Ezen információk kombinálásával biztonságosabbá tehetjük a pénzfizetési folyamatot. Így erősítve a felhasználók bizalmát a technológia felé.

Következtetés

Egy termék számtalan veszélynek van kitéve, ameddig a gyártótól el nem jut a fogyasztóhoz. A gyárból átkerül egy átmeneti raktárba, innen a nagykereskedő, majd a kiskereskedelmi cég elosztó központjába, végül pedig az áruházak polcaira. Ez elég hosszú folyamat, amely során az áruk elveszhetnek, összecserélődhetnek, ellophatják őket.

Az EU előírások a legtöbb árucikk esetében egyre messzebb tolják ki a gyártói felelősséget, ezért egyre inkább lényeges szemponttá válik a nyomon követhetőség, ami az RFID segítségével tökéletesen megvalósítható. A gyártás során nyomon követhető a termék útja, regisztrálhatók a technológiai sorrendek, a munkafázisok, a személyek, akik részt vettek a gyártásban, vagy bármilyen egyéb adat.

Az RFID rendszerek használata napjainkban is folyamatosan változik. Számos új technológia jelenik meg és a gyártók, multinacionális cégek törekednek arra, hogy ezeket az újdonságokat eljutassák a felhasználókig. A transzponderek napról napra egyre kisebb kivitelben és olcsóbban kerülnek ki a gyárakból, mely szintén segíti annak elterjedését. A széles körű elterjedésnek köszönhetően, egyre több szegmensben találhatóak meg ezek a rendszerek, így annak veszélyeire, sebezhetőségeire is sokkal nagyobb hangsúlyt kell fektetni. Magyarországon jelenleg is folynak az egyeztetések a mobillal való fizetési lehetőségekről, melynek elterjedése egy hatalmas mérföldkő lehet a fejlődésben. A felhasználók nincsenek tisztában ennek veszélyeivel, legtöbbjük nem tud, vagy nem is akar foglalkozni ehhez hasonló problémákkal. Így a gyártóknak folyamatosan figyelniük kell a biztonságra, figyelemmel kell követniük azokat a lehetőségeseket, melyek bármilyen sérülést, vagy adatlopást tudnánk okozni a felhasználót körülvevő rendszerekben. A csökkenő előállítási költségek révén az olcsó passzív RFID rendszerekre jellemző adattárolási limit is előbb vagy utóbb megszűnik. Felválthatják az aktív címkék, melyek már sokkal nagyobb biztonsággal használhatóak, és nem kell speciális algoritmusokat kidolgozni, hogy működni tudjanak az egyszerűbb rendszereken is.

Irodalom

[1] Klaus Finkezeller – RFID Handbook, Third Edition, 2010

[2] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez Tapiador and Arturo Ribagorda – LMAP: A Real lightweight Mutual Authentication Protocol for Low-cost RFID tags - http://events.iaik.tugraz.at/rfidsec06/program/papers/013%20-%20lightweight%20mutual%20authentication.pdf

[3] Vajda István és Buttyán Levente – Lightweight Authentication Protocols for Low-Cost RFID Tags

[4] Ziv Kfir and Avishai Wool – Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems - http://eprint.iacr.org/2005/052.pdf

[5] Dr. Imre Sándor, Kis Zoltán, Molnár László, Pogátsa Attila, Schulcz Róbert, Tóth Gábor – RFID rendszerek vizsgálata felhasználás és technológia szempontjából - http://www.rfid.answare.hu:8080/site/kutatasi-erdmenyeink/radios-megoldasok/2006/rfid-rendszerek-vizsgalata-felhasznalas-es-technologia-szempontjabol.pdf/view

[6] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, Kwangjo Kim (KOMSCO, ICU, WPI **Mutual Authentication Protocol for Low-cost RFID** 2005

[7] Sebastien Canard, Iwen Coisel (Orange Labs R&D, Caen, France) **Data Synchronization in Privacy-Preserving RFID Authentication Schemes** 2008

[8] Hee-Jin Chae, Daniel J. Yeager, Joshua R. Smith, and Kevin Fu (University of Massachusetts) **Maximalist Cryptography and Computation on the WISP UHF RFID Tag** 2007

[9] Sindhu Karthikeyan and Mikhail Nesterenko_Kent State University RFID Security without Extensive Cryptography 2005

[10] M. McLoone and M.J.B. Robshaw (Queen's University, Belfast, U.K.) Public Key Cryptography and RFID Tags 2008

[11] Markku-Juhani O. Saarinen, Daniel Engels: A Do-It-All-Cipher for RFID: Design Requirements IACR Cryptology ePrint Archive 2012 (2012): 317

[12] SAARINEN, M.-J. O. Cryptanalysis of Hummingbird-1. In FSE 2011 (2011), A. Joux, Ed., vol. 6733 of LNCS, Springer, pp. 328–341.

[13] NIST. Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC. NIST Special Publication 800-38D, 2007.

[14] JOUX, A. Authentication failures in NIST version of GCM. NIST Comment, 2006.

[15] KROVETZ, T., AND ROGAWAY, P. The software performance of authenticated-encryption modes. In FSE 2011 (2011), A. Joyx, Ed., vol. 6733 of LNCS, Springer, pp. 306–327.

[16] ENGELS, D., SAARINEN, M.-J. O., SCHWEITZER, P., AND SMITH, E. M. The Hummingbird-2 lightweight authenticated encryption algorithm. In RFIDSec 2011 (2011), A. Juels and C. Paar, Eds., vol. 7055 of LNCS, Springer, pp. 19–31.