RÁDIÓFREKVENCIÁS AZONOSÍTÁS ÉS BIZTONSÁG

Sziklai Péter
kandidátus, egyetemi docens
ELTE Számítógéptudományi Tanszék,
ELTECRYPT – sziklai@cs.elte.hu

Nagy Dániel
PhD,
ELTE Számítógéptudományi Tanszék,
ELTECRYPT – nagydani@epointsystem.org

Ligeti Péter
kutató, ELTE Számítógéptudományi Tanszék, ELTECRYPT
MTA Rényi Alfréd Matematikai Kutatóintézet
turul@cs.elte.hu

1. Bevezetés

Rádiófrekvenciás azonosítás (RFID) alatt legáltalánosabban olyan rádiófrekvenciás (RF) kommunikációt értünk, amelynek elsődleges célja a kommunikációban résztvevők legalább egyikének azonosítása (IDentifikálása), illetve bizonyos tulajdonságainak megállapítása. Tipikusan kisméretű, olcsó adóvevők (*bélyeg*, angol szóval *tag*) az azonosítás tárgyai.

A rádiófrekvenciás azonosítás első alkalmazása a Brit Királyi Légierő IFF (identification: friend or foe, azonosítás: barát vagy ellenség) adóvevője volt 1939-ben (s végig a második világháború folyamán), azaz egy tipikus biztonsági alkalmazás (Landt, 2001). Ahogy a kapcsolódó technológiák egyre olcsóbbak és elérhetőbbek lesznek, egyre több polgári alkalmazás jelenik meg a katonaiak mellett: beléptetés (itt embereket vagy járműveket azonosítunk), logisztika (itt árukat, csomagokat és járműveket akarunk azonosítani), fizetés (itt pedig fizetési ígéreteket) és egyebek. Mindezeknél szintén felmerülnek biztonsági szempontok, amelyeket kezelni kell.

A rádiófrekvenciás azonosításnál egy objektumhoz hely- és időkoordinátákat rendelünk. Nagy mennyiségű, ilyen jellegű információtömeg valós idejű feldolgozása csak jól kiépített infokommunikációs hálózatok révén lehetséges.

Ebben a cikkben betekintést nyújtunk az RFID technológia biztonsági vonatkozásaiba, bemutatjuk a biztonsági tervezés feladatát és alapfogalmait. Magyarországon RFID biztonsággal kapcsolatos alkalmazott kutatással az ELTE TTK Számítógéptudományi Tanszékén működő ELTECRYPT kriptográfiai kutatócsoport foglalkozik, mely jelentős támogatást élvez az Egyetemközi Távközlési és Informatikai Központtól, valamint a Nemzeti Kutatási és Technológiai Hivataltól.

2. Mi a biztonság?

A *biztonság* mindig valamilyen érdekellentét kontextusában merül fel, ún. *fenyegetés*ekkel kapcsolatban. A fenyegetés lehetőség olyan (aktív) cselekedetre valamilyen ellenfél részéről, amely neki hasznot, a vizsgált rendszernek pedig kárt okoz. A megvalósult fenyegetést

támadásnak, végrehajtóját pedig *támadónak* nevezzük. A támadó szemszögéből a támadásnak van valamilyen (várható) költsége és (várható) haszna. A támadót biztonsági tervezéskor racionálisnak feltételezzük, azaz arra számítunk, hogy költségeit minimalizálni, hasznát pedig maximalizálni próbálja a rendelkezésére álló információ alapján. A racionális szereplők viselkedésével a közgazdaságtan és a játékelmélet tudománya foglalkozik, ezért ezek elengedhetetlenek eszközeink biztonsági problémának vizsgálatakor.

A támadó költségei és nyereségei tipikusan nem azonos formában merülnek fel, és gyakran nem is egydimenziós mennyiségek, de a matematikai közgazdaságtan egyik alapösszefüggése, a *Debreu-lemma* (Debreu, 1954) értelmében általában találunk olyan függvényt, amely egyetlen valós számmal reprezentálja a támadó költségeit és nyereségét olyan módon, hogy az a nagyobb számot előnyben részesíti a kisebb számmal szemben, s negatív haszon esetén nem áll érdekében végrehajtani a támadást. A cikk további részében ezért minden költséget és hasznot összehasonlítható, pénzben kifejezhető valós értékként fogunk kezelni.

Biztonsági (más szóval védelmi) intézkedésnek nevezzük mindazt, ami a támadás költségeit növeli. Ezek két nagy csoportba oszthatók: a *proaktív biztonsági intézkedés*ek a támadás végrehajtásához szükséges erőforrások növelésével rónak költségeket a támadóra, a *reaktív biztonsági intézkedés*ek pedig a támadás végrehajtása miatt okoznak kárt a támadónak. Mint látni fogjuk, RFID technológiák mindkét fajta biztonsági intézkedés megvalósításához eredményesen alkalmazhatók. Egy biztonsági rendszer (biztonsági intézkedések összessége) akkor sikeres, ha megakadályozza, hogy a fenyegetésből támadás legyen.

3. A biztonsági matematika eszköztára

Biztonsági rendszerek tervezésekor általában az algebra, a bonyolultságelmélet, a számelmélet és a valószínűségszámítás eredményeit használhatjuk. Egy rendszer vagy annak egy részének biztonsága általában egy probléma vélt nehézségén, vagy valamely algebrai művelet megfordításának nehézségén múlik.

Egy rendszer biztonságának bizonyításának tipikus módszere, hogy belátjuk, hogy amennyiben a támadó képes sikeres támadást intézni a rendszer ellen, akkor képes megoldani egy nehéznek vélt matematikai problémát, például tetszőleges nagy összetett szám prímtényezőit meghatározni, vagy meg tud fordítani egy *egyirányú* függvényt. Az egyik legszélesebb körben használt kriptográfiai eljárás, az RSA rendszer biztonsága is számelméleti alapokon nyugszik, jelesül, ha fel tudunk törni RSA alapú rendszereket, akkor tetszőleges számnak meg tudjuk határozni az Euler-függvényét, ami hasonló nehézségű, mint megadni a prímtényezős felbontását.

Az algebrai módszerek közül kiemelendő a diszkrét logaritmus probléma: adott egy *csoport* és annak egy *generátoreleme* úgy, hogy a csoportban gyorsan tudjunk hatványozni, viszont tetszőleges csoportelemről ne lehessen belátható időn belül eldönteni, hogy a generátorelemnek hányadik hatványa. A csoport többnyire egy véges test multiplikatív csoportja szokott lenni. Újabban egyre inkább elterjed az elliptikus görbéken alapuló kriptográfia, ahol a csoportunk egy *véges test* felett értelmezett görbe pontjain van értelmezve. Az ilyen rendszerek implementálása ugyan nem könnyű, és meglehetősen bonyolult matematikai apparátust használ, viszont sokkal kisebb kulcsméret mellett ugyanakkora biztonságot garantál, mint, mondjuk, az RSA.

4. Az RFID és a biztonság

A rádiófrekvenciás azonosító rendszereknek általában három fő építőkövük van: az adóvevők (*bélyeg*ek), a leolvasók, valamint ez utóbbiakkal összeköttetésben lévő feldolgozó szerverek. A bélyegek valójában kisméretű, antennával ellátott mikrocsipek, melyek az olvasótól érkező kérdésre küldenek valamilyen választ. Ezt az olvasó továbbítja a feldolgozó szervernek. A legtöbb esetben ez mindenféle titkosítás nélkül történik, ami alapvető biztonsági problémákat vethet fel. Az RFID bélyegek három csoportra oszthatóak: passzív, szemiaktív és aktív, aszerint, hogy honnan kapják a működésükhöz szükséges energiát.

A *passzív bélyeg*ek a leolvasó rádiófrekvenciás sugárzásából veszik az energiát, azt szórják vissza megfelelő módon. Ezt a technikát először lehallgatáshoz használták a Szovjetunióban a II. világháborút követően a titkosszolgálatok (Landt, 2001). Fontos tulajdonságai a hosszú (gyakorlatilag korlátlan) üzemidő, alacsony költségek. A korszerű logisztikai és ellenség-barát felismerő rendszerek ilyen eszközöket használnak.

A *szemiaktív bélyeg*ek a feldolgozáshoz szükséges energiát más energiaforrásból veszik, de a kommunikáció itt is a leolvasó sugárzásának visszaszórásával történik. Az eredeti IFF adóvevő ilyen volt.

Az *aktív bélyeg*ek kizárólag információt merítenek a leolvasó jeléből, s energiaszükségletüket más forrásból fedezik. Ilyen eszközökkel jóval kisebb leolvasó-teljesítménnyel is megvalósítható a leolvasás. Az aktív bélyegek egyik típusa a „szoftverbélyegnek" nevezett megoldás, amikor adóvevővel felszerelt eszközbe (például mobiltelefonba) szoftver segítségével építenek azonosításra alkalmas üzemmódokat.

Lássunk néhányat az RFID alkalmazások közül. Talán a legfontosabb alkalmazás a bolti vonalkódok következő generációjának szánt Elektronikus Termék Kód (EPC), ami a közönséges vonalkódokkal ellentétben teljesen egyedi azonosítást tesz lehetővé. Ennek segítségével nyomon követhető egy konkrét termék útja a szállítási lánc teljes hosszán a gyártól a kasszáig. A gond ott kezdődik, hogy amennyiben nincsen semmilyen védelmi intézkedés (és manapság legtöbbször ez a helyzet), mindez folytatódik a pénztár elhagyása után is: egy leolvasó segítségével bárki megtudhatja, hogy éppen milyen EPC-vel felcímkézett áru van nálunk.

Itt elérkeztünk az RFID technológia elterjedésének egyik legkomolyabb akadályához, a biztonság kérdéséhez. A követhető csipek alkalmazása a mindennapi életben személyiségi jogi problémákat vet fel, ezért vásárlói oldalról egyelőre negatív visszajelzések tapasztalhatóak, az emberek többsége az RFID-ről George Orwell Nagy Testvérére asszociál.

Az Európai Központi Bank tervei között szerepelt, hogy a nagycímletű euró bankjegyeket RFID címkékkel látja el, ami a feketepiaci pénzmozgások felderítéséhez nyújtana segítséget (Yoshida, 2001). Itt fontos kiemelni, hogy a rendszernek egyik feltétele, hogy csak bizonyos hatóságok képesek követni ezeket a pénzfolyamokat, magánszemélyek vagy bankok nem, ugyanakkor egy pénzintézet a pénz eredetiségét már le tudja ellenőrizni.

RFID ellen a következő támadásokat különböztetjük meg a támadás módja és célja szerint. Hogyan történnek a tipikus támadások? (RF):

1. *Passzív lehallgatás*. Arra jogosulatlan támadó érzékeny vevőkészülékkel belehallgat a kommunikációba, s ezzel olyan információhoz jut, amellyel a rendszernek kárt okozhat.

2. *Aktív üzenetbeiktatás*. Itt a támadó olyan üzeneteket sugároz, amelyek az azonosító (leolvasó) vagy az azonosított (bélyeg) működését megváltoztatják, s az a rendszer helyett (vagy mellett) a támadó céljainak megfelelően működik.
3. *Zavarás*. Itt a támadó egyszerűen oly módon akadályozza meg az azonosítórendszer működését, hogy zavaró jelet sugároz, amely elnyomja az RFID kommunikációt.

Mik általában a támadás céljai? (ID)

1. *Nemkívánatos azonosítás*. A támadó egyik célja lehet, hogy azonosítson olyan dolgokat, amelyeknek azonosítására nem jogosult. Például IFF rendszer esetében nem előnyös, ha az ellenség is azonosítani tudja repülőgépeinket. Hasonlóan, egy kereskedő nem biztos, hogy örül, ha a konkurencia leltározza a raktárát.
2. *Félreazonosítás*. A támadó gondoskodik róla, hogy a rendszer hibásan azonosítson dolgokat. Maradva az IFF példájánál, az ellenség szeretné, ha saját gépeit barátként, a mi gépeinket pedig ellenségként azonosítaná légvédelmünk. Földhözragadtabb példaként egy RFID-alapú beléptetőrendszerrel védett épületbe akar bejutni a támadó, vagy el akar indítani egy RFID technológiával immobilizált gépkocsit annak indítókulcsa nélkül.
3. *Meghiúsított azonosítás*. Ebben az esetben a támadó meg akarja akadályozni az azonosítást. Általában ilyen támadással fennakadást lehet okozni a rendszerben, ami a rendszernek kárt, a támadónak pedig hasznot okoz.

5. Az RFID tipikus biztonsági alkalmazásai

1. *Jogosultság*. Ekkor az RFID-t arra használjuk, hogy eldöntsük valakiről, hogy jogosult-e bizonyos szolgáltatások igénybevételére. Ennek speciális esete a fizetés, amikor a jogosultság pont az igénybevétel miatt megszűnhet. Másik speciális eset az eredetiség, amikor egy áru bizonyos márkanéven való eladhatóságát ellenőrizzük RFID azonosítással. Ezt lehet proaktívan és reaktívan is csinálni: megtagadjuk a jogosultságot a jogosulatlanoktól, vagy azonosítjuk a jogosulatlanokat későbbi büntetés céljából. Erősen ellentmondásos alkalmazás a határátlépés jogosultságának elbírálásához használt RFID útiokmány.
2. *Követés*. Ekkor az azonosított dolgok helyét akarjuk időben nyomon követni. Ez általában reaktív biztonsági intézkedések foganatosítására ad lehetőséget. Egy meglepő példa a hamisítás elleni védekezés, amikor egy adott termék követésekor kiderülhet, hogy olyan helyen jelenik meg valami egy adott pillanatban, ahol az eredeti abban a pillanatban egyszerűen nem lehet (például mert ugyanakkor máshol van).

6. RFID: biztonság korlátozott erőforrásokkal

Joggal merül fel a kérdés, hogy amíg a mindennapi élet részét képező hálózatok (internet, GSM és újabban már a WLAN) tele vannak (többnyire) jól működő biztonsági protokollokkal, miért nincsen semmi a legtöbb RFID rendszerben? Az okok a bélyegek árában, méretében és külső energiafelvételében keresendők. A legolcsóbb és legelterjedtebb passzív bélyegek kisebbek egy gombostű fejénél, előállítási költségük 10 eurócent körül mozog, ezek következtében az eszközök roppant korlátozott erőforrásokkal rendelkeznek: tárolási kapacitásuk 32 és 128 bit közötti, számítási kapacitásuk is nagyon csekély, mindössze néhány ezer logikai kapu, melyek nagy része a bélyegek alapfunkcióit szolgálják. Egy szemléletes összehasonlítás: a 2001 óta szabványos

blokktitkosító, az AES (Advanced Encryption Standard) algoritmus 20 000–30 000 kaput használ. Másrészről az olvasótól kapott rádiójel olyan rövid időre tölti fel őket energiával, hogy amúgy sem tudnák elvégezni a kívánt műveleteket.

Mindezekből látható, hogy a hagyományos kriptográfiai módszerek az RFID esetében általában nem alkalmazhatóak, a problémák kezelése másfajta szemléletet kíván.

Az alábbiakban ismertetünk néhány régebbi és teljesen friss ötletet, melyek bizonyos támadások ellen nyújtanak védelmet.

1. *Bélyegdeaktiválás*. Az egyik legelterjedtebb módszer, használat után „megölni" a bélyeget. A „halott bélyeg nem beszél többet" koncepciójánál a leolvasó küld egy *kill* parancsot, vagy a deaktiválás történhet fizikai úton is. Hasonlóval találkozhatunk például könyvesboltok kasszájánál, vagy nagyobb áruházakban a szeszes italoknál, ahol általában csak a bolti lopás megelőzésére használják a bélyegeket. A pénzbe ültetett RFID címkéket viszont nem feltétlenül előnyös megölni…
2. *Faraday-kalitka*. Valójában nem más, mint egy fémből készült tároló alkalmatosság, ami blokkolja a rádiójeleket, ezzel lehetetlenné téve az illetéktelen leolvasókat. Mérete széles skálán mozoghat a szállítási láncban használt fémkonténerektől egészen a fémszálakkal bélelt pénztárcáig. Ugyanakkor bármely könyváruházban egy hasonló elven működő táskába csúsztatva az *Állatfarm*-ot és az *1984*-et, nyugodtan kisétálhatunk…
3. *Zajos bélyeg*. Ezen eljárás segítségével az olvasó és a bélyeg olcsón generálhat titkos kulcsokat (Castelluccia – Avoine, 2006). Itt az alapötlet az, hogy beiktatunk egy extra egységet, a zajos címkét, ami kicsit többet tud számolni, mint egy közönséges címke (ezáltal drágább is lesz, de ebből sokkal kevesebb kell, mint bélyegből), feltesszük továbbá, hogy van egy közös titka a leolvasó egységgel. Ennek segítségével titkos kulcsokat készít a leolvasó és a bélyeg számára. Ezek után már csak az olvasó és a leolvasandó bélyeg kommunikál a frissen gyártott titkos kulcs segítségével. Ez az ötlet boltokban vagy raktárakban hasznos lehet, ipari kémkedés elkerülésére.
4. *Titkosítás jelmodulálással*. Ez az eljárás a rádiós csatorna sajátosságait használja (Yu et al., 2006). Itt a címke teljesen nyilvánosan sugározza ki az azonosítóját, de úgy, hogy lehallgatása nagyon költséges. Itt feltesszük, hogy a rendszer minden leolvasója és címkéje rendelkezik egy globális közös titokkal. Ezután egy közös nyilvános adatból (idő, számláló vagy kihívás) és a közös titokból meghatározza, mely időintervallumokban sugározzon impulzusokat a bélyeg. A teljes leolvasás 10 ms-ot vesz igénybe, az időintervallumok pedig mindössze 954 ps hosszúak, ezáltal a lehallgatás költsége nagyságrendekkel meghaladja a várható nyereséget. Ez a megoldás raktáraknál szintén hasznos lehet, gyenge pontja az egész rendszerre jellemző globális kulcs, ami ha nyilvánosságra kerül, az egész rendszer biztonságát aláássa.

7. Kihívások, feladatok

Amikor bármiféle RFID rendszert tervezünk, amelyben felmerülnek biztonsági szempontok, kulcskérdés a megfelelő kompromisszumok megkeresése, a különböző paraméterek optimalizálása az erőforráskorlátok figyelembevételével. Sikeres biztonsági rendszerek vizsgálatakor gyakran azt találjuk, hogy a támadások megakadályozásához nem szükséges azok lehetetlenné tétele; sok esetben elég, ha a támadó számára azok végrehajtása már

többe kerül, mint amennyi haszna lehet belőle. Erre tipikus példa a GSM biztonsági rendszere, amelynek feltörése elméletileg és – kellő erőforrások megmozgatásával – gyakorlatilag is lehetséges, ám a valóságban szinte soha nem célpontja támadásoknak (ellentétben a GSM előtti mobilhálózatokkal). Az RFID technológiák tömeges elterjedésének még mindig a költségek a legnagyobb kerékkötői, így költséghatékony, ám gyakorlati szempontból mégis (lehetőleg bizonyítható-an) biztonságos megoldások kidolgozása nagyban hozzájárulhat a technológiához fűzött remények valóra váltásában. Az ELTECRYPT kutatócsoportban ezért különböző diszciplínák (kriptográfia, játékelmélet, elméleti villamosságtan stb.) eredményeit felhasználva igyekszünk megtalálni a kellően olcsó és hatékony megoldásokat.

Kulcsszavak: *informatikai biztonság, kriptográfia, matematika, rádiófrekvenciás azonosítás*

IRODALOM

Carluccio, Dario – Lemke-Rust, K. – Paar, C. - Sadeghi, A.-R. (2006): *E-passport: The Global Traceability or How to Feel Like an UPS Package*. Workshop on RFID Security, Graz

Castelluccia, Calude - Avoine, Gildas (2006): *Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags*. International Conference on Smart Card Research and Advanced Applications - Cardis

Debreu, Gerard (1954): *Representation of a Preference Ordering by a Numerical Function*. Decision Process. 159–165.

Landt, Jerry (2001): *Shrouds of Time: The history of RFID*. AIM, Inc. http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf

Yoshida, Junko (2001): *Euro Bank Notes to Embed RFID Chips by 2005, EE Times*. http://www.eetimes.com/story/OEG20011219S0016

Yu, Pengyuan - Schaumont, P. - Ha, D. (2006): *Securing RFID with Ultra-wideband Modulation*. Workshop on RFID Security, Graz