ACTA CAROLUS ROBERTUS

Károly Róbert Főiskola tudományos közleményei
Alapítva: 2011

3 (1)

ADATBIZTONSÁG AZ RFID ALKALMAZÁSAKOR

RADVÁNYI TIBOR

Összefoglalás

Ebben a cikkben az RFID (Rádiófrekvenciás azonosítás) technológia használata által felvetett adatbiztonsági kérdések kerülnek megtárgyalásra. Milyen támadási lehetőségek vannak, és milyen védekezési lépéseket tehetünk ezek kivédésére.

Egy termék számtalan veszélynek van kitéve, ameddig a gyártótól el nem jut a fogyasztóhoz. Ez elég hosszú folyamat, amely során az áruk elveszhetnek, vagy 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. Ezek a megtakarítások számos ponton anyagi haszonra is lefordíthatók. Fontos, hogy meg tudjuk óvni rendszerünket az illetéktelen behatolókkal szemben. Ehhez meg kell ismerni a támadási lehetőségeket.

Kulcsszavak: *RFID, adatbiztonság, kriptográfia*

Data security at the application of RFID

Abstract

In this article we would like to introduce some issues in connection with the use of RFID technology (Radiofrequency Identification). What are the possibilities of getting attack are and what steps can be done to counteract them.

A product can be exposed to many hazards until it gets the consumer. During this is long process goods can get lost or stolen.

Regulations referring to most of the products in the EU are making manufactures less responsible for their products. That's why the importance of traceability is increasing – which could be the best field of using RFID. During the manufacturing process the product's way can be followed, technological orders, phases of the production, and people who took part in the production can be registered as well as any other details.

This savings then can be turned into material benefits in a lot of aspects. So it is quiet important to be able to protect own system from unauthorized intruders. We should get to know the possible ways of attacks.

Keywords: *RFID, privacy, cryptography*

Bevezetés

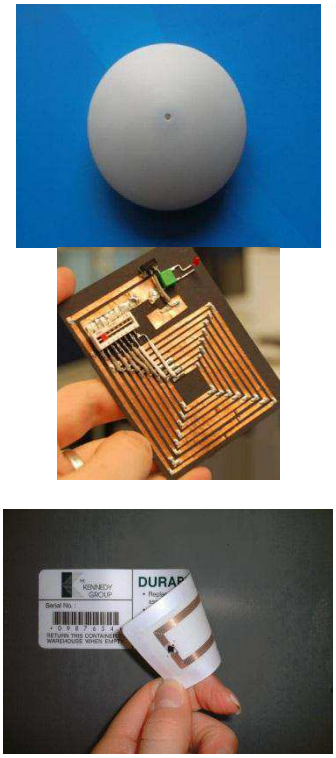
A rádiófrekvenciás azonosító technológia felhasználási lehetőségei szinte végtelenek. Az RFID technológia a manapság igen komoly helymeghatározó rendszerekkel - mint például a GPS is - kombinálva lehetővé teszi a közúti, légi és vízi szállítás teljes nyomon követését, és nem utolsó sorban ellenőrizhetővé válik annak minőségi állapota a szállítás folyamán. A postai gyors szolgáltatások nagy része e technológia előnyeinek köszönheti azt, hogy percre pontosan meg tudja állapítani, hogy mikor érkezik meg a

csomag a feladótól a címzettig, vagy, hogy éppen merre jár a kézbesítendő küldemény. 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.
Kísérletek folynak az automatizált üzletek kialakítására, illetve világszerte bevezették már a RFID alapú autópálya fizetési megoldásokat is. Az autóipar is felismerte, hogy az RFID új lehetőségeket teremthet a biztonsági megoldások területén, így manapság már a legtöbb indításgátló és elektronikus kulcs már ezzel a technológiával dolgozik. Látható, hogy szinte megszámolhatatlan azon alkalmazási területek száma, ahol nem csak használható lenne e technológia, de szükséges is volna bevezetése időmegtakarítás és a teljesítménynövelés javításának érdekében, nem beszélve arról, hogy a biztonsági-kérdések megoldása is hatékonyabbá válhatnának.

Az RFID rendszer elemei

A bélyegek

Az adatok tárolásaként funkcionáló RFID bélyegek általában egy antennából és egy mikro chipből állnak. Nagyobb funkcionalitású változataik ezeken felül rendelkezhetnek belső energiaforrással és összekapcsolhatók különféle szenzorokkal. (http://www.vonalkod.hu)



1. ábra: RFID tagek

A tag típusától függően különféle mennyiségű adatokat tárolhat néhány byte-tól akár több megabyte-ig. A tárolt adat mennyisége mindig azon múlik, hogy az alkalmazást

milyen környezetben szeretnénk használni és ehhez a környezethez milyen típusú tag illik a legjobban. A tag által tárolt adat formátuma szintén lehet többféle, de korlátozott mindaddig, amíg az olvasó és a tag képes azt kezelni.
A tag jelet fogad és küld vissza a leolvasónak. A típusok meghatározása többféle szempont szerint lehetséges: működésük elve szerint, illetve energia ellátásuk szerint, amik így lehetnek passzívak, aktívak és félig-aktívak.
A passzív transzpondereknek a működése jellemzően az alacsonyabb frekvenciatartományban van. Az LF (125kHz), HF (13,56MHz) és az UHF (860-960MHz) típusok a legelterjedtebbek. Az LF és a HF rendszerek általában induktív csatolást alkalmaznak, míg az UHF rendszerek propagation csatolást alkalmaznak. Ezért nehezebben ellenőrizhető, mert a hullámok nagyobb távolságra szóródnak szét a térben. A hullámok visszaverődnek a felületeken, és elérhetnek olyan tag-eket, amit nem is akarunk olvasni. Az LF és HF rendszerek jobban működnek fém- és folyadékfelületek közelében, mint az UHF rendszerek. Az olvasási problémák elsősorban UHF rendszereknél jelentkeznek.

Az olvasók és antennák

Az RFID-olvasó antennák kialakítása éppúgy függ egy adott alkalmazás igényeitől, mint a bélyegek esetében. Az antennákat úgy alakítják ki, hogy hatósugaruk, kivitelük, formájuk illeszkedjen az egyes alkalmazások igényeihez. Az RFID-olvasó a hozzá kapcsolt antenna, esetleg antennák segítségével létrehozott elektromágneses mezőben képes olvasni a gerjesztett bélyegek által visszasugárzott adatokat és ugyanilyen módon képes írni is ezen bélyegek memóriájába (csak az írható bélyegekébe). Az újabb olvasókba már integrálják az adatfeldolgozó szoftvert futtató egységet is, ezáltal leegyszerűsítve a kialakítandó automatikus azonosítási rendszer infrastruktúráját. Megkülönböztetünk csak olvasni képes olvasókat, olvasni és írni is képes olvasókat illetve a Smart olvasókat, melyek az adatfeldolgozó egységet is magukban foglalják.

2. ábra: RFID olvasók

A middleware

Middleware-nek nevezzük azt az elemet, ami az olvasó és a vállalati alkalmazás között helyezkedik el. A middleware kulcsfontosságú a rendszer szempontjából, mert a middleware kapja a nyers adatot az olvasótól, megszűri az adatokat, és küldi a háttéralkalmazásnak. A middleware kulcsszerepet játszik abban, hogy a megfelelő információ, a megfelelő időben a megfelelő alkalmazáshoz jusson el. Több RFID middleware alkalmazás található a piacon. Ezek mindegyike elvégzi az alapvető szűrési műveleteket, sok közülük további funkciókat nyújt. Ilyen lehet pl. az RFID olvasó felügyelete, konfigurálása, szoftver upgrade letöltések, stb. Az RFID middleware eszközök árai sok tényezőtől függ: a telepítések számától, az alkalmazás bonyolultságától, és még sok egyéb tényezőtől. A Forester Research adatai alapján az

RFID middleware rendszerek árai 183.000 és 12 milliárd US dollár között volt az elmúlt években. Az RFID alkalmazásokhoz általában külön szervert is szoktak használni, melyet ún. „edge" szervernek neveznek, mert a hálózat peremén van, ahol a digitális világ a valós világgal találkozik.

Az RFID kutatása és fejlesztése a hatékonyság növelése érdekében

Biztonság vagy hatékonyság

A mai RFID protokollokat, hogy szabályozzák a kommunikációt az RFID-olvasók és a címkék közt a teljesítmény optimalizálására fektetnek nagyobb hangsúlyt, s kevesebbet a fogyasztók adatvédelmi biztonságaira.

Javaslatot tehetünk arra, hogy a jövőben ún. titoktartó RFID protokollokat kellene alkalmazzunk annak érdekében, hogy támogassuk ezzel és tisztességes módon megőrizhessünk minden információt a rádiófrekvenciás interfészen keresztül az olvasó és a címke közt amellett, hogy a különféle feladatkörök bővítése a működés teljesítményét csupán kis mértékbe befolyásolja. Ezzel hatékonyabbá és biztonságosabbá téve a kommunikációt az azonosítás alatt. (Weis, 2005)

Mark Weiser úgy gondolta hogy akkor tudjuk megfelelően kihasználni e rendszerek képességeket ha anélkül használjuk őket hogy észrevennénk azokat.

A mai kiskereskedelmi környezetekben használatos RFID központú azonosító-követő rendszerek élő példája e rejtett működési elvnek, de ugyanakkor számos veszélyek is fennállnak eme működés miatt. Általánosságban ezt úgy képzeljük el, hogy a fogyasztók által használt személyes eszközök észrevétlen mikrochipeket tartalmaznak, s ezen keresztül finom, diszkrét ellenőrzések is végrehajthatóak egyes munkafolyamatok során. Ezen ellenőrzések folytán, mivel ilyenkor adatáramlás és adatcsere sorozatai folynak le a rendszerben, a véletleneknek köszönhetően, de leginkább a mai világ gigantikus fejlődési léptei miatt külső személyek, felhasználók is hozzájuthatnak mások személyes információihoz. Erre mutat Orwellian jövőképe is ezen rendszerekkel kapcsolatban. Ezen problémák pedig nagyon fontosak, és mielőbb megoldást igényelnek, hiszen a mai világban a személyes információk védelme a legfontosabb szempont egy számítógépes rendszer futtatása alatt. Történtek már kísérletezések e probléma orvosolására, s közülük alkalmaznak is néhányat, de néha még velük sem biztonságos a technológia.

Végül is hamar belátták azt, hogy első szempont mindig az információkezelés biztonságos és akadálymentes kezelése legyen, s a hatékonyságot ezzel a háttérbe szorították. Véleményem szerint is a legfontosabb az adatok biztonságban tartása, főként az olyan rendszerek esetében, ahol nélkülözhetetlen a titoktartás. Pl. egy banki szolgáltatás inkább legyen lassabb, és biztonságosabb, mint legyen gyors, majd nem sokkal később idegen hozzáférések miatt ismétlődő folyamatok, eljárások ezrei következzenek, amelyek nem biztos, hogy orvosolni tudják a rendszerben bekövetkezett károkat, nem beszélve vagyonunk hiányáról. (Floerkemeier)

A Economic Cooperation és Development Organizationje (OECD) által 1980-ban kiadott Fair Information Practices (FIP) egy elfogadott irányelv a felhasználók adatvédelmére. Elvük egészen a gyökerekig nyúlnak le, leírja az információ közlés átvitelének és az ezzel kapcsolatos korlátokat az egyes tagállamok között. A következő elvek nyolc pontban foglalhatóak össze:

1. *Gyűjteménykorlátozás*: az adatgyűjtő csak összegyűjti a szükséges információkat és ehhez az érintett teljes jogú beleegyezése szükséges.
2. *Az adatok minősége*: az eltárolt adatokat rendszeresen frissíteni kell majd a frissített állományt el kell tárolni.

3. *A cél meghatározása*: meg kell határoznunk a célunkat, vagyis hogy az eltárolt, esetlegesen bejelentett információkkal mit szeretnénk elvégezni, milyen céljaink vannak velük kapcsolatosan.
4. *Felhasználói korlátozás*, megszorítás: az adott alkalmazás csak akkor hajtható végre a megfelelő adatokkal, ha abban az érintett teljes jogú beleegyezését nem adta.
5. *Biztonsági véd intézkedések*: szigorú védelmet kell biztosítani az adatok tárolásánál bármilyen illetéktelen, jogosulatlan hozzáféréstől vagy annak nyilvánosságra hozásáról.
6. *Nyitottság*: biztosítani kell az érintett személyeknek bármilyen problémakezelés esetén, hogy kapcsolatba léphessenek az adatkezelővel.
7. *Egyéni részvétel*:az érintett személyek számára lehetővé kell tenni a adatainak teljes körű hozzáférését, tehát például az adatmódosítás vagy adatlekédezés megoldható legyen.
8. *Felelősségre vonhatóság*:ezen elvek betartásáért az adatkezelőknek felelősséget kell vállalniuk.

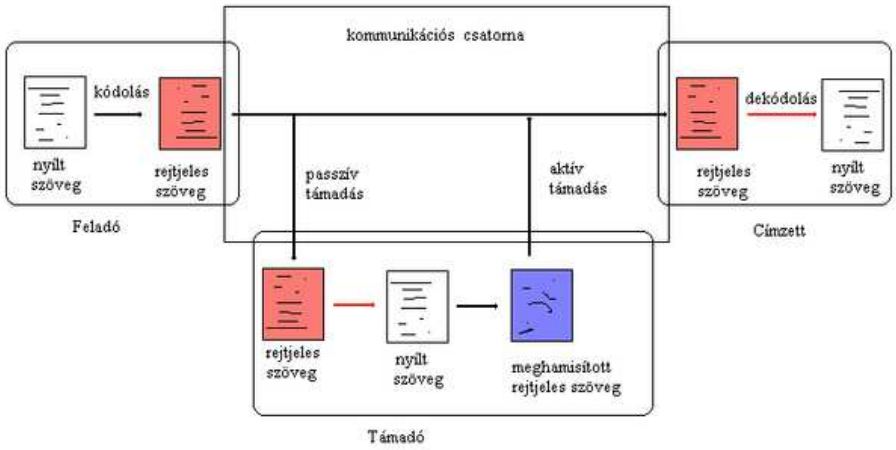
Láthatjuk, hogy a hatékonyság kérdéskörei háttérbe szorultak, de azért ezen területen is történtek, és máig is folynak fejlesztések.

RFID támadások és védekezés

Az üzleti előnyök mellett az RFID technológia napjainkban tömegessé váló használata újabb biztonsági aggályokat is felvet. A chipek távoli, általunk nem érzékelt ki-olvasásával kémkedhetnek, személyes adatokat gyűjthetnek rólunk, akár mozgásunkat is részletesen feltérképezhetik. Szintén gondot okozhat az RFID alapú személyi azonosítás, amelyet épületek, termek, szobák, vagy akár járművek, eszközök védelméhez rendelhetnek. A köztesszoftver gyengeségeit (verem túlcsordulás, szkript nyelvek), valamint az adatbázisokba történő rosszindulatú "kódfecskendezés" lehetőségét használhatják ki. (Junichiro, 2006; Hee-Jin, 2007)

Főbb támadási lehetőségek

Algoritmikus támadások: az átviteli csatornán hajtja végre a támadó. Itt is megkülönböztetünk aktív és passzív támadási módszereket. A passzív módszer alapvető jellemzője, hogy a támadó a nyilvános csatorna lehallgatásával rejtett szövegű üzenetek birtokába jut. A passzív támadásokkal szemben az aktív támadás jellemzője, hogy a támadó maga is forgalmaz a csatornán. (Moore, 2004)



3. ábra: Aktív támadás a kommunikációs csatornán

Elárasztás: Denial of Service (röviden DoS), egy szervert olyan sok kéréssel bombáznak, hogy a rendszer a feladatokat egyszerűen nem képes ellátni, és legrosszabb esetben összeomlik.
Ennek egy este a szinkronizációs elárasztás, mely a TCP/IP protokoll kapcsolatkiépítése során a SYN és ACK csomagok cseréjét használja elárasztásra.

Biztonsági célok

A rejtjelezés alapvetően a passzív támadások ellen véd, az aktív támadások elleni védekezéshez kriptográfiai protokollokat használunk, ami előre meghatározott üzenetcsere-folyamatot jelent. Ennek során észleljük az aktív támadásokat, és kivédjük azok káros következményét.
A publikált protokolloknak sok közös vonásuk van. (McLoone and Robshaw, 2008) Fő lépéseik:

1. Az olvasó kérést sugároz a tag-nek
2. A tag azonosítja magát az olvasónak (megadja a tárolt adatokat)
3. Az olvasó továbbítja az adatokat a háttér szervernek
4. A szerver adatbázisa alapján feldolgozza az adatokat
5. A szerver elküldi a hitelesítést és a feldolgozott adatot

A különbség a különböző szinteken kriptográfiai primitívek alkalmazásában van. (Shindu, 2005) A tag hash-seli az adatokat mielőtt továbbítja az olvasónak. A háttér szerver a közös kulccsal visszafejti az üzenetet, adatbázisában megkeresi és feldolgozza azt.

Összegzés

Ma már sok területen előnyben részesítik az új technológiát a hagyományossal (pl. vonalkód) szemben. Egyre nő az elterjedése, az új igényeknek köszönhetően új fejlesztések, kutatások indulnak, és ennek eredményeképpen új termékeket gyártanak. Új technológiák, alkalmazási területek jelennek meg, sokszor sci-fi-be illő elképzelésekkel. Már az emberbe ültetett RFID nem csupán nincs messze, hanem megvalósult.
A fejlesztések néhány konkrét terv köré koncentrálódnak: vékony, nyomtatható kártyák, megnövelt biztonság, csoportos programozási lehetőség, nagyobb memóriakapacitás, fejlett ütközésfeloldó algoritmusok stb.

Az RFID technológia gyorsan fejlődik, és várható, hogy hatékonyabb lesz, teljesítménye még tovább növekszik, funkcióinak száma még tovább bővül, és az ára is lejjebb megy. Az élet számos területére befolyással van, és lesz még.
De vajon mely területeket fog meghódítani?
Az egyik lehetséges válasz a mobil forrásgazdálkodás. Ezzel az aktív és passzív RFID-technológiát egyaránt hasznosító rendszerrel személyek, munkafolyamatok, újrafelhasználható tárolók és járművek egyaránt nyomon követhetők egy zárt ellátási láncban. Például a legtöbb egyesült államokbeli cég a többször felhasználható konténerek négy-tizenöt százalékát veszíti el. Az azonosítók segítségével pontosan tudhatjuk, hol vannak a tárolóink, így megelőzhetjük elvesztésüket.
A másik lehetséges fejlődési irány az aktív, többször felhasználható RFID-cimkéké lesz. Ilyeneket már használnak például a Fordnál a kész járművek elosztásában. A gyártósorról legördülő kocsik visszapillantó tükrére helyezik a címkét, mielőtt az a trélerre kerülne. A szállítmányoknak az üzem területén töltött várakozási ideje öt napról félnapra csökkent. Amióta bevezették a rendszert, gyakorlatilag nincsenek ismert hibával kikerülő gépkocsik.

Hivatkozott források:

Weis, S. A. (2005): Security Parallels Between People and Pervasive Devices, USA 2005 - security
Floerkemeier, C., Schneider, R., Langheinrich, M.: Scanning with a Purpose
Moore, B. (2004): Recognize the Lies about the RFID, Material Handling Management, 2004
Vonalkód Rendszerház Rendszerfejlesztõ, Tanácsadó és Kereskedelmi Kft. honlapja: http://www.vonalkod.hu
Saito, J., Ryou, J. C., Sakurai, K. (2006) (Chungnam National University): Enhancing privacy of Universal Re-encryption scheme for RFID tags 2006
Chae, H. J., Yeager, D. J. Smith, J. R., Fu, K.(2007) (University of Massachusetts): Maximalist Cryptography and Computation on the WISP UHF RFID Tag 2007
Karthikeyan, S., Nesterenko, M.Kent State University(2005): RFID Security without Extensive Cryptography
McLoone, M., Robshaw, M. J .B. (Queen's University, Belfast, U.K.)(2008): Public Key Cryptography and RFID Tags 2008

Szerző

Radványi Tibor, PhD
adjunktus
Eszterházy Károly Főiskola
Matematikai és Informatikai Intézet
radvanyi.tibor@ektf.hu