RFID rendszerek sebezhetőségének vizsgálata

Biró Csaba, Radványi Tibor, Takács Péter, Szigetváry Péter
{birocs, dream, takip, szigipet}@aries.ektf.hu
Eszterházy Károly Főiskola
Matematikai és Informatikai Intézet

Absztrakt

Az RFID rendszereket arra tervezték, hogy rádiófrekvenciás elektromágneses tereken keresztül képesek legyenek különböző objektumok *(tárgyak, élőlények)* detektálásra, automatikus azonosítására, nyomon követésére és a tag-ekről szerzett információk biztonságos tárolására és továbbítására. Napjainkban már a legelterjedtebb műszaki rendszerek közé sorolható technológia, amely alapvetően három fő komponensből áll: címkék *(adathordozók)*, olvasók/írók és a kommunikációs eszközök. Népszerűségét széleskörű alkalmazhatóságának és viszonylagosan alacsony megvalósítási költségeinek köszönheti. Cikkünkben először csoportosítjuk a különböző RFID rendszereket veszélyeztető, jól ismert támadási *(zavarás, illetéktelen lehallgatás, elárasztás, tag-ek klónozása, stb.)* módokat. Majd rámutatunk arra a tényre, hogy a gondos rendszertervezés és kivitelezés mennyire kulcsfontosságú ennél a technológiánál.

Kulcsszavak: RFID rendszerek, tag-ek klónozása, elárasztás, külső hatások, illetéktelen lehallgatás, vírusok, zavarás

Analysis of vulnerabilities in RFID systems

Csaba Biró, Tibor Radványi, Péter Takács, Péter Szigetváry
{birocs, dream, takip, szigipet}@aries.ektf.hu
Eszterházy Károly College
Institute of Mathematics and Informatics

Abstract

RFID systems are developed to function through electromagnetic fields of radio frequency and be able to detect, automatically identify and track various objects (items, or even beings) by storing and securely transmitting information. Nowadays it earned its place amongst the most

prevalent technological systems, although it consists of only three main components: tags (data storing), scanners/writers and the communication protocols. Its widespread applicability and relatively low manufacturing cost is to thank for its popularity. In this paper first of all we classify the various well-known attack methods (*jamming, unauthorized interception, flooding and cloned tags*) threatening RFID systems. Then we point out the fact how much attentive system design and implementation is of the essence with this technology, and lastly we propose some measures that might increase the security of certain systems.

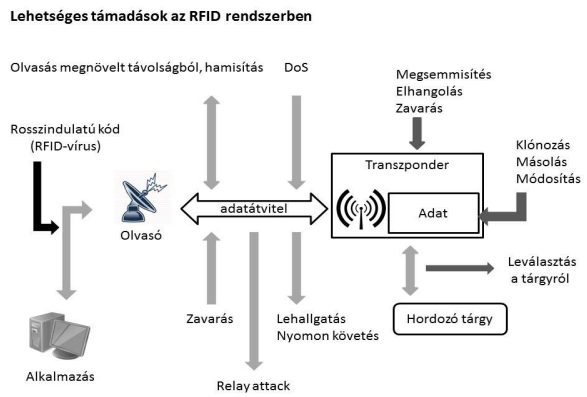
Keywords: RFID systems, tag cloning, flooding, interferences, unauthorized interception, viruses, jamming

Bevezetés

Mára mindennapi életük szerves részévé vált az automatikus azonosítás. A legtöbben annyira hozzászoktunk, hogy figyelmünket jellemzően már csak rendszer hibája kelti fel. Gyakori jelenség a boltokban a nehezen leolvasható vonalkódok okozta bosszankodás, várakozás a sorban. Valójában ettől lényegesen szélesebb körben elterjedt technológiáról beszélhetünk, mivel a rendszer szolgáltathat információt emberekről, állatokról, termékekről, postai csomagokról, gyártás közbeni nyomon követésről, stb. Felhasználás szempontjából megkülönböztetünk nyílt és zárt rendszereket, aktív és passzív felhasználókkal. A zárt rendszerek esetében *(pl.: gyártás nyomon követése)* az aktív és a passzív fél nincs különválasztva, a rendszer üzemeltetője egyben a felhasználója is. A nyílt rendszerek esetén az aktív fél szolgáltatja az infrastruktúrát, adminisztrálja és kezeli a keletkezett adatokat. Passzív félként pedig azokra a felhasználókra tekintünk, akik igénybe veszik a szolgáltatást és tudatosan, vagy tudtuk nélkül adatokat szolgáltatnak. Közösségi közlekedés esetén a közlekedési vállalat az aktív, az utasok a passzív fél. Bizonyos helyzetekben harmadik résztvevőként megjelennek azok, akik jogosulatlanul kívánnak behatolni, jobb esetben csak a kihívást keresve, rosszabb esetben ártó szándékkal.

Lehetséges támadások az RFID rendszerben

A továbbiakban a rendszer működését valamilyen formában zavaró külső hatásokat, az egyszerűség kedvéért támadásnak nevezzük. [1] Sokféle támadás létezik az eszközök széles skáláján.



2. ábra Lehetséges támadások az RFID rendszerben

Tag-eket veszélyeztető támadások

Fizikai támadások

A legegyszerűbben támadható eleme a rendszernek, mivel jellemzően ezzel az eszközzel találkoznak a felhasználók, *pl.:* az áruházakban a termékeken elhelyezett lopás gátló címkék. A sérülések lehetnek véglegesek, vagy átmeneti működési zavart okozóak, az ezt kiváltó okok pedig mechanikai, kémiai, vagy elektronikai jellegűek. A legegyszerűbb támadás a mechanikus megsemmisítés, például az antenna levágása, vagy a chip összetörése. További hatásos támadás, amikor fémfelületet használnak arra, hogy ”leárnyékolják” a tag-et az olvasó elektromágneses sugárzásától. Ezt a legegyszerűbben úgy lehet elérni, hogy alumínium fóliával becsomagoljuk, melynek következtében a passzív tag még a chip kezeléséhez szükséges energiát sem tudja felvenni. Amint eltávolítottuk a fémes felületet a transzponder újra működőképessé válik. [1]

Cloning – Klónozás

A klónozás elleni védelem egyik alapköve a megelőzés, a másik a detektálás. Az RFID tag-ek gyártói arra törekszenek, hogy minél nehezebben klónozható tag-eket (TID, PUF) gyártsanak. Ennek köszönhetően természetesen növekszik a tag-ek előállítási költsége. Azonban ezekkel az eljárásokkal csak a klónozás nehezíthető, a transzponder-ek továbbra is ki vannak téve a lehallgatásoknak. Az illetéktelen lehallgatások elleni védekezés fontos szegmense, a hálózati kommunikáció biztonságának növelése, titkosítás olvasó-tag és tag-olvasó között [2], [3], [4].

A gyártók a klónozhatóság megnehezítésére az alábbi két eljárást alkalmazzák:

1. Az első kizárólag EPC szabványnak megfelelő tag-ek esetén alkalmazható. Ezen tag-ek tartalmaznak egy gyárilag programozott, csak olvasható transzponder azonosítót (TID), továbbá jelszóval védhetők és bármikor kilőhetők (KILL parancs). A transzponder azonosító felépítése hasonlít a hálózati kártyák MAC címéhez [5].

2. A másik eljárás a PUF (Physical Unclonable Function), amely egy biztonságos és olcsó mechanizmus szilícium chip-ek hitelesítésére. Minden egyes chip a szilícium fizikai jellemzőinek és az eltérő IC gyártási folyamatoknak köszönhetően egyedülálló módon jellemezhető, „klónozhatatlan” [6], [7].

Spoofing – Hamisítás

Az adattárolás fejlettebb megoldása, amikor már nem csak a sorozatszámot, hanem külön memóriaterületen egyedileg felvitt adatot is találunk a tag-en. A támadó ezeket az adatokat ki tudja olvasni, vagy módosíthatja a saját igényeinek megfelelően. Egy említésre méltó kísérletet végeztek a Johns Hopkins Egyetemen, melynek keretében egy módosított RFID címkét fölhasználva gázolajt vásároltak, továbbá feltörtek egy RFID védelemmel felszerelt autót. Általánosan elmondható, hogy mindegyik csak

olvasható és írható-olvasható tag veszélyeztetett, ami nem rendelkezik titkosítással [1],[2].

Az olvasó és a tag közötti adatátvitelt érő támadások

Eavesdropping – Lehallgatás

Az RFID rendszer elektromágneses hullámokat használ a jelátvitelhez, mely elég könnyen és egyszerű eszközökkel lehallgatható, korlátot inkább az olvasási távolság jelent. Az olvasó és a tag közötti leolvasási távolság a néhány centimétertől (ISO/IEC 14443, 13.56MHz) a méteres tartományig terjed (ISO/IEC 18000-6, 868MHz). A lehallgatás sikerességét befolyásolja az átviteli protokoll fajtája, az esetlegesen használt titkosítás és a környezetből érkező zavaró hatások [1],[2].

Jamming – Zavarás

A jelátvitel megzavarása, akadályozása az olvasó és a tag között valamilyen interferenciát okozó jel segítségével, az egyik legegyszerűbb megoldás arra, hogy működésképtelené tegyük az RFID rendszert. A hatékony zavarás érdekében a zavaró jelet kibocsájtó eszköznek, vagy közel kell lennie az olvasóhoz, vagy kellően nagy antennával kell rendelkeznie, vagy elég nagy energiával kell sugározni [1],[2].

Tracing – Nyomon követés

Egyes pontokon elhelyezett olvasók képesek rögzíteni az arra járó egyedi címkéket, majd ebből azonosítani a személyt, vagy azt a valamit, amin a címke megtalálható. Problémát okozhat, ha mindez az érintett fél beleegyezése nélkül következik be, mert ez személyiségi jogokat sérthet [1], [2].

Denial of Service (DoS) - túlterheléses támadás

A korszerű olvasók képesek kommunikálni nagyszámú tag-el, az olvasási terükön belül, az azonosításhoz jellemzően a tag-ek sorozatszámát

fölhasználva. Az egyidejű adatátvitel kezelésére különböző ütközés-mentesítést megvalósító protokollt használnak, a két leggyakoribb az ALOHA és a bináris fa. A támadást egy olyan speciális blokkoló tag-el hajtják végre, ami képes szimulálni annyi gyári szám kombinációt, melyet az algoritmusoknak akár évekbe is beletelhet feldolgozni. Egy ilyen támadás eredménye képen a rendszer működése lelassulhat, adott esetben teljesen leállhat [1],[2].

Relay Attack – zsebtolvajlás

Speciális támadási forma, amelyben a tag-et fizikai hozzáférés nélkül használja fel a támadó a saját céljára. Ezt a fajta támadást hívhatnánk virtuális zsebtolvajlásnak is, mely arra épít, hogy bizonyos tranzakciók nem igénylik a felhasználó visszaigazolását. Ilyen például a napjainkban egyre népszerűbb Paypass fizetési rendszer, ahol bizonyos értékhatár alatt (5000Ft) PIN kód használata nélkül fizethetünk. Ezeket a szolgáltatásokat NFC képes mobiltelefonokkal is igénybe lehet venni [1],[2].

RFID rendszereket veszélyeztető kártékony szoftverek

Férgek

A féreg egy olyan típusú vírus, ami képes saját magát reprodukálni és terjeszteni a hálózaton. Abban különböznek az egyszerű vírusoktól, hogy nem igényelnek semmilyen felhasználói aktivitást. Képesek feltérképezni a megtámadott számítógépet és tulajdonosáról hasznos információkat küldeni a támadó felé, akinek ezeken adatok birtokában már „egyszerű” dolguk van. Az RFID bázisú féreg sem igényel semmilyen felhasználói aktivitást, hanem terjed a címkével együtt, ha alkalma adódik rá. A folyamat akkor kezdődik, amint a féreg megtalálja és feltérképezi a middleware-t majd megfertőzi azt. A férgek képesek átírni a tag-eken lévő adatokat és terjeszteni magukat címkéről címkére, megfertőzve a hozzá kapcsolódó összes programot [8], [12], [13].

RFID malware

Az RFID tag-ek a middleware-t használják közvetlenül. Erőforrásuk annyira korlátozott, hogy még magukat sem képesek megvédeni. Szóval hogyan is indíthatnának támadást? Az igazság az, hogy 1Kb-nál kevesebb adat is képes lenne megtalálni a biztonsági réseket a middleware-en, ami veszélyeztethetné a számítógépet vagy akár a teljes hálózatot. A rendszer beolvasás közben a legsebezhetőbb. Ez az a folyamat, amikor egy RFID olvasó beolvassa a címkét, és arra számít, hogy tájékoztatást kap róla egy előre meghatározott formátumban. Elsődleges célpontok a nem meglelően védett, könnyen támadható felületek, mint webes felületek, adatbázisok, stb… Az RFID malware-ek egyre dinamikusabban terjednek, egyre nagyobb veszély jelentenek az RFID rendszerekre [8], [9], [10], [13].

Vírusok

Míg a férgeknek szükségük van internet kapcsolatra, egy önreplikáló vírusnak nincs. Teljesen önellátó. A támadó készít egy vírusos címkét, majd egy macska nyakörvébe helyezi el. Elviszi az orvoshoz, hogy talált egy kóbor macskát. Az orvos készít egy címkét a talált állatkának, miközben a fertőzött címke az állaton van, és készen áll arra, hogy megfertőzze az adatbázist. Ez olyan, mint egy biológiai vírus, ami képes terjedni állatról állatra. [8], [11], [12], [13].

További tervek

Több ismert hitelesítési protokoll ismert, ezek általában kulcs nélküli kriptográfiai primitívek *(véletlen sorozatok, bitenkénti műveletek, egyirányú permutációk, hash függvények, stb…)*. De léteznek különböző szimmetrikus titkosításra épülő hitelesítési protokollok is *(pl. AES)*. Napjainkban aktívan kutatott terület, az aszimmetrikus primitívek *(pl. ECC Elliptic Curve Cryptography)* alkalmazása RFID tag-ek esetén. Továbbiakban célunk a hálózati kommunikáció biztonságának növelése érdekében *(titkosítás olvasó-tag és tag-olvasó között)* a különböző hitelesítési protokollok és titkosítási eljárások behatóbb tanulmányozása. Továbbá a lehetséges, támadási módok

ellen egy egységes védelmi mechanizmusra javaslatok tétele, illetve bizonyos pontokon a védelem kidolgozása.

Összefoglalás

Cikkünkben csoportosítottuk és bemutattuk az RFID rendszereket érintő lehetséges, mind a fizikai, mind az adatokat érintő támadási módokat. Megvizsgáltuk az ellenük való védekezés lehetőségeit. Elsődlegesen az adatokat érintő támadásokkal, azon belül is a kártékonyon szoftverekkel foglalkoztunk.

Nagyon sok megoldás, megoldási javaslat született már arról, hogy lehet kivédeni ezeket a támadásokat a különféle eszközökön, vagy magában a rendszerben felismerni azt, ami nem oda való. Általánosan elmondható, hogy egy támadási fajtára többféle megoldás vagy ellenintézkedés is eszközölhető. Megállapítható, hogy a leghatékonyabb védekezési forma az autentikáció és a hitelesítés. Ez a két módszer kiszűri a támadások nagy részét, mivel azután kerül be a tag adat tartalma a rendszer körforgásába, amikor sikeresen átjutott ezen a két „akadályon”. Egy másik nagyon hatásos módszer a titkosítás, mivel a titkosított adatokat nehéz lehet megfejteni vagy egyáltalán nem is lehet. Az alkalmazások valójában a titkosítást és hitelesítést általában egyszerre használják a nagyobb biztonság érdekében.

Hivatkozott források

1. Klaus Finkenzeller: RFID HANDBOOK Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication, third edition, WILEY, ISBN: 978-0-470-69506-7
2. Mojtaba Alizadeh, Mazdak Zamani, Ali Rafiei Shahemabadi, JafarShayan, Ahmad Azarnik :A Survey on Attacks in RFID Networks
3. Qinghan Xiao1 Thomas Gibbons Hervé Lebrun: RFID Technology, Security Vulnerabilities, and Countermeasures

4. Lehtonen, M., Ostojic, D., Ilic, A. , Ilic, M.:Securing RFID systems by detecting tag cloning, Lecture Notes in Computer Science Volume 5538, 2009, pp 291-308
5. EPCglobal Inc.: Class-1 Generation-2 UHF RFID Conformance Requirements Specification v. 1.0.2. (2005).
6. Srinivas Devadas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, Vivek Khandelwal: Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications
7. Masoumeh Safkhani1, Nasour Bagheri2 and Majid Naderi: Security Analysis of a PUF based RFID Authentication Protocol
8. http://www.rfidvirus.org/
9. Rieback, M.R., Crispo, B., and Tanenbaum, A.S.: RFID Malware: Truth vs. Myth, IEEE Security and Privacy, vol. 4, pp. 70-72, July/Aug. 2006.
10. Rieback, M.R., Simpson, P.N.D., Crispo, B., and Tanenbaum, A.S.: RFID Malware: Design Principles and Examples, Pervasive and Mobile Computing (PMC) Journal, vol. 2, pp. 405-426, Elsevier, 2006.
11. Rieback, M.R., Crispo, B., Tanenbaum, A.S.: Is Your Cat Infected with a Computer Virus?, Proc. Fourth IEEE Int'l Conf. on Pervasive Computing and Commun., IEEE, pp. 169-179, 2006.
12. Mitrokotsa, A., Rieback, M., and Tanenbaum, A.S.: Classification of RFID Attacks, Proc. Int'l Workshop on RFID Technology, pp. 73-86, 2008.
13. Mitrokotsa, K., Rieback, M.R., and Tanenbaum, A.S.: Classifying RFID Attacks and Defenses, Information Systems Frontiers,

A kutatás az Európai Unió és Magyarország támogatásával, az Európai Szociális Alap társfinanszírozásával a TÁMOP 4.2.4.A/2-11-1-201-0001 azonosító számú "Nemzeti Kiválóság Program Hazai hallgatói, illetve kutatói személyi támogatást biztosító rendszer kidolgozása és működtetése konvergencia program" című kiemelt projekt keretei között valósult meg.

Szerzők

Biró Csaba
Tanársegéd, *birocs@aries.ektf.hu*
Dr. Radványi Tibor
Főiskolai docens, *dream@aries.ektf.hu*
Takács Péter
Számítástechnikus, *takip@aries.ektf.hu*
Szigetváry Péter Kari informatikus, *szigipet@aries.ektf.hu*
Eszterházy Károly Főiskola