# SIGURNOST I PRIVATNOST U RFID SISTEMIMA
# SECURITY AND PRIVACY IN SYSTEMS

Božidar Popović, *Elektrotehnički fakultet Istočno, Sarajevo*
Miroslav Kostadinović, *Saobraćajno tehnički fakultet, Doboj*

**Sadržaj** - U ovom radu biće opisani osnovni i najozbiljni problemi koji se javlja pri upotrebi RFID sistema. Ispitivanje realnih i praktičnih pretnji po privatnost i sigurnost sistema je od velikog značaja da se preduhitre i onemoguće potencijalne zloupotrebe. Pošto je pravo na privatnost je jedno od osnovnih, neotuđivih i apsolutnih ljudskih prava svakog pojedinca kojim se obezbeđuje integritet i dignitet ljudske ličnosti, radi očuvanja tajnosti i slobode njegovog privatnog života. Postavlja se pitanje kako zaštititi privatnost kada se RFID tagovi svaki put odazovu čitaču ako su u njegovom dometu i pošaljumu informaciju koja je upisana u njih. Ovakve informacije mogu neovlašćenom korisniku omogućiti da ugrozi sistem. Recimo postoje prijdlozi svjetskih banaka i monetarnih fondova da se u novčanice ugrađuju RFID tagovi, što direktno narušava privatnost jer niko ne želi da iznos novca koji ima kod sebe bude dostupan svakome ko ima odgovarajući RFID čitač.

**Abstract** – This paper describes basic and the most serious problems that are present in RFID systems usage. Inspection of real and practical threats on system privacy and security is of great significance in order to prevent and disable their potential misusage. The privacy policy is one of the basic, inalienable and absolute human rights which enables integrity and dignity of human beings. In order to preserve secrecy and private life freedom, the question is how to protect privacy when the RFID tags respond to the reader if they are in its range and send the information that is written in them. Information like this can enable an unauthorized user to endanger the system. World banks and monetary funds propose RFID tags to be embedded in bank notes, but that directly violate privacy because nobody wants to have a sum of money that is transparent to every person who has the RFID reader.

## 1. UVOD

RFID (Radio Frequency Identification) je tehnologija koja koristi radio-talase za automatsku identifikaciju pojedinačnih proizvoda. Prve varijante ove tehnologije su korišćene još tokom Drugog svjetskog rata, a uz njihovu pomoć je saveznička protivavionska odbrana nastojala da razlikuje svoje od neprijateljskih aviona. Kao preteča RFID tehnologije uzima se izum Leona Termina (Leon Theremin), ruskog pronalazača, koji je 1945. konstruisao špijunski alat, vrstu bubice za prisluškivanje koja je koristila energiju radio talasa da bi se napajala i slala signale.

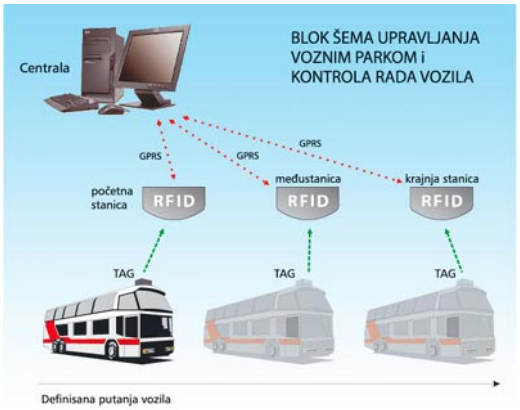
RFID tehnologija se tek u posljednje vrijeme počinje masovno koristiti u skoro svim područjima ljudskog djelovanja. Savremena RFID tehnologija ubrzava i povećava efikasnost proizvodnje, olakšava praćenje tokom transporta, uklanja potrebe za inventurama skladišta i trgovina, omogućava nadzor nad pacijentima u bolnicama i ubrzava sve djelatnosti kod kojih je neophodna identifikacija, kao npr. naplata roba i usluga ili kontrolu pristupa. Komunikacija između RFID tag-a u proizvodu i čitača se odvija bežično. Postoji nekoliko načina identifikacije objekata, a najčešće primjenjivana metoda je zasnovana na činjenici da je u svakom RFID tag-u sačuvan EPC (Electronic Product Code), jedinstveni serijski broj. Ovo znači da i svaki pojedini proizvod u istoj grupi ima svoj jedinstveni broj, a ne jedan broj za veću količinu istih proizvoda. Pored serijskog broja kojim se identifikuje proizvod, RFID čipovi mogu da sadrže i druge informacije. Mogućnosti upotrebe RFID tehnologije su praktično neograničene u svim aplikacijama u kojim je potrebna bilo kakva identifikacija i razmjena podataka. Ovakve osobine RFID sistema otvaraju i brojne mogućnosti njegove zloupotrebe [1].

## 2. PRIMJENA RFID SISTEMA

Primjena RFID tehnologija je idealna za procese u kojim je potrebna sigurna i jedinstvena identifikacija kao i izuzetna otpornost identifikatora na razne specifične uticaje okoline, a bez direktne optičke vidljivosti. U većini okruženja RFID sistemi postižu od 99.5% do 100% uspješnost prvog očitanja. Trenutno se RFID tehnologija najviše koristi u transportu, logistici, proizvodnji i kontroli. Takođe se koristi za označavanje životinja i praćenje nihovog životnog ciklusa, praćenje proizvoda u lancima smadbijevanja, praćenje poštanskih pošiljki, prtljaga u aviosaobraćaju, naplatu parkinga i putarina za korišćenje autoputeva, kontrolu pristupa vozilima,kontrolu ulaza i radnog vremena, itd.

Karakteristike RFID sistema u velikoj mjeri zavise od frekvencija na kojima rade, pa se primjene RFID sistema mogu podjeliti prema istom kriterijumu na:

- NF RFID sistemi koriste se za:
  - identifikaciju životinja,
  - sigurnosnu kontrolu,
  - praćenje imovine.
- VF RFID sistemi koriste se u:
  - kontroli pristupa i radnog vremena,
  - platnim odnosno „ pametnim“ karticama.
- UHF RFID sistemi koriste se za:
  - praćenje poštanskih pošiljki,
  - praćenje prtljaga u aviosaobraćaju,
  - naplatu parkinga i putarina za korišćenje autoputeva,
  - transport robe,
  - upravljanje voznim parkom (slika1.).




Slika 1. Blok šema upravljanja voznim parkom

RFID tagovi implantirani u živim bićima ispod kože mogu se koristiti za njihovu identifikaciju. Danas se tehnologija implantacije RFID tagova (biočip) koristi u preko 300 zooloških vrtova, mnogim biološkim laboratorijima, kao i za praćenje kućnih ljubimaca. Kod ljudi bi univerzalni biočip zamijenio sve postojeće kartice koje osoba danas koristi (lična karta, pasoš, zdravstvenu knjižicu, vozačku dozvolu, kreditne kartice, itd.). Potrebno bi bilo usaglasiti da odgovarajući RFID čitači očitavaju samo specifični skup informacija za koje je ovlašten, bez narušavanja privatnosti.
Ovakva primjena RFID tehnologijama koristi se kao pilot projekat u zatvorima za označavanje zatvorenika kao preventiva kako bi se sprečili bijegovi. Ovo je dovelo i do značajnog smanjenja količine nasilja zbog svijesti zatvorenika da su stalno nadgledani. Američka vojska kao veliki zagovornik RFID tehnologije planira zamijeniti identifikacione pločice vojnika RFID tagovima. Takođe i bolnice već eksperimentišu s RFID narukvicama pomoću kojih medicinsko osoblje dobija informacije o pacijentima. Postoje prijdlozi svjetskih banaka i monetarnih fondova da se u novčanice ugrađuju RFID tagovi, kao i od starne hotelijera korištenje RFID narukvice u hotelima s tzv. all inclusive uslugom, na koncertima i fudbalskim utakmicama umjesto propusnica.

## 3. PIVATNOST I ZAKONSKA OGRANIČENJA

Osnovno i neotuđivo pravo svakog pojedinca je pravo na privatnost kojom se obezbjeđuje integritet i dignitet ljudske ličnosti, zbog očuvanja tajnosti i slobode privatnog života svake ljudske jedinke. Ovo pravo je apsolutnog karaktera i ničim se ne smije ograničiti, pa makar to bili i viši interesi države i društvene zajednice. U današnje vrijeme primjenom ICT tehnologije ovo pravo se jednostavno i gotovo neprimjetno može ugroziti. Zbog toga se razvio poseban vid privatnosti koji se naziva informaciona privatnost i koji se definiše kao pravo pojedinca da kontroliše koji, kako i za koga podaci o njemu mogu postati dostupni drugim osobama ili organizacijama. Navedeni su neki nedostaci RFID sistema koji mogu dovesti do neželjenih narušavanja privatnosti.

Kako RFID sistem ne zahtijeva liniju vidljivosti između čitača i taga, čitač može da pročita informacije sa taga iako se ne nalazi u njegovoj blizini i ne postoji fizička vidljivost. Ovo je i jedna od osnovnih prednosti RFID tehnologije a istovremeno čini je i ranjivom. Recimo, ako osoba sa sobom nosi obilježene proizvode, treće lice može sa distance da sazna koji su to proizvodi. Kupac može biti u potpunosti nesvjestan da nosi proizvode obilježene tagovima i da neko čita te tagove. Trenutni dometi pasivnih tagova su oko tri metra, dok aktivni tagovi imaju domet i do 100 m, što ih čini znatno pogodnijim za zloupotrebu. Ali pošto su aktivni tagovi dosta veći i mnogo skuplji, njihova upotreba je ograničena na skupe poslove.

Praćenje pojedinačnih proizvoda može se iskoristiti za povezivanje kupca sa predmetima koje kupuje. Ako se pretpostavi da je neki kupac kupio odjelo (koje na sebi ima RFID tag) i da ih je platilo platnom karticom, tada prodavac može povezati identitet osobe sa kupljenim odjelom. Tako da kupac može biti identifikovana na osnovu kupovine koju je obavio, a potom i automatski locirana praćenjem proizvoda koje poseduje.

Zakonska ograničenja - U većini država su propisani zakoni kako bi se očuvala privatnost i bezbjednost pojedinca i zaštitili lični podaci. Američka državna komisija za trgovinu je objavila četiri široko prihvaćena principa kojima se štite građani (kupci ili korisnici usluga).

Obavještavanje - Sve kompanije, ustanove i udruženja koji skupljaju informacije moraju to javno i transparentno raditi, kako bi se korisnici usluga upoznali da se vrši pribavljanje njihovih ličnih podataka. To znači da korisnik usluge treba da zna koje informacije se skupljaju, kako se skupljaju i koja je svrha skupljanja tih podatka. U RFID sistemima korisnici usluga bi trebali da znaju ako su proizvodi označeni tagovima, koja informacija se nalazi upisana u tag-u, kao i koja informacija o korisniku usluge će biti povezana sa tim tagom.

Izbor - Korisniku se mora dati mogućnost da može odluči da li će i kako će prikupljene lične podatke moći da koriste kompanije i u koje namjene. Ovakvim izborom će se odrediti sekundarna upotreba informacija, kao što su upis na marketing liste ili davanje informacija drugim kompanijama. Korisniku treba pružiti mogućnost da može da odbije da se o njemu prikupljaju informacije.

Pristup - Potrebno je obezbijediti da korisnici mogu pristupiti svojim ličnim podacima da ih mogu potvrditi ili demantovati. To znači da korisnik treba da zna da se određeni podaci, koji se tiču njega, prikupljaju i da mu se obezbijedi pristup tim podacima kako bi mogao da potvrdi njihovu vjerodostojnost.

Bezbjednost - Sve kompanije, ustanove i udruženja koji prikupljaju ovakve podatke moraju preduzeti određene korake kako bi se osigurali da su podaci bezbedni i da je uklonjena mogućnost zloupotrebe ličnih podataka. Identitet korisnika i njihovi lični podaci se moraju čuvati i njima se mora upravljati sa posebnom pažnjom.

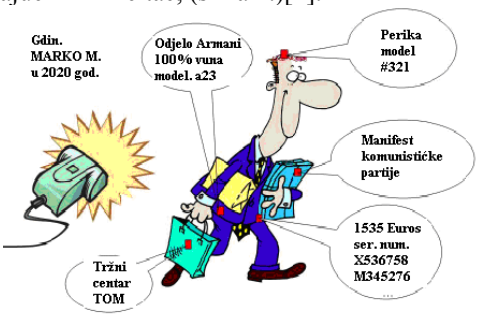
Kompanija EPCglobal naglašava probleme vezane za privatnost kao ključne odrednice u procesu prihvatanja RFID tehnologije. EPCglobal je dala smjernice i navela kako se treba boriti za očuvanje privatnosti podataka, kao i da korisnik treba da bude svjestan da se neki podaci o njemu prikupljaju i da mu se mora pružiti pravo da odluči da li će to dozvoliti. Sveobuhvatno da bi se povećala bezbjednost podataka i očuvala privatnost korisnika potrebno je ispoštovati sledeća prava:

- Pravo korisnika da zna koji proizvodi nose RFID tag;
- Pravo da deaktivira ili ukloni tag, kada kupi proizvod;

- Pravo da zna gdje, kada i zašto se RFID tag čita;
- Pravo na proizvod i uslugu, iako je odlučio da ne koristi tagove;
- Pravo da zna koje se informacije čuvaju na tagu.

## 4. RANJIVOST RFID SISTEMA

Osnovni i najozbiljniji problem koji se javlja pri upotrebi RFID sistema je kako zaštititi privatnost i onemogućiti neovlašćeno praćenje kada se tagovi svaki put odazovu čitaču ako su u njegovom dometu i pošalju informaciju koja je upisana u njih. Ovakve informacije mogu neovlašćenom korisniku omogućiti da ugrozi sistem. Kao što je ranije navedeno, postoje prijedlozi svjetskih banaka i monetarnih fondova da se u novčanice ugrađuju RFID tagovi, što direktno narušava privatnost jer niko ne želi da iznos novca koji ima kod sebe bude dostupan svakome ko ima odgovarajući RFID čitač, (slika 2.)[4].




Slika 2. Narušena privatnost

RFID sistemi su ranjivi i na:
- ometanje radio talasima,
- fizičke napade,
- prisluškivanje,
- promjenu identiteta proizvoda,
- impersonaciju legitimnog taga,
- neovlašćenu analizu komunikacija.

Fizički napadi na RFID tagove podrazumijevaju promjenu elektronskih osobina, ometanje signala takta i sondiranje. RFID tagovi nemaju skoro nikakvu zaštitu od ovakvih napada. Neovlašćena analiza komunikacije se svodi na prisluškivanje (slika 3.), tj. presretanje, i analizu informacionih poruka koje se izmjenjuju između tagova i čitača da bi se pribavile informacije ili identifikovali komunikacioni uzorci [5]. Pribavljanje informacija se može vršiti čak i ako je poruka šifrovana. Generalno, što je veći broj posmatranih poruka to se više informacija može ekstraktovati.


Slika 3. Neovlašćena analiza komunikacije

Smatralo se, takođe, da se RFID tagovi ne mogu zaraziti virusima zbog malog i ograničenog memorijskog kapaciteta. Grupa istraživača koju je predvodio Andrew S. Tanenbaum je napravila malwer (malicious softwer), prvi virus za RFID. Otkrili su ako postoje propusti u RFID softveru da se jednostavno RFID tag može zaraziti virusom, koji se vremenom može proširiti na bazu podataka koju koristi RFID softver.

RFID iskorištavač (RFID exploit) je tag u koji je neko namjerno ili slučajno upisao neobičan sadržaj u određenom formatu. Pošto se komunikacija čitač - tag svodi na skeniranje i očekivanje dobijene informacije određenog formata, ako je dobijena informacija koja je pročitana iz taga toliko neočekivana za RFID čitač može se onesposobiti softver čitača kao i sama baza, što bi blokiralo čitav sistem. Razlikujemo dvije vrste RFID iskorištavača:
- RFID crvi su iskorištavači koji koriste mrežno okruženje da bi se multiplicirali. RFID softver zaražen crvom može zaraziti ostale tagove upisivanjem kopije koda RFID crva.
- RFID virusi su iskorištavači koji samostalno multipliciraju svoj kod na nove tagove. Zaraženi tag zarazi RFID sistem preko čitača koji ga je skeniro a novi tagovi se zaraze preko ovog sistema.

## 5. SIGURNOST I BEZBJEDNOST RFID SISTEMA

Poseno je važno uzeti u obzir potencijalne prijetnje po integritet i upotrebljivost određenog RFID sistema. Sa tačke bezbjednosti, bezbjednosne potrebe se razlikuju od sistema do sistema, a nivo bezbjednosti je određen osjetljivošću podataka kojima se upravlja i mogućim gubicima usljed novlašćenog pristupa informacijama koje se prikupljaju [3]. Jako je bitno da bezbjednosni zahtjevi budu obezbijeđeni na svakom dijelu RFID sistema. Povezanost podrazumijeva određen nivo povjerenja, ali pošto se radi o osjetljivim podacima koji se mogu iskoristiti za narušavanje privatnosti onda se mora obezbijediti visok nivo bezbjednosti podataka. Problem bezbjednosti RFID sistema, obično, uključuje pitanje lažnih ili nelegitimnih tagova i nešto ređe čitača. Bezbjednosni problemi se javljaju ako podaci na tagu nisu enkriptovani i ako su proizvodi bez fizičkog nadzora. Najčešće razlozi su ekonomski, jer enkripcija dodatno košta i zahtijeva više memorijskog prostora na tagu čime se povećava cijena taga. Ako su proizvodi bez fizičkog nadzora, sva lica sa dozvolom pristupa tagu mogu da ga uklone ili zamijene drugim čime namjerno narušavaju bezbjednost RFID sistema. Ovakve zloupotrebe se mogu iskoristiti da se tag sa artikla koji ima nižu cijenu postavi na skuplji artikal. Postoji mogućnost praćenja osoba prateći proizvode koje nose i na takav način se može napraviti precizan profil te osobe, njene životne navike, navike pri kupovini, zdravstveno stanje, itd. Takođe, može se sakriti obilježeni predmet u metalni okvir i tako onemogućiti čitanje.

Mjere koje se mogu primijeniti da bi se povećala bezbjednost i smanjila ranjivost RFID sistema su [2]:
- Samouništenje: U tagove se upisuje jedinstvena lozinka. Tag koji primi "kill" poruku sa tačnom lozinkom automatski i nepovratno se deaktivira (koristi se za označavanje proizvoda koji se kupuju u marketima i pri prolasku kroz kasu se deaktivira tag tako da je onemogućeno njegovo dalje praćenje).

- Blokirajući tag: To je pasivi tag koji može da simulira veći broj tagova i tako blokira rad RFID čitača u svom dometu. Ovaj tag se može iskoristiti i za napade na RFID sisteme.
- Kriptografija: Korišćenjem write-read tagova moguće je čestim promjenama kriptografskog ključa onemogućiti neovlašćeno čitanje i praćenje taga.
- Symmetric Key Encryption: Implementacija AES algoritma u RFID sistemima.
- Public Key Encryption: Baziran na kriptografskom konceptu „Re-Encryption“
- Korišćenje hash funkcija
  a) Hash zaključavanje je sigurna metoda gdje svaki tag posjeduje jedinstvenu oznaku (metalID). Dok je zaključan tag odgovara samo slanjem svoje oznake - metalID i čeka da mu čitač na poslanu oznaku odgovori ključem k (metalID = hash(k)). Ključevi su upisani u bazu koja je na PC-ju povezanim sa čitačem.
  b) Nasumično hash zaključavanje je proširenje prethodno opisane metode čiji je glavni nedostatak to što omogućava neovlašćeno praćenje tagova. Podrazumijevaju se učestane i nepredvidive promjene metalID oznake. Kako bi se koristo ovaj metod tagov bi morali imati hash funkciju i generator pseudo-slučajnih brojeva.
  c) Hash-Chain metoda koristi dvije ili više hash funkcija ugrađene u tag za onemogućavanje fizičkih napada na tagove.
- PRF (Pseudo Random Function) autorizacija: Osigurava zaštitu privatnosti taga koji se javlja. Ova autorizacija koristi zajednički ključ i PRF za osiguravanje komunikacija čitač tag.
- TBP (Tree Based Private) autorizacija: Radi tako što smanjuje opterećenje poslužitelja (kod metoda zasnovanih na hash funkcijama) koje je proporcionalno broju tagova.
- HB+ autorizacija ( Hopper i Blum): Koristi simetričan kriptografski ključ, pruža zaštitu od aktivnog i pasivnog prisluškivanja. Jednostavnost ove autorizacije je čini primamljivom i za primjenu na jeftinijim tagovima.
- Aktivno ometanje: Vrši se ometanjem na radnoj frekvenciji RFID sistema čime se blokira čitav sistem, alternativa je zaštiti privatnost primjenom Faradejevog kaveza.
- Faradejov kavez: Obezbjeđuje zaštitu privatnosti RFID taga tako što se izoluje od vanjskih elektromagnetnih uticaja.
- Metode koje ne koriste šifrovanje, realizuju se pomoću jednostavnih algoritama za autorizaciju. Na tag se memoriše jedinstvena lista znakova, na postavljeno pitanje tag odgovara sljedećim znakom sa liste i na taj način se provjerava njegova autentičnost.
- Odvajanje EPC koda od bilo koje osetljive informacije po kompaniju ili kupca.
- Korišćenje RW tagova samo tamo gde je prikladno i gde postoje dodatni sistemi zaštite.
- Čitači treba da zahtijevaju odgovarajuću potvrdu ovlašćenja ili dozvolu da bi omogućili pristup svojim servisima.
- Ako je mreža bazira na internetu, moraju se obezbijediti firewall-ovi i sistemi za detektovanje napada.

## 6. ZAKLJUČAK

Zbog jednostavnosti i fleksibilnosti RFID sistemi pružaju mogućnosti unapređenja svih područja ljudskog djelovanja. Ubrzavanje i povećanje efikasnosti proizvodnje, praćenja proizvoda u svim fazama životnog vijeka od proizvodnog procesa, prodaje do krajnje namjene, uklanjanje potrebe za inventurama skladišta i trgovinskih lanaca, nadzor zatvorenicima i pacijentima u bolnicama te povećanje efikasnosti svih djelatnosti kod kojih je potrebna identifikacija, kao što su naplata robe i usluga ili kontrola pristupa, mogućnosti su koje osiguravaju siguran prodor RFID sistema u sve pore modernog društva. Širok dijapazon mogućnosti upotrebe RFID sistema otvara i brojne mogućnosti zloupotrebe. Zato je potrebno pažljivo pristupiti analizi upotrebe RFID sistema i pronaći odgovarajuća rešenja za implementaciju i primjenu u osjetljivim oblastima kao što su medicina i obilježavanje novčanica, tj. gdje se ne pruža zadovoljavajuću nivo sigurnosti.

Mogućnosti i želje proizvođača da prate pojedinačne proizvode nisu još česte pa ostaje da se u budućnosti vidi šta će se dešavati. Smatra se da će se u narednih nekoliko godina, na nivou proizvoda, pratiti novčanice, hartije od vrijednosti, ljekovi, skupocjene pošiljke, vrijednonosna dokumenta, skupi predmeti, umjetnički radovi. Takođe, kompanije se savjetuju da ne postavljaju tagove na sam proizvod, već na njegov omot ili ambalažu, kao i obavezu korišćenje “kill“ komande gdje je to poželjno.

## LITERATURA


[1] Dr. P. Sanghera, F. Thornton, B. Haines, F. Kung Man Fung, J. Kleinschmidt, Anand M. Das, H. Bhargava, A. Campbell “How to Cheat at Deploying and Securing RFID” PUBLISHED BY Syngress Publishing, Inc.

[2] Yan Zhang, Paris Kitsos “Security in RFID and Sensor Networks” Auerbach Publications.

[3] F. Thornton, B. Haines, Anand M. Das, H. Bhargava, A. Campbell, J. Kleinschmidt “RFID Security”, PUBLISHED BY Syngress Publishing, Inc.

[4] Ari Juels, “RFID Security and Privacy: A Research Survey” RSA Laboratories.

[5] Thomas Hollstein, Manfred Glesner; TU Darmstadt, Ulrich Waldmann; Fraunhofer SIT Darmstadt , Henk Birkholz, Karsten Sohr; Universität Bremen “Security challenges for RFID key applications“.