

Primjena kriptografije u automobilskej industriji

- DIPLOMSKI RAD -

Student:

Profesor:

Edin Ćatovićdoc. dr Saša Adamović
br. indeksa: 230064/2013

Bijeljina, Juli 2015. godine



Edin Ćatović Primjena kriptografije u automobilskoj industriji

UNIVERZITET SINERGIJA

FAKULTET ZA RAČUNARSTVO I INFORMATIKU

Bijeljina, Raje Baničića BB

Kandidat: Edin Ćatović

Broj indeksa: 230064/2013

Smjer: Računarstvo i informatika

Tema: Primjena kriptografije u automobilskoj industriji

Zadatak: Opisati i objasniti dosadašnju primjenu, te ponuditi vlastito rješenje.

Datum odobrenja rada:

MENTOR:

Bijeljina, ____, ____, ____.

doc. Dr Saša Adamović



Primjena kriptografije u automobilskoj industriji

Sažetak : U radu težište je na opisu primjene kriptografije u automobilskoj industriji od samog početka pa do danas. Osim toga bitno je bilo istaknuti kakve nam sve prednosti donosi njena primjena, a koje nedostatke. To se prije svega odnosi na primjenjena kriptografska rješenja, kao i opis hardwera koji je djelimično ili u cjelosti učestvovao u implementaciji istih. U tu svrhu su detaljno opisani, sve vrste automobilskih ključeva, kao i primjenu RFID sistema u automobilima. Nakon detaljno obradjene problematike, cilj je bio ponuditi vlastito rješenje, te isto i implementirati. Kao razvojno okruženje korišten je Arduino IDE (Arduino Uno R3 board), uz podršku namjenskog hardware-a. Ponuđeno rješenje, dio je oblasti biometrije, preciznije paljenje automobila nakon skeniranja otiska prsta (Adafruit biometric fingerprint sensor).

Ključne riječi: Kriptografija, automobilska industrija, RFID, biometrija, Arduino

The use of cryptography in the automotive industry

Summary : The paper focuses on the description of the application of cryptography in the automotive industry from the very beginning until today. Furthermore it was important to point out what advantages brings its application, and which disadvantages. This primarily refers to the applied cryptographic solutions, as well as a description of hardware that is partially or fully involved in the implementation thereof. To this purpose are described in detail all kinds of car keys, as well as the application of RFID systems in cars. After thoroughly deals with the problems, the goal was to offer my own solution, and implement it. As a development environment is used Arduino IDE (Arduino Uno R3 board), with the support of dedicated hardware. The solution that is offered is part of the field of biometrics, more precisely ignition car after scanning a fingerprint (Adafruit biometric fingerprint sensor).

Keywords: Cryptography, automotive industry, RFID, biometrics, Arduino



SADRŽAJ

1.	Uvod	1
1.1.	Zašto je tema interesantna?	1
1.2.	Kakva je primjena kriptografije i na kojim nivoima?	3
1.3.	Struktura rada	6
2.	Pregled u oblasti istraživanja	7
2.1.	Vrste ključeva	7
2.1.1.	Klasični metalni ključevi	7
2.1.2.	Metalni ključevi sa imobilajzerom	8
2.1.3.	Remote keyless entry ključevi	9
2.1.4.	Remote keyless ignition sistem ključeva	10
2.2.	Pregled dosadašnjih kriptoloških rješenja	11
2.2.1.	Imobilajzeri	13
2.2.2.	Texas Instruments DST (Digital Signature Transponder)	14
2.2.3.	KeeLoq	14
2.2.4.	HITAG2	14
2.2.5.	Megamos Crypto	15
3.	Teorijske osnove istraživanja	16
3.1.	RFID	16
3.1.1.	Historijski razvoj RFID sistema	16
3.1.2.	Vrste RFID transpondera	17
3.2.	Pasivni transponderi	20
3.3.	Djelimično aktivni transponderi	20



Edin Čatović Primjena kriptografije u automobilskoj industriji

3.4.	Aktivni transponderi	20
3.5.	RFID etikete	21
3.6.	RFID čitači	21
3.7.	Trenutna i buduća primjena RFID sistema	22
3.8.	Ranjivost RFID sistema	23
3.9.	Zaštita RFID transpondera	23
3.10.	Biometrija	24
3.10.1.	Fizička biometrija	25
3.10.2.	Biometrija ponašanja	25
3.10.3.	Multimodalna biometrija	25
3.11.	Otisak prsta	26
3.11.1.	Karakteristike otiska prsta	28
4.	Evaluacija bezbjednosti kriptografskih mehanizama u automobilskoj industriji	31
4.1.	Poznati napadi	31
4.1.1.	Indirektan fizički pristup	31
4.1.2.	Bežični pristup kratkog dometa	32
4.1.3.	Bežični pristup velikog dometa	32
4.1.4.	Napad na telematski sistem	33
4.1.5.	MP3 maliciozni program	33
4.1.6.	Neovlaštene aplikacije	33
4.1.7.	Zaključavanje vrata	34
4.1.8.	Daljinsko otključavanje automobila	34
4.2.	Preventiva	35
4.2.1.	Napad na automobilski hardver	36
4.2.2.	Zaštita automobilskog hardvera	37



4.2.3.	Zaštita automobilskeg softvera	37
4.3.	Predloženo rješenje	38
4.3.1.	Softversko-hardversko okruženje	38
4.3.2.	Eksperimentalni rad	39
5.	Zaključak	51
5.1.	Prijedlog za budući rad	51
6.	Literatura	52



1. Uvod

1.1. Zašto je tema interesantna?

Svjedoci smo svakodnevnih naslova, u elektronskim, a i štampanim medijima, tipa „Automafija ne poznaje granice“, „Automafija i ove godine korak ispred policije“, „Automafija hara Balkanom“ i sl. Sve to ukazuje da je jedan od glavnih problema, u regionu, a i Evropi, kako zaustaviti, ili bar smanjiti krađu vozila na tim prostorima.

Naime, dnevno se u BiH ukradu tri vozila, a pronalaze ih u Crnoj Gori, Albaniji, Rusiji, Srbiji i na Kosovu. Krađe automobila u Bosni i Hercegovini ponovo postaju sve ozbiljniji problem, a policijske agencije ukazuju na gotovo dramatičan porast broja ukradenih vozila. Posljedica je to djelovanja organiziranih i opasnih grupa kriminalaca, opremljenih visokosofisticiranom opremom, odnosno automafije.

Osim u BiH, automobili se masovno krađu u Srbiji, Hrvatskoj, Crnoj Gori, na Kosovu. Koriste se slični ili isti principi, a dosta tih automobila završi u BiH. Na osnovu zahtjeva evropskih osiguravajućih kuća na prostoru Balkana potražuje se čak 130.000 ukradenih vozila, od toga samo u BiH više od 20.000!

Prema dostupnim informacijama Federalne uprave policije (FUP) i Ministarstva unutrašnjih poslova Republike Srpske (MUPRS), od januara do jula 2012 godine u BiH je ukradeno čak 607 automobila. To znači da se u BiH dnevno ukradu najmanje tri automobila. Također, izvještaji crne hronike u dnevnim novinama i u julu i avgustu iste godine bili su prepuni informacija o ukradenim autima.

Samo na području Federacije BiH automafija je u prvom polugodištu 2012. godine u nepoznatom pravcu odvezla 526 vozila, što predstavlja rast od skoro 30 posto u odnosu na godinu ranije.

Najviše osoba je bez svog ljubimca ostalo u Sarajevskom Kantonu – čak 340. Također, u nekim dijelovima Federacije BiH broj ukradenih vozila porastao je i do 900 %.

Istovremeno, u Republici Srpskoj je ukraden 81 automobil, što predstavlja smanjenje u odnosu na 2011 godinu kada su ukradena 104 automobila. Od tog broja, vlasnicima su vraćena 53 automobila. Među njima je bilo i 19 vozila ukradenih na području FBiH. Pronađeno je i 12 automobila za kojima je tragao Interpol.¹

¹http://www.slobodna-bosna.ba/vijest/2107/automafija_hara_balkanom.html



Na meti automafije najčešće su automobili marke „Volkswagen“, popularna VW vozila. U prvoj polovici ove godine ukradeno je čak 356 takvih vozila na području Federacije BiH. Slijede vozila marke "Škoda", ukradeno je njih 34, pa 28 automobila marke "Audi", 21 BMW, 19 "Reanulta" . Inače, automobili njemačke, francuske ili češke proizvodnje na meti su i u drugim balkanskim gradovima.

Nakon krađe, slijedi ucjena vlasnika vozila. Osim toga aktualna je varijanta rastavljanja vozila u dijelove. Na ovaj način vozilu se gubi svaki trag, a automafija nesmetano šalje rasklopljeno vozilo do nove destinacije. Zabilježeni su slučajevi kada se za transport tako rasklopljenog vozila koristili kamioni sa „plombama“, određenih autoprevoznika (vozila koja mogu biti otvorena samo uz nalog i od strane lica iz MUP-a). Treba navesti, da je automafija u uskoj vezi i sa autootpadima sirom regiona, sto im olakšava distribuciju dijelova ukradenih vozila. Nije rijedak slučaj da imaju svoje ljude i u policiji.



Slika 1. Ilustracija pokušaja krađe vozila

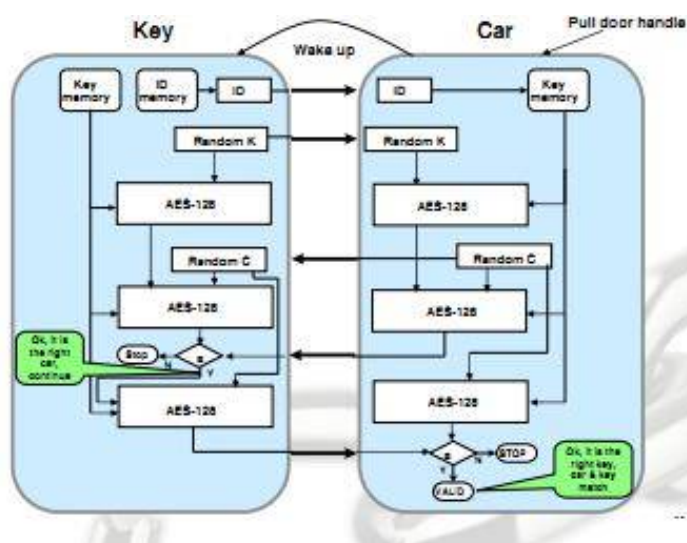
Izvor: www.google.ba

Iz svega navedenog se vidi da je tema i više nego aktuelna. Ovo je izražen problem i u mnogo razvijenijim zemljama, od zemalja regiona. Nalazimo se u vremenu kada stabilna i praktična kriptološka rješenja imaju neprocjenjivu vrijednost u svijetu autoindustrije.

1.2. Kakva je primjena kriptografije i na kojim nivoima?

Kriptografija u autoindustriji, veže se za kraj 80-ih i početak 90-ih godina, sa pojavom pristupa vozilu bez ključa (eng. Remote Keyless Entry, RKE) i pokretanju vozila bez ključa (eng. Keyless Go). Nakon toga dolaze elektronski imobilajzeri. U izoliranom sistemu, kakav je današnji automobil, imamo dosta kriptografskih rješenja. Međutim, o njima se jako malo govori. Govori se zapravo tek onda, kada neko od rješenja poklekne pred napadima zlonamjernih ljudi. Kao primjer ću navesti, 40 bitnu enkripciju, na transponderima firme Texas Instruments, koja je vrlo brzo probijena. Osim ovoga, imamo i Hitag2 enkripciju, vlasništvo NXP-a, koja je takođe probijena. RKE sistem KeeLoq, koji se koristio za otvaranje garažnih vrata, ali i na nekim automobilima, postao je nepopularan, nakon što su otkriveni propusti, uslijed par napada.

Pored svega, zadnjih godina se puno radilo na razvijanju jakih kriptografskih rjesenja za autentifikaciju. Na primjer, 2014 godine, firma Atmel, predstavila je novi „single chip“ AES-128 imobilajzer i „keyless entry“ AVR mikrokontroler.



Slika 2. Atmel AES 128 imobilajzer;

Izvor: www.atmel.de



Čak se sada raspravlja i o asimetričnim solucijama, a kao primjer navešću ECC Remote Control Entry, od Fraunhofer SIT, razvijen uz pomoć Siemens.

Osim toga, u posljednjim godinama kriptografija se sve više upotrebljava za zaštitu ECU-a koji upravlja parametrima motora. Manipulacija pritiskom goriva, turbine i sl. čime najčešće manipulišu tunerske kuće (popularni čip tuning). Proizvođači ulažu novac kako bi kriptološki zaštitili svoje kontrolne jedinice od neovlaštenog pristupa i modificiranja, a u isto vrijeme nude fabrički tuning, po znatno većoj cijeni, ali bez gubitka fabričke garancije na vozilo.

Takodje, ulaže se i u zaštitu njihovih multimedijalnih sistema, koji su danas jako kompleksni. Prilikom svog rada, takvi sistemi koriste i neke povjerljive informacije vlasnika vozila. Zaštita se bazira na principu kriptološke zaštite pristupa, te sprječavanju narušavanja privatnosti vlasnika.

Sve veći trend povezanosti modula unutar vozila, znači da nema dobre sigurnosti bez prethodno dobre zaštite. Opcije zaštite uključuju danas ne samo zaštitu od fizičkog pristupa ili skrivanje povjerljivih podataka, nego i zaštitu kritičnih sigurnosnih sistema.

Proizvođači moraju predvidjeti sve oblike napada, kako bi na taj način spriječili pristup ugrađenim sistemima i podacima. U isto vrijeme, autoindustrija u cjelini mora razviti standarde, specifikacije i smjernice za sigurnost vozila, koje omogućavaju interoperabilnost.

U zadnje vrijeme, postoji značajan porast interesovanja za sigurnost mikrokontrolera u automobilske industriji. Kada se elektronika počela primjenjivati u autoindustriji, davne 1970 g. , bila je prilično jednostavna, možda bolje reći diskretna, i nije bila povezana sa ostalim komponentama vozila, kao što je to slučaj danas.

Recimo komponenta koja je kontrolirala svjećice na motoru, nije međusobno komunicirala sa brzinomjerom na instrumentnoj tabli. Ne tako davno, prije nego je Bluetooth i Wifi tehnologija zaživjela u automobilima, možemo reći da je putni računar bio najsavremenija tačka novog automobila.

Tokom vremena, kombinacija povećane elektronske složenosti sa drugim fiksnim i prenosnim komponentama unutar vozila (pristup vozilu bez ključa „keyless entry“, audio sistem, telematika, bežična komunikacija „Wifi“, itd) pretvorila je male elektronske dijelove u elektronske sisteme, duboko usađene u vozilo.

Sistemi koje koriste sami vlasnici vozila, sadrže privatne, a samim tim i povjerljive informacije. Ti isti sistemi su fizički vezani za vozilo, sto znači da ukoliko je bilo koji od njih kompromitovan, na bilo koji način, javlja se prilika za krađu samog vozila, ili bilo koji vid nanošenja štete od strane vanjskih subjekata.



Vozila koja se prodaju danas, sadrže čak i više privatnih informacija, jer su postala kao pametne kartice na točkovima. Sve to produkt je želje proizvođača da se pojednostavi plaćanje računa na benzinskim pumpama, punktovima za dopunu (električni automobili), plaćanje na parkinzima, naplatnim kućicama na autoputu i sl. U bliskoj budućnosti očekujemo da će automobilima biti omogućeno plaćanje, ali bez imalo uticaja čovjeka.

Sigurnost je prešla dalek put, sjetimo li se početaka, kada su uvedeni auto alarmi, ili pristup vozilu bez ključa („keyless entry“). U današnjim vozilima to više nije samo zaštita fizičkog pristupa vozilu, ili zaštita povjerljivih informacija. Danas se tu podrazumijeva i kontrola mnogih drugih sistema (sistem kočenja, sistem upravljanja vozilom i sl.). Ono što je najbitnije, što automobilske proizvođači žele da smanje, ili u potpunosti onemoguće, je ugradnja krivotvorenih dijelova sa drugih automobila, te spriječavanje korištenja jedne kontrolne jedinice (ECU) na više automobila. Ovo je jedino moguće upotrebom protokola za autentifikaciju.

Osim navedenog, radi se na zaštiti izmjene operativnih parametara, koji su smješteni u memoriji. Sigurnosne postavke, mogu spriječiti, ili upozoriti na nedozvoljenu radnju nad operativnim podacima u memoriji, te poduzeti neku radnju da se isti eliminišu, ukoliko je do izmjena došlo. Definisanje i implementacija arhitekture mikrokontrolera zahtijeva velike mentalne napore. Dizajner samog sistema mora razmišljati poput hakera, te pokušati implementirati neprobojan sistem, koji će osigurati pristup i manipulaciju povjerljivim informacijama.

Veliki napori se ulažu u autoindustriji u razvoj standarda, specifikacija i smjernica za sigurnost vozila. Standardizacija omogućava veću interoperabilnost između komponenti sistema, koje su isporučene od različitih proizvođača. Kada je standard postavljen, znači da svi proizvođači imaju priliku da učestvuju u proizvodnji sigurnosnih sistema, ili njihovih dijelova.



1.3. Struktura rada

Prije svega osvrnuli smo se na same početke primjene kriptografije u automobilskoj industriji i hardvera koji je bio potreban za njenu implementaciju. Shodno tome, istraživanje je započeto od ključeva, preko „keyless entry“ sistema, objašnjenja za način funkcionisanja i primjenu RFID uređaja (obzirom da su obuhvaćeni imobilajzeri, samim tim i transponderi kao glavni njihov dio). Nakon što su detaljno obrađeni pomenuti pojmovi, opisani su i napadi kojima su podložna dosadašnja kriptografska rješenja.

Glavni doprinos rada:

Imajući na umu atraktivnost biometrije i njeno usmjerenje ka budućim vremenima, odlučeno je da budući sistemi zaštite u autoindustriji budu vezani za biometrijske sisteme. Radi se zapravo o paljenju automobila, prethodno koristeći biometrijski senzor otiska prsta, kao način autentifikacije.

Prvo poglavlje, donosi uvod u problematiku, i objašnjenje zašto je ova tema toliko aktuelna, pogotovo u zadnjih desetak godina. Tu se nalazi i kratak opis načina primjene kriptografije, i nivoi na kojima je to primjenjeno u automobilskoj idnustriji.

U poglavlju dva, dat je detaljan pregled u oblasti istraživanja. Detaljno je objašnjeno sve o hardveru i softveru, koji se koristi prilikom implementacije kriptoloških rješenja u automobilima.

Treće poglavlje orijentisano je na opis teoirjskih osnova istraživanja. Pa su tako obuhvaćeni RFID tehnologija, biometrija, te na kraju i implementirani, otisak prsta.

Poglavlje četiri, daje opis svih poznatih napada, te preporuke za preventivu, kako automobilskeg hardvera tako i softvera.

Poglavlje pet

U radu je ponuđeno i praktično rješenje, kako softverski, tako i finalnom hardverskom implementacijom. Sve to, ali i mnogo više slijedi u nastavku.



2. Pregled u oblasti istraživanja

2.1. Vrste ključeva

Prema dosadašnjim istraživanjima prvi ključ u automobilskoj industriji, korišten je 1949 godine, kao ključ za pokretanje automobila, od strane Chrysler korporacije. Ovo rješenje kombinovalo je tada dvije odvojene funkcije, starter i paljenje u jednom prekidaču. Odsustvo tipki, primjenjivalo se prije svega u svrhu prevencije, kako djeca ne bi slučajno pokrenula automobil, dok je u brzini.



Slika 3. Prvi ključ, Chrysler korporacija, 1949 g.

Izvor: Andrej Šimko, Security of car keys, 2014 g.

2.1.1. Klasični metalni ključevi

Već pomenuti ključevi, predstavljeni i pušteni u upotrebu 1949 godine, od strane Chrysler korporacije. Nisu pružali neki nivo sigurnosti, jer se auto mogao lako paliti „na žice“. dakle to su bili obični ključevi, koji sa sobom nisu nosili nikakav sigurnosni mehanizam, što ih je činilo veoma lakim za kopiranje.



Slika 4. Klasični metalni ključevi;

Izvor: Andrej Šimko, Security of car keys, 2014 g.

2.1.2. Metalni ključevi sa imobilajzerom

Da bi se pokrenulo auto sa ovim tipom ključa, bile su potrebne dvije komponente. Prva, sam metalni ključ, koji bi stavili u bravu automobila, a druga, ujedno i bitnija, sakrivena u plastičnom kućištu, nazvana imobilajzer. Radilo se o skrivenom RFID transponderu, pasivnog tipa, (nije imao vlastito napajanje, nego se napajao elektromagnetnom indukcijom). Radio je na niskim frekvencijama, između 125-130 kHz, što mu je omogućavalo i uspostavljanje komunikacije sa računarom automobila (ECU-om).



Slika 5. Metalni ključ sa imobilajzerom;

Izvor: Andrej Šimko, Security of car keys, 2014 g.



Ovaj način zaštite, bio je otporan na paljenje automobila „na žice“. Čak je bilo lako i eksperimentisati sa ovom vrstom zaštite i moglo se provjeriti da li sistem zaista i radi. Naime poznavajući da RFID sistemi su podložni uticaju Faradejevog kaveza (to je i jedan od napada), plastično kućište ključa se umota u aluminijsku foliju. Aluminijska folija tako pravi Faradejev kavez, i sprječava komunikaciju transpondera sa ostalim entitetima, u ovom slučaju računarnom automobila.

Ukoliko ne možemo upaliti automobil, imobilajzer je prošao test. Dok u drugom slučaju, zaštitu smo zaobišli. Važno je napomenuti, da je upotreba imobilajzera u automobilu, znatno smanjila broj ukradenih automobila u svijetu. Prema nekim informacijama iz 2001 g. zabilježen je pad od nekih 70%.²

Bitno je imobilajzere podijeliti u dvije grupe. Ovi o kojima je prethodno bilo riječi, ili elektronski imobilajzeri. Iako su imali slabu entropiju i bili podložni mehaničkoj manipulaciji, donijeli su pad u oblasti autokriminala.

Druga vrsta su kriptografski imobilajzeri, ujedno i pioniri kriptografije u automobilizmu. Kako i samo ime kaže, koristili su kriptografske protokole, a fizički skoro identični elektronskim imobilajzerima. Međutim, brzo se javio nedostatak, koji se ogleda u tome, da velike firme koriste vlastita kriptografska rješenja, te svjesno prikrivaju njihove nedostatke. Poznato je da su podložni reverznom inženjeringu i to RC4 šifre, zatim A5/1 i A5/2 šifre takođe korišteni kod sim kartica i gsm telefona.

2.1.3. Remote keyless entry ključevi

Ključevi koji služe za daljinsko otključavanje i zaključavanje automobila, kao i otvaranje gepeka na daljinski, te aktivaciju i deaktivaciju alarma. Za razliku od imobilajzera, aktivni su, dakle imaju vastito napajanje. Stariji modeli radili su na infra-red principu, dok noviji rade na principu radio talasa i to na frekvencijama između 315-433 MHz. Domet varira od 10-100 metara zavisno od modela.

Prvi automobil, sa ovakvim sistemom u primjeni bio je Renault Fuego, 1982 godine.

²Andrej Šimko, Security of car keys, 2014 g.



Slika 6. Remote keyless entry ključ;

Izvor: Andrej Šimko, Security of car keys, 2014 g.

2.1.4. Remote keyless ignition sistem ključeva

Najnovija generacija ključeva, također aktivna verzija. Ne sadrže nikakav metalni ključ ni za pristup ni za paljenje vozila. Omogućavaju pristup (otvaranje) i pokretanje (paljenje vozila) sa ključem u džepu. Potrebno je samo da dotaknete odgovarajući senzor, na vratim za pristup, i na kontrolnoj tabli za paljenje. Izrađeni su u obliku plastične kartice pa se neki mogu umetnuti u za to predviđen slot.

Koriste dva radio kanala, prvi niskih frekvencija, za otvaranje auta sa ključem u džepu. Preporučena udaljenost od auta je 10-15 cm, zbog mogućih zloupotreba. Npr. krađa auta na benzinskoj pumpi, ili prilikom odlaganja stvari u gepek. To su frekvencije između 120-135 kHz. A drugi kanal ultra visokih frekvencija radi između 315-433 Mhz, i koristi se za otvaranje automobila na udaljenostima između 50 i 100 metara.



2.2. Pregled dosadašnjih kriptoloških rješenja

Zastarjele metode nude vrlo neizvjestan i neučinkovit pristup, za zaštitu najmodernijih okruženja. Danas se implementira sigurnost u kombinaciji sa kriptografskim algoritmima, koji nisu skriveni, čak štaviše dostupni su javnosti.

U inženjerskoj automobilske zajednici, dobar broj specifikacija aktivnosti je na putu, ili je već dobio status standarda. Na primjer, Secure Hardware Extension (SHE), specifikacija razvijena od Escrypt-a, za BMW i Audi preko HIS Working Group u kooperaciji sa Freescale-om 2008 godine, već sada je prihvaćena kao slobodan standard.

SHE specifikacija definira skup funkcija i programski model (API) koji omogućava sigurnu zonu za koegzistenciju sa bilo kojom elektronskom kontrolnom jedinicom, smještenom u vozilu.

Najznačajnije karakteristike te zone su skladištenje i upravljanje sigurnosnim ključevima, plus enkapsuliranje autentifikacije, enkripcija i dekripcija algoritama kojima aplikacijski kod može pristupiti preko API-a. Ove karakteristike daju mogućnost da povećamo fleksibilnost i smanjimo troškove.

Kao primjer ove arhitekture, imamo implementaciju SHE specifikacije na Freescale's MPC5646C single-čip mikrokontroleru, namjenjenog kontroli aplikacija samog vozila, dok se u vidu sigurnosti može iskoristiti za zaštitu krađe vozila, manipulaciji ECU-a, i aktivaciji imobilajzera.

EVITA Projekt, koji finansira EU, razvio je niz smjernica koje detaljno objašnjavaju dizajn, verifikaciju i prototipove niza sigurnosnih arhitektura za automobilske ECU.

Brojne kompanije su bile aktivne u Evita projektu, uključujući BMW, Continental, Fujitsu, Infineon i Bosch. EVITA definira ukupnu funkcionalnost tri različita hardverska sigurnosna pristupna modula: Full, srednje i „light“. Štaviše, ona specificira razradu seta funkcija i njihovih parametara, za upravljanje sigurnosnim ključevima, a isto tako i za operacije enkripcije i dekripcije.

Novi projekt koji je finansiran od strane EU, zove se PRESERVE, a nastao je od članica koje su učestvovala u kreiranju EVITE. Cilj ovog novog projekta je razviti, implementirati i testirati, skalabilan sigurnosni podsistem za vehicle-to-vehicle i vehicle-to-infrastructure aplikacije. Razvoj ovog sistema je u punom jeku i očekuje se završetak do kraja 2014 godine.



Napori projekta PRESERVE usmjerene su ka obezbijedenju sigurnog prijenosa i kontrole podataka za buduće inteligentne transportne sisteme (ITS). Implementacija sigurnosnog modula kao hardvera uključit će Elliptic Curve Cryptography (ECC), koja je ustvari forma kriptografije javnim ključem.

Naredni dobar primjer sigurnosnog standarda dolazi iz Nacionalnog Instituta za Standarde i Tehnologiju (NIST) koji je izdao FIPS (Federal Information Processing Standards) 140 standarda za obje vrste, i hardverske i softverske komponente.

FIPS 140-2 definira 4 nivoa sigurnosti, od nivoa 1 (sa jednostavnom jednom sigurnosnom funkcijom, i bez fizičke sigurnosti) do nivoa 4 (sa sigurnosnom funkcijom i fizičkom zaštitom uz zaštitu od napada iz okoline, zloupotrebom napona ili temperature).

Još jedan „proprietary“ izdavač specifikacija i smjernica za pomoć u razvoju i sigurnosti ugrađenih uređaja, a koje je bitno napomenuti je ARM. ARM je razvio svoj TrustZone, sigurnosnu infrastrukturu koja se ugrađuje u mikontrolere i mikroprocesore ozbiljnih proizvođača, uključujući Freescale's, MX serije i Vybrid porodicu uređaja.

Treba istaknuti još jednu organizaciju za standarde, a to je Trusted Computing Group (TCG), koja postavlja međunarodne, interoperabilne standarde iz oblasti pouzdanog računarstva. Bitna specifikacija koju su oni izdali je njihov Trusted Platform Module (TPM). Kao i SHE specifikacija, i TPM koristi sigurnosne ključeve za autentifikaciju i funkciju enkripcije. Programeri koriste TPM kao eksterni periferal sa komunikacijskim bus-om, do drugog kontrolera u sistemu.

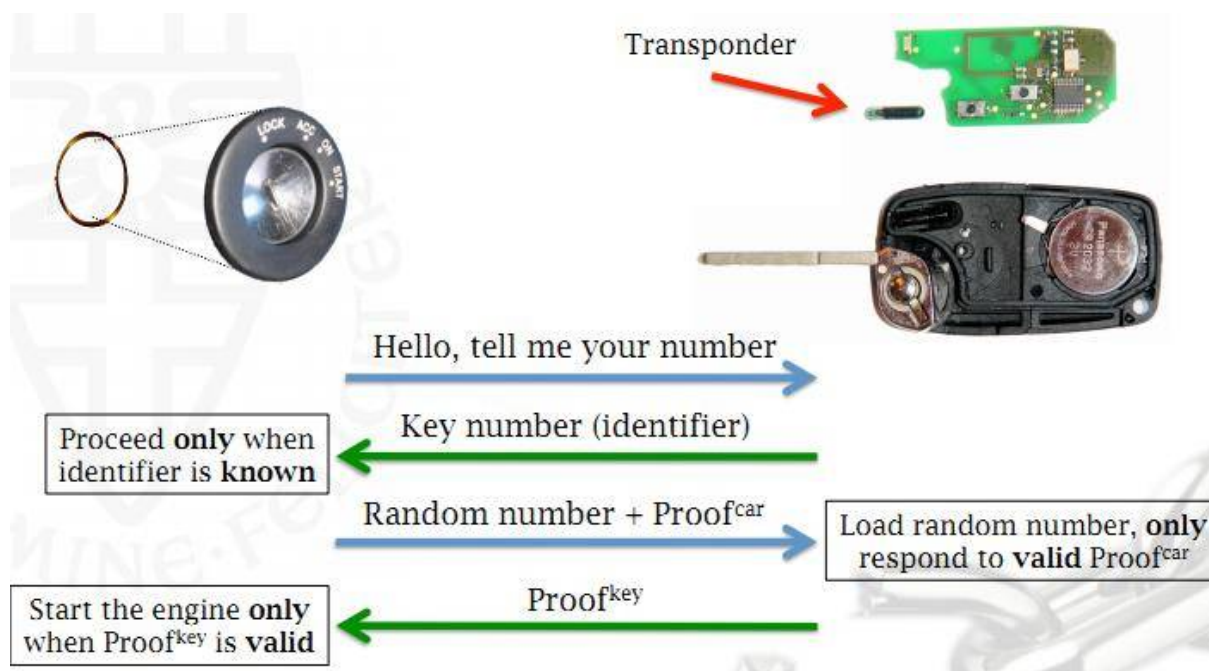
TPM specificira non-volatile memoriju, pohranu tajnog ključa, generator slučajnog broja, RSA, SHA-1, HMAC and Vernam jednokratni pad algoritam. Advanced Encryption Standard (AES) je opcija za TPM uređaje.

Ovo je dakle ono što je aktuelno, na čemu se radi, ili se u međuvremenu uspješno implementiralo. Međutim moram se osvrnuti i na same početke, te napomenuti neka rješenja koja su obilježila kraj 80-ih i početak 90-ih godina. Neka od tih rješenja su do danas više puta modificirana, neka su izbačena iz upotrebe.

2.2.1. Imobilajzeri

Imobilajzer je pionir kriptografije u automobilskoj industriji. Naime, to je elektronski uređaj koji je služio kao zaštita od neovlaštenog pokretanja vozila. Baziran je na identifikaciji putem radio frekvencije (eng. Radio Frequency Identification – RFID).

Predstavljen je devedesetih. To je zapravo jedan pasivni transponder koji se nalazio u kućištu ključa. Radio je na frekvenciji od 125 kHz. Da ne bi bilo zabune, daljinsko zaključavanje/otključavanje radilo je na frekvenciji od 433/868 Mhz, zavisno od proizvođača (Evropa, SAD).



Slika 7. Način komunikacije transpondera i automobila;

Izvor: Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer,

Roel Verdult, Baris Ege;



2.2.2. Texas Instruments DST (Digital Signature Transponder)

- Zaštićen kriptografskim algoritmom koje je TI razvio (eng. Proprietary);
- Algoritam koristi tajni ključ veličine 40 bita;
- Kompleksna 240 enkripcija (iscrpno pretraživanje obzirom na hardver koji se koristio u to vrijeme);
- Zamijenjen sa DST80 ili TRPWS21 (AES 128 bit);

2.2.3. KeeLoq

- Predstavljen 1996;
- Dužina ključa 64 bita;
- Kompleksna 2^{44} enkripcija; (slide / meet-in-the-middle)
- Ne koristi se više u autoindustriji;

2.2.4. HITAG2

- Predstavljen 1996 godine;
- Dužina ključa 48 bita;
- Kompleksna 2^{37} enkripcija (za taj vremenski period);
- Zamijenjen sa Hitag3 ili Hitag-Pro (AES 128-Bit);

HITAG2 imao je slab kriptografski algoritam, i tada već zastarjeli dizajn šifre (rane devedesete).



Slika 8. Hitag2 transponder;

Izvor: www.google.ba

2.2.5. Megamos Crypto

- Predstavljen 1995/1996 godine;
- Dužina ključa 96 bita;
- Imao je slične nedostatke kao i HITAG2, te je i razbijan istim napadima kao i HITAG2;
- I dalje u primjeni u autoindustriji;



Slika 9. Audi can Megamos Crypto ID48 glass type (TP25) transponder;

Izvor: www.bord.cz/transpondery



3. Teorijske osnove istraživanja

3.1. RFID

RFID (eng. Radio Frequency Identification) naziv je za sve primjenjene tehnologije koje koriste radio valove, kako bi identificirali željene objekte (automatski). Ovakav način komunikacije, baziran je na proizvodnji elektromagnetnih valova u odašiljačima, te njihovom prepoznavanju i prijemu, na samim prijemnicima.

U praksi imamo nekoliko metoda identifikacije objekata, ali najčešće se koristi pohranjivanje identifikacijskog broja (ID-a) ili neke druge informacije, na nekom mikročipu. Takav mikročip, uparen sa antenom, predstavlja RFID transponder.

Komunikacija transpondera sa čitačem odvija se korištenjem radio signala. Način ove komunikacije može biti jednosmjernan ili dvosmjernan, s tim da je čitač uvijek povezan sa računarom, na kojem se nalazi baza podataka.

Tako npr. jednostavan ID, pohranjen na transponderu, u bazi je povezana sa informacijama o označenom proizvodu. Ogromna raznovrsost RFID sistema, uz njihovo svakodnevno usavršavanje, pruža nam mogućnost za njihovu svestranu primjenu. Ugrađivanje RFID transpondera u pretežno sve što okružuje ljude, od odjeće, automobila, bijele tehnike, pa sve do primjene u samim ljudima. Ovo sve pruža nam neslućene mogućnosti, i svakodnevne poslove čini višestruko lakšim. Poučeni iskustvom, uvidjeli smo da svaka tehnologija osim dobrih, svjesno ili ne, donosi i one loše strane. Ni RFID nije izuzetak, te je tako podložna mnogim zloupotrebama.

U nastavku testa, osvrnut ću se na historiju RFID sistema, opisat ću od kojih komponenti su sačinjeni, te do kojih nivou su danas dospjeli u primjeni. Osim toga, bit će riječi i o mogućim budućim primjenama, kao i ranjivostima kojima su podložni, i sigurnosnim elementima istih.

3.1.1. Historijski razvoj RFID sistema

Historijski razvoj počinje 1939, kada su britanci osmislili IFF (eng. Identification Friend or Foe) sistem, koji se koristio za identifikaciju aviona. Ovakav sistem, podrazumijevao je radarski sistem, koji se nalazio na zemlji, koji vrši komunikaciju sa transponderom, skrivenim negdje u avionu. Transponder (eng. trans(mitter) + (res)ponder) predstavlja uređaj koji nakon prijema nekog signala, emituje vlastiti signal.



Tehnologija je nazvana SSR (eng. Secondary Surveillance Radar), a danas još uvijek ima primjenu, i to u civilnoj avijaciji.

Patent, Marca Cardulla iz 1973. godine, bio je prvi moderni RFID osmišljen sistem. Bio je to zapravo RFID transponder, koji je radio na pasivan način, a imao je i određenu količinu memorije (16 bita). Primjena mu je bila u kontroli transporta kroz luku, te naplata provizija.

3.1.2. Vrste RFID transpondera

Transponder čine, prethodno pomenute dvije komponente. To su čip, u koji se pohranjuju podaci bitni za komunikaciju, i antena. Sve skupa, sklopljeno je u plastično kućište, te dobro zaštićeno, kako ne bi bilo podložno soljašnjim uticajima. Dijelovi mikročipa su : radio prijemnik, radio modulator (koristi se za slanje odgovora prema čitaču), upravljačka logika, memorija i sistem koji upravlja napajanjem.

Transpondere je moguće podijeliti u nekoliko različitih grupa, npr.

- Prema načinu njihovog napajanja imamo: pasivne, djelimično aktivne, i aktivne transpondere.

- Prema mogućnosti programiranja dijelimo ih na : transponderi koje je moguće samo čitati (read only); prilikom procesa proizvodnje, dobiju jedinstven serijski broj, koji je naknadno nemoguće promijeniti. Transponderi koji omogućavaju jednostruko programiranje, prvobitno unešene vrijednosti ili podatke, ne možemo mijenjati. Transponderi koji omogućavaju višestruko programiranje – imaju trajan serijski broj, koji se utisne prilikom proizvodnje, a na njega se nadodaju zapisivani podaci. Njihova primjena je u zahtjevnijim sistemima.

- Prema frekvencijama koje koriste za svoj rad, pa tako imamo : oni koji rade na niskim frekvencijama (oko 125 kHz), visokim frekvencijama (13,56 MHz), ultravisokim frekvencijama (UHF 860-960 MHz), mikrovalnim frekvencijama (2,45 GHz).

- Prema fizičkoj varijanti: RFID etikete (eng.tag), RFID naljepnice, RFID štampane pločice.

Domet signala RFID transpondera zavisi prije svega od korištene frekvencije, ali isto tako i od vrste napajanja. U praksi, domet transpondera koji koriste niske frekvencije je 30 cm, na visokim do 1m, a na UHF do 6 metara. Naravno, upotrebom aktivnih transpondera, koji kao napajanje imaju odgovarajuću vrstu baterije, ovaj domet moguće je znatno povećati.

Utrošak energije, sposobnost emitiranja signala kroz razne materijale, sve to zavisi o frekvenciji na kojoj transponder radi. Tako npr. Transponderi niskih frekvencija bolje emituju signal kroz različite materijale, od UHF transpondera, i pri tom troše manje energije i jeftiniji su. Ipak ono gdje UHF transponderi imaju prednost je, znatno veći domet, ali i brži protok podataka.

Edin Ćatović Primjena kriptografije u automobilskej industriji

U skorije vrijeme, nekoliko kompanija radi na razvoju RFID transpondera od polimernih poluprovodnika. Ukoliko zažive, trebali bi zamijeniti današnje silikonske. 2005 godine njemački PolyIC i holandski Philips, eksperimentalno su prikazali rad štampanih polimernih transpondera, i to na frekvenciji od 13,56 MHz. Ukoliko bi se ideja komercijalizovala, polimerni transponderi bili bi dosta pristupačniji i cijenom, obzirom da se štampaju u rolama. Šira globalna primjena, mogla bi u nekom periodu da ih učini čak i besplatnima, kakve su danas bar-kod oznake.



Slika 10. Vrste RFID transpondera³;

Vodeća standardizacijska organizacija u ovoj sferi, EPCGlobal, dala je dvije podjele RFID transpondera i to na šest klasa i u dvije različite generacije. Podjele slijede u tabeli 1.

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

Tabela 1. Podjela RFID transpondera na klase , EPCGlobal⁴;

³Izvor: CCERT-PUBDOC-2007-01-179;

⁴Izvor: CCERT-PUBDOC-2007-01-179;



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

Tabela 2.Podjela RFID transpondera na generacije , EPCGlobal⁵;

⁵Izvor: CCERT-PUBDOC-2007-01-179;



3.2. Pasivni transponderi

Ovakva vrsta transpondera nema vlastito (unutarnje) napajanje. Izvor njihovog napajanja je energija koja se priklupi iz dolazećeg radio signala, a koja nosi sa sobom određena svojstva. Obzirom da nemaju unutarnje napajanje, u kućištu moraju imati nešto kako bi skladištili prikupljenu energiju od primljenog signala, najčešće neka vrsta kondenzatora.

Dakle mora postojati energija, kako bi se vratio signal, u trenutku kada čitač prestane slati. Postoji i opcija kada čitač konstantno šalje signal tokom komunikacije, što dalje znači da transponder odgovara, i to na različitim frekvencijama. Odgovor nije striktno ograničen na slanje ID-a, osim ID-a, može sadržavati različite vrste podataka, zavisi od vrste i količine memorije koju transponder posjeduje (ukoliko je posjeduje).

Do danas, su poznata tri načina uparivanja čitača i pasivnih transpondera, i to : elektromagnetska indukcija (uglavnom za male udaljenosti), reflektovanje (eng. Backscatter) za veće udaljenosti, elektrostatičko uparivanje (antene čitača i transpondera ponašaju se kao nabijene ploče), ujedno i najrjeđe korištena.

Uzmemo li u obzir da nemaju unutarnje napajanje, pasivni transponderi, daju mogućnost da se proizvode u veoma malim dimenzijama, prikladni za razne vrste namjene. Zbog jeftine izrade, jako su popularni u trgovačkim lancima. Domet signala je od 10 cm do nekoliko metara, u zavisnosti od veličine transpondera, dizajna antene, te frekvencije na kojoj smo odabrali da transponder radi.

3.3. Djelimično aktivni transponderi

Kod ove vrste transpondera, u kućištu imamo bateriju. Uloga baterije je da napaja mikročip, dok se za rad antene koristi energija prikupljena od dolaznog signala koji je emitovao čitač. Ovakvi transponderi se nalaze negdje na sredini između aktivnih i pasivnih transpondera, uzmemo li u obzir strukturu napajanja, ili radnje karakteristike. Djelimično aktivni (možemo ih nazvati i djelimično pasivni) transponderi nose sa sobom dobre a i loše strane obje vrste transpondera.

3.4. Aktivni transponderi

Aktivni RFID transponderi, imaju vlastito napajanje. Napajanje se koristi i za mikročip, a i za rad same antene. Ove karakteristike ih čine veoma pouzdanim i omogućavaju im uspostavljanje sesije sa čitačem. Osim toga, imajući u vidu njihovo unutarnje napajanje, mnogo su bolji u primjeni u različitim sredinama, npr. voda (bitna stvar kod primjene na ljudima i životinjama, jer znamo da voda čini visok procenat i kod jednih a i kod drugih), kroz razne metalne i betonske prepreke. Neki se čak koriste i na udaljenostima od nekoliko stotina metara, za šta je zaslužno baš unutarnje napajanje. Baterija koja napaja ovakve transpondere u prosjeku traje 10-ak godina.



Moguće je uparivanje ove vrste transpondera sa raznim senzorima. Do sada je zabilježeno da su se koristili sa senzorima temperature, vlažnosti, vibracija, radijacije, svjetla i sl.

Aktivni transponderi sadrže znatno veću količinu memorije od pasivnih transpondera. U praksi, nekim verzijama aktivnih transpondera, to omogućava da pamte informacije dobijene od strane čitača.

3.5. RFID etikete

Možemo ih naći danas u veoma širokom spektru primjene. Proizvode se u različitim veličinama, različitih oblika, i količine memorije. U posljednje vrijeme aktuelne su male RFID etikete, koje se ubacuju pod ljudsku kožu. Odavno su slične etikete u upotrebi kod praćena životinja u velikim rezervatima. U oblasti trgovine, odavno su u upotrebi, u vidu malih privjesaka, koji sprječavaju otuđenje raznih vrsta roba. U oblasti industrije, njima se označavaju kamioni, kontejneri, radne mašine, što višestruko skрати proces identifikacije i praćenja.

Gotovo sve su zaštićene kućištem, raznih vrsta i namjena. Zaštita se prvenstveno odnosi na hemikalije, fizičke udarce, spoljašnje utjecaje i sl.

Osim etiketa, bitno je napomenuti i RFID naljepnice (bar code) i štampane pločice (eng. PCB - Printed Circuit Board).

3.6. RFID čitači

U zavisnosti od vrste transpondera sa kojima rade, tako se razlikuju i RFID čitači. Njihova uloga je prenos podataka do računara na kome se vrši dalja obrada. Sastoje se od dvije komponente, upravljački dio koji komunicira sa računarom, i antena preko koje čitač komunicira sa transponderom. Najjednostavniji čitači mogu raditi samo sa jednom vrstom transpondera, na samo jednoj frekvenciji i mogu koristiti samo jedan protokol. Kod složenijih (skupljih) čitača, logično, situacija je drugačija. Omogućavaju rad sa više transpondera, protokola i na više frekvencija. Najčešće su aktivni, jer konstantno šalju signal, kako bi otpočeli komunikaciju sa transponderima koji su im ušli u domet. Isporučuju se u različitim veličinama, zavisno od namjene. Pa tako imamo čitače veličine desktop računara, koji je spojen sa posebnom karticom na veći broj antena, koje komuniciraju sa transponderima i bilježe podatke. Dok imamo i čitače, veličine poštanske markice. Njihova primjena je u oblasti mobilne telefonije.

Slika 11. RFID čitači⁶;

3.7. Trenutna i buduća primjena RFID sistema

Uzimajući u obzir da karakteristike RFID sistema, uveliko zavise od frekvencija na kojima rade, onda na taj način možemo izvršiti i njihovu podjelu.

RFID sistemi koji rade na niskim frekvencijama (eng.LF), primjenjuju se kod sistema za sigurnosni nadzor, praćenja životinja i praćenja imovine. RFID istemi koji za svoj rad koriste visoke frekvencije(eng.HF), imaju primjenu u radu sa pametnim karticama i kontroli pristupa. I na kraju RFID sistemi, koji rade na ultra visokim frekvencijama (eng.UHF), svoju primjenu su našli u željeznicama, identifikaciji vozila, transportu robe.

Ovdje bih još samo napomenuo minijaturne RFID biočipove, koji se ugrađuju pod kožu životinjama, radi lakšeg praćenja. Prvi put upotrijebljen je 1983 godine. U skorije vrijeme počelo se sa sličnom primjenom i na ljudima. Naime, ljudski biočip bi zamjenio sve čovjekove identifikacijske dokumente, od lične karte, pasoša i sl. Za očitavanje podataka koristio bi se poseban čitač, koji bi čitao podatke za koje je ovlašten.

Prvi ovakav čip, za primjenu na ljudima razvila je kompanija Verichip, 2001 godine. Veličine je zrna riže, i ugrađuje se ispod kože. Reaguje u blizini njemu namjenjenih čitača. U mogućnosti je da pohrani veoma malu količinu informacija, radi se o 10-15 znakova.

⁶Izvor: CCERT-PUBDOC-2007-01-179;



3.8. Ranjivost RFID sistema

Glavni problem kod RFID sistema, je zaštita privatnosti. Naime, transponder kada se nađe u neposrednoj blizini RFID čitača, on na upit čitača, odgovara slanjem informacija. Često se radi o veoma povjerljivim informacijama, i ukoliko pristup čitaču ima neovlaštena osoba, sistem je u najmanju ruku kompromitovan.

Drugi problem, je zaštita privatnosti, jer poznato nam je da se neovlašteno praćenje može vrlo lako izvesti. Osim ova dva problema, RFID sistemi ranjivi su i na fizičke napade, ometanje radio signala, krivotvorenje manipulisanjem transpondera, prevara preuzimanjem uloge postojećeg transpondera, neovlašteno prisluškivanje, neovlaštena analiza komunikacije.

3.9. Zaštita RFID transpondera

Kako bi se spriječile i otklonile navedene ranjivosti, moguće je primjeniti slijedeće metode: samouništenje, faradejev kavez, aktivno ometanje, klasična kriptografija, blokirajući transponder, hash funkcije, PRF autorizacija, TBP autorizacija, HB autorizacija, te metode koje ne koriste enkripciju.

Što se tiče klasične kriptografije u upotrebi su simetrična enkripcija te enkripcija sa javnim ključem.



3.10. Biometrija

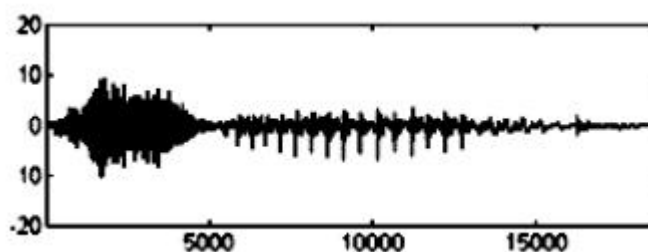
Biometriju čini skup automatizovanih metoda koje nam olakšavaju prepoznavanje ljudi, na osnovu njihove jedne ili više fizičkih, ili karakteristika ponašanja. (grč. Bios = život, grč. Metron = mjera).

U informacijskoj tehnologiji, možemo je podijeliti na dva dijela. Prvi dio bazirao bi se na tehnologije koje bilježe na jedinstvene fizičke karakteristike kao npr. prepoznavanje lica, skeniranje rožnice oka, otisak prsta. Drugi dio, bazirao bi se na bilježenju karakteristika ponašanja, npr. tipkanje, način hoda, rukopis.

Biometrija, sama po sebi, uključuje upotrebu specijalnih uređaja, koji nam služe za praćenje određenih fizičkih, ili karakteristika ponašanja. Osim toga, neophodni su nam programi, koji će izvršiti analizu i upoređivanje dobijenih rezultata. Pri radu se koristi kombinacija uzorkovanja sa umjetnom inteligencijom. Uzorci se digitalizuju, i nakon toga upoređuju.

Bitni je istaći da podatke koje dobijemo raznim skeniranjima, potrebno je pretovriti u digitalni oblik, kako bi računar mogao raditi s njima. Za to nam služi digitalni audio-video konverter ili skraćeno DAC.

Svi DAC uređaji nisu isti, razlika je u kvaliteti senzora koji se koriste. Pa shodno tome, što je bolji (skuplji) senzor, bolji je i uzorak koji dobijamo.



Slika 12. Izgled digitalizovanog uzorka⁷;

⁷Izvor: CCERT-PUBDOC-2006-09-167;



3.10.1. Fizička biometrija

Dio je biometrije koji se bavi prikupljanjem uzoraka, jedinstvenih fizičkih karakteristika. Njen temelj je ljudska fizička jedinstvenost, koja i omogućava raspoznavanje ljudi. Za to se koriste jedinstveni opisi uzoraka. Uz takve uzorke, i ostale klasične zapise, poput imena i prezimena, moguće je opisati jednu osobu.

Ovoj grani biometrije pripadaju čitanje DNK zapisa, skeniranje rožnice, prepoznavanje lica, geometrija šake, provjera/skeniranje vena, i otisak prsta. Zbog velikog obima pomenutih metoda, neću biti u mogućnosti da obradim svaku metodu pojedinačno. Detaljno, u nastavku, će biti opisan otisak prsta, obzirom da je izabran kao implementirano rješenje.

3.10.2. Biometrija ponašanja

Biometrija ponašanja opisuje karakteristike kao što su kretanje u prostoru, izgled, glas. Kao i kod fizičke biometrije, i kod biometrije ponašanja uzorci su jedinstveni. Uzorci se opisuju krivima, a na osnovu uzoraka je moguće raspoznavati ljude.

Ovdje spadaju, prepoznavanje glasa, prepoznavanje rukopisa ili potpisa, dinamika tipkanja, dinamika hoda, dinamika mirisa.

3.10.3. Multimodalna biometrija

Ovaj tip biometrije podrazumijeva kombinaciju svih prethodno navedenih tehnika biometrije. Za izgradnju jednog bezbijednog informacionog sistema, ključ je korištenje više biometrijskih tehnika istovremeno. U praksi je to korištenje biometrije ponašanja sa fizičkom biometrijom, a takve sisteme imamo implementirane na carinama.



3.11. Otisak prsta

Čovjek je još od samih početaka počeo da obraća pažnju na otisak prsta, i uvidio je da ima neki značaj. O tome nam svjedoče iskopine čak iz doba neolita, kada su pronađeni predmeti na kojima su bili oslikani otisci prsta.



Slika 13. Iskopina iz doba neolita;

Izvor: www.google.ba

Nakon toga, ponovo se otisak prsta pominje u drevnom Babilonu, i njegova upotreba na glinenim tablicama, prilikom transakcija u poslovanju. Prvi detaljniji prikaz (kraj 18-og vijeka) veže se za njemačkog ljekara Mayera. On je po prvi put napravio detaljan prikaz reljefa prsta, i pominje karakteristike papilarnih linija (ispupčenja na prstu).



Slika 14. Mayerov crtež;

Izvor: www.google.ba



Prva jasna klasifikacija, otisaka prsta, veže se za čeha Jana Purkinjea. Otiske prsta podijelio u 9 klasa.



Slika 15. Purkinjeova klasifikacija;

Izvor: www.wikipedia.org

Prvi koji je uvidio mogućnost primjene otiska prsta za identifikaciju osobe bio je Henry Faulds, naučnik iz Škotske (1880 g.). Francis Galton, engleski naučnik, 1888 godine otkrio je značaj individualnosti i postojanosti otiska prsta. On takođe prvi put pominje pojam minucije (varijacije i različitosti papilarnih linija).

Rezultate Galtonovih istraživanja, prvi put je iskoristio, Juan Vucetich (rođen na Hvaru), u vidu kreiranja prve kartoteke otisaka prstiju.

Pravilo o 12 identičnih tačaka na otisku prsta, kao uslov uspješne identifikacije, predložio je Edmond Locard 1918 godine. Poznat je još po tome što je na neki način izgradio temelje, i postavio princip forenzičke nauke, a on glasi : „Svaki kontakt ostavlja trag“ (eng. Every Contact Leaves a Trace).

I na kraju, u ne take dalekoj prošlosti, 1991 godine, zaživela je i praktična primjena računara, u oblasti prepoznavanja otisaka prstiju. Još nešto je karakteristično za tu godinu, uveden je prvi sistem koji je kao osnovu koristio računare – Automatic Fingerprint Recognition System, skraćeno AFIS.

3.11.1. Karakteristike otiska prsta

Otisak prsta nije ništa drugo nego kombinacija udubljenja i ispupčenja. Linije koje formiraju ispupčenja, nazivaju se papilarne linije. Formiraju se veoma rano kod svake individue, u fazi embrija čak, dakle 6-7 sedmica. Od prilike oko 21 sedmice potpuno su formirane. Njihova varijacija od individue do individue, te nepromjenjivost tokom vremena, daju za pravo da se neko identifikuje sa velikom pouzdanošću. Razlikuju se čak i kod blizanaca.

Klasifikacija otiska prsta koja je uvaŹena jeste ona na osnovu fizičkih svojstava, varijacije papilarnih linija, baziranih na minucijama. Tako imamo 7 grupa i to : luk, jeloviti luk, petlja, dvostruka petlja, jamičasta petlja, spirala, i mješoviti.

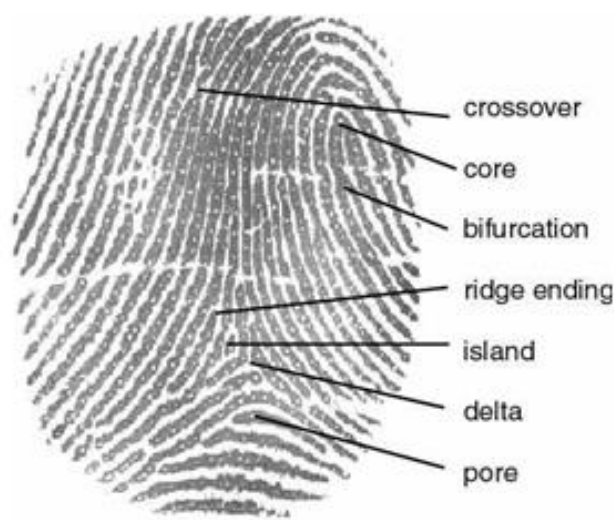


Slika 16. Tipovi otiska prsta;

Izvor: www.google.ba

Otisci iz grupe petlji (jednostruka, dvostruka i jamičasta) su najzastupljeniji medju ljudima (oko 60%). Najrjeđi je mješoviti tip (oko 5%).

Osim fizičkih karakteristika, koje sam prethodno naveo, jako bitni za samo prepoznavanje otiska prsta, su i singularne tačke ili terminusi. Naime, radi se o tačkama koje u kojima se manifestuju nagle promjene usmjerenosti papilarnih linija.



Slika 17. Terminusi;

Izvor: www.wikipedia.org

Te tačke su crossover- ukrštavanje, core-središte, bifuraction-račva, ridge ending-završetak linije, island-ostrvo, delta-delta, pore-pora;

Ono što je bitno napomenuti je da se verifikacija vrši na osnovu 7 prethodno navedenih grupa, dok se identifikacija vrši na osnovu osnovu ovih 7 tačaka (terminusa).

Ono što papilarne linije čini pogodnim i sigurnim za identifikaciju je: Nepromjenjivost rasporeda i broja minucija (niko nema mogućnost da manipulise sa njima ili da ih modificira; jedino sto je moguće uraditi jeste da se potpuno unište); Neponovljivost, odnosno velika varijacija minucija, tako da je nemoguće ponavljanje dva ista otiska. Francuski matematičar, Baltasar, dokazao je ovu tvrdnju, i pokazao matematički da je vjerovatnoća skoro jednaka nuli. Grupisanje je veoma bitna osobina, koja nam donosi uštedu na vremenu prilikom identifikacije, a provodi se na osnovu globalnih karakteristika.

U procesu automatskog prepoznavanja otiska prsta postoji šest (standardizovanih) koraka, i to : akvizicija odnosno snimanje otiska prsta, zatim segmentacija slike, rekonstrukcija slike, ekstrakcija karakteristika, poređenje minucija (traženje para), i klasifikacija (smještanje u jednu od 7 grupa-petlja, duplja petlja i sl.)

Za akviziciju najpogodniji su skeneri koji optički (optičkom metodom) skidaju otisak prsta, tako se dobija bolja kvaliteta (najčešće 512 dpi). Segmentacija se odnosi na dvajanje slike, dobijene skenerom, od pozadine. Rekonstrukcija podrazumijeva povećanje kontrasta između grebena i dolina, te ponovo povezivanje grebena koji imaju prekid. Što se tiče ekstrakcije, imamo onu koja se zasniva na binarizaciji, i drugu koja se naziva neposredna skala sivog.

Nakon ekstrakcije minucije, ona se čuva i služi kao templejt. Kod procesa autentifikacije, ulazni otisak prsta se poredi sa postojećim templejtom, a sam postupak se naziva uparivanje minucija.



Slika 18. Original (lijevo) vs ekstraktovani terminusi;

Izvor: www.wikipedia.org

Na kraju da konstatujemo da je otisak prsta najstarija biometrijske metoda. Razvoj je počeo a i našao najveću primjenu u kriminalističkoj sferi, pri identifikovanju i pronalaženju počinioca krivičnih dijela. Danas ova metoda ima primjenu u svim bitnijim sferama života, koje imaju potrebu za adekvatnom i sigurnom zaštitom. Pa tako danas senzori otiska prsta štite objekte, trezore, ali i računarske sisteme, te povjerljive aplikacije. Cilj mog rada je da ovakav vid biometrijske zaštite implementiram u automobile.



4. Evaluacija bezbjednosti kriptografskih mehanizama u automobilskoj industriji

4.1. Poznati napadi

Na samom početku ovog poglavlja moram naglasiti da je osnovna stvar pri definisanju tipa prijetnje, razlikovati tehničke i operacijske mogućnosti napadača. Tehničke mogućnosti, opisuju znanja napadača o automobilima na koje je usmjeren njegov napad. Osim toga, moramo poznavati i njegove informatičke vještine za analizu sistema, odnosno da li je sposoban za razvoj i umetanje malicioznog koda, na bilo koji od ulazno-izlaznih uređaja u automobilu.

Operacijske mogućnosti, ukratko, opisuju zahtjeve napadača za isporuku malicioznog koda do ulazno-izlaznih uređaja automobila. Možemo ih svrstati u tri grupe. Prva bi bila indirektan fizički pristup, zatim, bežični pristup kratkog dometa, i na kraju, bežični pristup velikog dometa.

4.1.1. Indirektan fizički pristup

Automobili novije generacije, proizvedeni od 2005 g., pa do danas, moraju da osiguraju nekoliko fizičkih interfejsa, koji imaju pristup mrežama automobila. Ako kažemo fizičke napadačke površine, onda se misli na ovaj pristup, kada im napadač ne mora direktno pristupiti, nego to može uraditi posredno.

Kao prvi izbor za to, na meti je OBD (eng. On Board Diagnostics) priključak. Ujedno je i najznačajniji interfejs, jer preko njega jednostavno pristupamo sabirnici (eng. CAN-Controller Area Network), nakon čega je moguće manipulirati sa većinom sistema u automobilu. Navedeni priključak, nalazi se sa donje lijeve strane kontrolne table, i primarna namjena mu je dijagnostika i servisiranje. Ukoliko želimo zaštititi svoj automobil, preporučeno je da se ovaj priključak, koji je inače standardan na svim vozilima, zamjeni nekim drugačijeg i jedinstvenog oblika. Adapter za pristup takvom priključku, imao bi samo vlasnik. Druga opcija za zaštitu OBD-a, je da se izmjesti na neko neobično mjesto (standardno je sa donje lijeve strane kontrolne table).

Druga kritična tačka, kada pominjemo fizičke interfejse, su sistemi za zabavu. Gotovo svi današnji automobili, već fabrički sadrže CD-player, a većina njih i USB (eng. Universal Serial Bus) i iPod priključak. Svi oni nam služe za medijsku kontrolu sistema za zabavu. Upravo ove tačke, korisnik može iskoristiti kako bi ubacio maliciozni kod, putem CD-a, kao datoteku, ili muzički fajl. CD player, gledajući sam po sebi ne predstavlja prijetnju, ali ako imamo u vidu da su svi navedeni elementi povezani sa sabirnicom onda je to već problem. Nakon što se naruši jedan sistem, već postoji mogućnost da se to prenese i na ostale.



4.1.2. Bežični pristup kratkog dometa

Ovo je složeniji vid napada, koji zahtijeva veliku preciznost kod ciljanja napada, jako je zahtijevan, i ne omogućava nam vrijeme planiranja napada. Ovom vidu napada, podliježu napadačke površine za bežične interfejsne na automobilu. Operacijski zahtjevi kod ovog napada su na niskom nivou.

Pod bežičnim pristupom kratkog dometa podrazumijevamo:

Bluetooth, koristi se u automobilima već dugo, najzastupljeniji kod telefonskih poziva, bez korištenja ruku, što doprinosi sigurnoj vožnji (eng. Hands free). Bluetooth uređaji koji se koriste u automobilskoj industriji, imaju domet od 10 metara.

Daljinsko otključavanje automobila (eng. Remote Keyless Entry), zastupljeno na svim automobilima novije generacije. Služi za otključavanje i zaključavanje automobila sa veće ili manje udaljenosti. Neki sistemi nude i daljinsko paljenje automobila (eng. Remote Keyless Ignition).

RFID keys, odnosno radiofrekvencijski identifikacijski ključevi. Uloga im je spriječavanje neovlaštenog pokretanja automobila.

Sistem za nadzor pritiska u automobilskim gumama, (eng. Tire Pressure Monitoring System, TPMS).

Wifi (eng. Wireless fidelity) , uopšteno razmjena podataka u automobilu, preko bežične računarske mreže.

Usmjerene komunikacije sa kratkim dometom (eng. Dedicated Short-Range Communications, DSRC), trenutno su u fazi razvoja. Prvenstvena uloga im je, komunikacija među vozilima, s ciljem izbjegavanja gužvi, mjesta nesreće i sl. Smatra se da je ova vrsta komunikacije ranjiva ukoliko napadač postavi bežični odašiljač, a udaljenost zavisi od kanala. Može biti između 5 i 300 metara.

4.1.3. Bežični pristup velikog dometa

Digitalni pristupni kanali velikog dometa prije svega dijele se na dvije podgrupe, kanali koji šalju ili odašiljački kanali (eng. broadcast channels) i adresabilni kanali (eng. addressable channels).

Odašiljački kanali nisu direktno usmjereni prema automobilu, ali im je moguće uključiti na zahtjev prijemnika. Adresabilni kanali su veoma ranjivi, prije svega zbog veoma lake dostupnosti napadačima.



U automobilu danas, implementirani su razni prijemnici za signale velikog dometa. Neki od njih su GPS (eng. Global Positioning System), prvenstveno se koristi za navigaciju, zatim, digitalni radio, satelitski radio, sistem radio podataka (eng. Radio Data System, RDS) , i kanal poruka o saobraćaju (eng. Traffic Message Channel, TMC) .

Vjerovatno najvažniji dio bežične napadačke površine sa velikim dometom, predstavlja stalna izloženost udaljenim telematskim sistemima, koji osiguravaju stalnu povezanost, putem govornih ćelija i mreža podataka.

Problem predstavlja omogućen pristup sa proizvoljne udaljenosti, i na razne načine, uglavnom anonimno. Osim toga, imaju veliku širinu pojasa, i mogu se pojedinačno adresirati.

4.1.4. Napad na telematski sistem

Ovakav sistem u automobilu u mogućnosti je da obavijesti policiju da je došlo do nesreće, pružiti vozaču dijagnostičke informacije na „remote“ principu, onesposobiti ukradeno vozilo sa udaljene lokacije, uglavnom može biti spojen sa većinom sistema koje automobil posjeduje. Napad na ovakav sistem nije nimalo lak, naprotiv jako je složen i iziskuje velike operacijske napore. Poznato je da su svi sistemi u automobilu povezani na sabirnicu (CAN). Pristup bilo kojem od sistema telematski, značio bi mogućnost modifikacije, i narušavanja rada ostalih sistema, koji rade odvojeno od onog sistema koji je kompromitovan.

I pored složenosti ovakvog napada, ozbiljniji proizvođači automobila nisu oklijevali da dodatno pojačaju sigurnost vanjskih komunikacija, a i samih mreža koje su u funkciji u automobilu.

4.1.5. MP3 maliciozni program

Svakim neovlaštenim „skidanjem“ muzičkih fajlova sa interneta, prijeti nam opasnost, da uz te fajlove, sasvim nesvjesno skinemo još nešto. Radi se o zlonamjernom kodu, koji je prikriven u .mp3 datoteci. Njegov cilje je pronaći putanju do sabirnice, čime mu je otvoren put da nanese štetu ostalim sistemima u automobilu.

Sistemi zabave u automobilu iz godine u godinu sve više dobijaju na značaju, ali ih danas proizvođači, sasvim diskretno, žele odvojiti od ostalih sistema, kako ne bi došlo do neželjenih posljedica.

4.1.6. Neovlaštene aplikacije

Danas sve jače mobilne platforme imaju svoje online trgovine, na kojima možemo besplatno skinuti, ili kupiti neku aplikaciju, ukoliko želimo full kontrolu i opcije. Tome su težili i u automobilskoj industriji. Naime, svi veći proizvođači razvijali su aplikacije za svoje sisteme. Bilo za zabavu ili neke druge namjene, download se mogao izvršiti sa online trgovine proizvođača. Upravo u takvim aplikacijama, korisnik može sasvim nesvjesno skinuti maliciozni kod na svoj sistem.



U posljednje vrijeme, uvidjevši opasnost, proizvođači su počeli reducirati broj aplikacija koji se može instalirati na njihove sisteme. Prednjače Toyota i Ford, koji dopuštaju tek mali broj aplikacija.

4.1.7. Zaključavanje vrata

U svim vozilima koja posjeduju ovaj mehanizam (misli se na centralnu bravu), isti je povezan sa ostalim sistemima. Tako iz sigurnosnih razloga, imamo opciju da se vrata, nakon postizanja određene brzine, „sama“ zaključaju u vožnji, ili da se „sama“ otključaju u slučaju aktiviranja zračnih jastuka. Neki Volvo modeli imali su senzor koji je otključavao vrata u slučaju požara. Nakon namjernog podmetanja požara ispod modela ovakvih vozila, u cilju pristupa i otuđenja, Volvo je povukao pomenuti sistem.

4.1.8. Daljinsko otključavanje automobila

Prvenstveno je namijenjeno za otvaranje automobila iz neposredne blizine, ili paljenje automobila kada je vlasnik unutra. Međutim, švicarski naučnici, uspjeli su presresti i produžiti domet signala. Za ovaj eksperiment trebala im je oprema koja košta nešto manje od 100 američkih dolara. Ovakvim načinom se ne replicira signal, nego se proširi domet signala, tako da automobil „misli“ da je daljinski ključ bliže, nego što to ustvari jeste. U izvršavanju ovakvog napada koriste se repetitori.



4.2. Preventiva

U današnje vrijeme, napadači konkretno u segmentu autokriminala, imaju za cilj krađu vozila ili neke njegove vrijedne komponente (npr. navigacijski sistem). Osim toga vrše se i razne manipulacije, od samih vlasnika vozila, kao npr. vraćanje prijeđene kilometraže, u svrhu povećanja vrijednosti samog vozila i bolje prodaje. Zabilježeni su i slučajevi kada se vozilima povećavala kilometraža na isti način, u svrhu smanjenja carinskih i poreskih dadžbina. Naime poznato je da vozila sa većom prijeđenom kilometražom imaju manju vrijednost prilikom carinjenja.

Manipulacije su zabilježene i u oblasti izmjene vozničkih parametara vozila, modifikacijom ECU-a. Popularni chip-tuning, modifikacija vozničkih karakteristika vozila (pritisak turbine, omjer goriva i vazduha, otvaranje ventila i sl.) prilikom čega se poboljšavaju vozne karakteristike.

Sa sve većom primjenom IT-tehnologija u automobilizmu, otvaraju se nove šanse za napadače da manipulišu i mijenjaju parametre vozila.

Razlika napada u svijetu računarskog kriminala, i napada u automobilske industriji, prvenstveno je da napadači na personane računare, laptope, servere i sl. rijetko kad imaju fizički pristup meti. Dakle radi se u 99% slučajeva o udaljenim napadima sa drugih lokacija, dok je to potpuno drugačije kod napadača u oblasti automobilske kriminala gdje se u 99% slučajeva napadač nalazi u neposrednoj blizini ili unutar same mete (automobila). To im omogućava izmjenu ili potpunu deaktivaciju sigurnosnih sistema. Ukoliko onesposobe sistem određenog modela nekog od proizvođača, isti modus mogu primijeniti na sve automobile istog tipa i istog proizvođača, što nosi sa sobom nesagledive posljedice. Osim toga, napadi u sektoru autokriminala su u najvećem dijelu „offline“ napadi.

Zbog svih ovih informacija, napadače u automobilske kriminalu možemo svrstati u tri grupe.

Prvu grupu bi činili vlasnici samih vozila. Njihovi motivi navedeni su u prethodnom dijelu teksta. Dakle nezakonita manipulacija parametrima zbog poboljšanja performansi, te uvećavanje i smanjivanje vrijednosti vozila i sl.

Drugu grupu bi činili organizovane kriminalne grupe. Njihov osnovni motiv je sticanje materijalne dobiti. Automobili se prvo prate, zatim krađu te rastavljaju ili prilagođavaju novim papirima, kako bi ponovo bili legalni. Osim toga, veoma često manje vrijedni automobili se nude vlasnicima na ponovni otkup. To je veoma unosan biznis na prostorima regiona, a procjenjuje da se radi o desecima miliona eura.



Treću grupu obuhvataju konkurentski proizvođači automobila. Motiv ovog napada je sticanje konkurentskog intelektualnog vlasništva (eng. IP-intellectual property). Misli se prvenstveno na tehnička rješenja, koncepte, proizvodne i poslovne planove i sl. Sve ovo omogućava bolju poziciju na tržištu što direktno utiče na dobit. Ovakve vrste napada u skorije vrijeme su i zabilježene. Nije teško zaključiti da su na meti anonimnih kineskih proizvođača automobila bile vodeći njemački automobilske giganti poput BMW-a, Mercedes Benz-a, VW-a.

4.2.1. Napad na automobilske hardver

Napad na automobilske hardver podrazumijeva izmjenu ključnih dijelova sa onim koji nisu legalni. Zabilježeni napad ovakve vrste odnosi se na napad u slučaju kada napadač ima ECU za odgovarajuće vozilo, te code ključ od istog. Spajanjem tog ECU-a na vozilo, umjesto originalnog, vozilo očitava podatke sa novog ECU-a, i vozač svojim code ključem, koji je prilagođen novoj jedinici, sasvim normalno pali vozilo.

Hardverski dijelovi koji pružaju neke osnovne kriptografske mehanizme su tahograf, brzinomjer, i zdračni jastuci. Ovi mehanizmi su u ulozi onemogućavanja neovlaštene modifikacije, ili bar identifikacije pokušaja neovlaštene modifikacije. Nažalost u većini slučajeva, ove zaštite budu onemogućene, razbijanjem ili čitanjem tajnog ključa, deaktivacijom alarm kanala, te prisluškivanjem njihovog rada i komunikacije.

Danas, se definiše 5 tačaka, koje timovi koji rade na automobilskoj sigurnosti moraju ispuniti, kako bi stvorili siguran automobil. To su:

1. Povjerljivost podataka: neovlašten pristup zaštićenim podacima mora biti neizvodiv.
2. Integritet podataka: neovlaštene modifikacije podataka moraju biti neizvodive, ili ukoliko se dese, moraju biti registrovane i otkrivene.
3. Integritet hardvera i softvera: modifikacija automobilske hardvera i softvera mora biti neizvodiva, ili ukoliko se desi automobil to treba prepoznati i zabilježiti.
4. Dostupnost: autorizovani hardver i softver moraju imati odgovarajući pristup do podataka i servisa koji su striktno njima namijenjeni.
5. Jedinstvenost : neovlašteno kloniranje hardverske komponente mora biti neizvodivo, ili ukoliko se dogodi, mora biti okarakterisano kao neautentično.



4.2.2. Zaštita automobilskeg hardvera

Ogleda se u postavljanju kompjuterskih tagova (oznaka) na komponente od velikog značaja, a sve informacije bi bile sakupljene i pohranjene u specijalno dizajnirani sigurnosni modul. Oznake (tagovi) bili bi integrisani u bitne hardverske komponente i nemoguće bi ih bilo ukloniti. Takođe bi mogli komunicirati medju sobom, a i sa specijalnim sigurnosnim modulom.

4.2.3. Zaštita automobilskeg softvera

Svjesni smo činjenice da današnji automobili imaju pristup internetu. Iz tog razloga bitno je obezbijediti da vozilo prihvata samo originalni softver. Ograničiti download i instalaciju softvera koji mijenja ponašanje i parametre vozila.

Ukoliko se desi da je jedna elektronska kontrolna jedinica ugrožena, onemogućiti da to utiče na ostale jedinice. Drugo sto je bitno napomenuti, a za dobrobit je zaštite softvera, bitno je da zaštitimo komunikacione kanale. U automobilima postoje tri vrste:

1. Komunikacioni kanal unutar vozila (razni senzori)
2. Komunikacioni kanal izmedju dva vozila - razmjena podataka o gužvama i uslovima na cesti
3. Komunikacioni kanal vozila sa infrastrukturom - komunikacija senzora u automobilu sa sensorima ugrađenim u podlogu (cestu), kao povratnu informaciju dobijamo da je cesta klizava, pomrzla, i sl. , sto nas upozorava da vožnju prilagodimo trenutnim uslovima. Osim toga moguće je korigovanje svjetla na semaforu, ukoliko se ne možemo sigurno zaustaviti, a pri tome nećemo ugroziti druge učesnike u saobraćaju.



4.3. Predloženo rješenje

U poglavlju koje se odnosi na rješenje koje sam ponudio, prvo ću navesti podatke o okruženju u kojem sam radio, te ukratko opisati isto. Nakon toga slijedi i prikaz koda, odnosno softverskog dijela i analiza dobijenih rezultata. Takođe ću navesti gdje bi, rješenje koje sam ponudio, moglo naći svoju primjenu.

Na kraju par riječi o budućnosti i rješenjima koja nas čekaju u skorije vrijeme, a vezana su za biometriju, te zaključak.

4.3.1. Softversko-hardversko okruženje

Kao softversko okruženje odabrao sam Arduino. Arduino predstavlja fizičko-računarsku platformu otvorenog koda. Arduino hardver je jednostavan (otvorenog tipa), i sastoji se od arduino ploče, sa Atmel AVR procesorom i pratećim ulazno-izlaznim komponentama.

Arduino softver se sastoji od standardnog kompajlera i bootloader koji se nalazi na samoj ploči. Razvojno okruženje je aplikacija napisana u Java programskom jeziku.

Arduino integrisano razvojno okruženje dolazi sa C/C++ bibliotekom zvanom "Wiring" koja čini uobičajene ulazno-izlazne operacije veoma jednostavnim. Arduino programi se pišu u C/C++ programskom jeziku, mada korisnici moraju da definišu samo dve funkcije kako bi napravili izvršni program⁸. Te funkcije su:

- `setup()` - funkcija koja se izvršava jednom na početku i služi za početna podešavanja
- `loop()` - funkcija koja se izvršava u petlji svo vrijeme dok se ne isključi ploča

Što se tiče hardvera, za implementaciju mog rješenja, koristio sam Arduino Uno R3 ploču, Ardafruit biometrijski senzor otiska prsta, par dioda, testnu ploču, dupont kablove.

⁸<https://sr.wikipedia.org/wiki/Arduino>

4.3.2. Eksperimentalni rad

Prvo ćemo se osvrnuti na softverski dio implementacije. Obzirom na činjenicu, da sam koristio Adafruit biometrijski senzor otiska prsta, prvo sam morao napraviti funkciju za uzimanje otiska prsta. Arduino Uno R3 ploča pruža mogućnost pohranjivanja do 160 različitih ID-a, dakle 160 različitih otisaka prsta. Kao finalni produkt, zamišljena je implementacija na automobilu, tačnije startanje automobila otiskom prsta.

```
UzimanjeOtiska2 | Arduino 1.6.4
File Edit Sketch Tools Help

#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>

uint8_t getFingerprintEnroll(int id);

// pin #2 is IN from sensor (GREEN wire)
// pin #3 is OUT from arduino (WHITE wire)
SoftwareSerial mySerial(2, 3);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

void setup()
{
  Serial.begin(9600);
  Serial.println("fingertest");
}

Done uploading.
is 32,256 bytes.

Global variables use 921 bytes (44%) of dynamic memory, leaving
1,127 bytes for local variables. Maximum is 2,048 bytes.

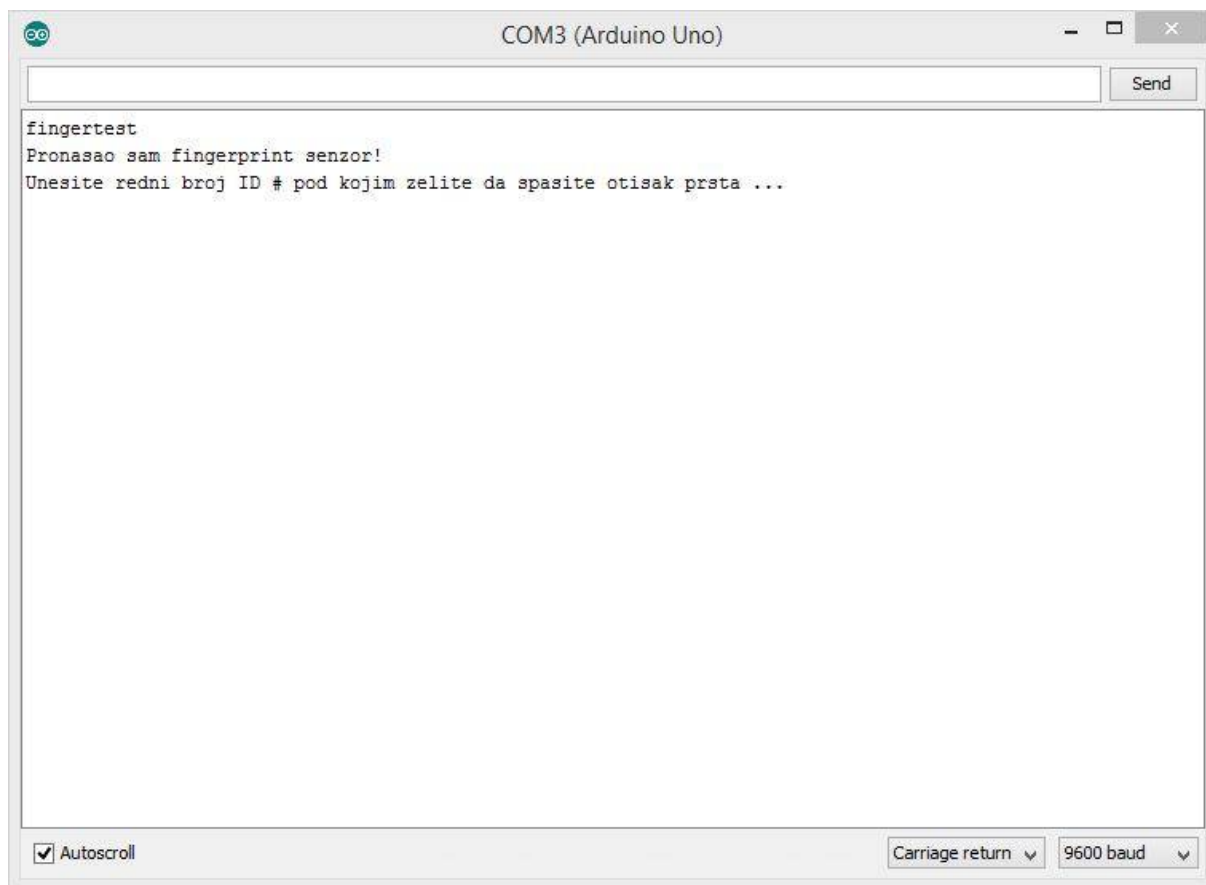
1 Arduino Uno on COM3
```

Slika 19. Funkcija kojom se uzima i pohranjuje otisak prsta

uz usklađivanje sa željenim ID-om;



Nakon uspješno napisane funkcije, potrebno je izvršiti upload na Arduino Uno R3 ploču, kako bi izvršili uzimanje otiska, i uparivanje sa žečkenim ID-om.

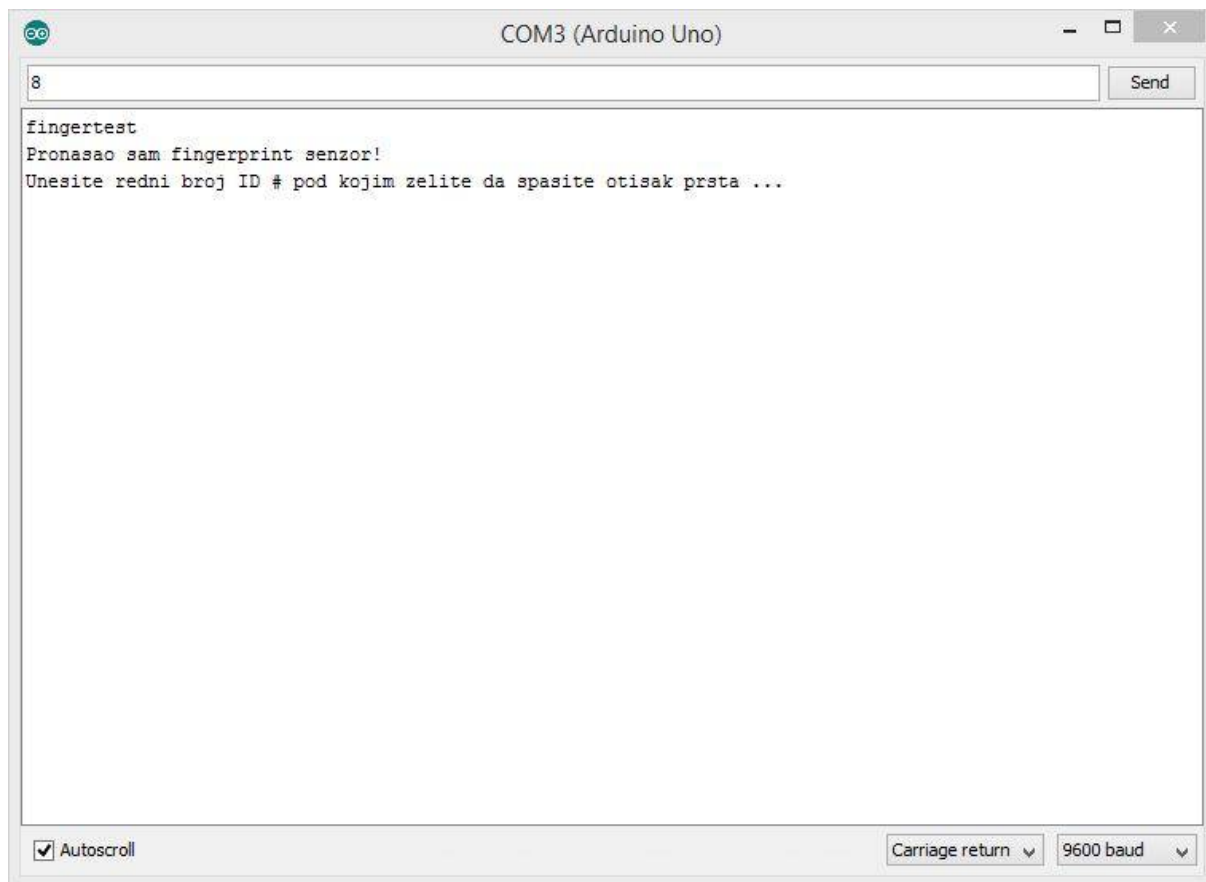


Slika 20. Arduino serial monitor;

Vidimo da je komunikacija, uspješna, na COM3 portu. Nakon uspješno upisane funkcije na Arduino Uno R3 ploču, pokrećemo serial monitor, i slijedimo upute.

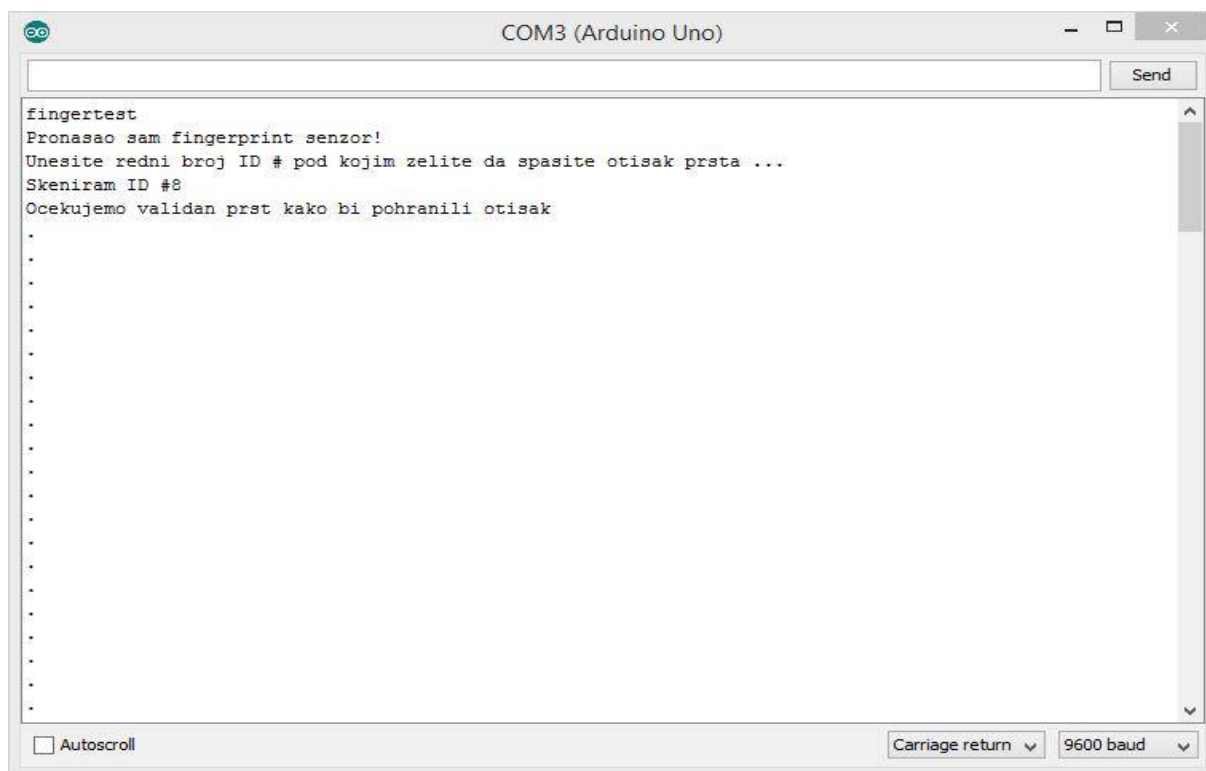
Vidimo da je program uspješno prepoznao senzor otiska prsta, nakon odrađenog testa, i sve je spremno da unesemo ID, pod kojim želimo da pohranimo otisak.

Jednostavno unesemo broj pod kojim želimo da se nalazi naš otisak (npr. broj 8), i pritisnemo tipku enter.

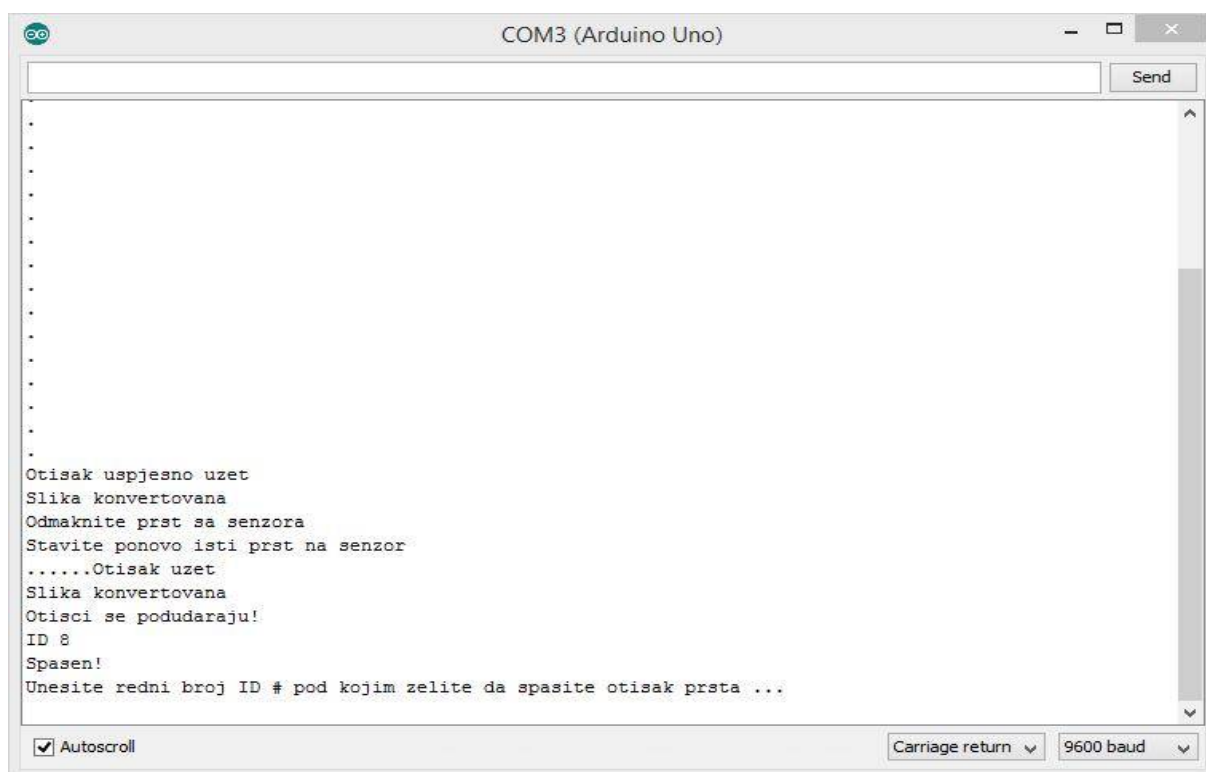


Slika 21. Unos broja, pod kojim želimo spasiti otisak;

Nakon što smo unijeli željeni broj, na serial monitoru ispisuje nam se poruka, da se očekuje da pozicioniramo željeni prst na senzor, kako bi se uspješno uzeo otisak, kao što se može vidjeti na slijedećoj slici br.22.



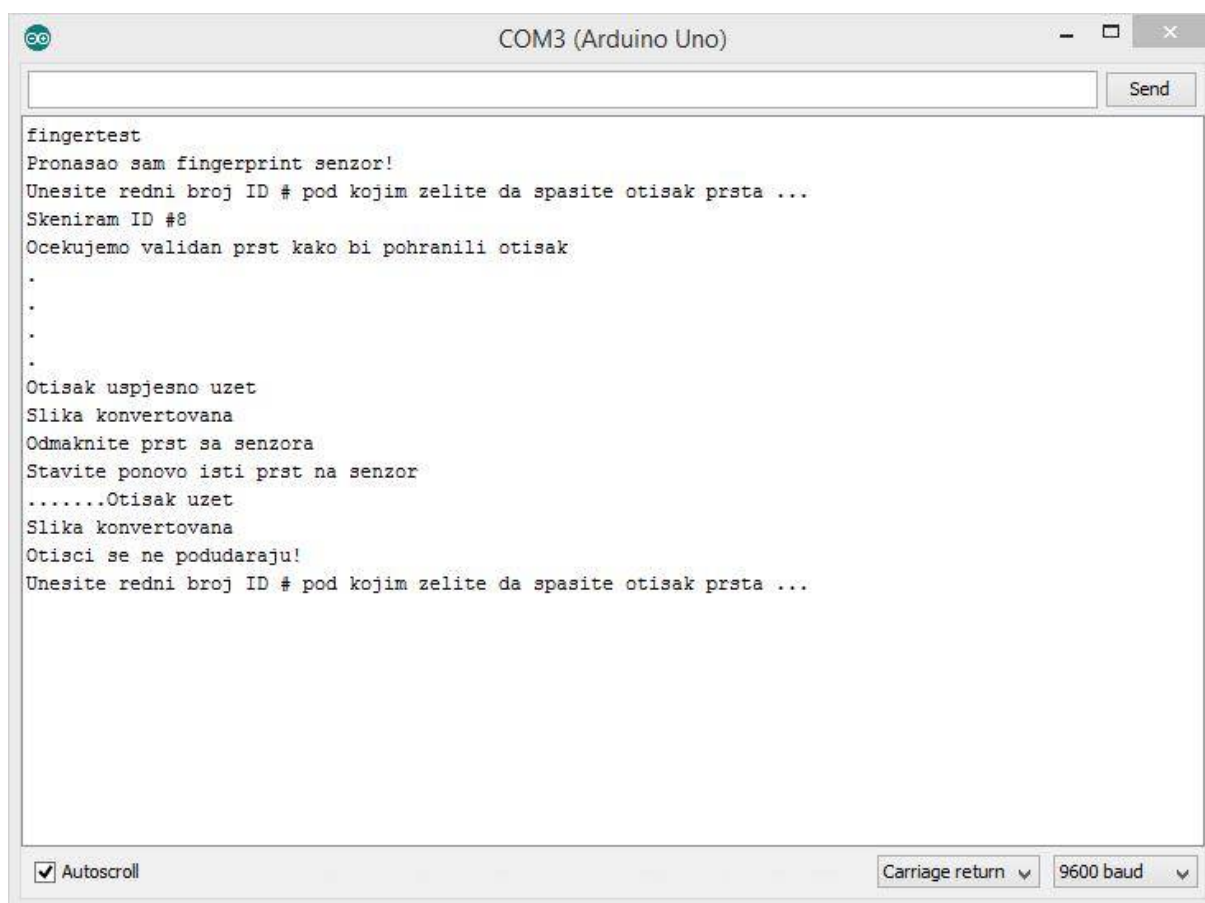
Slika 22. Senzor je spreman, očekuje pozicioniranje prsta;



Slika 23. ID uspješno pohranjen;



Na slici 23. vidi se da je otisak uspješno uzet. To je slučaj kada smo pravilno pozicionirali prst oba puta, i otisci se podudaraju. U slučaju da se otisak broj 1 i broj 2 ne podudaraju, ID neće biti pohranjen. Umjesto toga dobit ćemo ispis kao na slijedećoj slici br.24.



```
fingertest
Pronasao sam fingerprint senzor!
Unesite redni broj ID # pod kojim zelite da spasite otisak prsta ...
Skeniram ID #8
Ocekujemo validan prst kako bi pohranili otisak
.
.
.
.
Otisak uspjesno uzet
Slika konvertovana
Odmaknite prst sa senzora
Stavite ponovo isti prst na senzor
.....Otisak uzet
Slika konvertovana
Otisci se ne podudaraju!
Unesite redni broj ID # pod kojim zelite da spasite otisak prsta ...
```

Slika 24. Prvi i drugi otisak se ne podudaraju, ID nije pohranjen;

Kada već imamo uspješno pohranjen željeni broj ID-a, potrebno je da na našu Arduino Uno R3 ploču učitamo drugu funkciju. Radio se o funkciji koja nam pretvara ovaj mali sistem, u sredstvo za biometrijsku autentifikaciju. Svi ID-evi, koje smo pohranili, imat će pristup sistemu, objektu, ili automobilu, u zavisnosti na čemu će senzor vršiti autentifikaciju.

```
FingerprintSaDiodama2 | Arduino 1.6.4
File Edit Sketch Tools Help

FingerprintSaDiodama2
  Serial.println("Fingerprint senzor pronadjen!");
} else {
  Serial.println("Fingerprint senzor nije pronadjen : (");
  while (1);
}
Serial.println("Ocekujem da pozicionirate validan prst na senzor");
}

void loop() // run over and over again
{
  getFingerprintIDez();
  digitalWrite(12,HIGH); //don't ned to run this at ful
}

uint8_t getFingerprintID() {
  uint8_t p = finger.getImage();
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Uzorak uzet");
  }
}

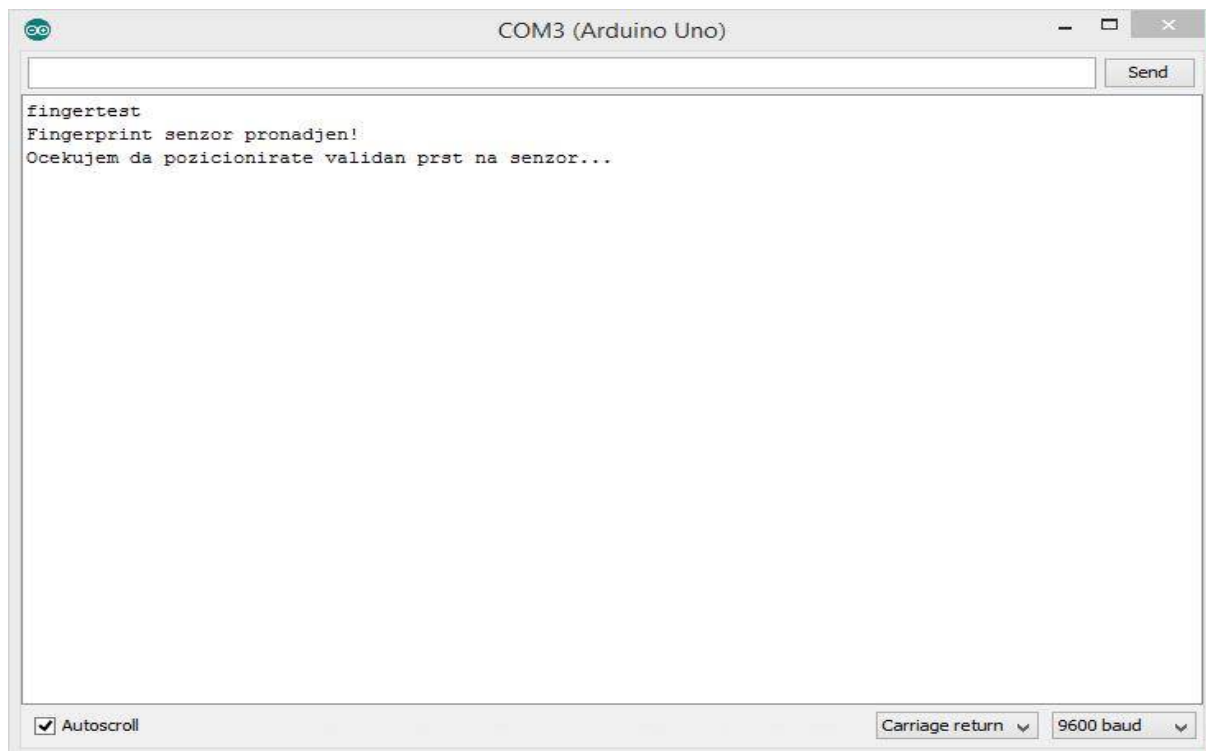
Done uploading.
is 32,256 bytes.

Global variables use 773 bytes (37%) of dynamic memory, leaving
1,275 bytes for local variables. Maximum is 2,048 bytes.

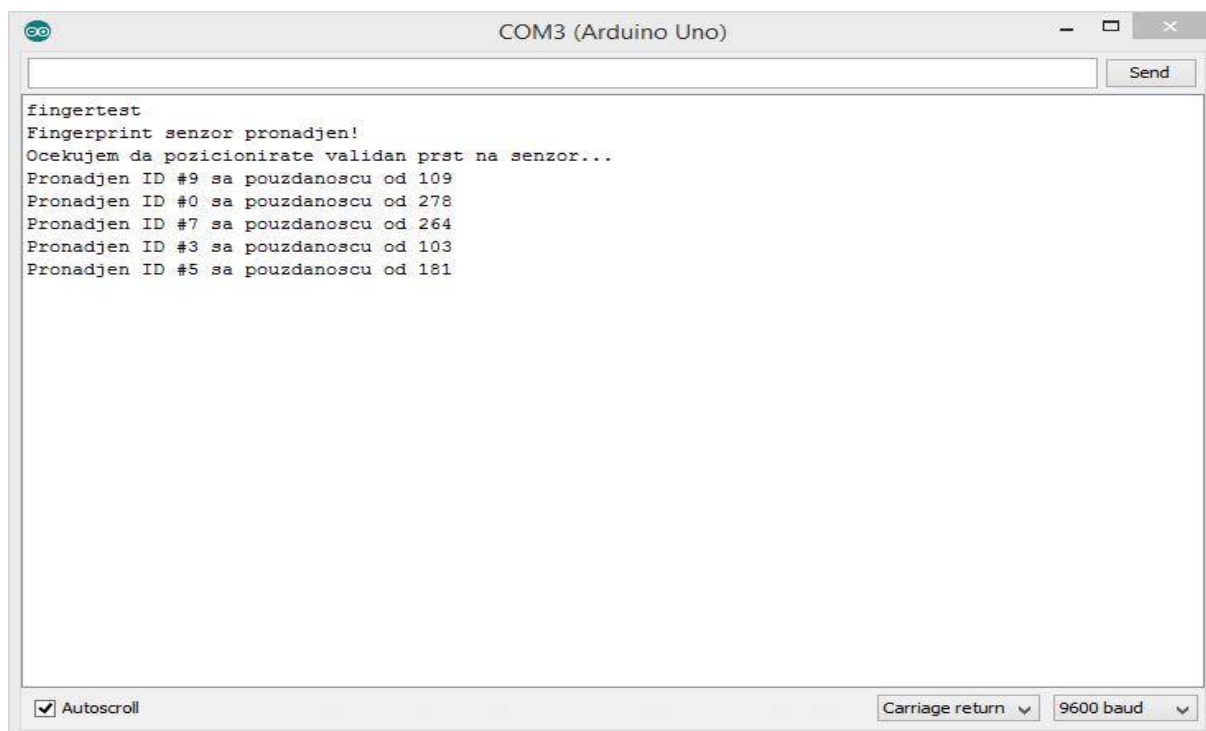
19 Arduino Uno on COM3
```

Slika 25. Funkcija za autentifikaciju;

Nakon uploada funkcije na Arduino Uno R3 ploču, sistem je spreman za autentifikaciju. Možemo testirati one ID-eve koje smo unijeli, i vidjeti sa kojom pouzdanošću će ih senzor prepoznati.



Slika 26. Serial monitor, senzor je spreman;



Slika 27. Imamo uvid u pronađene ID-eve, i sa kojom pouzdanošću;

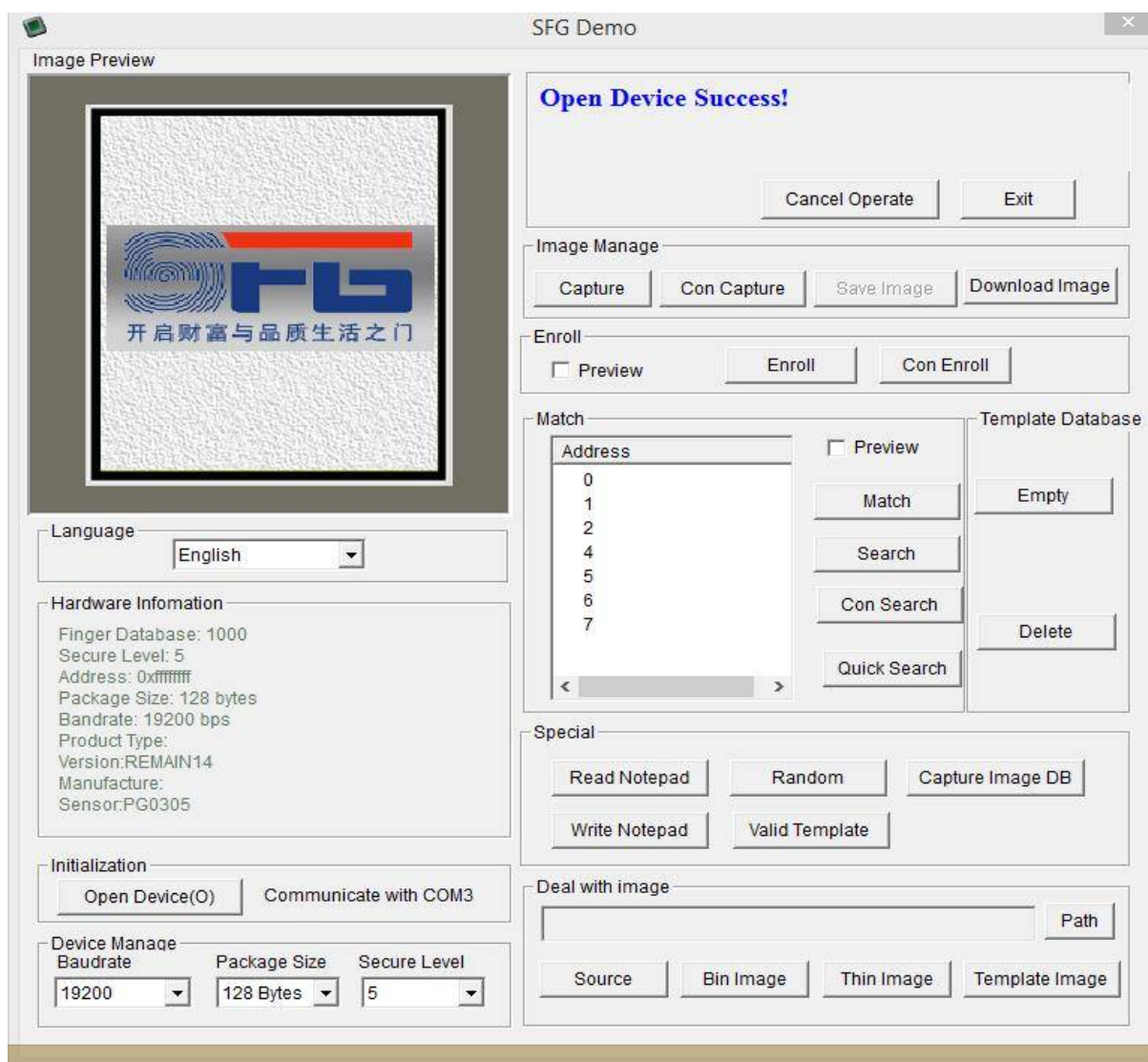


U scenariju koji je osmišljen, prilikom pronalaska ID-a, koji se nalazi pohranjen na ploči, palila bi se zelena dioda, što označava da je autentifikacija uspješna. Ukoliko ID ne odgovara onima koji su pohranjeni na ploči, crvena dioda konstatno gori, što znači da ID ne odgovara, i isti nema pristup sistemu (automobilu, objektu i sl.).

Osim u ovakvim sistemima, Ardafruit biometrijski senzor otiska prsta, može se koristiti za direktno uzimanje otiska prsta, uz sliku otiska. Za to nam je potreban dekstop računar ili laptop, Arduino Uno R3 ploča, i senzor.

Na Arduino Uno R3 ploču potrebno je uploadovati posebnu funkciju, kako bi ploča bila u ulozi bridge-a između senzora, i računara/laptopa.

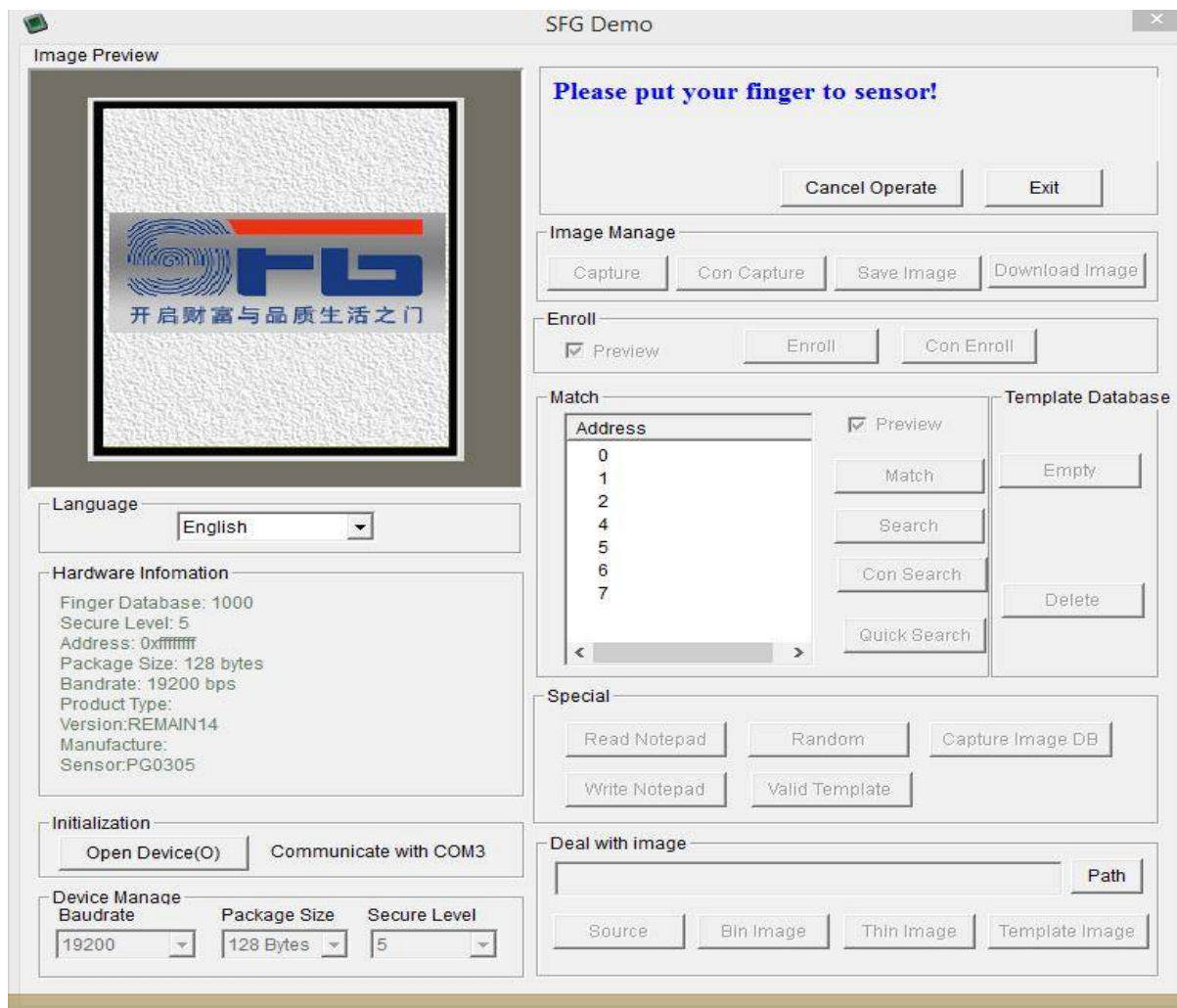
Prikaz ovog scenarija slijedi u nastavku. Pored navedenog koristimo i SFGV2 softver.



Slika 28. SFGV2 interface;

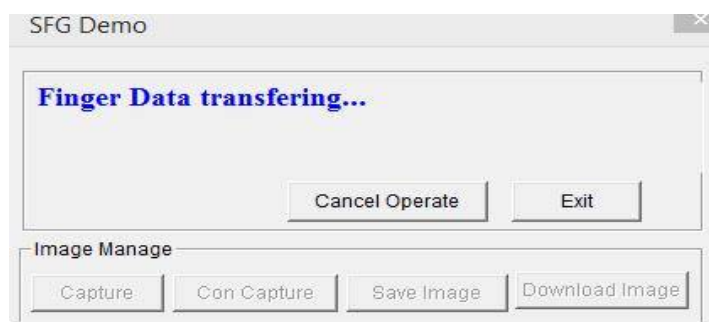


U ovom softveru možemo pregedati već unijete korisnike (ID-eve), te unijeti nove, i eventualno pohraniti sliku željenog otiska.

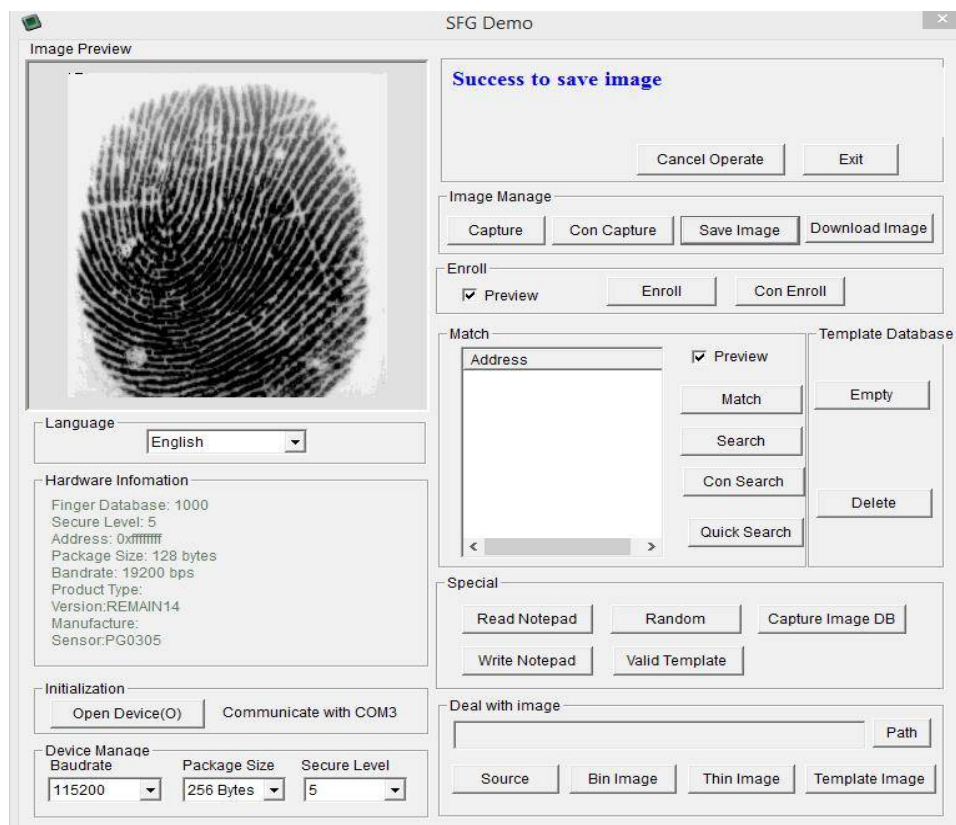


Slika 29. Nakon podešavanja parametara, senzor je spreman;

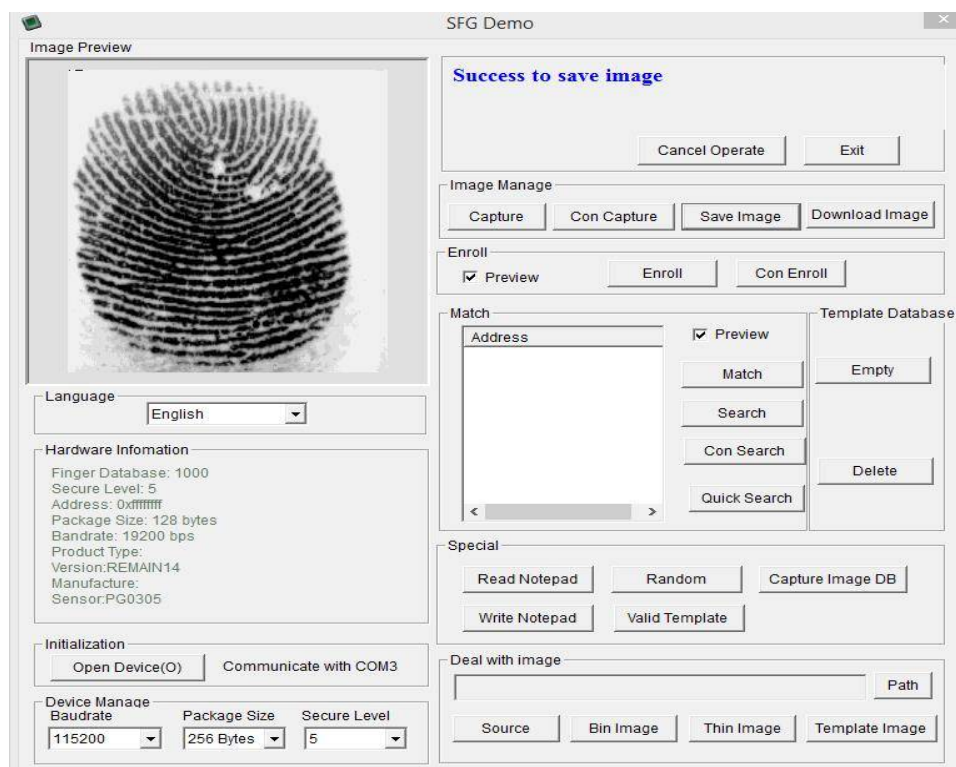
Dakle sve što preostaje da uradimo, je da pozicioniramo željeni prst, i sačekamo pohranjivanje slike. Nakon uspješne pohrane, na malom displeju, moći ćemo vidjeti i sliku prethodno uzetog otiska.



Slika 30. Transfer uzetog otiska;



Slika 31. Primjer uzetog otiska ID1;



Slika 32. Primjer uzetog otiska ID2;



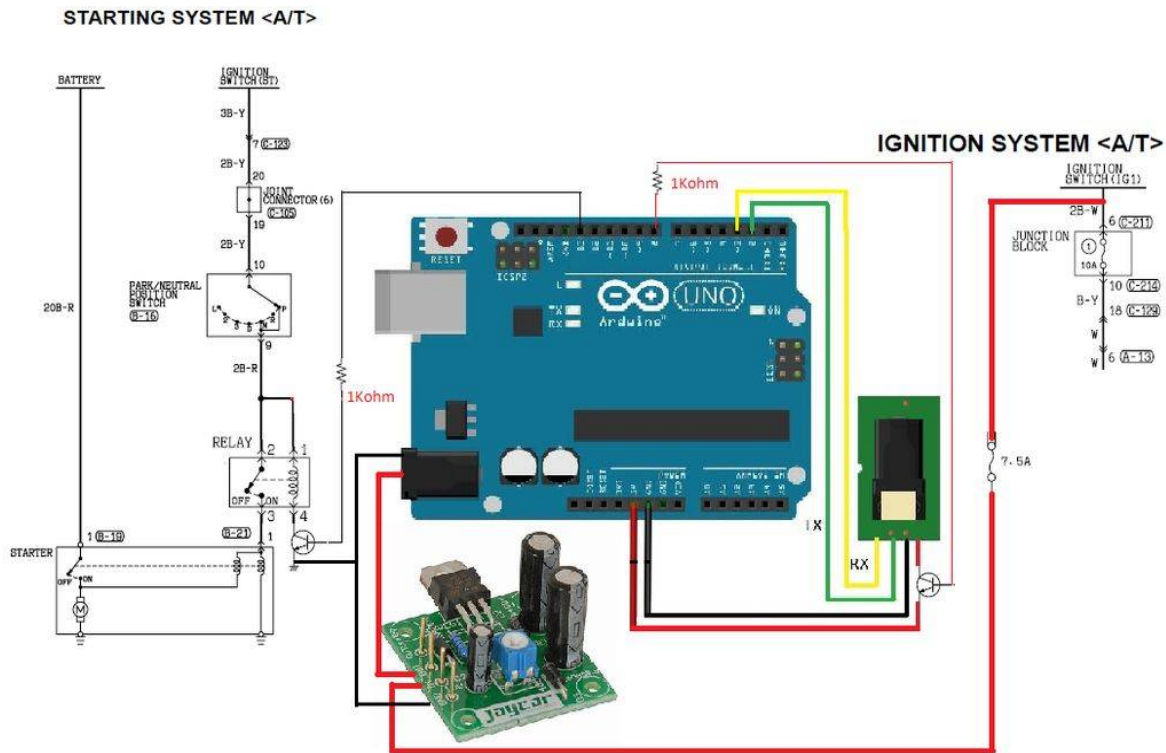
Nakon kompletiranih prethodnih koraka, imamo gotove uzorke otisaka, u obliku slike .bmp formata.



Slika 33. ID1 .bmp;



Slika 34. ID2 .bmp;



Slika 35. Shema potrebna za implementaciju rješenja na automobil;

Osim do sada navedenih dijelova (Arduino Uno R3 ploča, senzor, kablovi), uz prethodno pohranjene ID-eve, bit će nam potreban relej izvor napajanja u automobilu (12 volti). Treba istaknuti da se shema spajanja, razlikuje od automobila do automobila, i da je prije instalacije potrebno prethodno poznavanje rasporeda i načina spajanja elektronskih uređaja u datom automobilu.



5. Zaključak

U radu je razvijeno rješenje bazirano na biometriji otiska prsta, . Slična rješenja su u ponudi u nekim zemljama (Sjedinjene Američke Države) po veoma visokoj cijeni (cca. 700 USD). Primarna primjena zamišljena je u automobilima, kao sredstvo za autentifikaciju. Međutim postoji mogućnost veoma široke primjene i u drugim sferama (zastita objekata, kuća, garaža i sl.).

Kada gledamo u prošlost, vidimo da su kriptografska rješenja, korištena za zaštitu na automobilima, „padala“ prije ili kasnije. Naročito su bili kritični „proprietary“ sistemi, čije je kompromitovanje vješto skrivano. Rješenja bazirana na kriptografskim algoritmima, u kombinaciji sa remote keyless sistemima, uvijek su bila ograničena hardverom. Ukoliko se primjeni malo zahtjevnije rješenje, odma bi se postavljalo pitanje da li će hardver biti usko grlo, u smislu sporog pretraživanja ili sporog odgovora. Ne tako rijetko, i napajanje je znalo biti ograničavajući faktor.

Prije izrade novog rješenja i eksperimentalnog rada, napravljen je detaljan uvid u trenutno stanje u oblasti. Ono u šta možemo sada biti još sigurniji (mada smo mogli dosta sigurni biti i prije) je da nema kriptološkog rješenja (primjenjenog u automobilske industriji) koje može pružiti 100% zaštitu. Da bi automobil učinili sigurnim, moramo razmišljati glavom napadača. Mislim da je upravo tu ključ, za koliko toliko sigurno rješenje. Dakle uvijek moramo biti korak ispred.

Zbog toga je i odabranabiometrija otiska prsta, kao rješenje. Vjerovatnoća da se na neki način kompromituje je veoma niska, gotovo nikakva. Uz pomoć još par mudrih poteza (uklanjanje brave sa vozačevih vrata, promjenu OBD konektora, bilo kakav tip mehaničke brave na letvi volana) mislim da će Vaš automobil biti krupan zalogaj i za napadače čiji je staž dvocifren u tom „poslu“.

5.1. Prijedlog za budući rad

Ono što je u planu u skorijoj budućnosti, jeste pronalazak rješenja za zaštitu (softversku i hardversku) Arduino Uno R3 ploče, od nezakonitog pristupa, te manipulacije podacima na istoj. Kreiranje shema instalacije, za više vozila, naravno onih koja su zastupljenija na našem tržištu, i tržištu regiona.



6. Literatura

- [1] Bogdanov, A. (2010). Cryptanalysis of the KeeLoq block cipher.
- [2] CARNet. (2006). Biometrija.
- [3] CARNet CERT, L. (2007). RFID identifikacija .
- [4] CIS. (2012). Sigurnost automobila .
- [5] Kagin, R. (2007). Keyless Entry.
- [6] MarkoWolf, A. W. (2007). State of the Art: Embedding Security in Vehicles.
- [7] Qinghan Xiao, T. G. (2008). RFID Technology, Security Vulnerabilities, and Countermeasures .
- [8] Roel Verdult, F. D. (2009). Gone in 360 Seconds: Hijacking with Hitag2.
- [9] Schütze, D. T. (2011). Automotive Security: Cryptography for Car2X Communication.
- [10] Soja, R. (2014). Automotive Security: From Standards to Implementation.
- [11] Šimko, A. (2014). Security of car keys .