HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Papp Zoltán
pappz.szeged@gmail.com

AZ ÚJ TECHNOLÓGIÁK VESZÉLYEI: RFID ÉS AZ ELEKTRONIKUS ÚTLEVÉL

Absztrakt

A tudomány és technika legújabb vívmányai szinte észrevétlenül jelennek meg a társadalom hétköznapjaiban, anélkül, hogy ezek jelenléte a felhasználókban tudatosulna. Úgy használják, hogy tisztában lennének a működés elveivel, technikai hátterével, így az új szolgáltatások előnyeit anélkül élvezik, hogy az alkalmazás esetleges veszélyei nem válnak ismertté előttük, ami a visszaélések elleni védekezés hatékonyságára is negatív hatással van. A cikkben a szerző egy, az élet szinte minden területén egyre nagyobb teret nyerő új technológiát, az RFID-t és annak veszélyeit mutatja be.

The latest achievements of science and technology become a part of everyday life in our society, without the users being really aware of their presence. They use them without properly knowing the principles of their operation, technological background so they enjoy the benefits of the new services without becoming aware of the potential threats lying in their applications, which has a negative impact on the efficiency of protection against abuse. In this article, the author presents RFID, a new technology that gains an increasing role in nearly all areas of life, as well as its risks.

Kulcsszavak: *RFID, terrorizmus, elektronikus útlevél, terrorism, electronic passport*

Napjainkban világszerte egyre nagyobb hangsúlyt fektetnek a terrorellenes küzdelemre, melyek érdekében újabb és újabb biztonsági intézkedéseket foganatosítanak, illetve újabb és újabb technológiákat vetnek be, melyektől a fejlett országok kormányzatai a biztonsági helyzet javulását remélik. A várakozások szerint ezekkel az új intézkedésekkel és az új eszközökkel a terrorcselekmények potenciális elkövetői kiszűrhetők, országhatárokon történő mozgásuk és tevékenységük akadályozható. A közvélemény azonban ezeket a szabályokat, illetve technológiákat sok esetben kényszerintézkedésként éli meg, mivel személyes

szabadságjogaik és személyes adataik védelmének korlátozását látják bennük, ami csökkenti a bevezetett technológiák támogatottságát a társadalom körében. A hatóságok eszköztárában egyik ilyen újdonság az elektronikus adatokkal ellátott útlevél lett.

Az útlevél egyik borítólapjába egy úgynevezett RFID chip-et tartalmazó lemezkét ültetnek be, amelyet a külső oldal felől, a papír-műanyag kompozit borítóba elhelyezett árnyékoló fémháló véd az illetéktelen letapogatás ellen. Az útlevelekbe beépített chip a szokásos, a vizuálisan is megjelenítethető adatokon túl a tulajdonos más biometriai adatait is tárolhatja, melyek tipikusan a fénykép, az ujjlenyomat, valamint a retinalenyomat lehet, melyek alapján ki lehet jelenteni, hogy egy ilyen típusú útlevél egy adott személyt teljes hitelességgel tud azonosítani.

1. ábra. Az RFID chip egy lehetséges elhelyezkedése az útlevélben
(forrás: www.meritummedia.com)

Az RFID rövidítést a Radio Frequency Identification (rádiófrekvenciás azonosítás) szavak kezdőbetűiből képezték, és az egyedi azonosító technológiák (AUTO ID) családjába tartozik, hasonlóan a vonalkódokhoz, csak épp működési elvében tér el. Ez egy olyan automatikus azonosításhoz és adatközléshez egyaránt használt technológia, melynek lényege adatok tárolása és továbbítása RFID címkék és jelolvasó eszközök segítségével.

Az RFID elvének megszületése a II. Világháború idejére tehető, amikor a radart feltaláló Sir Robert Watson-Watt vezetésével egy titkos projekt keretében a britek kifejlesztették az első aktív saját-repülőgép felismerő rendszert. Ennek előzménye az volt, hogy a radar rendszerek katonai felhasználását nagyban nehezítette, hogy a radarképernyőn megjelenő repülőgépekről a légvédelem nem tudta eldönteni, hogy melyik katonai erőhöz tartoznak, ami folyamatosan megnehezítette a radar készülékek adatainak értelmezését, illetve lehetetlenné tette a hatékony légvédelmi reagálást. A németek észlelték először, hogy amikor a pilóta billegteti a repülőgép szárnyait, a gépről visszaverődő rádióhullámok által a monitoron megjelenő kijelzések megváltoznak. Ez a kezdetleges módszer nevezhető az első passzív RFID rendszernek, mely alkalmas volt egy objektum azonosítására. A britek tovább fejlesztve az alapelgondolást egy adót helyeztek el saját légierejük gépeire, mely amint jeleket vett a hazai földi radarállomástól egyedi azonosító jeleket kezdett visszasugározni, majd ezt a jelet a földi állomás érzékelve sajátként azonosította a repülőgépet. Ezzel a britek megalkották az első aktív saját repülőgép

felismerő rendszert (IFF - Identify Friend or Foe). Az aktív RFID rendszerek azonosításának elve gyakorlatilag pontosan ugyanez [1].

A chip köré épített áramkör a bejövő rádióhullámokból indukál áramot, így gyakorlatilag a leolvasó hozza működésbe az eszközt, és a benne lévő adatokat az egyben antennaként is funkcionáló áramkörön keresztül sugározza vissza a leolvasó egységnek. Az adatok általában egyszer kerülnek betöltésre, később már nem írhatóak át, azaz a leggyakrabban használt chip-típus az egyszer-használatos, eldobható. Az RFID címkéknek több típusa van, közös jellemzőjük, hogy rendelkeznek antennával. A címkéket elsősorban energiaellátásuk alapján különböztetik meg [2]:

- Passzív RFID

  A passzív címkék nem tartalmaznak saját energiaforrást. Az olvasó által kibocsátott rádiófrekvenciás jel elegendő áramot indukál az antennában ahhoz, hogy a lapra épített apró, CMOS technológiával készült integrált áramkör feléledjen, és választ küldjön az adatkérésre. Az antenna tehát speciális tervezést igényel: nem elég, hogy összegyűjti a szükséges energiát, a válaszjelet is közvetítenie kell. A válaszjel általában egy egyedi azonosítószám, de előfordul, hogy a címke egy kisméretű memóriát is tartalmaz, ami lekérdezéskor ennek tartalmát is továbbítja az olvasó felé. Passzív címkék 125 kHz, 13,56 MHz, és UHF (860-960 MHz) tartományban működnek. Némely rendszer a 2,45 GHz-es sávot illetve egyéb sávot is használhat. A passzív lapkák rendkívül kisméretűek, jelenleg 0.4x0.4 milliméteres felületű, papírnál is vékonyabb címke a kereskedelemben kapható legkisebb darab. A passzív lapok hatótávolsága néhány méterig terjed, azaz ekkora távolságból olvasható ki a tartalmuk a használt frekvenciától függően. Alacsony előállítási költségének köszönhetően jelenleg ez a legelterjedtebb típus.

- Fél-passzív RFID

  A fél-passzív azonosítók annyiban térnek el a passzív társaiktól, hogy tartalmaznak egy apró, beépített elemet. Ez lehetővé teszi, hogy az integrált áramkör folyamatosan üzemeljen. Nincs szükség az antenna energiagyűjtő kialakítására, ezért azt adásra optimalizálják. Ennek köszönhető, hogy az ilyen típusú azonosítók válaszideje jobb, és az olvasási hibák aránya kisebb, mint passzív társaik esetén.

- Aktív RFID

  Az aktív RFID címkék vagy jeladók beépített energiaforrással rendelkeznek, melyek elegendő energiát biztosítanak bármilyen integrált áramkör üzemeltetéséhez és magához a jeladáshoz is. Nagyobb hatótávolságot és memóriakapacitást biztosíthatnak passzív változatuknál, némelyik még a vevő által küldött adatok rögzítésére is képes. A használt frekvencia általában 455 MHz, 2,45 GHz vagy 5,8 GHz és az olvasási távolság általában 20-100 méter. Néhány aktív címke impulzusszerűen üzemel, hogy takarékoskodjon az energiával, így akár 10 évig is képes üzemelni. A jelenleg kapható legkisebb aktív RFID jelző nagyjából fémpénz méretű.

A szakirodalomban elterjedten használják még a működési frekvencia szerinti csoportosítást is [3]:

- LF 125 kHz

  E frekvenciával működő chipek olvasási távolsága 0,5 méternél kisebb, energiaellátásuk alapján általában passzív (induktív csatolás) kategóriába sorolhatók. Hátránya, hogy még nagy mennyiségben gyártva is relatíve drágának számít, mivel az alacsony frekvencia drága rezet igényel. Legelterjedtebben beléptető rendszerekben, állatok nyomkövetésében, járművek indításgátlóiban alkalmazzák.

- HF 13,56 MHz

  Ezen a frekvencián működő chipeknek általában 1 méter az olvasási távolsága, túlnyomórészt passzív (induktív vagy kapacitív csatolás) energiaellátásúak. Előnye, hogy előállításuk olcsóbb az LF chipekénél. Tipikusan Smart-Card-ok és termék nyomkövetés esetében alkalmazzák.

- UHF 868-915 MHz

  E tartományban üzemelő chipeknek maximális olvasási távolsága 3 méter. Az aktív működésű chipek általában elemmel működnek, míg a passzívak kapacitív csatolásúak. Előnye, hogy az IC technológia fejlődése révén olcsóbb mind az LF, mind a HF chipeknél, illetve sok chip párhuzamos olvasásának esetében is megbízható. Fő felhasználási területük raklap és konténer nyomkövetés, csomagkezelés és díjfizető rendszerek.

- Mikrohullám 2,45 GHz és 5,8 GHz

  Ezen a magas frekvenciatartományban működő chipek olvasási távolsága 1 méter. Energiaellátásuk hasonló az UHF chipekéhez, az aktív chipek elemmel működnek, míg a passzívak kapacitív csatolásúak. Az UHF-hez hasonló olvasási karakterisztikával rendelkezik. Főleg ellátási láncokban és díjfizetési rendszerekben alkalmazzák.

Az RFID technológia fontos eleme az olvasó, melynek mérete, kivitelezése nagyban függ attól, hogy milyen funkcionalitással bírnak. Léteznek „buta” olvasók, korlátozott számítási képességekkel, és „okos” olvasók, melyek már beépített számítógépet tartalmaznak, így képesek az adatokat szűrni, tárolni, illetve különböző parancsokat végrehajtani. A gyors olvasók képesek többféle protokollal kommunikálni a chipekkel, továbbá léteznek olyan multi-frekvenciás olvasók is, melyek különböző frekvenciájú chipeket képesek olvasni.

Az RFID olvasók külső, illetve belső antennával egyaránt rendelkezhetnek. A külső antennával rendelkező RFID olvasókhoz egy, vagy akár több porton keresztül csatlakoztatható az antenna. Az olvasó rendelkezhet bemeneti és kimeneti portokkal, amelyeken keresztül külső eszközök csatlakoztathatók. Az olvasó rendelkezhet egyéb portokkal, amelyeken keresztül számítógéphez vagy hálózathoz csatlakoztatható. A régebbi típusú olvasók soros porttal rendelkeznek, azonban a legtöbb új típusú olvasó már USB, Ethernet, vagy akár Wi-Fi portokkal rendelkezik [3].

Az RFID chipeknek más technológiákkal szembeni nagy előnye, hogy tetszőleges helyen rögzíthetők, vagy akár be is építhetők az azonosítani kívánt objektumba, ami lehet tárgy, például egy árucikk, vagy alkatrész, illetve lehet élőlény is, így akár egy ember is. Már RFID

címkéket használnak a nagy logisztikai cégek, alkatrész raktárak, áruházak stb. a vonalkód helyett, hiszen így a különböző tárgyakon nem kell megkeresni a vonalkód helyét az azonosításhoz, ami jelentős időmegtakarítással jár. A gyorsaság mellett további nagy előny, hogy olcsó is, és a parányi méretéből adódóan egészen apró tárgyak azonosítására is alkalmas [4].

Az útlevelek esetében kizárólag a passzív chipeket használják, melyek – mint a bevezetőben már megemlítésre került – a vizuálisan is megjelenítethető adatokon kívül az okmány tulajdonosának más biometriai adatait is tárolhatja. A terrorfenyegetettségre hivatkozva a fejlett világ egyre több országa döntött az ePassport, vagyis az RFID chip-et tartalmazó elektronikus útlevél alkalmazása mellett, ami alól az Európai Unió tagállamai sem kivételek, így már Magyarországon is bevezetésre került ez a technológia.

Az érintett országok az új okmányok bevezetésére óriási pénzösszegeket áldoztak, ami azonban a szakértők véleménye szerint nem áll arányban a technológia által nyújtott biztonsággal. Már a bevezetés megkezdése előtt informatikai szakértők jelezték, hogy a technológia biztonsága korántsem akkora, mint azt a bevezető országok próbálják meg elhitetni állampolgáraikkal. Az e-útlevél gyengesége pontosan az, aminek érdekében az RFID technológiát kitalálták: egy adatszolgáltató rendszer, amely kérésre készségesen kiadja az érintettek személyes adatait, például vámvizsgálatnál, a repülőtereken, illetve más hivatalokban. A Nemzetközi Polgári Repülési Szervezet (ICAO) az elektronikus útlevél használatával kapcsolatosan ajánlásokat is megfogalmazott, mivel a kételkedő szakértőkhöz hasonlóan a szervezet sem osztotta a bevezetés mellett döntő országok optimizmusát, mely szerint az új típusú útlevél majd drasztikusan képes lesz csökkenti a visszaélések számát.

Az elektronikus útlevelek használatának metódusa nem tér el a chip nélküli okmányokétól. Határátlépéskor a hivatalnok a kinyitott útlevelet vizuálisan ellenőrzi, miközben az utas ujjlenyomatát az ujjlenyomat olvasómodulon keresztül beszkenneli egy számítógép. Magasabb fokú biztonság esetén egy kamera a szivárványhártya mintázatát is rögzítheti. A nyitott útlevél RFID chipjéből eközben a gép kiolvassa az információkat, melyeket összevet a szkennelt adatokkal, a hivatalnoknak egy képernyőre kivetíti az útlevél tulajdonosának fényképét, aki pedig eldönti, hogy az utas arca azonos-e a szkennelt fényképpel. Ez a procedúra szinte nem is vesz igénybe többlet időt a hagyományos útlevél ellenőrzéséhez képest.

Közelebbről megvizsgálva a technológiát, illetve annak felhasználási módját, az RFID chippel ellátott útlevél már közel sem tűnik olyan biztonságosnak. Egy nemzetközi konferencián egy Lukas Grünwald nevű német hecker az általa két hét alatt kidolgozott módszer segítségével saját útlevelén mutatta be, hogy teljesen legálisan és könnyen beszerezhető eszközökkel – laptop, RFID chipolvasó, üres RFID chip, chip-író – az útlevél adatai egy üres útlevél chipjére pillanatok alatt rögzíthetők.

Részleges biztonságot jelent az a tény, hogy az eredeti chip adatai nem írhatók át, tehát az ellopott, elvesztett útlevelet nem tudják közvetlenül felhasználni más személy biometriai adataival, viszont a tulajdonos személyiségét ellophatják. Ez azok számára lehet értékes zsákmány, akik valamilyen tiltólistán szerepelnek (például beutazási és tartózkodási tilalom alá esnek), viszont a megszerzett adatokkal a szabad mozgás lehetősége megnyílik számukra. Egy kis gondatlanságot, biztonsági rést kihasználva idegen adatokkal és egy kis szerencsével átjuthatnak az ellenőrzéseken.

Valójában azonban arra sincs szükség, hogy megszerezzék a kérdéses útlevelet. Akár egy táskába rejtett, megfelelő érzékenységű RFID olvasó segítségével gyakorlatilag észrevétlenül hozzájuthatnak az adatokhoz. Csak annyit kell tenni, hogy az olvasót a „hivatalos" olvasó közelébe kell jutatni. Amikor az útlevél kisugározza az adatokat a „titkos" olvasó, - ha megfelelő távolságon belül van - szintén veszi és rögzíti azokat. Ezután akár a helyszínen egy gépkocsiban, vagy mosdóban is megírható az új chip, a kérdéses útlevél elektronikus klónja. A klónozási eljárás legnehezebb pontja talán az üres RFID chippel rendelkező biankó útlevél megszerzése, vagy egy hamisított útlevélben a chip és a fénykép kicserélése.

Az elmúlt idők tapasztalatai azt mutatják, hogy a terroristák minden, számukra elérhető eszközt igyekeznek felhasználni akcióik végrehajtása során. A terrorszervezetek fiatalabb generációinak felnövésével arra lehet számítani, hogy az új technológiákra elődeiknél már jóval fogékonyabb fanatikus fiatalok jelentősen ki fogják bővíteni a terrorizmus eszköztárát. E generációnak már nem jelent problémát a számítástechnika, a programozás, a telekommunikáció. Az RFID technológia esetében nem a klónozás egyszerűsége az egyetlen veszélyforrás. Az említett konferencián a Flexilis Inc. munkatársai bemutattak egy videofilmet, amely egy megdöbbentő kísérletet rögzítettek. A jelenlegi, nem megfelelő árnyékolással rendelkező útlevélmodell nem mindig rejti el az adatokat. Amennyiben táskában, zsebben kicsit megnyitva van az útlevél, annak adatai már kiolvashatók. A videofilm azt mutatta be, amint egy bábu zsebébe helyezett útlevél adatait egy szemeteskukába rejtett leolvasó kiolvasta, majd az adatok alapján egy detonátort indított el.

Azonban egy RFID olvasó beállítható oly módon is, hogy akár csak egy nemzet útleveleire, vagy akár egyetlen kiválasztott személynek az adataira adjon jelet a detonátornak. Különböző megfontolásokból (például parkolási és autópálya díjbeszedés, sorompók mozgatása) ma már RFID chipeket szerelnek a járművekre is, így a fenti példához hasonlóan támadhatóak ezek is. Ettől kezdve a bombák akár személyre, járműre, illetve különböző tárgyakra is szabhatók.

A közeljövőben várható, hogy az Európai Unió több tagállama fog rendszeresíteni különböző, RFID technológiára épülő személyi azonosító kártyákat (például személyazonossági igazolványt), melyeknek az árnyékolása még annyira sincs megoldva, mint az útleveleké, így ezekből az adatok még könnyebben, még messzebbről kiolvashatóvá válnak. Fantáziánkat szabadra engedve azt is elképzelhetjük, hogy a nem túl távoli jövőben egy állampolgár egy ilyen személyi okmánnyal a zsebében belép egy épületbe, ahol már az ajtóban nevén köszöntik, majd személyére szabott információkat kap egy kijelzőn. A kiolvasott információk birtokában egy számítógép akár azt is könnyen meghatározhatja, hogy a chip birtokosa melyik marketing-célcsoportba tartozik, így annak a piaci szegmensnek szánt multimédiás reklámot közvetíti.

Az RFID azonosítási technológia terjedése megállíthatatlan, az élet egyre több területén (raktározás, gyártás-ütemezés, biztonsági beléptető-rendszerek, postai és futárszolgálatok, légi szállítás, tömegközlekedés, elektronikus fizetőkártyák, háziállatok azonosítása) alkalmazzák. Népszerűségét jelezheti az is, hogy 2006-ban az Egyesült Államokban, a Kaliforniai Egyetemen már RFID felsőfokú képzést is indítottak. Az RFID technológián alapuló azonosítási rendszerek tulajdonságaiból, alkalmazási területeiből szinte törvényszerűen következnek a jogvédők aggályai is, akik látomása szerint, ha a kormányzat vagy a multinacionális cégek megfelelő szenzorokat helyeznek el az utcákon, különböző épületekben, járműveken akkor nyomon követhetővé válnak az állampolgárok, felderíthetővé válnak szokásaik, az általuk fogyasztott termékek, baráti vagy tágabb ismeretségi körük. Az RFID és más új azonosítási technológiák a jogvédők megítélése szerint közelebb hozzák

George Orwell 1984 című regényében már vizionált, a „Nagy Testvér szemmel tart” jelmondat valósággá válását.

Összegzés

A tudomány területéről a hétköznapokba beszivárgó új technológiák értelemszerűen a társadalom szélesebb köre, a biztonsági szakterület és a gazdasági szektor számára is előnyökkel bírnak, az emberek kényelmét, a szolgáltatások színvonalát, a termelékenységét-költséghatékonyságot, vagy épp az ellátás biztonságát növelik, így elterjedésük megállíthatatlan. Azonban ezeknek a technológiáknak nem körültekintő felhasználása, vagy épp az alaprendeltetéstől merőben idegen területen történő alkalmazása, arra való ráerőltetése során olyan nem kívánt mellékhatások is jelentkezhetnek, melyek a technológiák által nyújtott előnyöket kérdésessé teszik. A cikkben vázolt példa is ezt támasztja alá, az elektronikus okmányok terjedése összességében növeli a társadalom biztonságát, azonban a személyes adatok biztonsága területén pedig mind az állam, mind pedig a bűnözők számára kiszolgáltatottá teszi az egyént.

Irodalomjegyzék

[1.] Vonalkód Centrum – Az RFID technológiáról (letöltve 2010. szeptember 15. (http://www.vonalkodcentrum.hu/index.php?page=234))

[2.] Wikipedia (letöltve 2010. szeptember 17. (http://hu.wikipedia.org/wiki/RFID))

[3.] BCS Hungary RFID Tudástár (letöltve 2010. december 4. (http://www.bcs.hu/hu/tudastar/tudastar_centrum/rfid_tudastar/))

[4.] Turcsán Tamás - RFID - Mi mindent lát a Nagy Testvér? (letöltve 2010. szeptember 16. (http://nonstopuzlet.hu/rfid-mi-mindent-lat-a-nagytestver-20090216.html))