



UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Kriptologija u automobilske industriji

- Diplomski rad -

Mentor:

Doc. dr Saša Adamović

Student:

Nevena Ilić

Br. Indeksa: 2011/202009

Beograd, 2015.

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Beograd, Danijelova 32.

Kandidat: Nevena Ilić

Broj indeksa: 2011/202009

Smer: Informatika i računarstvo

Tema: Upotreba kriptologije u automobilske industriji

MENTOR

Datum odobrenja rada:

Beograd, _____.____._____.

Doc. dr Saša Adamović

DEKAN

Prof. dr Dragan Cvetković

Kriptologija u automobilskoj industriji

Sažetak: S napredovanjem tehnologije interakcija između automobila i čoveka postaje sve veća. U ovom radu biće analizirani sigurnost i bezbednost ličnih informacija u automobilima. Akcenat je stavljen na analizu bezbednosti kriptografskih protokola hardvera i softvera koji se trenutno koriste a i onih koji su i dalje u fazi ispitivanja i razvoja, s obzirom na to da je ova oblast u ekspanziji. Postoji više hardverskih i softverskih rešenja koja pružaju više ili manje zadovoljavajući nivo sigurnosti podataka, u ovom radu ćemo ih objasniti, analizirati i pokazati njihove jake i slabe strane.

Daćemo detaljni pregled rešenja koja se trenutno koriste, koji su trenutni ozbiljni bezbednosni problemi i koji su projekti u ovoj oblasti aktuelni u svetu.

Ključne reči: automobil, protocol, kriptografija, bezbednost, sigurnost

Cryptography in automotive industry

Abstract: As technology develops interaction between vehicles and human starts raising. In this paper we are going to analyze safety and security of personal information in vehicles. We are going to analyze safety of cryptography protocols of hardware and software which are in use in the moment and those which are still being tested and developed because this field is very popular. There are several hardware and software solutions which provide more or less satisfying level of security of data in vehicles and in this paper we are going to try to analyze and explain them and show strong and poor side of them.

We are going to explain the solutions which are now in use, what are the serious security problems in the moment and which projects are topical in this field.

Keywords: vehicle, protocol, cryptography, safety, security

SADRŽAJ

1. Uvod	- 4 -
2. Teorijski pregled.....	- 7 -
2.1 Beskontaktni sistem otključavanja.....	- 7 -
2.2 Beskontaktni sistem imobilizatora.....	- 14 -
3. Predloženi scenariji za poboljšanja sistema zaštite.....	- 21 -
3.1 Identifikacija otiskom prsta i upotreba AES algoritma	- 21 -
3.2 Identifikacija venskim otiskom prsta.....	- 30 -
3.3 Bezbednosni problemi kod modela automobila visoke klase	- 32 -
4. Zaključak.....	- 35 -
4.1 Predlog za budući rad	- 36 -
Literatura	- 37 -

Spisak slika

1.1 BESKONTAKTNO OTKLIČAVANJE/ZAKLIČAVANJE VOZILA	- 6 -
2.1 KOMUNIKACIJA PRIVESKA I VOZILA	- 7 -
2.2 SISTEMI KOJE POKREĆE IMOBILIZATOR	- 15 -
3.1 PROCEDURA IDENTIFIKACIJE	- 22 -
3.2 PRIVEZAK SA SENZOROM ZA OTISAK PRSTA	- 23 -
3.3 FAZE KOMUNIKACIJE VOZILA I PRIVESKA	- 24 -
3.4 STRUKTURA PAKETA	- 25 -
3.5 KOMUNIKACIJA U NOVOM SISTEMU	- 27 -
3.6 STRUKTURA PRIVESKA	- 28 -
3.7 FAZE KOMUNIKACIJE U NOVOM SISTEMU	- 29 -
3.8 VOLAN SA UGRAĐENIM SENZOROM	- 31 -
3.9 STRUKTURA SENZORA	- 31 -

Spisak tabela

3.1 NAJNOVIJI PODACI	- 33 -
----------------------------	--------

1. Uvod

Radio-frekvencijska identifikacija (*Radio-frequency identification* - RFID) tehnologija (1) u današnjoj formi, predstavljena je i koristi se od 1973. Relativno skoro je počela masovno da se koristi zbog svoje niske cene i visoke pouzdanosti. Mnoštvo aplikacija kojima je potreban visok nivo bezbednosti koriste ovu tehnologiju. U automobilske industriji je takođe u širokoj upotrebi u sistemima za daljinsko otključavanje i pokretanje automobila „bez ključa“ (2). U ovom radu ćemo predstaviti pregled bezbednosnih aspekata RFID tehnologije koja se primenjuje u automobilske industriji, napade na njene protokole kao i kako povećati bezbednost vozila.

Mehanički ključ automobila ima više funkcija, od otvaranja automobila, otvaranja haube i gepeka do pokretanja automobila. Tradicionalni automobilske ključevi su mehaničke prirode i kao takvi su podložni uobičajnim bezbednosnim rizicima: krađa, pravljenje duplikata ključa, obijanje brave i mnogi drugi. Takođe poznata je i metoda prespajanja žica koja uključuje premošćavanje istih kako bi se uključio automobil odnosno pokrenuo motor bez ključa. RFID tehnologija je uspela da se izbori sa ovim tradicionalnim problemima ali donela je neke nove.

Kako bi se unapredili stari sistemi ali i udobnost klijentima, takozvani sistem bez upotrebe ključa (*Remote Keyless System* - RKS) (3), prvi put je predstavljen u automobilske industriji u modelu Renault Fuego 1982. Skoro svi proizvođači automobila, još od 1995. počeli su da ugrađuju RFID imobilizatore, predajnike, koji su bili osposobljeni da prime radio signal i automatski pošalju drugi signal (*transponder-enabled*). Od 1998. zbog propisa Evropske Sigurnosne Agencije mnogi proizvođači su bili u obavezi da ugrađuju ove uređaje. RKS sistem se mogao ugraditi u svaki automobil gde se koristio sistem daljinskog otključavanja. Većina RKS sistema radi koristeći kratke radio signale, obično na razdaljini od 5 do 20 metara. Funkcionalnost RKS sistema je ugrađena na takozvani privezak ključa, odnosno mali daljinac. Sistem se aktivira kada se ovaj privezak nalazi u blizini odgovarajućeg vozila pritiskom na njegove tastere otključaj, zaključaj ili povlačenjem brave na vratima automobila što se još naziva i sistem „pasivnog otvaranja“ vozila. RKS sistem uključuje dve funkcionalnosti: sistem otvaranja automobila bez ključa RKE (*Remote Keyless Entry System* ili *Passive Keyless Entry* – PKE) i sistem pokretanja automobila bez ključa (*Remote Keyless Ignition System* - RKI) koji se odnosi na pokretanje motora.

Ranije, RKS sistem nije bio dizajniran tako da omogući zaštitu od napadača već samo da omogući korisniku udobnije korišćenje ključa. Obično je bio implementiran bez ikakvog sistema zaštite i nije rešavao probleme kao što su obijanje brave ili prespajanje žica koje koriste lopovi. Da bi se izborili sa ovim sigurnosnim

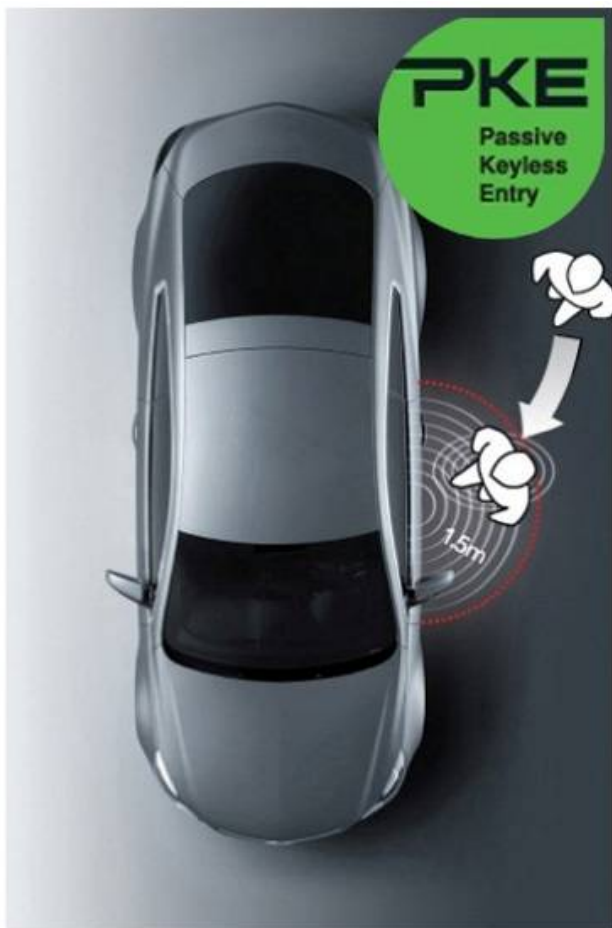
problemima, razvijeni su imobilizatori (*immobilizers*) za pokretanje automobila. Imobilizatori su elektronske bezbednosne sprave koje se nalaze u automobilu i ne dozvoljavaju pokretanje motora ukoliko odgovarajući ključ (token) nije prisutan.

Sistem je ugrađen je tako da se RFID predajnik nalazi u privesku ključa (kasnije je ovaj sistem potpuno zamenio tradicionalni mehanički ključ) i RFID primopredajnik (obično se nalazi u blizini kontakt brave za startovanje motora) koji je povezan sa jedinicom za kontrolu motora vozila (*engine control unit* - ECU). Predajnik obično ima i EEPROM memoriju (*Electrically Erasable Programmable Read-Only Memory*) za čuvanje dodatnih konfiguracija ili tajnih podataka.

Kada se ključ za pokretanje motora približi kontakt bravi, ECU pokreće primopredajnik da pošalje signal koji aktivira predajnik, a zatim sledi i komanda. Predajnik zatim odgovara sa šifrovanom porukom koju će ECU verifikovati. Predajnici su uglavnom pasivni uređaji ali mogu biti i aktivni, ako sadrže internu bateriju ponašaju se slično kao i pasivni s tim da mogu izvršavati više računskih radnji i složene zadatke. U oba slučaja, njihovu aktivaciju uglavnom pokreću signali primopredajnika.

Nakon autentifikacije, ECU će dozvoliti protok goriva i startovanje motora. Ako nije izvršena autentifikacija, ako ključ nije prisutan ili je pogrešan, motor neće biti pokrenut. U nekim modernim automobilima, neautorizovani pokušaji pokretanja motora će pokrenuti niz događaja kao što je zaključavanje automobila i komunikaciju preko satelita sa kompanijom zaduženom za sigurnost, takodje se zapisuju informacije u vezi sa brzinom i geografskom lokacijom vozila, težinom vozača i druge koje se kasnije mogu upotrebiti u krivičnim istragama i na sudu.

Mnogi proizvođači su mehaničke ključeve počeli potpuno da zamenjuju "pametnim" ključevima koji sadrže sve RKS funkcionalnosti (takodje i funkcionalnosti imobilizatora). Ovo je omogućilo da vozač ne mora da ubaci mehanički ključ u kontakt bravu i da se samim tim što se nalazi u automobilu dozvoli pokretanje motora. U početku, pri implementaciji, funkcionalnosti RKE sistema i sistema imobilizatora bili su potpuno razdvojeni ali danas su kombinovani u jedno integrisano kolo (*Integrated Circuit* - IC), zahvaljujući nisko frekvenciskoj anteni sa kalemom za funkcionisanje predajnika i ultra visoko frekvencijskim UHF predajnikom za funkcionisanje RKE sistema. U ovakvim scenarijima, imobilizatori predstavljaju jedini mehanizam zaštite.



1.1 Beskontaktno otključavanje/zaključavanje vozila

2. Teorijski pregled

2.1 Beskontaktni sistem otključavanja

Devedesetih godina prošlog veka, sistemi koji su korišćeni u automobilske industriji a koji su zasnovani na RFID tehnologiji smatrani su potpuno bezbednim i neprobojnim. Ipak, poslednjih par godina, veliku pažnju medija privukao je veliki broj uspešnih napada na sigurnosne šeme RKE sistema i sisteme imobilizatora (4) (5) (6). Takođe, bilo je puno kriminalnih aktivnosti gde su neovlašćene osobe koristila ove propuste (7) (8), kako bi došle u posed tuđeg vozila ili vrednih predmeta unutar njih.

Uopšteno, sigurnost sistema koji je zasnovan na RFID tehnologiji može se posmatrati iz dva ugla: RKE (*Remote Keyless Entry*) sistema i sistema imobilizatora. Nekada, zbog nedostataka u dizajnu, ovi sistemi imaju deljene sigurnosne sisteme ali često se protokoli i kriptografski algoritmi preklapaju.



2.1 Komunikacija priveska i vozila

2.1.1 Bezbednost sistema

U radu (9), vidimo da postoji nekoliko načina kako vozilo i privezak razmenjuju poruke i da postoje različiti nivoi sigurnosti:

Statičke šifre: U startu, RKE sistemi su se oslanjali na fiksirane šifre gde je izabrana šifra bila čuvana na privesku. U zavisnosti od korisnikove akcije, privezak emituje ovu šifru i kada je upareno vozilo u blizini ono proverava da li je šifra ispravna. Ako jeste, izvršiće se definisana operacija.

Jednokratne šifre: Ova tehnika se naziva i inkrementalne šifre gde se pri svakoj komunikaciji koristi različita šifra i ova šema je veoma korišćena u RKE sistemima. U sistemu koji koristi ovu tehniku postoji brojač koji vodi računa da se različita šifra koristi pri svakoj uspostavi veze između priveska i automobila. Vrednost tih brojača je obično šifrovana korišćenjem blok algoritma za šifrovanje. Algoritam KeeLoq je jedan od najčešće korišćenih u ove svrhe (10). Nakon komunikacije brojač u privesku se inkrementira ili uvećava. U vozilu se takođe nalazi sekvencijalni brojač. Nakon prijema signala iz priveska, automobil dešifruje taj signal kako bi dobio vrednost brojača priveska, koji zatim, upoređuje sa vrednostima svog brojača. Poruka je validna i akcija se izvršava ukoliko se razlika ovih vrednosti nalazi u određenom opsegu. Ako su svi ovi koraci uspešno izvedeni nakon akcije, brojač u automobilu se takođe inkrementira, uvećava.

Izazov-odgovor: Autentifikacija koja se bazira na šemi izazov-odgovor se najviše koristi u sistemima imobilizatora (11) (12) (13) ali je uvedena i u neke RKE sisteme. U ovoj šemi koristi se obostrana komunikacija u kojoj privezak i vozilo dele tajni ključ za šifrovanje. Nakon aktivacije (u pasivnim RKE sistemima, kada vozač povuče bravu na vratima automobila) vozilo pošalje neki slučajni broj (takozvani izazov) privesku ključa. Privezak zatim dešifruje izazov koristeći zajednički ključ za šifrovanje i šalje ovaj odgovor vozilu. Vozilo zatim verifikuje, upoređuje dešifrovani izazov (odgovor priveska) i izazov koji je poslao, ako se podudaraju zahtevana akcija se izvršava.

2.1.2 Napadi na sisteme zaštite

Poznati su mnogi scenariji napada na spomenute RKE sisteme (9). Mnogi od ovih napada predstavljaju ogroman problem za žrtve sa zakonske strane i aspekta osiguranja vozila, zato što posle većine ovih napada ostaje vrlo malo dokaza ili ih i nema. Zato je dokazivanje da se krađa uopšte dogodila (da nije u pitanju prevara) veoma teško.

Napad proverom svih mogućnosti, iscrpljivanjem: Napad poznatiji pod imenom brute-force. U zavisnosti od dužine ključa, RKE sistem može biti podložan brute-force napadima ili ne.

U slučaju kada se koristi šema sa statičkom šifrom može se izvršiti obimna pretraga ključeva pod pretpostavkom da je dužina ključa prilično mala.

A ako se koristi izazov-odgovor šema, može se izvesti specifični tip brute-force napada (poznatiji kao napad skeniranjem) gde se svakom izazovu vraća jedan isti odgovor dok ne pogodi pravi.

U suštini, na bilo koji sistem za autentifikaciju sa dovoljno velikim brojem mogućih ključeva (ili izazov-odgovor parovima) brute-force napad ne bi bio izvodljiv.

Napad ponavljanjem: Napad snimanjem i ponavljanjem jeste napad gde napadač snima poruke koje privezak ključa šalje vozilu i te poruke zatim čuva kako bi ih kasnije iskoristio.

U slučaju kada se koristi šema sa statičkom šifrom, napadač može lako da ponovo pošalje uhvaćenu poruku i automatski dobije pristup vozilu, s obzirom da se poruka ne menja pri narednom uspostavljanju veze.

Šema se jednokratnim šiframa je razvijena kako bi onemogućila ovu vrstu napada, i pri pravilnoj implementaciji ona ispunjava prvobitnu namenu. Inkrement a samim tim i šifra se menjaju posle svake uspešne akcije, što znači da napadaču ne bi uspeo napad sa ponovnim slanjem uhvaćene poruke.

I izazov-odgovor šema takođe onemogućava ovu vrstu napada s obzirom da se novi izazov koristi za svaki novi zahtev za autentifikaciju.

Ipak, moguće je uspešno kombinovati ovu vrstu napada sa napadom ometanja frekvencije (jamming attack) koji će kasnije biti razmatran.

Man in the middle (MIM) napad: Ova vrsta napada (9) (14) (15) je poznata i kao napad sa dva napadača. Uključuje napadača koji postavlja elektronski "most" između vozila i priveska. Napadač treba da povuče bravu na vratima vozila (ovo je

moguće kod sistema gde se koristi pasivni RKE sistem) što inicira slanje poruke privesku, koju će napadač uhvatiti preko pomenutog "mosta". On zatim tu poruku pošalje na drugu stranu "mosta" a zatim do samog priveska kome je poruka i bila namenjena. Privezak odgovara na ovu poruku a napadač taj odgovor istim putem proslediti do vozila koje zatim odobrava pristup. Kod ovakvog scenarija, vozač može biti u svom domu a napadač ispred. Napadač bi snimio prvu poruku koju je automobile poslao, prišao kući i prosledio tu poruku privesku. Odgovor koji je privezak poslao bi prosledio vozilu i tako dobio pristup istom. Ova vrsta napada se najlakše izvodi sa dva napadača, ali moguće je instalirati pasivnu opremu u blizini frekventnih lokacija kretanja ciljanog vozila što omogućava i jednom napadaču uspešnu realizaciju napada.

I šema sa jednkokratnim šiframa i izazov-odgovor šema su osetljive na ovu vrstu napada. Kada napadač jednom dobije pristup vozilu ovakvim "premošćavanjem" poruka kod RKE sistema, sledeći korak bi mogao biti korišćenje iste vrste napada ali ovog puta na imobilizator koji pokreće motor vozila, što omogućava napadaču da pokrene automobil i da se odveze. S obzirom da je nebezbedno isključiti motor vozila koje je u pokretu pa i u slučaju da ključ nije u vozilu, većina vozila neće zahtevati da se vozač ponovo autentifikuje (kod nekih vozila će doći do ograničavanja brzine ili će se pojaviti poruka vozaču u automobilu da privezak nije prisutan).

Kako bi se predupredila ova vrsta napada moguće je preduzeti neke mere. Najjednostavnija bi bila zaštititi ključ i privezak, kada nisu u upotrebi, faradejevim kavezom, od RF signala. Ovakva komercijalna rešenja su već dostupna na tržištu ali se retko koriste.

Bolji način zaštite bi naravno bio upotreba šeme koja ograničava razdaljinu (distance bounding) koja definiše kolika sme biti maksimalna fizička razdaljina između vozila i priveska da bi se uspostavila veza.

Napad predviđanjem: Kod ove vrste napada (tzv forward-prediction napad), napadač pokušava da, u komunikaciji vozila i priveska, predvidi, pretpostavi šta će biti sledeći izazov. On bi ovo mogao uraditi analizom prethodnih izazova koje je dobio ("uhvatio") povlačenjem brave na vratima vozila više puta (kod pasivnih RKE sistema) ili prisluškivanjem kanala koji je žrtva više puta koristila pri ulasku u vozilo.

Ako je napadač u stanju da predvidi sledeći izazov koji će vozilo poslati (zbog npr loše implementacije pseudo generatora), on bi mogao da ga pošalje privesku i kada se nalazi daleko od vozila, snimi odgovor priveska i kasnije upotrebi taj odgovor kako bi dobio pristup vozilu.

Šema sa jednkokratnim šiframa nije ranjiva na ovaj tip napada (pod pretpostavkom da su poruke šifrovane i da je ključ tajan).

Kako bi se onemogućila ova vrsta napada šema izazov-odgovor bi trebalo da koristi pseudoslučajni generator brojeva (*Cryptographically-Secure Pseudo-Random Number Generator* - CSPRNG) za generisanje izazova. Takođe, sistem bi trebalo dizajnirati tako da generator prestane da šalje izazove ako nije dobio odgovor na određen broj prethodno poslatih. Na ovaj način se smanjuje broj generisanih izazova u jedinici vremena i otežava napad.

Napad rečnikom: Napad rečnikom podrazumeva da napadač koristi elektronski rečnik sa ispravnim izazov-odgovor parovima ključa. Ovo bi uradio tako što bi generisao i slao nasumične izazove u blizini priveska a zatim skupljao njegove odgovore. Privezak bi automatski odgovarao na svaki izazov s obzirom na to da ne poseduje sistem autentifikacije pošiljaoca. Nakon pravljenja dovoljno velikog rečnika, napadač bi mogao da ode do vozila i povlačenjem brave na vratima, neprestano pokreće zahtev za autentifikaciju dok ne dobije izazov koji se nalazi u rečniku. Zatim bi upotrebio odgovarajući odgovor iz rečnika i time dobio pristup vozilu.

Kako bi se onemogućio ovaj napad, privezak bi trebalo da zaustavi generisanje odgovora posle izvesnog broja izazova ukoliko se nikakva akcija ne izvrši. Takođe, trebalo bi da postoji neka vrsta autentifikacije u privesku. Jedan takav scenario je predstavljen u radu (14), gde se u komunikaciju uključuje i neka vrsta identifikacije. Jedan deo tog IDa se šalje kao otvoreni tekst a drugi deo nadovezuje na izazov i šifruje. Takva se poruka zatim šalje privesku koji upoređuje deo IDa u otvorenom tekstu sa kopijom iz svoje memorije i ako se podudara, dešifruje ostatak poruke. Ako se i drugi deo IDa, koji se nalazi u dešifrovanoj poruci, podudara on će ponovo šifrovati izazov koristeći drugi deljeni ključ i poslati poruku vozilu kao odgovor.

Napad ometanjem frekvencije: Ovo je dobro poznati napad koji napadači izvode koristeći radio ometače. Najjednostavnije se izvodi tako što napadač pusti jači (ometajući) signal na istoj frekvenciji na kojoj radi i privezak koji napada. Zbog toga, kada korisnik želi da upotrebi svoj privezak i zaključa vozilo, vozilo neće primiti taj signal i ostaje otključano. Da bi napad bio uspešno izvršen potrebno je da korisnik ne obraća pažnju na vizuelne znake (trepćuća svetla) i audio znake (zvuke sirene) koji potvrđuju da je vozilo zaključano.

Ovaj napad bi se takođe mogao izvesti u kombinaciji sa napadom ponavljanja poruka, pri napadu na šeme sa jednkokratnim šiframa, što je dosta komplikovanije izvesti. Kako bi uspešno izveo napad, napadač bi morao da pri pokušaju korisnika da zaključa svoj automobil ometa i zaustavi taj signal kako ne bi stigao do vozila ali ga pritom treba i snimiti. Drugi pokušaj korisnika pri istoj akciji (zaključavanje automobila) treba takođe onemogućiti ometanjem signala i presretanjem poruke. Odmah po zaustavljanju drugog signala, napadač mora automobilu poslati prvu poruku koju je snimio kako bi korisniku predstavio video i audio signal da je automobil zaključan. Nakon što se korisnik udalji od automobila, napadač može

iskoristiti signal tj poruku koju je snimio pri drugom pokušaju zaključavanja i u kombinaciji sa modifikovanom porukom pošalje automobilu kako bi ga otključao. Ono što ovaj napad čini izuzetno teško izvodljivim jeste njegova delikatnost jer ako napadač "ispusti" jednu poruku koju privezak šalje, odnosno ako ona dospe do automobila, sve prethodne poruke koje je napadač snimio neće više biti važeće, odnosno napadač ne bi mogao da ih iskoristi.

Jedan od načina da se onemogući ovakav kombinovani napad bi bio pravilna implementacija kriptografskog slanja zahteva. S obzirom na to da su zahtevi jedinstveni za svaku sesiju, napadač kada presretne i snimi jedan zahtev i kada kasnije pokuša da ga ponovnim slanjem upotrebi kako bi otključao automobil, to ne bi bilo moguće zato što on ne bi odgovarao trenutnoj sesiji.

Kriptografski napadi i napadi bočnim kanalom: Pored svih pomenutih napada, napadač bi takodje mogao iskoristiti propuste u kriptografskim algoritmima i njihovoj implementaciji koji se koriste u protokolima komunikacije. Pošto specifikacije protokola i algoritama kao i detalji same implementacije variraju od proizvođača do proizvođača analiziramo jedan koji se najčešće koristi a to je KeeLoq.

Razvijen je sredinom 80-ih i bio je najčešće korišćen algoritam u RKE sistemima jer podržava i šeme sa jednokratnim šiframa (za RKE) i izazov-odgovor šeme (za imobilizatore). KeeLoq radi sa šemom sa jednokratnim šiframa uz dodatak što, pri svakoj razmeni poruka, uključuje i statički deljenu diskriminantu i vrednost funkcije koja određuje zadatak koji treba izvršiti (npr otključavanje brave) kao i redni brojač. Diskriminanta služi da se predajnik identifikuje primaocu signala nakon dešifrovanja. KeeLoq šifra je nelinearni pomerački registar sa povratnom spregom (Non - linear Feedback Shift Register - based block) sa blokovima veličine 32 bita, ključem od 64 bita i 528 rundi.

Proizvođači opreme dobijaju potpisani ključ, proizvođačev ključ k_m koji se čuva u svim njegovim prijemnicima. Kada se napravi novi predajnik, poziva se funkcija za derivaciju ključa f i izračunava se jedinstveni ključ za taj uređaj po formuli $k_{dev}=f(ID, k_m)$. Derivacija može biti obična XOR funkcija i dešifruje se korišćenjem k_m ključa kako bi se obezbedila jedinstvenost, neponovljivost čak i kada su k_{dev} i ID poznate vrednosti. Predajnik slanjem svog ID a omogućava primaocu da sazna njegov ključ tako što će izvršiti pomenutu derivaciju a na taj način dobiti i sačuvati ID i k_{dev} . S obzirom na to da je KeeLoq postao najčešće korišćen algoritam širom sveta između 1995. i 2006. došao je u centar pažnje i objavljeno je puno radova sa različitim vrstama napada na ovaj sistem (16) (17) (18) kao i različiti nivoi praktične primene.

Jedan od najboljih kriptanalitičkih napada jeste kombinacija pomeračkih napada (slide) (19) i man in the middle napada (mim) (20) zbog toga što se pri kreiranju KeeLoq šifrata koristi ista funkcija f što je podložno tzv napadima na otvoreni tekst.

Kako bi se napadala izazov-odgovor šema Keeloq potrebno je 2^{16} poznatog otvorenog teksta (za 65 minuta se može doći do ove količine podataka) i 7,8 dana računanja. Za malo složeniju varijantu ovog napada potrebno je 2^{16} izabranog otvorenog teksta i 3,4 dana računanja. Ovi napadi su mogući zato što se onaj ko šalje izazove ne autentifikuje što olakšava napadaču da dobije koliko god mu je otvorenog teksta potrebno dok kod šeme sa jednokratnim šiframa može dobiti samo šifrate. Ovakvim napadom moguće je samo klonirati predajnik. U slučaju da je i metod za derivaciju ključa loše implementiran tada je moguće doći do glavnog ključa proizvođača koji je neophodan za kreiranje novog predajnika. Iako su ovi napadi na slabosti Keeloq algoritma značajni pokazalo se da su teško praktično izvodljivi za razliku od brute-force napada (ključ je moguće dobiti iz 48 bita inicijalnog stanja za manje od 6 sati) koristeći već postojeću opremu (21). Odbrana od ove vrste napada zahteva korišćenje mnogo jačih algoritama, kao što je AES (22).

Kada je otkriven novi napad preko diferencijalne analize energije (*Differential Power Analysis* - DPA) na Keeloq (23), stvari su se promenile. Ovim napadom se vrši statistička analiza potrošnje struje mikroprocesora ili nekog drugog harvera pri vršenju operacija koristeći tajni ključ. DPA napad je potpuno razbio Keeloq algoritam i omogućio napadaču da primenom ovog napada na otiske struje, koje je sakupio "uhvatio", sazna ključ proizvođača koji se nalazi u primaocu kao i ključ uređaja u predajniku. Ovaj napad bočnim kanalom je moguće izvesti i na izazov-odgovor šemu kao i na šemu sa jednokratnim šiframa. Praktični rezultat ovog napada je pokazao da je moguće uz pomoć samo dve presretnute poruke klonirati predajnik za samo par minuta (iz 5 do 30 otisaka struje). Ako napadač ima pristup i primaocu moguće je doći i do ključa proizvođača a nakon toga i generisati novi predajnik. Ipak otkrivanje ključa proizvođača je malo komplikovanije, duže traje (potrebno je oko 10.000 otisaka struje što traje satima) i zahteva više resursa.

Inicijalno se mislilo da bi dobar vid odbrane od ove vrste napada bilo poboljšanje algoritma tako što bi njegovo početno, inicijalno stanje bio blok dužine 60 nasumično generisanih bitova. U radu (24) je objašnjeno da i pored ovog poboljšanja, sa dovoljno vremena i paralelnim izvršavanjem napada, moguće je doći do ključa.

Pojavila su se i poboljšanja samog napada (25), gde je moguće da napadač, uz smanjenu kompleksnost, iz samo jednog merenja, koristeći jednostavnu analizu potrošene energije (*Simple Power Analysis* - SPA) otkrije ključ proizvođača. Ovaj napad se bazira na tome što softverska implementacija u primaocu za svaku operaciju troši istu količinu vremena sem za pretraživanje tabele operacija. Iz tog razloga vreme izvršavanja za različite šifrate varira i čini ga ranjivim na ovaj napad.

Neke mere su preduzete kako bi se SPA i DPA napadi sprečili, jedna od njih je uvođenje konstantnog vremena (vreme izvršavanja svake operacije je uvek isto). Neki od fizičkih napada kao što je injekcija grešaka bi se mogli izvesti u budućnosti zato što trenutna implementacija koja koristi vreme koje nije konstantno, otkriva potencijalne ranjivosti na vremenske napade.

2.2 Beskontaktni sistem imobilizatora

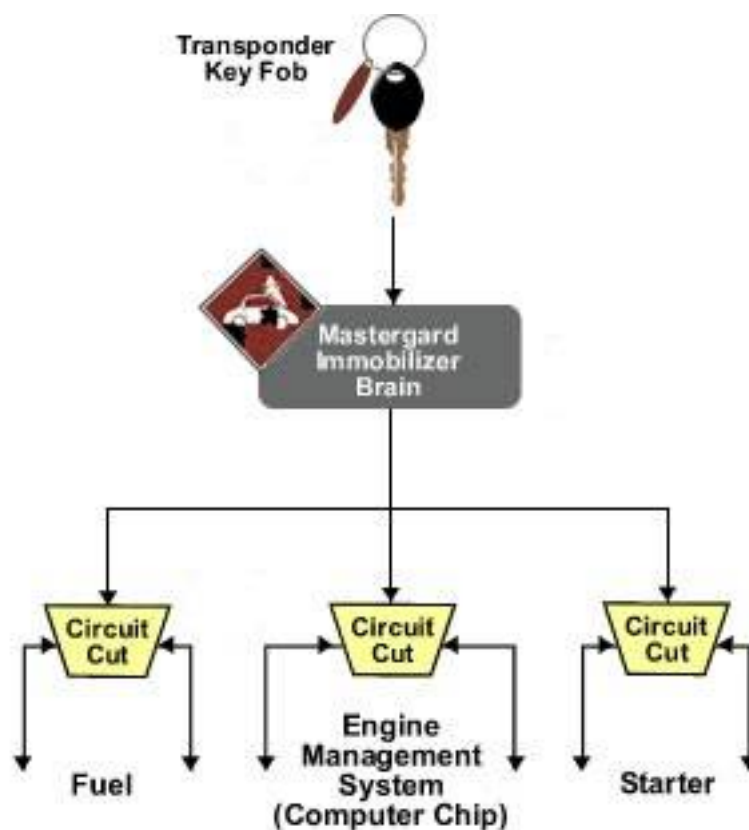
U imobilizator sistemu se najčešće koristi izazov-odgovor šema za autentifikaciju i razmenu poruka između vozila i priveska ključa. Ovaj sistem je veoma sličan RKE sistemu, funkcionišu gotovo isto, ali razdaljina u kojoj se vrši komunikacija je manja i neophodno je prisustvo mehaničkog ključa u kontakt bravi i on takođe učestvuje u izazov-odgovor šemi. Na osnovu ove sličnosti i neki sigurnosni propusti kao i napadi koji su otkriveni kod RKE sistema, uz neke varijacije, primenljivi su i na ovaj sistem. Kako ne bismo ponavljali već pomenute napade na RKE sisteme, razmotrićemo samo razlike ova dva sistema koje se tiču bezbednosti.

Ključna stvar koja razlikuje napade na RKE i imobilizator sisteme jeste to da se kod drugih komunikacija vrši u dosta manjem "bezbednom" radijusu oko primaoca. Ovaj radijus je obično ograničen na par centimetara kod imobilizatora kod kojih je neophodno da mehanički ključ bude prisutan pre aktivacije ili metar (u unutrašnjosti vozila) u slučaju imobilizatora sa "pametnim" ključevima. Preduslov napadu na imobilizator mora biti nasilan ulazak u vozilo (razbijanje prozor) ili uspešan napad na RKE sistem. Ovo ipak ne čini napade rečnikom i man in the middle napade manje izvodljivim. Pravljenje rečnika je i dalje moguće, iako je neefikasno kod nekih implementacija ovog sistema, ako se napadač nalazi dovoljno blizu priveska (koji odgovara na izazove koje šalje vozilo) i oba napada se mogu izvesti ako se napadač već nalazi u vozilu.

Kod nekih implementacija imobilizatora je dozvoljeno da se poslednji odgovor koji je poslat vozilu ponovo pošalje, što daje napadaču više vremena da dođe do originalnog odgovora i pošalje ga vozilu i na taj način zaobiđe zaštitu distance bounding protokola.

U suštini svi već pomenuti napadi koji su primenljivi na izazov-odgovor šemu moguće je izvesti i ovde, uz male izmene zbog ograničenja razdaljine, osim napada radio ometanjem koji je specijalno osmišljen kako bi se onemogućilo zaključavanje vozila.

Jedan od najpoznatijih napada (26) (27), specijalno osmišljen za sisteme imobilizatora, najviše je ciljao BMW automobile. Kod ovog napada napadači dobijaju pristup automobilu (obično kroz napade radio ometačima) zatim instaliranjem opreme za dijagnostiku u unutrašnjosti vozila (dostupne na tržištu). Napadač bi pristupio portu (*On Board Diagnostics* - OBD) vozila kako bi saznao ključ imobilizatora i kasnije mogao da napravi novi predajnik. Takođe se ugrađuje skriveni GPS uređaj kako bi pratili gde se vozilo nalazi i kako bi ga kasnije, sa kloniranim predajnikom, ukrali. Ovakvi napadi su mogući zato što se, pri komunikaciji sa OBD portom, ne vrši autentifikacija i zato što proizvođači retko obezbeđuju pristup ovom portu, što se kasnije promenilo postavljanjem malih tastera preko porta. Postoji još puno napada preko OBD porta gde su napadači uspešno premošćavali i zaobilazili zaštitni sistem imobilizatora.



2.2 Sistemi koje pokreće imobilizator

2.2.1 Napadi na imobilizatore

Napade na ovaj sistem razmatraćemo u odnosu na tehnologiju koja se koristi. Postoji puno različitih tehnologija dostupnih na tržištu ali su tri dominantne: DST, Hitag i Megamos. Objasnićemo kako funkcioniše svaka i neke poznate napade na njih.

DST: Texas Instruments' Digital Signature Transponder (DST) (28) jeste RFID predajnik sa ugrađenim kriptološkim sistemima, razvijen je 1995. i koristi se za sistem autentifikacije imobilizatora. DST šema se ugrađuje u sistem imobilizatora koja sadrži pasivni predajnik, izazov-odgovor protokol i koristi se postojeća blokovska šema za šifrovanje. Prva verzija DST šeme poznatija kao DST-40 je blokovska šifra koja koristi ključ od 40 bita za pravljenje 40 bita šifrata koji se zatim smanjuje na 24 bita i šalje kao odgovor na izazov od 40 bita koji je poslao automobil.

Istraživači su 2005., koristeći reverzni inženjering, uspjeli da dokažu da ovo nije savršena zaštita kako se verovalo. Izveli su brute-force napad i uspjeli da dobiju ključ koji su kasnije koristili kako bi klonirali predajnik. Za potrebe brute-force napada isprogramirali su nekoliko integrisanih kola (*Feld-Programmable Gate Array* - FPGA) na osnovu poznatih izazov odgovor parova i uspjeli su da dođu do ključa za jedanaest sati koristeći samo jedan FPGA. Koristeći šesnaest FPGA do ključa su došli za manje od sat vremena. Kada su za kreiranje tabele parova izazova i odgovora takođe koristili ove FPGA komponente smanjili su vreme dobijanja ključa na samo nekoliko sekundi.

Kako bi dobili ključ i klonirali predajnik napadačima je bilo dovoljno da uhvate samo dva para izazov-odgovor šeme.

Kada je u pitanju aktivni napad, napadač bi poslao izabrani izazov ciljanom predajniku i sačuvao odgovor koji dobije. S obzirom da DST predajnik odgovara na osam ovakvih zahteva u sekundi, ova faza bi se mogla izvesti iako se napadač i ciljani predajnik, ključ, samo kratko nalaze na "dozvoljenoj" razdaljini (ovo je preduslov za komunikaciju u sistemu imobilizatora). S obzirom da napadač bira izazove, on može unapred smanjiti svoju tabelu i time smanjiti vreme koje je potrebno za dobijanje ključa. Ovo omogućava napadaču da napravi uređaj za kloniranje koji će sadržati unapred smanjene tabele i koji će kada se aktivira automatski klonirati svaki predajnik tj ključ.

Kada je u pitanju pasivni napad napadač koristi opremu za prisluškivanje (može se nalaziti na udaljenosti od nekoliko metara) kako bi snimao legitimnu komunikaciju između vozila i predajnika a kasnije primenio opisani brute-force napad koristeći FPGA komponente. Ovi napadi su mogući zbog nedostatka DST-40 šifrata a to su kratki ključevi. Iako je ovo kasnije poboljšano verzijom DST-80, pokazalo se da je primena kriptanalitičkih napada i dalje moguća (29), mada nije još uvek praktično izvedena.

Kako bi se onemogućili ovi napadi na DST moguće je koristiti RFID džepove ili novčanike (30) (rade na sistemu Faradejevih kaveza) ili tzv RSA oznake (31), koje odgovaraju pozitivno na sve neautorizovane zahteve, tako blokirajući neke skenere da čitaju RFID tagove u blizini. Ovim se dakle uvodi posrednik u komunikaciji između napadača i predajnika.

Hitag: Hitag kompanije Philips/NXP (11) ima nekoliko varijanti, najčešće se koristi u RFID sistemima predajnika za imobilizatore ili u RKE sistemima (kao rezervni mehanizam u slučaju kada se pametnom ključu isprazni baterija). Novija varijanta Hitag2 je predstavljena 1996. i jedna je od najviše i najčešće korišćenih u sistemima predajnika na svetu. Hitag sistem podržava tri operacije:

1. Javna: gde se sadržaj memorije predajnika jednostavno prenosi kao otvoreni tekst kada se uključi.
2. Sa šifrom: prijemnik (receiver) i predajnik (transponder) se autentifikuju razmenjujući šifre. Pošto ovo vrše otvoreno, bez ikakve zaštite, ovaj je sistem ranjiv na napade sa ponovnim slanjem poruke.
3. Sa upotrebom kriptologije: U ovom modu, koji se koristi kod imobilizatora, Hitag prijemnik i predajnik dele zajednički tajni ključ. Na početku svake sesije, prijemnik koji se nalazi u vozilu šalje komandu predajniku koji zatim šalje odgovor sa svojim serijskim brojem. Kako bi se predupredio napad ponavljanjem poruke, inicijalni vektor IV se generiše za svaku sesiju korišćenjem tajnog ključa, IV i serijski broj se šalju za inicijalizaciju Hitag šifrovanja. Nakon inicijalizacije Hitag pravi niz bitova tj niz ključa (keystream) gde se prva 32 bita koriste za autentifikaciju a naredna 32 bita za šifrovanje. Prijemnik zatim šalje IV od 32 bita i 32 bita dug autentifikator predajniku. Predajnik zatim računa autentifikator i upoređuje ga sa dobijenim. Ako se poklope, šifruje koristeći ostatak ključa svoje konfiguracijske podatke i šifru (koristeći Hitag algoritam) i šalje kao odgovor prijemniku.

Razlika između Hitag1 i Hitag2 algoritma najviše leži u tome što Hitag2 koristi tajni ključ dužine 48 bita za razliku od Hitag1 gde je on 32 bita.

S obzirom na to da se Hitag1 potpuno oslanja na tajni ključ od 32 bita, uspešno su izvedeni brute-force napadi (29) za samo par minuta. Takođe, u radu (32) je pokazano da su i Hitag1 i Hitag2 ranjivi na napade modifikovanim rečnikom. Pošto se autentifikacija u Hitag algoritmu vrši preko izazov-odgovor šeme uspešno je izveden i napad rečnikom, tzv napad u tri koraka, tako što pre inicijacije regularnog napada rečnikom, napadač prvo sakupi seriju izazova sa ispravnim autentifikatorom. Ovo čini tako što pokreće komunikaciju sa prijemnikom koji mu ove izazove šalje jer ne zna da je u pitanju napadač. Ovaj napad bi se mogao preduprediti implementiranjem dodatnih ograničenja. Na primer mogao bi se ograničiti broj neuspešnih sesija na prijemniku (npr sa nekim istekom vremena), a mogao bi se ograničiti i broj autentifikacionih sesija na strani predajnika.

Opštiji sistem prevencije bi bio veći opseg parova izazov-odgovor šeme ili da se ograniči vreme sesije kako bi se povećala kompleksnost samog napada rečnikom to tačke neizvodljivosti.

Kako se širila upotreba algoritma Hitag2, povećavao se i broj napada na isti i nastale su razne varijacije dizajna i implementacije.

Drugi kryptoanalitički napad razvijen je za Hitag2, u pitanju je tzv kocka napad (cube attack) (33). Da bi ovaj napad bio uspešno izveden, dovoljan je minut na

prosečnom računaru. Mada, pošto se ovim napadom napadaju samo IV, njegova primena ostaje samo teorijska zato što ona najviše zavisi od same implementacije protokola Hitag2. Kako bi se sprečio ovaj napad, sigurnost šifrata (a i dužina ključa) bi trebalo da se poveća, najbolje koristeći javno dostupne jake kriptografske šeme.

Takođe, pored ovih napada, Hitag2 algoritam je bio žrtva i brute-force napada. U jednom od njih (34) napadač bi prisluškivao jednu sesiju između vozila i predajnika kako bi saznao serijski broj predajnika, IV i autentifikator pre generisanja i testiranja svih mogućih ključeva kojih ima 2^{48} . Svaki ključ se zatim propušta kroz Hitag2 algoritam i rezultujući autentifikator se poredi sa autentifikatorom koji je napadač snimio, ako se ključ poklopi on postaje kandidat. Kako bi se pronašao ispravan kandidat, svi kandidati se proveravaju preko druge snimljene sesije (koja ima drugi IV i autentifikator). Kandidat koji se poklopi jeste zapravo tajni ključ. Ako se brute-force napad izvodi na standardnom Pentium 4 procesoru trajao bi 4 godine i samim tim nije bas praktičan. Mada ako se izvršava na FPGA integrisanom kolu dobijaju se mnogo bolji rezultati, ključ je moguće dobiti za dva sata. Pošto je ovakav hardver veoma skup koristi se OpenCL framework (35) na običnom CPU i na ovako razvijenoj platformi moguće je doći do ključa za manje od 11 sati.

Rad koji je objavljen 2012. (11) otkriva još puno propusta i slabosti Hitag2 algoritma. Najznačajnije slabosti koje su otkrivene jesu:

1. Proizvoljna dužina niza ključa (keystream-a): Moguće je da napadač, bez poznavanja tajnog ključa i sa samo jednim snimljenim pokušajem autentifikacije, sazna proizvoljnu dužinu niza ključa od predajnika. Hitag2 predajnici daju mogućnost produžavanja svake komande sa 5 bitova (do maksimalne dužine poruke od 5010 bitova) koristeći redudansu poruke. Pošto se prijemnik ne autentifikuje predajniku (predajnik ne sadrži PRNG generator), moguće je ponoviti zahtev i autentifikator par i poslati predajniku. Predajnik će odgovoriti samo ukoliko je primljena poruka dešifrovana ispravno. Ponavljanjem presretnutog para i povećavanjem komande redudansom poruke (po 5 bitova) napadač treba da napadne samo 32 bita niza ključa po odgovoru da bi saznao odgovarajući niz.
2. Zavisnost sesija: U određenom trenutku šifra je potpuno inicijalizovana i od tada ona samo proizvodi nizove bitova ključa. Otkriveno je da u bloku od 48 bita šifre koja se pravi nasumično za zahtev od 32 bita, što u ovom stanju utiče samo na gornju polovinu linearnog pomeračkog registra a donja polovina ostaje konstanta, izazivajući jaku zavisnost kroz sesije tako što ovih 16 bitova ostatka odgovaraju bitovima $k_0..k_{15}$ tajnog ključa.

3. Slabe funkcije filtera: Zbog nedostatka u dizajnu same šifre (4 filtrirana bita pokrivaju 14 bita unutrašnjeg stanja) postoji šansa da 1 od 4 izlaznih bitova šifre bude određen samo sa 34 bita od 48 bita unutrašnjeg stanja. Logično, od svih pokušaja autentifikacije, 0,25% njih može otkriti jedan bit tajnog ključa.

Ove slabosti se mogu upotrebiti u sledećim scenarijima:

- a. Napad savitljivosti: algoritam je „savitljiv“ ako je moguće šifrat promeniti u drugi šifrat koji odgovara istom otvorenom tekstu.

Kod ovog napada se koristi propust generatora brojeva ili izazova kod prijemnika na delu predajnika koji je eksploatisan time što je napadač snimio ispravan pokušaj autentifikacije. Tada bi napadač mogao da analizira poruku i sazna niz ključa. On bi zatim mogao koristeći ovaj niz da pročita bilo koji memorijski blok pa čak i tajni ključ. Ako je ispravno konfigurisan predajnik ne bi mogao da pročita tajni ključ, mada, većina implementacija nije ispravno konfigurisana.

- b. Napad vremensko – memorijskom nagodbom: drugi napad (sporiji ali je primenljiv na šifre sa linearnim pomeračkim registrom) oslanja se na vremensko – memorijsku nagodbu kada je u pitanju generisanje tabele sa 2^{37} parova stanja i niza ključa. Napadač zatim imitira predajnik kako bi saznao par zahtev-autentifikator i pošalje ih ciljanom predajniku koristeći niz ključa i na taj način saznao 256 bajtova narednog niza ključa. Napadač zatim prolazi kroz ovaj niz u blokovima od 48 bita i traži ih u svojoj tabeli. Ako dođe do niza poklapanja, on ga sačuva kao kandidata unutrašnjeg stanja. Ostatak se koristi kako bi se potvrdilo unutrašnje stanje. Koristeći snimljeno unutrašnje stanje, napadač izvodi napad na šifrat kako bi saznao tajni ključ. Trajanje napada je oko minut (30 sekundi da se prikupi 256 bajtova niza ključa iz predajnika i 30 sekundi da se pregleda tabela).

- c. Kriptoanalitički napad: za treći i najjači napad potrebno je samo 136 pokušaja autentifikacije vozila (njih će sakupiti napadač imitirajući predajnik) kako bi saznao tajni ključ (uzimajući u obzir da napadač ima ispravni serijski broj predajnika). Napadač pretpostavi prva 34 bita ključa i proverava autentifikator kako bi eliminisao neodgovarajuće kandidate. Ovaj test napadač može izvršiti više puta i tako eliminiše što više pogrešnih kandidata. Na kraju, ostaće mu približno 2-3 kandidata i vrši pretragu kako bi saznao zadnjih 14 bitova. Ceo napad je moguće izvesti za svega 360 sekundi.

Kao dodatak na ove navedene propuste, dosta proizvođača pravi ozbiljne greške pri implementaciji što smanjuje još više sigurnost. Najčešće greške u implementaciji su: fabrička ili predvidiva šifra predajnika, pokretanje motora sistemom bez ključa u kojoj nije uopšte potrebna upotreba fizičkog ključa, slab pseudoslučajni generator brojeva u vozilu, tajni ključ sa šablonima koji se ponavljaju, slaba konfiguracija predajnika. Svi testirani automobili imaju liste serijskih brojeva predajnika sa kojima mogu stupiti u kontakt i da bi napadač izveo napada morao bi da sazna i koristi jedan od tih brojeva.

Kako bi predupredili ovakve napade, preporučuje se prelazak na kriptografski sigurne algoritme, produžavanje šifre predajnika kao i odlaganje komunikacije nakon neuspele autentifikacije. Takođe, korišćenje kriptografski sigurnog pseudoslučajnog generatora (Cryptographically Secure Pseudo-Random Number Generator – CSPRNG) i uvođenje u protokol autentifikaciju predajnika bi takođe poboljšalo sigurnost. Hitag kompanije NXP ima jedno rešenje gde koriste kriptografski sigurni AES, mada ne može se detaljno analizirati ova sigurnost zato što je i protokol iz iste firme.

Megamos: Megamos kompanije EM je još jedan sistem imobilizatora koji je veoma korišćen. Skoro, istraživanja su pokazala da je Megamos ranjiv na slične napade kao i Hitag2 sa sličnim nivoima praktičnosti. Istraživači nisu napadali Megamos direktno već posrednički preko softvera koji ga implementira. Otkrili su tri slabosti: slabe tajne ključeve (iako Megamos koristi ključeve od 96 bita), neredovno osvežavanje ključeva i ranjivost na kriptanalitički napad. Zbog nekih zakonskih prepreka, radovi koji su se bavili ovim, zabranjeni su i nikada nisu objavljeni. Jedan rad koji su uspeali da objave predstavio je slabost izazov-odgovor šeme u kojoj se predajnik ne autentifikuje vozilu.

3. Predloženi scenariji za poboljšanja sistema zaštite

U ovom poglavlju predložićemo različite scenarije koji implementiraju napredne kriptografske tehnike koje se zasnivaju na biometrijskim sistemima, za postizanje višeg nivoa zaštite automobila. Razmatramo:

- Identifikaciju otiskom prsta i upotreba AES algoritma;
- Identifikaciju venskim otiskom prsta;

3.1 Identifikacija otiskom prsta i upotreba AES algoritma

Trenutno postoje tri načina kako možemo ući u svoj auto i pokrenuti motor, upotrebom mehaničkog ključa, sistemom udaljenog otključavanja (alarm) i sistemom bez ključa. U svakom od ovih slučajeva vozač mora imati ključ koji automobil može prepoznati. Ključ koji vozač nosi može biti ukraden ili ga on može izgubiti a lopov naći što predstavlja veliku sigurnosnu šupljinu u prevenciji krađe. Takođe verifikacija samog ključa kod vozila nije dokaz da je osoba kod koje se ključ nalazi zapravo vozač.

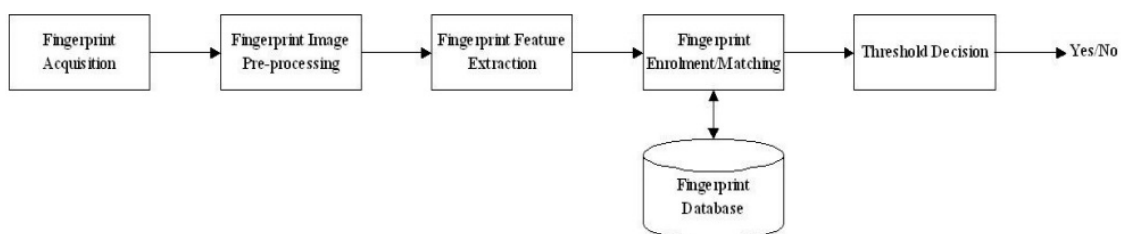
Identifikacija uz pomoć biometrije pruža rešenje za gore navedene probleme. Biometrijska identifikacija se vrši preko bioloških karakteristika svake osobe, u ovom slučaju vozača, što drastično smanjuje rizik od krađe i gubitak imovine usled vozačevog nemara. Postoji više načina biometrijske identifikacije, otisak prsta, prepoznavanje lica, iris, otisak dlana, prepoznavanje glasa kao i višefaktorska identifikacija. Prema podacima International Biometric Group (IBG) (39), identifikacija metodom prepoznavanja otiska prsta čini čak 58,9% svih biometrijskih identifikacija koje se koriste danas. Razlog za to je niža cena komponenti što je naravno prihvatljivije na tržištu.

Sistem otključavanja automobila bez ključa sa integrisanom biometrijskom identifikacijom u boljoj je mogućnosti da spreči ranije opisane napade kao što su brute-force sa pogađanjem ključa, statističke napade, maskirane napade kao i krađe.

Identifikacija otiskom prstom se danas puno koristi na laptop računarima gde se upotrebljava umesto unošenja lozinke preko tastature. Koristi se takođe i u raznim uređajima kao što su USB memorije ili mobilni telefoni. Viđa se i u sistemima koji obezbeđuju otvaranje vrata ili nekih drugih dragocenosti. Postoji određena procedura identifikacije koja se mora ispoštovati.

- U fazi prikupljanja otisaka, prikupljaju se slike otisaka sa senzora. Postoji više vrsta senzora a danas se najviše koristi silikonski senzor koji koristi elektro signale kako bi stimulisao epiderm i čuva promene ovih signala koristeći matrice.

- U fazi obrade slike otiska prsta, normalizuju se podaci i primenjuju filteri koji uklanjaju šum.
- U fazi izdvajanja karakteristika, otisci se konvertuju u određene vrednosti gde je veoma važno da one budu različite. Algoritam pretražuje detalje otiska kao što su razmaci, prekidi, petlje itd. Na kraju, ove koordinate i karakteristike se konvertuju u krajnje vrednosti.
- U fazi upoređivanja otisaka, karakteristike otiska prsta jednog korisnika se čuvaju u bazi podataka ili se upoređuju sa onima koji su već u bazi. Na kraju, ako dođe do poklapanja, ta se vrednost uzima i upotrebljava u sledećoj fazi.
- U fazi donošenja odluke, dobija se konačna odluka, da li je došlo do poklapanja vrednosti otisaka ili ne.



3.1 Procedura identifikacije

3.1.1 Sistem beskontaktnog otključavanja

Sistem otključavanja automobila bez ključa (Keyless Entry Sistem) kombinuje sistem udaljenog korišćenja ključa, otvaranje automobila bez ključa i sistem imobilizatora (40). Vozačev prenosivi predajnik komunicira preko UHF ili LF signala. Vozilo podatke predajniku šalje uvek preko LF signala.

Kada vozač povuče bravu na vratima automobila i pokuša da otvori vrata, antena koja se nalazi u automobilu šalje LF signal predajniku koji se nalazi u privesku ključa koji se nalazi kod vozača. Predajnik se aktivira nakon prijema ovog signala. Mana ovakve komunikacije jeste što će taj signal stići do svih predajnika koji se nalaze na dozvoljenoj razdaljini ali samo jedan od njih će biti izabran za sigurnosnu proveru i komunikaciju. Nakon što je odgovarajući predajnik identifikovan, antena u automobilu će poslati signal da se otvore vrata i još jedan signal kontrolnoj jedinici u vozilu kako bi se podesile automatske postavke vozila prema vozačevim željama. Kontrolna jedinica će zatim podesiti sedišta i retrovizore kako to vozač želi.

Kada je u pitanju funkcionalnost udaljene kontrole (remote control functionality) korisnik može otključati i zaključati vozilo putem neke aplikacije sa veće razdaljine. Pritiskom dugmeta na prenosivom predajniku, koji se nalazi na privesku, predajnik šalje jednosmerni UHF signal koji će „probuditi“ UHF prijemnik koji se nalazi u vozilu. UHF prijemnik zatim obrđuje signal i šalje skup bitova anteni u vozilu. Ona zatim validira ove

kodove i određuje koju je akciju korisnik zahtevao.

Sistem koji funkcioniše bez ključa sadrži sledeće komponente:

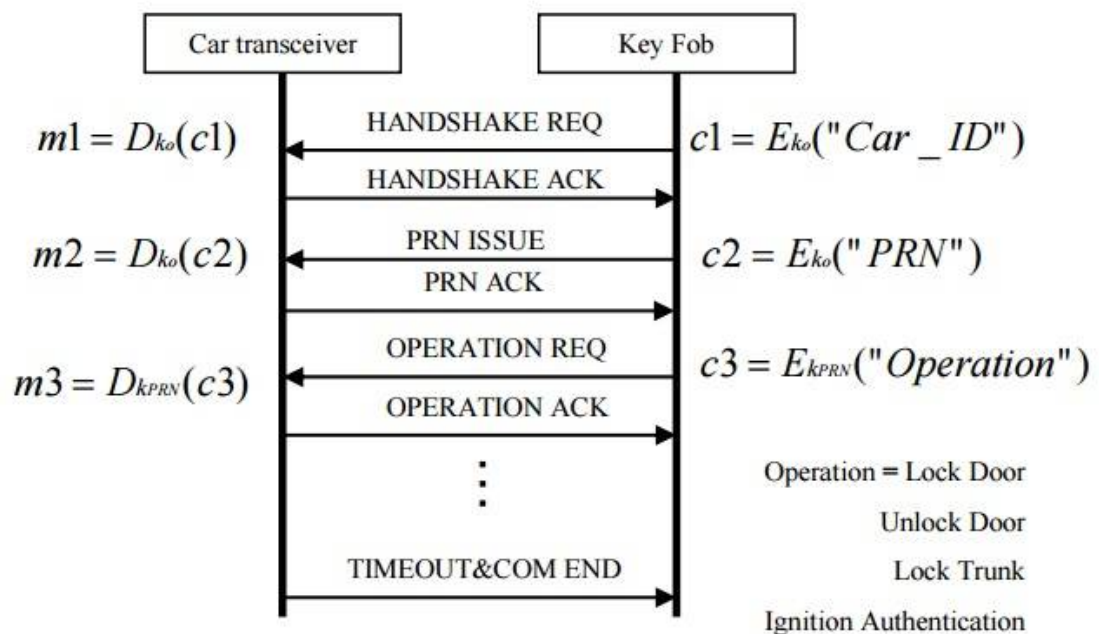
- Prenosivi predajnik koji se sastoji od logičkog kola sa interfejsima za spoljne komponente kao što su kalem, baterija, UHF odašiljač i dugme.
- LF antena koja je ugrađena u retrovizor na vozačevim vratima automobila.
- UHF prijemnik koji se pokreće kada primi sekvencu/signal od prenosivog predajnika. UHF prijemnik je povezan sa kontrolnom jedinicom u automobilu. Nakon što se sekvenca identifikuje, UHF prijemnik šalje kontrolnoj jedinici zahtev da se otvore vrata.
- Brava na vratima, u pitanju je postojeća ugrađena brava u koju se integriše dodatno dugme koje pokreće proces zaključavanja nakon uspešne verifikacije.
- Modul u vratima automobila koji kombinuje antenu i magistrale. Ovaj modul je povezan sa bravom i pokretačima. Određeni interfejs povezuje ovaj modul i CAN (Controller Area Network) magistrale.
- Kontrolna jedinica je povezana sa CAN magistralom. Kontrolna jedinica obezbeđuje kontrole automatskog podešavanja prema željama vozača koje smo spomenuli. Ona takođe kontroliše pokretače za globalno otključavanje i zaključavanje.



3.2 Privezak sa senzorom za otisak prsta

3.1.2 AES sigurnosni protokol

RKE sistem uključuje prenosivi predajnik koji se nalazi kod vozača i set primopredajnika koji se nalaze u automobilu. Komande su predstavljene putem bežičnog signala koji se prenosi između prenosivog predajnika i radio primopredajnika. S obzirom da se bežični signal prenosi u vazdušnom prostoru postoji mogućnost odavanja tajnog ključa napadaču. U predizajniranom novom AES sigurnosnom protokolu (ASP) (38), prenosivi predajnik i radio uređaj će uspostaviti vezu nakon što prenosivi predajnik inicira konekciju. Stalni, fiksirani ključ se koristi za šifrovanje poruke rukovanja (handshake) i pseudoslučajnog broja (PRN). Ovaj broj generiše prenosivi predajnik i služiće kao promenljivi ključ. Na ovaj način se može efikasno osigurati komunikacija od današnjih poznatih napada kao što je brute-force napad kojim se pogađa ključ, maskirani napad i statistički napad.



3.3 Faze komunikacije vozila i priveska

Prvo prenosivi predajnik šalje zahtev za "rukovanje" (handshake) primopredajniku koji se nalazi u automobilu. Jednačina $c1 = E(\text{KEY}, \text{Car_ID})$ znači da je šifrat $c1$ rezultat šifrovanja vrednosti koja se dobije kada se izvrši računanje nad Car_ID fiksnim ključem (KEY). Jednačina $m1 = D(\text{KEY}, c1)$ znači da se otvoreni tekst poruke $m1$ dobija dešifrovanjem šifrata $c1$ ključem (KEY). Očigledno, $m1$ predstavlja ID automobila.

Nakon što se ovaj ID autentifikuje, primopredajnik u automobilu šalje potvrdu prenosivom predajniku. Sve ove potvrde se šalju kao otvoreni tekst. Jednačina $c2 = E(\text{KEY}, \text{PRN})$ znači da prenosivi predajnik kreira 128 bita pseudoslučajnog broja (PRN) koji šifrjuje ključem (KEY). Jednačina $m2 = D(\text{KEY}, c2)$ znači da se otvoreni tekst $m2$ dobija dešifrovanjem $c2$ ključem (KEY) i $m2$ predstavlja PRN.

Ako primopredajnik u automobilu primi i uspešno dešifruje c2 poslaće potvrdu. Kada prenosivi predajnik dobije ovu potvrdu, PRN koji radi kao promenljivi ključ biće sinhronizovan u predajniku i primopredajniku. Protokol zatim ulazi u fazu iteracije operacije koje mogu biti “otključaj/zaključaj vrata”, “otvori gepek”, “autentifikuj imobilizator” i druge.

Jednačina $c3=E(\text{PRN}, \text{OPERATION})$ znači da je operacija šifrovana promenljivim ključem (PRN). Jednačina $m3=D(\text{PRN}, c3)$ znači da se otvoreni tekst m3 dobija dešifrovanjem c3 ključem (PRN) i m3 predstavlja OPERATION. Broj operacija je proizvoljan ali vremenski brojač je podešen da vodi računa koliko je vremena prošlo od zadnje operacije. Prenosivi predajnik će poslati komandu o raskidanju veze nakon što ovaj brojač dođe do granice do koje je podešen.

Sloj veze

Sloj veze (data link layer) kod ASP-a sadrži ključne informacije koje opisuju kako bi privezak ključa i primopredajnik u automobile trebalo da implementiraju mehanizam bezbednog prenosa podataka.

Length	Car ID	Direction	Type	Command	Data	Checksum
--------	--------	-----------	------	---------	------	----------

3.4 Struktura paketa

- Length – dužina – broj bajtova u paketu
- Car ID – jedinstvena identifikacija automobila
- Direction – smer – postoje dve vrste zapisa, ako je paket poslao privezak (0x00) a ako ga šalje automobil (0x01).
- Type – tip – odnosi se na tip komande: komande su kategorisane u zahteve (Request) (0x00) i obaveštenja (Acknowledge) (0x01).
- Command – komanda – kodovi komandi koji se definišu kao: rukovanje (Handshaking) (0x00), PRN emisije (PRN Issue) (0x01), opcija operacije automobila (Car Operation option) (0x02), prekid konekcije (Disconnection) (0x03).
- Data – podaci – sadržaj ovog polja može varirati u zavisnosti od tipa komande. Npr, u slučaju komande “handshaking” ovo polje i ne postoji u zahtevu. Pri odgovoru, treba poslati potvrdu da je paket primljen što znači da će ovde stajati 0x00 ako je pozitivan ili 0x01 ako je negativan. Za komandu “Operation

request” ovo polje sadrži opciju operacije za vrata automobila i pozitivnu (ili negativnu) potvrdu da je prethodni paket primljen. U slučaju PRN emisije, sadrži 124 bita pseudoslučajnog broja i potvrdu.

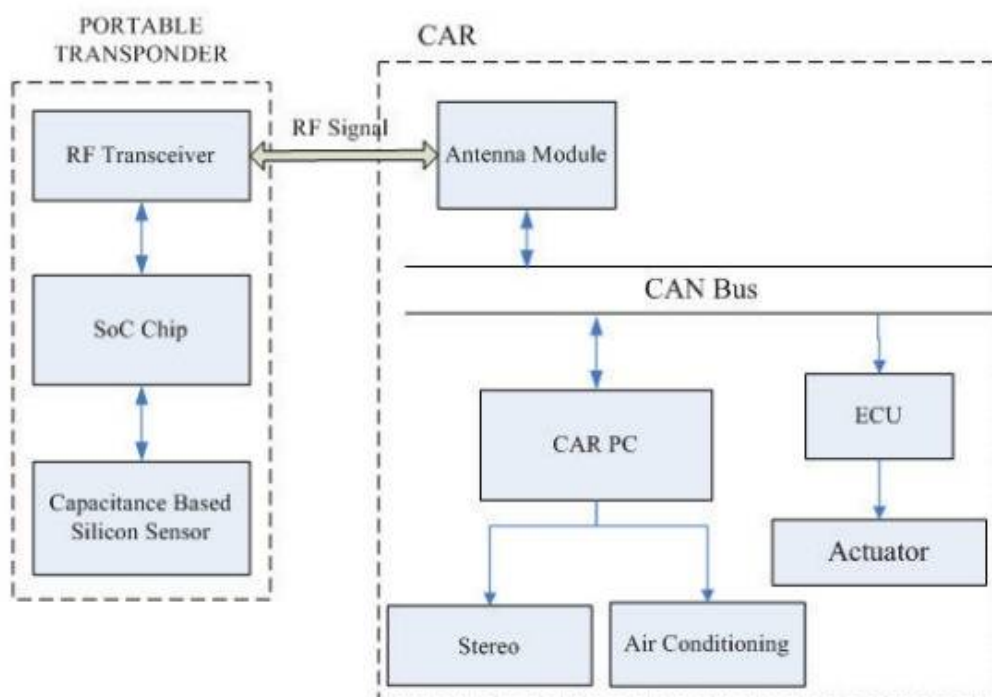
- Checksum – kontrolna suma – CRC16

3.1.3 Arhitektura novog sistema

Arhitektura novog sistema koji koristi otisak prsta za identifikaciju u RKE sistemu je prikazana **Slika 3.5**. Ovaj sistem se sastoji od prenosivog predajnika, modula za antenu, brave na vratima, modula za vrata i računara u vozilu. Prenosivi predajnik neće moći da koristi niko ko nije prošao identifikaciju otiskom prsta. Nakon što se vozač identifikuje otiskom prsta, pasivna dvosmerna komunikacija predajnika biće aktivirana. Kada vozač povuče bravu na vratima vozila, antena u vozilu šalje LF signal prenosivom predajniku. Ovim signalom se predajnik predstavlja automobilu i započinje sigurnosnu proveru. Nakon što predajnik prođe ovu sigurnosnu proveru, modul u vratima šalje jedan signal da se otvore vrata i drugi kontrolnoj jedinici da se aktiviraju specifična podešavanja vozila. Prenosivi predajnik identifikuje vozača preko njegovog otiska prsta i šalje vozačev ID modulom za bežičnu mrežu do računara u vozilu.

Ovaj bi se sistem sastojao od sledećih komponenti:

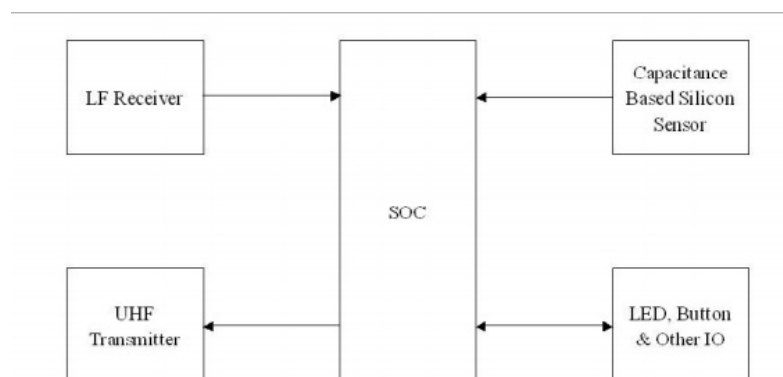
- Prenosivi predajnik koji se sastoji od SoC čipa (*System On a Chip* - SoC) sa interfejsom ka spoljnim komponentama kao što je silikonski senzor, navoji, baterija, UHF odašiljač i dugme.
- Modul za antenu koji se sastoji od antene, UHF prijemnika, magistrala i kružne antene. Ova kružna antena se nalazi u retrovizoru vozila.
- Brava na vratima
- Modul za vrata
- Računar u vozilu koji je povezan sa CAN magistralom. Ovaj računar kontroliše i automatska podešavanja vozila.



3.5 Komunikacija u novom sistemu

3.1.4 Dizajn prenosivog predajnika

U sistemu otvaranja automobila bez ključa, prenosivi predajnik je najvažnija komponenta za identifikaciju kako bi vozač mogao da pristupi svom vozilu i pokrene motor. U ovom slučaju sistem identifikacije pomoću vozačevog otiska prsta je ugrađen u prenosivi predajnik. S obzirom na to i u slučaju da je privezak sa ovim predajnikom ukraden ili izgubljen, niko ne bi mogao da otključa i pokrene automobil. **Slika 3.6** predstavlja dizajn ovakvog predajnika. SoC čip dobija sa senzora slike u nijansama sive boje (dubina bita 8 piksela) koje predstavljaju otisak prsta vozača, pronalazi i izdvaja određene detalje koji su neophodni za dalju fazu identifikacije vozača. Koordinate i karakteristike ovih detalja se zatim transformišu u vrednosti specifične za tog vozača. Za proces upoređivanja i određivanja ovih karakteristika otiska odgovoran je SoC čip. On upoređuje vrednosti koje je dobio a koje opisuju otisak trenutnog korisnika sa onim iz svoje memorije i računa koliki je rezultat poklapanja. Da li je trenutni korisnik zapravo identifikovan kao vozač ovog vozila utvrđuje na osnovu praga koji je definisan u sistemu a koji predstavlja koliki rezultat poklapanja treba biti, odnosno koliko je dozvoljeno odstupanje, da bi vozač bio identifikovan. Nakon identifikacije vozača, uključuje se LED lampica na prenosivom predajniku koja označava da li je identifikacija uspešna i vozač je sada u mogućnosti da doda novi otisak ili obriše stari pritiskom na dugme. Kada prenosivi predajnik aktivira funkciju ključa vozila, predajnik će primiti podatke koje vozilo šalje preko LF prijemnika a LF prijemnik će prenositi podatke SoC čipu koji odgovara vozilu preko UHF odašiljača. SoC čip izvršava ceo proces bežične komunikacije a podaci koji se prenose šifruju se AES algoritmom.



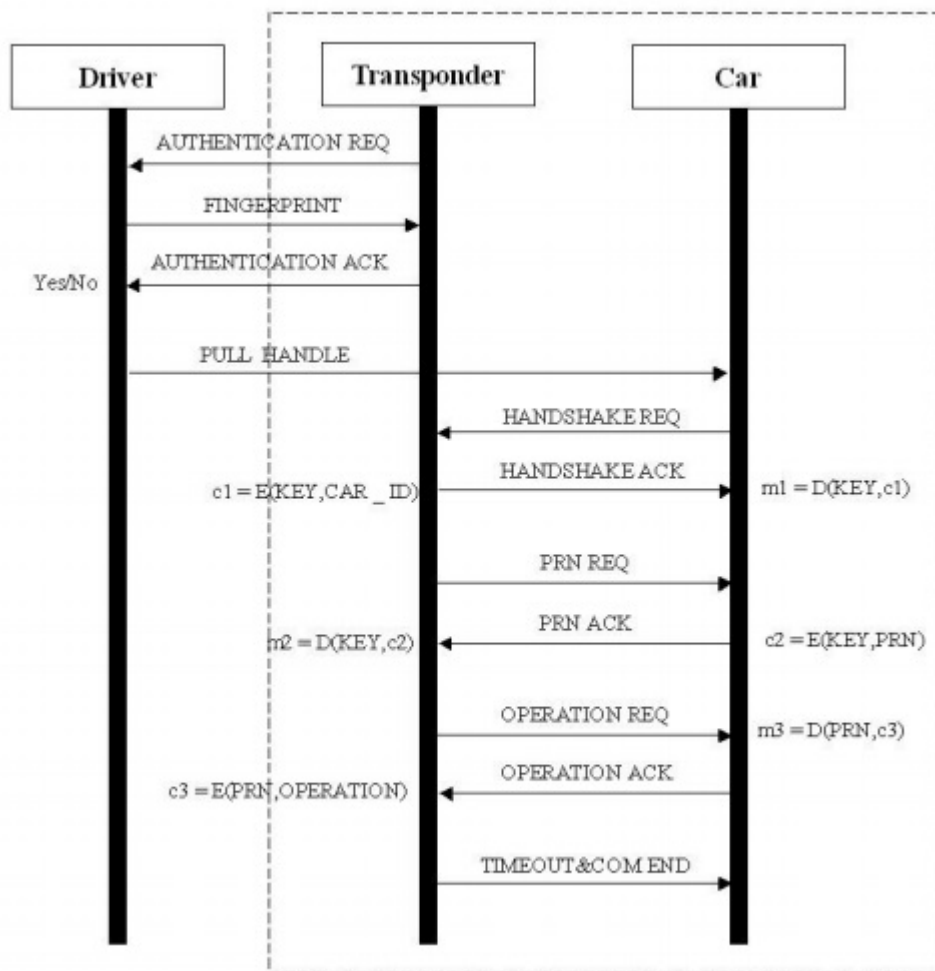
3.6 Struktura priveska

Kako bi se kontrolisao dizajn kontrolne jedinice predajnika, usvojeno je da se koristi SoC čip zato što je sistemu za identifikaciju otiska prsta potrebno dosta resursa za operacije koje izvršava a kontrolni sistem predajnika smešten je samo na jedan čip. Dakle, signali koji bi trebalo da se emituju eksterno, van predajnika, sada su signali koji se prenose unutar čipa. Ne samo što je ta distanca mnogo kraća već su protok i brzina signala drastično povećani što je rezultiralo boljim performansama. Smanjio se broj komponenti a i veličina samog čipa što je veoma važno za kompaktni prenosivi predajnik koji se nalazi u privesku. Potrošnja energije za spoljno emitovanje signala između kola komponenti je dosta manja a to produžava život bateriji predajnika. Kada je u pitanju senzor za otisak prsta, izabran je silikonski senzor koji je dosta jeftiniji od ostalih, kompaktan je i otporan na hemijske reakcije.

3.1.5 Sekvence komunikacije sistema

U RKE sistemu, komunikacijske sekvence između prenosivog predajnika i vozila su veoma važne za bezbednost. U ovom predlogu poboljšanja predlaže se korišćenje i implementacija modifikovanog AES bezbednosnog protokola (ASP). Sekvence komunikacije su predstavljene na **Slika 3.7**. Prvo, predajnik zahteva da se vozač autentifikuje a zatim vozač daje svoj otisak prsta. U zavisnosti od toga da li je otisak pronađen u bazi, predajnik vraća poruku vozaču Da/Ne. Ako je odgovor „da“ predajnik aktivira svoju funkciju ključa.

Pseudoslučajni broj se koristi za PRN u ASP algoritmu. To su slučajni brojevi koje generiše softverska simulacija generatora a kojoj je potrebno dosta prostora za računanja kao i snage. Iz tog razloga u dizajnu ovog sistema PRN broj generiše vozilo kako bi se sačuvala snaga predajnika. Takođe, izračunavanja AES algoritma koji se koristi zahtevaju dosta prostora. Zato se koristi SoC čip koji hardverski obezbeđuje dovoljno mesta i brzinu za AES šifrovanje i dešifrovanje.



3.7 Faze komunikacije u novom sistemu

Krađa predajnika – Ovakav napad bi podrazumevao da lopov dođe u posed predajnika sa ciljem da ukrade vozilo. Ali, u ovom sistemu potrebno je da se vozač identifikuje svojim otiskom prsta tako da iako bi lopov fizički posedovao pravi predajnik ne bi bio u mogućnosti da otključa automobil. S obzirom na to, ovakav vid napada ne bi bio koristan u ovom sistemu sem ako lopov ne poseduje prst vozača, za šta je verovatnoća mala.

Brute-force napad pogađanjem ključa – ASP koji se koristi u ovom sistemu, koristi AES kriptografski algoritam sa fiksnim ključem dužine 128 bita. Ovaj ključ nudi 2^{128} mogućih kombinacija ključeva. Trebalo bi više godina da bi se sve ove mogućnosti proverile, zato je ovaj napad neefikasan.

Statistički napad – Na ovaj način napadač pogađa moguće kombinacije ključeva na osnovu nekog poznatog dela šifrata. ASP koristi ključ za šifrovanje ID vozila u RKE sistemu. Ključ i ID vozila dodeljuje proizvođač svakom vozaču lično, zato je ovaj napad prilično jalov u ovakvom sistemu.

Maskirani napad – Kod ovakvog napada, napadač snima bežični signal koji šalje prenosivi predajnik. Ovaj signal može služiti napadaču za prerušeni napad. ASP koristi promenljive ključke kako bi sprečio ovakav napad. Vrednost ključa je jedinstvena za svaki pokušaj identifikacije tako da napadaču snimljeni signal nije od velike pomoći.

3.1.6 Bezbednost i pogodnosti

Ovakav sistem autentifikacije bi trebalo da spreči krađu automobila ali u praktičnoj upotrebi prenosivi predajnik neće raditi dok se ne izvrši proces identifikacije, odnosno ne dođe do poklapanja otisaka. Ovo bi moglo biti neugodno za vozače ukoliko se zahteva autentifikacija kada god on želi da pristupi vozilu. U odnosu na obične predajnike ovaj prenosivi predajnik troši više energije zbog dodatnih funkcionalnosti iako se vodilo računa o čuvanju baterije pri samom dizajnu. U budućnosti trebalo bi se pozabaviti o konfigurisanju vremena na predajniku prema potrebama vozača, npr važenje jedne identifikacije sat vremena tako da ako vozač napusti vozilo na trenutak nije potrebno da se ponovo identifikuje. Manji broj identifikacija znači i manja potrošnja energije ali povećava rizik od krađe a samim tim olakšan posao napadačima.

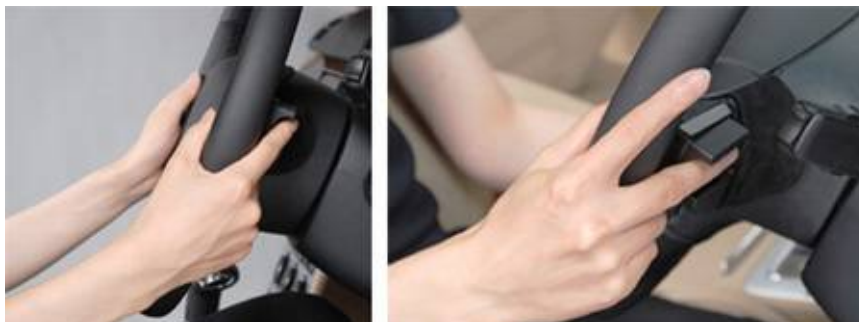
3.2 Identifikacija venskim otiskom prsta

Centralna istraživačka laboratorija Hitachi Ltd razvila je sistem autentifikacije uz pomoć rasporeda vena prsta. Od skoro su ovaj sistem prilagodili i svoje skenere podesili za upotrebu i potrebe automobilske industrije.

Kompanija ističe sigurnost i upotrebljivost kao prednosti upotrebe i instaliranja ovog sistema u volan automobila.

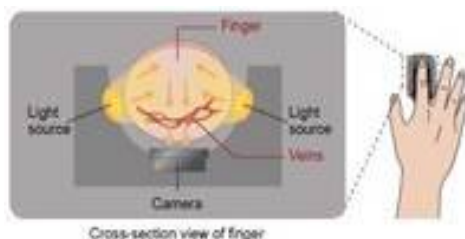
Kada je u pitanju upotrebljivost, upotreba sistema venske autentifikacije omogućava enterijer koji može zadovoljiti vozačeve zahteve (pozicija sedišta, podešavanje klime itd) kao i upravljanje raznim aplikacijama u automobilu (zvučna oprema, GPS itd). Kompanija namerava da modifikuje sistem tako da će moći da sačuva i identifikuje vensku mapu prsta više ljudi.

Ovaj sistem je razvijen po uzoru na sistem koji je vršio autentifikaciju na isti način ali se nalazio na bravi vrata automobila. Kako bi se ovaj sistem prilagodio morali su ga prilično smanjiti s obzirom da je periferija a i sam volan prilično popunjen raznim instrumentima i dodacima pa su morali pametno iskoristiti minimalan slobodan prostor.



3.8 Volan sa ugrađenim senzorom

Glavni moduli sistema autentifikacije venskim rasporedom prsta jesu izvor svetlosti i kamera. Kako bi rešili problem konkavnosti dodat je još jedan izvor svetlosti. Kada vozač postavi svoj prst na predvidjeni prostor svetlost osvetli prst sa obe strane a kamera se nalazi ispod prsta. Zbog robusnosti same opreme Hitachi je promenio jedan izvor svetlosti kamerom i prihvatio je metod koji koristi vene sa bočnih strana prsta za autentifikaciju.



3.9 Struktura senzora

Kako bi pokrenuo automobil, odnosno upalio motor, neophodno je da vozač postavi svoj prst na skener koji se nalazi na pozadini volana koji osvetljava prst, ovde se pravi slika rasporeda vena tako što se detektuje položaj hemoglobina bez kiseonika (koji je tamno plave-ljubičaste boje), ona se koduje i proverava da li postoji u bazi registrovanih vozača. Ako dođe do poklapanja, motor se pokreće.

Autentifikacija venskim otiskom prsta funkcioniše tako što se raspored vena skenira i snimi na IC (Integrated Circuit) karticu a svaki novi se upoređuje sa bazom radi poklapanja. Za razliku od otiska prsta i ostalih biometrijskih podataka koji se koriste za autentifikaciju i koji se nalaze van odnosno na našem telu, kada je venski raspored u pitanju, on se nalazi u nama i zbog toga je falsifikovanje ovih parametara ekstremno teško. Venski otisak prsta važi trenutno za jedan od najbezbednijih vidova biometrijske autentifikacije.

Još jedna prednost ovog sistema je što je oprema jeftinija od one koja se koristi za skeniranje irisa ili prepoznavanje lica/glasa. Takođe, broj pogrešno odbačenih (False Rejection Rate - FRR) je znatno niži u odnosu na sistem koji koristi otisak prsta i samim tim je pogodniji.

Kako bi se autentifikacija podigla na viši nivo, ovaj se sistem može kombinovati sa drugim biometrijskim sistemima. Ova kompanija je u saradnji sa kompanijom Sagem Securites razvila sistem koji kombinuje otisak prsta i venski otisak prsta. Razvili su, Finger VP, hardver i softver koji podržava ovakav vid autentifikacije ali on za sada nije predstavljen tržištu za komercijalnu upotrebu.

3.3 Bezbednosni problemi kod modela automobila visoke klase

Charlie Miller i Chris Valasek su u radu (47) predstavili trenutno stanje na tržištu odnosno modele automobila koji su najbezbedniji i najranjiviji na različite kriptografske napade.

Nakon provere 20 modela automobila došli su do zaključka da su 2014 Jeep Cherokee, 2015 Cadillac Escalade i 2014 Toyota Prius najranjiviji modeli. Ovi se propusti ogledaju u tome što kod ovim modela aplikacije automobila, Bluetooth, telematika koja povezuje automobil sa mrežom, se nalaze na istoj mreži kao i sistem za kontrolu motora, sistem za upravljanje, sistem za kočenje kao i sistem za regulisanje pritiska u gumama.

Takođe navodi se da model 2014 Infiniti Q50, čija je cena 37.000-45.500\$, je najranjiviji zato što telematika, Bluetooth i radio funkcionišu na istoj mreži kao sistem za kočenje što olakšava napadačima da preuzmu kontrolu nad svim operacijama automobila kojima upravlja kompjuter. Na najnovijim video materijalima koji su odradili istraživači vidi se da je moguće preuzeti kontrolu i nad vozilom koje je u pokretu.

Navodi se da je grupa studenata sa Univerziteta u Pekingu uspela da pronađe propuste najnovijeg modela Tesla S. Proizvođač je ponudio 10.000\$ istraživačima koji budu našli propuste a za ovu grupu se kaže da je uspela da otključa automobil, pristupili su sireni, unutrašnjim svetlima i sistemu za otvaranje krova dok je vozilo bilo u pokretu.

Takođe, rečeno je da je model 2014 Audi A8 najbezbedniji kao i modeli 2014 Dodge Viper i 2014 Honda Accord. U automobilu Audi A8 svi servisi i sistemi rade na odvojenim mrežama a povezani su preko mrežnog prolaza. Bežične konekcije unutrašnjeg kompjutera se ostvaruju na odvojenoj mreži u odnosu na mrežu za upravljanje.

Razdaljine sa kojih se može pristupiti nekim servisima variraju od jednog metra za sistem koji reguliše pritisak u gumama, 5 do 20 metara za pametne ključeve, 10 metara za Bluetooth do čak 100 metara za radio sistem.

Istraživači su nakon sastavljanja tabele u kojoj su naveli koliko je koji model ranjiv sastavili uređaj u vrednosti od 150\$ kojim se mogu otkriti propusti softvera automobila kao i mrežnog sistema. Ovaj uređaj predstavlja tehnologiju za detekciju i prevenciju

napada (attack detection and prevention technology). Ovo je jednostavan i jeftin način da se poboljša zaštita CAN mreže u automobilima a moguće je koristiti kod svih modela svih proizvođača s obzirom na to da sve komunicira preko CAN mreže.

MODEL	BEŽIČNA MREŽA	MREŽNA ARHITEKTURA	ELE. UPRAVLJANJE
2014 Jeep Cherokee	++	++	++
2015 Cadillac Escalade	++	+	+
2014 Ford Fusion	++	-	++
2014 Dodge Ram 3500	++	++	--
2014 BMW X3	++	--	++
2014 Chrysler 300	++	-	++
2014 Range Rover Evoque	++	-	++
2014 Toyota Prius	+	+	++
2010 Toyota Prius	+	+	++
2014 Infiniti Q50	++	+	+
2014 Audi A8	++	--	+
2010 Infiniti G37	+	++	+
2014 BMW 3 Series	++	--	+
2014 BMW i12	++	--	+
2014 Dodge Viper	++	-	--
2014 Honda Accord LX	+	+	+
2010 Range Rover Sport	-	--	-
2006 Range Rover Sport	-	--	-
2006 Toyota Prius	-	--	--
2006 Ford Fusion	--	--	--

3.1 Najnoviji podaci

“+” znak znači da je kod tog modela automobil „lakše izvršiti napad“, a znak „-“ da je „teže izvršiti napad“.

Bežična mreža predstavlja skup servisa u automobilu koji se mogu napasti: Bluetooth, Wi-Fi, mreža preko koje se povezuje sa telefonom, privezak ključa i sistem za merenje pritiska u gumama

Mrežna arhitektura predstavlja koliko gore pomenuti sistemi mogu pristupati drugim sistemima kao što su sirena, volan.

Elektronsko upravljanje predstavlja povezanost bežičnih sistema sa sistemima kao što su automatske kočnice i senzori za parking koji mogu biti kontrolisani putem bežičnih komandi.

Grupa istraživača i entuzijasta koji su pokrenuli i održavaju sajt (47) je napravila „Priručnik za hakovanje automobila“ čija je kopija besplatno dostupna na njihovom sajtu. Ovaj priručnik objašnjava brojne napade na starije ali i najnovije modele automobila kao npr napad na sistem za pritisak u gumama, mrežne napade, napade na pominjane RKE i RKS sisteme i imobilizatore kao i kako koristiti propuste proizvođača kod raznih modela automobila kojih i te kako ima.

4. Zaključak

U ovom diplomskom radu, bavili smo se bezbednosnim problemima u RKE sistemu i sistemima sa imobilizatorom. Na osnovu uvida u relevantnu literaturu u ovoj danas sve više atraktivnoj oblasti, prepoznali smo probleme i mogućnosti za implementaciju novih rešenja u tri sledeća segmenta:

Segment 1: Usporeni napredak

Unapređivanje i prelazak na novije modele RKE sistema i imobilizatora jeste vrlo usporeno. Čak i nakon što su neki sistemi prevaziđeni a njihovi propusti objavljeni javnosti, proizvođači su nastavljali da ih koriste i ugrađuju i to veoma dugo. Činjenica da se za propuste sistema DST-40 imobilizatora saznalo još 2005. a zamenjen je tek 2011. je pokazatelj na opšte naučno istraživačko stanje u ovoj oblasti, kao i da u budućnosti postoji mnogo prostora za istraživanja i potencijala za nove društvene i tehnološke doprinose.

Segment 2: Nedovoljno bezbedni kriptografski sistemi

Proizvođači se trude da kriptografski algoritmi koje koriste u sistemima imobilizatora i RKE sistemu ostanu tajni, takođe nisu detaljno javno ispitani kao ni njihova kriptografska funkcionalnost pre nego što su počeli da se upotrebljavaju. RFID uređaji imaju ograničenu memoriju i upotrebu struje što nameće određena ograničenja kriptografskih funkcija. Slabe i neispitane kriptografske sisteme je moguće zameniti pouzdanijim koji primenjuju sigurnije kriptografske algoritme kao što je AES. S obzirom na to da saznanje koji se algoritam upotrebljava olakšava posao napadaču koji će pokušati da pronađe bočne kanale i propuste, a predupređivanje ovih napada je skupo, nije ni čudo što su se proizvođači odlučili da algoritme koje upotrebljavaju drže u tajnosti. Sigurnost u mraku ne može ali mrak kao dodatak sigurnosti komplikuje posao napadaču.

Ipak, prelazak na sigurnije, jače šifre, bile one javne ili privatne, jeste svakako neophodno.

Segment 3: Greške u implementaciji:

Ovo jeste trenutno najveći problem u automobilske industriji. Ovaj tip grešaka samo dalje snižava sigurnost automobila i njihovih sistema. One često smanjuju kompleksnost napada ili čak poništavaju zaštitu sistema koji su za to predviđeni. Temeljna implementacija sistema koji primenjuje najbolja iskustva iz prakse i sigurnosnih analiza jeste nešto što je neophodno u budućnosti. Danas, najveći broj napada se bazira i koristi greške pri implementaciji softvera, zato je ovo najvažnija stavka.

Ekspanzijom digitalnih sistema i nagli broj napada na njih, proizvođači imaju dva izbora: zadržati jednostavne sisteme u vozilima i na taj način ograničiti i kontrolisati napade na njih ili investirati u ozbiljnije sisteme zaštite kako bi se eliminisali propusti u dizajnu i implementaciji kao i brza adaptacija na nove sisteme.

4.1 Predlog za budući rad

Uzimajući u obzir sve navedene propuste i poboljšanja koje smo u ovom radu naveli, daćemo dva predloga za buduća istraživanja u ovoj oblasti.

Prvi bi se odnosio na starije modele automobila, kod kojih je sistem koji se koristi teško ili nemoguće zameniti, treba istražiti i pokušati da u postojeće algoritme uvedemo svoj izvor slučajnosti kao jedan od parametara. Taj bi izvor bio "istinski" slučajan, npr koristiti neki šum, satelitski scenarijo ili iskoristiti neke parameter iz okoline.

Drugi se odnosi na novije modele, treba istražiti da li je veći problem nedovoljno dobar algoritam ili sama implementacija istog. Ako je u pitanju algoritam, treba pokušati i isprobati poznate algoritme kao što su 3DES, AES, takođe treba uvesti i već pomenuti sopstveni izvor slučajnosti radi bolje zaštite. Međutim, ako je u pitanju implementacija, treba razmotriti mogućnost što većeg i uspešnijeg razdvajanja komunikacije između automobila i priveska od ostalih komunikacija unutar vozila.

Literatura

1. http://en.wikipedia.org/wiki/Radio-frequency_identification.
2. *RFID: A Technical Overview and Its Application to the Enterprise*. Weinstein, Ron. 01-05-2005. IT Pro.
3. http://en.wikipedia.org/wiki/Remote_keyless_system.
4. <http://www.wired.com/wired/archive/14.08/carkey.html>.
5. <http://www.engadget.com/2011/01/16/research-shocker-keyless-car-entry-systems-can-be-hacked-easily/>
6. http://www.motorauthority.com/news/1024586_scientists-crack-keyless-entry-security-systems.
7. <http://hackaday.com/2012/07/07/keyless-bmw-cars-prove-to-be-very-easy-to-steal/>.
8. <http://www.telegraph.co.uk/news/uknews/crime/9623150/Lock-jammers-steal-cars-in-a-click.html>.
9. Alrabady, Ansaf Ibrahim. Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs. *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY*, VOL. 54, NO. 1. JANUARY 2005.
10. *An Introduction to Keeloq Code Hopping*. Marneweck, Kobus. 1996.
11. *Gone in 360 seconds: Hijacking with Hitag2*. Verdult, Roel. s.l. : Security'12 Proceedings of the 21st USENIX conference on Security symposium, 2012.
12. *Security Analysis of a Cryptographically-Enabled RFID Device*. Bono, Stephen C. s.l. : Proceedings of the 14th conference , 2005.
13. *Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer*. Verdult, Roel. s.l. : 22nd USENIX Security , 2013.
14. *Some Attacks Against Vehicles' Passive Entry Security Systems and Their Solutions*. Alrabady, Ansaf Ibrahim. s.l. : IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 52, NO. 2, MARCH 2003.
15. *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars*. Francillon, Aurelien. s.l. : Proceedings of the Network and Distributed System Security Symposium, NDSS, 2011.
16. Bogdanov, Andrey. *Cryptanalysis of the KeeLoq block cipher*. s.l. : Cryptology ePrint Archive, 2007.
17. *Attacks on the KeeLoq Block Cipher and Authentication Systems*. Bogdanov, Andrey. s.l. : 3rd Conference on RFID Security, 2007.
18. Eisenbarth, Thomas. *Physical Cryptanalysis of KeeLoq Code Hopping Applications*. s.l. : Cryptology ePrint Archive, 2008.
19. http://en.wikipedia.org/wiki/Slide_attack.
20. http://en.wikipedia.org/wiki/Meet-in-the-middle_attack.
21. *High-Performance Cryptanalysis on RIVYERA and COPACOBANA Computing*

- Systems*. Guneyasu, Tim. s.l. : High-Performance Computing Using FPGAs, 2013.
22. *AES Security Protocol Implementation for Automobile Remote Keyless System*. Ni, Xiao. s.l. : Vehicular Technology Conference, 2007.
23. *On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme*. Eisenbarth, Thomas. s.l. : Lecture Notes in Computer Science, 2008.
24. *Cryptanalysis of KeeLoq with COPACOBANA*. Novotny, Martin. s.l. : Special-purpose Hardware for Attacking Cryptographic Systems, 2009.
25. *KeeLoq and Side-Channel Analysis—Evolution of an Attack*. Paar, Christof. s.l. : Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009.
26. <http://www.telegraph.co.uk/news/uknews/crime/9369783/Thieves-placed-bugs-and-hacked-onboard-computers-of-luxury-cars.html>.
27. http://www.theregister.co.uk/2012/09/17/bmw_car_theft_hack/.
28. Kaiser, Ulrich. Digital Signature Transponder. *FID Security: Techniques, Protocols and System-on-Chip Design*. 2008.
29. Nohl, Karsten. Immobilizer security. *ESCAR*. 2011.
30. <http://www.epiguard.ch/ki/en/RFID-car-key-protection-55.html>.
31. http://en.wikipedia.org/wiki/RSA_blocker_tag.
32. *On the Security and Efficiency of Real-World Lightweight Authentication Protocols*. Bogdanov, Andrey. s.l. : Workshop on Secure Component and System Identification, 2008.
33. [http - http://en.wikipedia.org/wiki/Cube_attack](http://en.wikipedia.org/wiki/Cube_attack).
34. *Breaking Hitag2 with Reconfigurable Hardware*. Stembera, Petr. s.l. : Euromicro Conference on Digital System Design, 2011.
35. <http://sr.wikipedia.org/sr/OpenCL>.
36. *Broken keys to the kingdom Security and privacy aspects of RFID-based car keys*. Wetzels, Jos. s.l. : Kerckhoffs Institute, 2014.
37. *Fingerprint Identification Keyless Entry System*. Chih-Neng Liang, Huang-Bin Huang, and Bo-Chuan Chen. s.l. : World Academy of Science, Engineering and Technology, 2008.
38. *Automotive Application of Biometric Systems and Fingerprint*. Ichtermann, J., Pettit, R. s.l. : SAE World Congress, 2000.
39. *AES Security Protocol Implementation for Automobile Remote Keyless System*. iaoNi, WeirenShi, V.F. S. Fook. s.l. : IEEE 65th Vehicular Technology Conference, 2007.
40. <http://www.biometricgroup.com>.
41. *A New State-Of-The-Art Keyless Entry System*. Schmitz, C. Roser. s.l. : SAE International Congress and Exposition, 1998.
42. *On-Line, Low-Cost and Pc-Based Fingerprint Verification System Based on Solid-State Capacitance Sensor*. Mohamed K. Shahin, A. M. Badawi, M. S. kamel. s.l. : International Conference on Industrial Electronics, Technology and Automation IETA.
43. http://techon.nikkeibp.co.jp/english/NEWS_EN/20071023/141119/.

44. <http://www.wired.com/2007/10/next-step-in-ca/>.
45. <http://findbiometrics.com/biometrics-industry-news-roundup-brain-biometrics-naked-payments-and-persistent-authentication/>.
46. <http://thefutureofthings.com/5223-car-fingerprint-immobilizer/>.
47. <http://blog.hackthecar.com/wp-content/uploads/2014/08/236073361-Survey-of-Remote-Attack-Surfaces.pdf>.
48. <http://www.dailymail.co.uk/sciencetech/article-2719866/The-20-hackable-CARS-revealed-Report-lists-smart-vehicles-risk-having-systems-hijacked.html>.