HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

RFID identifikacija

CCERT-PUBDOC-2007-01-179

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

RFID (eng. *Radio Frequency Identification*) je naziv za tehnologije koje koriste radio valove kako bi automatski identificirali objekte. Radiofrekvencijska komunikacija temelji se na stvaranju elektromagnetskih valova u odašiljačima i njihovom otkrivanju na udaljenom prijamniku. Postoji nekoliko metoda identifikacije objekata, no najčešća je pohranjivanje identifikacijskog serijskog broja ili neke druge informacije na mikročip koji zajedno s antenom čini RFID transponder. Transponder komunicira s čitačem putem radio signala, jednosmjerno ili dvosmjerno, a čitač je povezan s računalom ili računalnom mrežom na kojemu se nalazi baza podataka. Jednostavna identifikacijska oznaka pohranjena na transponderu u ovoj bazi povezana je s informacijama o označenom proizvodu.
Velika raznolikost RFID sustava omogućuje izrazito velik broj primjena, koji s vremenom i tehnološkim napretkom sve brže raste. Ugrađivanje RFID transpondera u doslovno sve što okružuje ljude, od donjeg rublja, preko automobila i vlakova do kućnih ljubimaca pa i u same ljude, obećava brojne pogodnosti i nove, do sada neslućene, mogućnosti lagodnijeg i efikasnijeg obavljanja svih svakodnevnih poslova. Fleksibilnost i sveprisutnost RFID sustava ne omogućuju samo velik broj primjena već otvaraju vrata i brojnim mogućnostima zlouporabe.
U nastavku dokumenta opisan je povijesni razvoj RFID sustava, dan je pregled komponenti koje ih sačinjavaju, navedene su neke sadašnje i moguće buduće primjene te su ukratko opisane ranjivosti i sigurnosni elementi.

2. Povijesni razvoj RFID sustava

Povijest RFID sustava započinje 1939. godine kada su Britanci konstruirali IFF (eng. *Identification Friend or Foe*) sustav za identifikaciju zrakoplova. Ovaj sustav sastoji se od radarskog sustava na tlu koji komunicira s transponderom (uređaj koji nakon primitka određenog signala emitira svoj signal – eng. *trans(mitter) + (res)ponder*) smještenim na zrakoplovu. SSR (eng. *Secondary Surveillance Radar*) sustavi temeljeni na ovoj tehnologiji danas se koriste u civilnom zrakoplovstvu.
Godine 1946. Léona Theremina je za Sovjetsku vladu konstruirao špijunski uređaj koji, koristeći pasivnu elektromagnetsku indukciju, odašilje signal sa zvučnim zapisom. Vibracije zvučnih valova preko dijafragme neznatno mijenjaju oblik rezonatora i tako moduliraju frekvenciju reflektiranog radio signala. Iako ovo nije identifikacijska oznaka već pasivni prislušni uređaj, tehnološki predstavlja prethodnika RFID sustava.
Člankom naslova "*Communication by Means of Reflected Power*" (*Proceedings of IRE*, pp 1196-1204, 1948) Harry Stockman je postavio temelje razvoja RFID sustava i predvidio značajne istraživačke i razvojne napore prije no što ova tehnologija dođe u uporabu.
Patent Marca Cardulla iz 1973. godine predstavlja prvi moderni RFID sustav. Radi se o pasivnom radio transponderu s memorijom. Prvotni uređaj demonstriran je 1971. godine New York Port Authority lučkoj kapetaniji. Imao je 16 bita memorije i namjena mu je bila naplaćivanje pristojbi. Izvorni poslovni plan iznesen ulagačima 1969. godine najavljivao je uporabu uređaja u transportu (identifikacija vozila, naplata pristojbi, usmjeravanje i nadgledanje vozila), bankarstvu (elektronička čekovna knjižica i kreditna kartica), osiguranju (identifikacija osoba, automatizirana vrata, nadgledanje) i medicini (identifikacija, povijest pacijenata).
Godine 1973. izvršena je prva demonstracija modernih reflektivnih (eng. *backscatter*) RFID sustava u Los Alamos Scientific Laboratory laboratoriju.

3. RFID transponderi

Dvije osnovne komponente RFID transpondera su mikročip i antena koji su najčešće zaliveni u kućište otporno na utjecaj okoline. Mikročip sadrži radio prijamnik, radio modulator za slanje odgovora čitaču, upravljačku logiku, memoriju i sustav za upravljanje napajanjem.
Transpondere je u skupine moguće podijeliti prema:

- načinu napajanja:
    1. pasivni,
    2. djelomično aktivni,
    3. aktivni,
- mogućnosti programiranja:
    1. transponderi koje je moguće samo čitati – u procesu proizvodnje dobivaju jedinstven serijski broj koji nije moguće promijeniti,
    2. transponderi koji omogućuju jednostruko programiranje – prvi puta zapisani podaci trajno ostaju na transponderu,
    3. transponderi s mogućnošću višestrukog programiranja – obično imaju jedinstven i trajan serijski broj kojemu se nadodaju zapisivani podaci, a koriste se u zahtjevnijim primjenama,
- korištenim frekvencijama:
    1. niske frekvencije (oko 125 kHz),
    2. visoke frekvencije (13.56 MHz),
    3. ultravisoke frekvencije (UHF – 860 do 960 MHz),
    4. mikrovalne frekvencije (2.45 GHz),
- fizičkoj izvedbi:
    1. RFID etikete (eng. *tag*),
    2. RFID naljepnice,
    3. RFID tiskane pločice.

Domet signala RFID transpondera prije svega je vezan uz korištenu frekvenciju, ali i uz vrstu napajanja. Tako je tipičan domet transpondera koji radi na niskim frekvencijama do 30 cm, na visokim

frekvencijama do 1 m, a na UHF (eng. *Ultra High Frequency*) frekvencijama do 6 m. Upotrebom aktivnih, baterijski napajanih, izvedbi transpondera navedeni dometi mogu se povećati.
Potrošnja energije i sposobnost emitiranja signala također uvelike ovise o frekvenciji na kojoj transponder radi. Tako niskofrekvencijski transponderi troše manje energije i imaju veću sposobnost emitiranja signala kroz razne materijale od UHF transpondera, koji su ujedno i skuplji. Glavne prednosti UHF transpondera su veći domet i brži protok podataka.
Nekoliko tvrtki radi na razvoju RFID transpondera od polimerskim poluvodiča, kao zamjenu za današnje silikonske transpondere. Njemačka tvrtka PolyIC i nizozemska tvrtka Philips 2005. godine demonstrirale su rad jednostavnih tiskanih polimerskih transpondera na frekvenciji 13.56 MHz. U slučaju uspješne komercijalizacije, polimerski transponderi bit će tiskani u rolama i mnogo jeftiniji od današnjih silikonskih transpondera. Tehnološki napredak i masovna proizvodnja mogli bi ih učiniti praktički besplatnima, kakve su danas bar-kod oznake.

Slika 1: Različiti RFID transponderi

EPCglobal vodeća je standardizacijska organizacija na području RFID tehnologija.Ona je definirala dvije podjele RFID uređaja, na šest klasa i u dvije generacije. Navedene podjele dane su slijedećim dvjema tablicama.

EPC klasa	Definicija	Programiranje
Klasa 0	moguće samo čitanje	programira ih proizvođač
Klasa 1	jednostruko programiranje	programira ih korisnik
Klasa 2	višestruko programiranje	programibilni
Klasa 3	djelomično aktivni transponderi	
Klasa 4	aktivni transponderi	
Klasa 5	čitači	

Tablica 1: Podjela RFID uređaja na klase

Karakteristika	Generacija 1	Generacija 2
frekvencija	860–930 MHz	860–960 MHz
memorijski kapacitet	64 ili 96 bita	96–256 bita
'*field* programibilnost	da	da
reprogramibilnost	klasa 0 – samo čitanje klasa 1 – jednostruko programiranje višestruko programiranje	–
ostale karakteristike	–	brži i pouzdaniji čitači, bolje poštivanje ostalih globalnih standarda

Tablica 2: Generacije RFID čipova

3.1. Pasivni RFID transponderi

Pasivni RFID transponderi nemaju unutrašnji izvor napajanja. Za napajanje sklopovlja ovakvih transpondera koristi se energija prikupljena iz dolaznog radio signala određenih svojstava. Kako nemaju unutrašnji izvor napajanja pasivni transponderi moraju imati mogućnost skladištenja energije tijekom primanja signala, na primjer kondenzator, kako bi se omogućilo slanje odgovora kada čitač prestane odašiljati ili čitač odašilje tijekom cijele komunikacije što znači da transponder odgovara na različitoj frekvenciji. Odgovor ne mora nužno sadržavati samo identifikacijski broj. Osim njega može uključivati i razne podatke iz memorije transpondera, ukoliko ju ovaj posjeduje.

Postoje tri tehnike energetskog uparivanja čitača i pasivnih transpondera:

1. **Elektromagnetska indukcija** se koristi na malim udaljenostima. Antene čitača i transpondera građene su kao zavojnice s velikim brojem zavoja te zajedno tvore transformator. Električna struja u zavojnici antene čitača stvara magnetsko polje koje inducira električnu struju u zavojnicama antene transpondera. Čitač komunicira s transponderom modulirajući amplitudu, frekvenciju ili fazu vala nosioca. Transponder s čitačem komunicira variranjem opterećenja na svojoj anteni čime utječe na napon na čitačevoj anteni. Brzim uključivanjem i isključivanjem opterećenja transponder može stvoriti vlastiti val podnositelj (eng. *subcarrier*) čijim moduliranjem odašilje odgovor.
2. **Reflektiranje** (eng. *backscatter*) se koristi kod očitavanja transpondera na većim udaljenostima. Do reflektiranja dolazi kada se elektromagnetski val reflektira od neku površinu natrag prema odašiljatelju, a na tom načelu temelji se radar. Količina reflektirane energije ovisi o tome koliko dobro reflektirajuća površina rezonira s dolaznim elektromagnetskim valom. RFID transponderi koji komuniciraju korištenjem refleksije imaju antene koje mogu jako dobro ili jako loše reflektirati čitačev signal. Izmjeničnim paljenjem i gašenjem reflektiranja transponder stvara uzorak kojega čitač uočava.
3. **Elektrostatičko uparivanje** je najrjeđe korištena metoda energetskog uparivanja. Kod ovog pristupa antene čitača i transpondera djeluju kao nabijene ploče. Dodavanje elektrona na antenu čitača uklanja elektrone s antene transpondera, i obrnuto. Površina antena određuje domet ovakvih RFID sustava. Antene se mogu tiskati vodljivom tintom što transpondere čini vrlo fleksibilnim i jeftinim.

Nepostojanje unutrašnjeg izvora napajanja omogućuje izvedbe pasivnih transpondera vrlo malenih dimenzija, prikladnih za ugradnju u naljepnice ili pod kožu. Moguće su i izrazito jeftine izvedbe što pasivne transpondere čini najpopularnijima kod masovnih primjena u trgovačkim lancima. Ovisno o veličini i dizajnu antene te o odabranoj radio frekvenciji, domet signala je od oko 10 cm pa do nekoliko metara.

3.2. Djelomično aktivni RFID transponderi

Djelomično aktivni transponderi sadrže bateriju koja napaja mikročip, a za napajanje antene koristi se energija prikupljena iz signala čitača. Kako po strukturi napajanja tako i po radnim karakteristikama djelomično aktivni (ili djelomično pasivni) RFID transponderi nalaze se između pasivnih i aktivnih transpondera, s pojedinim prednostima i manama obje skupine.

3.3. Aktivni RFID transponderi

Aktivni RFID transponderi posjeduju unutrašnji izvor napajanja koji se koristi za napajanje sklopovlja i za emitiranje radio signala. Oni su mnogo pouzdaniji od pasivnih transpondera zbog mogućnosti uspostavljanja sjednice s čitačem. Veća snaga emitiranog radio signala, omogućena vlastitim napajanjem, čini ove transpondere mnogo učinkovitijim u zahtjevnim radnim okolinama kao što su voda (uključujući ljude i životinje koji su velikim postotkom građeni od vode) ili metal (kontejneri i vozila) te na većim udaljenostima. Mnogi aktivni transponderi upotrebljivi su na udaljenostima do nekoliko stotina metara i imaju životni vijek baterije do 10 godina.

U aktivne RFID transpondere moguće je ugraditi razne senzore. Tako se transponderi s temperaturnim senzorima koriste za nadzor sazrijevanja betona ili za nadgledanje temperature kvarljive robe. Osim s temperaturnim senzorima, RFID transponderi su do sada integrirani i sa senzorima vlažnosti, vibracija, svijetla i radijacije.

Aktivni transponderi mogu sadržavati veće memorije od pasivnih te postoje izvedbe koje mogu pamtiti podatke primljene s čitača.

3.4. RFID etikete

RFID etikete se proizvode u vrlo različitim oblicima, veličinama, s različitim kapacitetima memorije i različitim fizičkim karakteristikama. Mogu biti dovoljno male da se smjeste pod kožu životinje, mogu biti oblika čavala ili vijka za označavanje drvene građe ili u obliku kreditne kartice za korištenje u aplikacijama kontrole pristupa. Veliki plastični privjesci za sprečavanje krađe odjeće u trgovinama također su RFID etikete, a slični su i vrlo otporni transponderi u obliku bloka kojima se označavaju kontejneri u internim procesima proizvodnje, ili radni strojevi i kamioni u svrhu praćenja i održavanja. Gotovo svi su zaštićeni nekom vrstom kućišta od udaraca, kemikalija, vlage i prašine.

3.5. RFID naljepnice

Bar-kod kao tehnologija automatske identifikacije u upotrebi je već desetljećima i vrlo je dobro etabliran. Ipak, jednom otisnute, bar-kod naljepnice ne mogu više biti promijenjene, a da bi je skener pročitao mora mu biti u vidnom polju. Nova generacija "pametnih" naljepnica opremljena je RFID tehnologijom i nadilazi neka ograničenja tradicionalnog bar-koda. Integrirani elektronički sklop sadrži memoriju i može biti programiran ili reprogramiran korištenjem radiovalova.

3.6. RFID tiskane pločice

Tiskana pločica (eng. PCB - *Printed Circuit Board*) je namijenjena ugradnji u proizvod ili ambalažu. Prednosti su joj je niža cijena i sposobnost podnošenja uvjeta okoline koje RFID naljepnice ne bi podnijele.

4. RFID čitači

RFID čitači mnogo se razlikuju po složenosti, ovisno o vrsti transpondera s kojima čitač radi i o korištenim frekvencijama. Njihov je zadatak komunikacija s transponderima i prijenos podataka do računala gdje se obavlja daljnja obradba. Sastoje se od antene za razmjenu podataka sa transponderom i upravljačkog uređaja koji obraduje podatke i komunicira s računalom.

Kod jednostavnih RFID sustava čitačev impuls energije je na transponder djelovao samo kao sklopka za uključivanje i isključivanje. Kod složenijih sustava radio signal kojega čitač odašilje može sadržavati naredbe transponderu, instrukcije za čitanje i pisanje memorije pa i zaporke.

Najjednostavniji čitači omogućuju čitanje samo jedne vrste transpondera, koristeći samo jednu frekvenciju i jedan protokol, dok oni složeniji koriste različite protokole, omogućuju odabir podataka, provjeru i ispravljanje grešaka. Razne tehnike se i dalje razvijaju kako bi se poboljšao postupak očitavanja, pa tako neki čitači mogu registrirati više transpondera istovremeno.

RFID čitači su najčešće stalno aktivni, konstantno odašiljući energiju radio signalom u potrazi za transponderima koji su im ušli u domet. Kod nekih primjena ovo je nepotrebno, a ako se radi o baterijski napajanim uređajima može čak biti i nepoželjno sa stajališta štednje energije. Zbog toga je neke čitače moguće postaviti tako da odašilju radio impulse kao odgovor na neki vanjski podražaj. Na primjer, kod RFID sustava za naplatu cestarine čitači su stalno upaljeni kako bi zabilježili svaki prolazak vozila. S druge strane, čitači u veterinarskim ambulantama često su opremljeni nekom vrstom okidača te se aktiviraju samo u određenim situacijama.

Postoje RFID čitači različitih dimenzija. Najveći čitači mogu se sastojati od stolnog računala s posebnom karticom i većeg broja antena koje su sa spomenutom karticom povezane oklopljenim kablovima. Ovakvi čitači najčešće su povezani na računalnu mrežu preko koje dijele podatke očitane s transpondera. Najmanji čitači veličine su poštanske marke i namijenjeni su ugradnji u mobilne telefone.

Slika 2: RFID čitači

5. Pozadinsko računalo

Većina RFID transpondera odašilje samo svoju identifikacijsku oznaku, npr. 96-bitni broj. Nakon očitavanja takvog broja čitač ga najčešće šalje računalu s kojim je povezan.

Postupak koji se s identifikacijskim brojem transpondera provodi na računalu ovisi o namjeni RFID sustava. Ako se radi o sustavu za kontrolu pristupa, računalo provjerava nalazi li se očitani broj na listi brojeva kojima je dozvoljen pristup određenim vratima ili području. U slučaju da je broj prisutan na listi, računalo može pokrenuti postupak otključavanja vrata. Kod *Mobil Speedpass* sustava za naplatu roba i usluga serijski broj transpondera i njegov odgovor na nasumični upit čitača šalju se preko *Mobil* mreže, provjerava se njihova ispravnost te se, u skladu s rezultatom provjere, transakcija odobrava ili zabranjuje.

Ako se radi o sustavu za označavanje proizvoda EPC (eng. *Electronic Product Code*) oznakama, serijski broj očitan s transpondera šalje se na mrežu računala koja sačinjavaju ONS sustav. ONS (eng. *Object Name Service*) je velika distribuirana baza podataka koja se koristi za prikupljanje podataka o proizvodima označenim EPC oznakama. Baza podataka sastoji se od središnjeg, tzv. '*root*', poslužitelja i distribuiranih poslužitelja u svakoj tvrtci koja svoje proizvode označuje EPC transponderima. Upit o očitanom EPC kodu središnji poslužitelj usmjerava na poslužitelj odgovarajuće tvrtke koji odgovara podacima o dotičnom proizvodu. ONS sustav je po svojoj građi sličan DNS (eng. *Domain Name System*) distribuiranoj bazi podataka, a obje baze vodi i održava tvrtka VeriSign.

6. Trenutne i buduće primjene RFID sustava

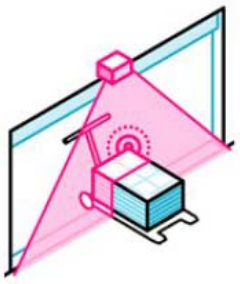
RFID tehnologija idealna je za primjene kod kojih je potrebna sigurna i jedinstvena identifikacija te dugotrajnost i izuzetna otpornost identifikatora na razne specifične utjecaje okoline, a bez izravne vidljivosti. U većini okruženja RFID sustavi postižu točnost prvog očitanja od 99.5% do 100%. Trenutno se ova tehnologija najviše susreće u transportu i logistici, proizvodnji i kontroli. Koristi se za označavanje životinja u uzgoju, praćenje proizvoda u opskrbnom lancu, praćenje poštanskih pošiljaka i prtljage u zračnom prometu, naplatu cestarina i parkirališta, kontrolu pristupa vozilima, zatim EAS (eng. *Electronic Article Surveillance*) nadzor artikala u trgovinama te zaštitu od krađe. Kontrola ulaza i radnog vremena je još jedna tipična primjena ove tehnologije.

Kako sve karakteristike RFID sustava u velikoj mjeri ovise o frekvencijama na kojima rade, tako se i njihove primjene mogu grupirati prema istom kriteriju:

1. RFID sustavi koji rade na niskim frekvencijama koriste se za:
   - sigurnosni nadzor,
   - identifikaciju životinja i
   - praćenje imovine.
2. Sustavi koji koriste visoke frekvencije primjenu nalaze u:
   - „pametnim“ karticama i
   - kontroli pristupa.
3. UHF RFID sustavi koriste se kod:
   - željeznica,

- identifikacije vozila i
- transporta robe.

U skladišta je moguće postaviti stacionarni RFID čitač koji kontrolira ulazak i izlazak robe. Svaki prolazak robe kroz vrata aktivira čitač koji očitava robu koja ulazi odnosno izlazi. Na takav je način omogućeno automatsko očitavanje prometa robe i održavanje ažurne evidencije skladišta.



Slika 3: Primjena RFID sustava u skladištima

U trgovini, pri prolasku kupca ispred RFID čitača, automatski je moguće očitati sve kupljene proizvode i izračunati ukupnu cijenu, bez nepotrebnog vađenja robe iz kolica, što uvelike ubrzava protok kupaca i smanjuje mogućnost pogrešnog očitavanja proizvoda.

Osim toga, RFID se već koristi u mnogim knjižnicama kako bi se ubrzao proces izdavanja i vraćanja knjiga, a postoji i slična primjena u videotekama. U nekim zemljama RFID se koristi i u zračnim lukama za praćenje putne prtljage kako bi se smanjile mogućnosti njenog gubitka.

Minijaturni RFID transponderi implantirani živim bićima ispod kože mogu se koristiti za njihovu identifikaciju. Tehnologija biočipa razvijena je 1983. godine u svrhu promatranja životinja. Danas se koristi u dvadesetak razvijenih zemalja svijetu u preko 300 zooloških vrtova, mnogim biološkim laboratorijima i promatranju životinja u divljini, a mnogi ljudi svoje kućne ljubimce označavaju biočipovima.

Kod ljudi bi univerzalni biočip zamijenio sve postojeće kartice koje osoba danas koristi (osobnu iskaznicu, putovnicu, vozačku dozvolu, zdravstvenu iskaznicu, kreditne kartice...). Odgovarajući čitač očitavao bi specifični skup informacija za koje je ovlašten.

Tvrtka Verichip 2001. godine razvila je prvi komercijalni biočip namijenjen korištenju na ljudima. Verichip je minijaturni RFID transponder veličine zrna riže koji se ugrađuje ispod kože, te se u blizini čitača aktivira i emitira identifikacijski broj koji korisniku omogućuje pristup različitim informacijama. Postojeći biočipovi omogućuju pohranu male količine podataka duljine 10 do 15 znakova.

Sustavi temeljeni na RFID tehnologijama koriste se u zatvorima za označavanje zatvorenika kako bi se spriječili bjegovi. Ovakvo označavanje dovelo je i do značajnog smanjenja količine nasilja zbog svijesti zatvorenika o stalnom nadgledanju. Američka vojska kao veliki zagovornik RFID tehnologije planira zamijeniti identifikacijske pločice vojnik RFID transponderima, a bolnice već eksperimentiraju s RFID narukvicama pomoću kojih medicinsko osoblje dobiva informacije o pacijentima. Razmatra se mogućnost korištenja RFID-a kako bi se spriječilo neovlašteno korištenje oružja. Postoje i planovi korištenja RFID narukvice u hotelima s tzv. *all inclusive* uslugom, na koncertima umjesto propusnica i slično.

7. Ranjivosti RFID sustava

Jednostavnost uporabe i sveprisutnost velike su prednosti RFID sustava, ali i izvori njihovih ranjivosti. Glavni problem kod RFID sustava je zaštita privatnosti jer transponderi na upit čitača odgovaraju slanjem informacija koje mogu biti osjetljive i koje neovlaštenom korisniku mogu omogućiti kompromitiranje sustava. Nitko ne želi da konfekcijski brojevi odjeće koju nosi ili iznos gotovine u novčaniku budu lako dostupni svakome s odgovarajućim čitačem.

Problem usko vezan uz zaštitu privatnosti je neovlašteno praćenje. Do njega dolazi zbog toga što su informacije koje transponderi odašilju predvidljive, često i do te mjere da transponder uvijek na upit odgovara jednakim identifikacijskim brojem. Na taj način je zlonamjernom korisniku jednostavno moguće povezati transponder s njegovim vlasnikom ili nosiocem. Čak i ako su transponderi postavljeni

tako da ne otkrivaju osjetljive informacije, u brojnim situacijama ipak je moguće primjenom posebnih tehnika, koje uključuju očitavanje većeg broja transpondera, pratiti njihovo kretanje.
Pored dva navedena problema RFID sustavi ranjivi su i na:

- **fizičke napade**,
- **napade uskraćivanjem usluga**, npr. ometanjem radio signala,
- **krivotvorenje** koje se odnosi na promjenu identiteta artikala, najčešće manipuliranjem transpondera,
- **prijevare** u kojima napadač preuzima ulogu postojećeg transpondera,
- **prisluškivanje** i
- **neovlaštenu analizu komunikacije**.

Kako bi se izveo fizički napad na RFID transponder potrebno ga je obraditi, najčešće u laboratoriju. Primjeri fizičkih napada na transpondere su:

- sondiranje,
- uklanjanje materijala oblikovanim nabojima ili vodenim jetkanjem
- tiskanje radijacijom,
- izmjena električnih krugova i
- ometanje signala takta.

Transponderi imaju slabu ili nikakvu zaštitu od ovakvih napada.
Neovlaštena analiza komunikacije odnosi se na presretanje i analizu poruka kako bi se priskrbile informacije ili uočili komunikacijski uzorci. Ovakvu analizu moguće je provesti čak i kada su poruke kriptirane i nije ih moguće dekriptirati. Općenito vrijedi pravilo da je iz većeg broja analiziranih poruka moguće dobiti više informacija.

8. Sigurnosni elementi RFID sustava

Kako bi se uklonile ranjivosti RFID sustava i spriječili napadi na njih moguće je primijeniti sljedeće sigurnosne elemente:

- samouništenje,
- Faradayev kavez,
- aktivno ometanje,
- blokirajući transponder,
- potrošačka prava,
- klasična kriptografija,
- hash funkcije,
- PRF autorizacija,
- TBP autorizacija,
- HB autorizacija i
- metode koje ne koriste enkipciju.

8.1. Samouništenje

Svaki RFID transponder s ovom mogućnošću ima jedinstvenu zaporku koja se programira tijekom procesa proizvodnje. Transponder koji primi poruku s točnom zaporkom automatski i nepovratno se deaktivira. Primjer upotrebe ovog mehanizma je onesposobljavanje transpondera kojima su označeni proizvodi na izlasku kupca iz trgovine čime se onemogućuje njegovo daljnje praćenje.
Ovaj pristup ima i neka ozbiljna ograničenja. Onemogućavanje transpondera nakon izlaska iz trgovine sprječava njihovu kasniju legalnu uporabu od strane kupca, npr. kod "pametnih" hladnjaka i ormara ili kod mikrovalnih pećnica koje upute za pripremu hrane čitaju iz transpondera. Time je ujedno uklonjena mogućnost recikliranja – ponovne upotrebe transpondera. Postavlja se i pitanje vraćanja proizvoda u slučaju nezadovoljstva kupca.

8.2. Faradayev kavez

Zaštitu privatnosti RFID transpondera moguće je postići i njihovim izoliranjem od vanjskih elektromagnetskih utjecaja. To je moguće učiniti pomoću tzv. Faradayevog kaveza, spremnika građenog od metalne mreže ili folije koji blokira radio signale određenih frekvencija.

8.3. Aktivno ometanje

Aktivno ometanje predstavlja alternativu zaštite privatnosti pomoću Faradayevog kaveza. Postiže se pomoću uređaja koji odašilje radio signale na taj način da u potpunosti onemogući radio komunikaciju i time onemogućuje rad RFID čitača. Ovakvo ometanje može biti ilegalno, posebno ako se radi o snažnom i neselektivnom ometanju velikog dometa.

8.4. Blokirajući transponder

Blokirajući transponder je pasivni RFID transponder koji može simulirati veliki broj običnih transpondera istovremeno. Takvim djelovanjem blokirajući transponder onemogućuje rad RFID čitača. Moguće je simulirati velik broj raznorodnih transpondera ili ograničiti blokiranje simuliranjem odabranog podskupa transpondera, npr. onih određenog proizvođača, te tako prikrivanjem stvarnog stanja zaštiti privatnost sustava.
Moguće su i zloupotrebe ovakvih transpondera. Univerzalni blokirajući transponder je po samoj svojoj prirodi zlonamjeran jer blokira sve RFID sustave u dometu pa može biti iskorišten za izvođenje napada uskraćivanjem usluga. Selektivni zlonamjerno podešen blokirajući transponder može sofisticiranim simuliranjem određene distribucije transpondera izbjeći detekciju.

8.5. Potrošačka prava

Poznavanje i poštivanje prava potrošača, korisnika predmeta označenih RFID transponderima, uvelike može pridonijeti sigurnosti ovih sustava i smanjiti opasnost od zlouporabe. Simson Garfinkel osmislio je listu prava '*Bill of Rights*' prema kojoj korisnici RFID sustava i kupci artikala označenih transponderima imaju pravo:

1. znati sadrži li kupljeni artikl RFID transponder,
2. uklanjanja, deaktiviranja ili uništavanja transpondera nakon kupnje proizvoda,
3. odabira alternative: korisnici ne smiju izgubiti prava, kao što su npr. pravo na vraćanje proizvoda ili pravo na putovanje određenom cestom, ako se odluče na neku od alternativa RFID sustavima ili ako odluče deaktivirati transpondere na kupljenim proizvodima,
4. znati koje informacije su pohranjene u RFID transponderima i u slučaju njihove netočnosti potrebno je osigurati način njihova ispravljanja ili nadopunjavanja,
5. znati kada, gdje i zašto se RFID transponderi očitavaju.

8.6. Klasična kriptografija

Klasične kriptografske metode moguće je primijeniti i kod RFID sustava. Korištenjem transpondera s mogućnošću višestrukog programiranja moguće je kriptirati identifikacijsku oznaku transpondera što uz učestao mijenjanje kriptografskog ključa onemogućuje njegovo praćenje.
Postoje implementacije autorizacijskih algoritama sa simetričnom enkripcijom te s enkripcijom s javnim ključem.

8.7. *Hash* funkcije

Često se sigurnost RFID sustava pokušava ostvariti različitim primjenama *hash* funkcija.

1. ***Hash* zaključavanje** je sigurnosni sustav kod kojega svaki transponder posjeduje jedinstvenu oznaku, tzv. *metaID*. Dok je zaključan transponder odašilje samo svoju *metaID* oznaku i čeka da mu čitač na nju odgovori ključem *k* (*metaID = hash(k)*). Ključevi su pohranjeni u bazi podataka na računalu povezanom s čitačem.
2. **Nasumično *hash* zaključavanje** je proširenje prethodno opisanog sustava čiji je glavni nedostatak to što omogućuje neovlašteno praćenje transpondera. Ono podrazumijeva

učestale i nepredvidljive promjene *metaID* oznaka. Kako bi ih se zaštitilo ovom metodom transponderi moraju imati *hash* funkciju i generator pseudo-slučajnih brojeva.

3. ***Hash-Chain*** metoda koristi dvije ili više *hash* funkcija ugrađene u transponder za onemogućavanje fizičkih napada na transpondere.

8.8. PRF autorizacija

PRF autorizacija omogućuje međusobnu autorizaciju čitača i transpondera uz osiguranu zaštitu privatnosti transpondera koji sudjeluje u procesu. Ovaj protokol koristi dijeljeni ključ i PRF (eng. *Pseudo Random Function*) za osiguravanje poruka razmijenjenih između transpondera i čitača.

8.9. TBP autorizacija

TBP (eng. *Tree-Based Private*) autorizacija uklanja opterećenje poslužitelja koje se javlja kod metoda temeljenih na *hash* funkcijama i koje je proporcionalno broju transpondera.

8.10. HB+ autorizacija

HB+ autorizacija nadogradnja je HB protokola, nazvanom po tvorcima (Hopper i Blum). HB+ protokol koristi simetričan kriptografski ključ, a jednostavnost ga čini primjenjivim i na jeftinim transponderima. Pruža zaštitu od aktivnog i pasivnog prisluškivanja.

8.11. Metode koje ne koriste enkripciju

Metode zaštite RFID sustava koje ne koriste enkripciju obuhvaćaju cijeli niz izrazito jednostavnih autorizacijskih algoritama koji se temelje na odgovaranju na upite (eng. *challenge-response*). Jedan od pristupa je i pohranjivanje jedinstvene liste znakova na svakom transponderu. Na svaki upit transponder odgovara sljedećim znakom s liste te se na temelju takvog niza provodi njegova identifikacija.

9. Zaključak

RFID sustavi zbog svoje raznolikosti i fleksibilnosti pružaju mogućnosti unaprjeđenja svih područja ljudskog djelovanja. Ubrzavanje i povećanje efikasnosti proizvodnje, olakšavanje praćenja tijekom transporta, uklanjanje potrebe za inventurama skladišta i trgovina, nadzor nad kućnim ljubimcima i pacijentima u bolnicama te ubrzavanje svih djelatnosti kod kojih je potrebna identifikacija, kao što su naplata roba i usluga ili kontrola pristupa, mogućnosti su koje osiguravaju siguran prodor RFID sustava u sve pore modernog društva i gospodarstva.

Goleme mogućnosti RFID sustava otvaraju i brojne mogućnosti zlouporabe. Što više informacija se pohrani u sveprisutne transpondere to će njihove korisnike biti lakše pratiti, prisluškivati, analizirati ili napasti na neki drugi način. Zbog toga je nužno pažljivo pristupiti razmatranju upotrebe RFID sustava i, unatoč brojnim prednostima, odgoditi njihovu implementaciju u primjenama kod kojih još ne pružaju zadovoljavajuću razinu sigurnosti.

10. Reference

[1] Jerry Landt, Barbara Catlin: Shrouds of Time – The history of RFID, AIM Inc., 2001.

[2] Nina Livun: Radio Frequency Identification, Fakultet elektrotehnike i računarstva, Zagreb, 2005.

[3] Pedro Peris-Lopez, Julio Cezar Hernando-Castro, Juan M. Estevez-Tapiador, Arturo Ribagorda: RFID Systems: A Survey on Security Threats and Proposed Solutions, International Conference on Personal Wireless Communication, 2006.

[4] Melanie R. Rieback, Georgy N. Gaydadijev, Bruno Crispo: A Platform for RFID Security and Privacy Administration, USENIX/SAGE Large Installation System Administration conference, 2006.

[5] Ari Jules, Ronald L. Rivest, Michael Szyidlo: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, 8th ACM Conference on Computer and Communications Security, pp. 103-111, ACM Press, 2003.

[6] Simson Garhttp: Bill of Rights, http://www.technologyreview.com/InfoTech/12953/, siječanj 2007.

[7] Zhaoyu Liu, Dichao Peng: A Secure RFID Identity Response Protocol for Physical Attack Resistance, Journal of Communications, 1(4), pp 31-40, 2006.