SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 6351

Kontrola ulaza korištenjem beskontaktnih kartica

Filip Ptiček

Zagreb, lipanj 2019.

Umjesto ove stranice umetnite izvornik Vašeg rada.
Da bi ste uklonili ovu stranicu obrišite naredbu `\izvornik`.

SADRŽAJ

1. Uvod

U današnjem svijetu pokušavamo povezati sve više stvari, uređaja i pomagala s tehnologijom. Na taj način se pokušava olakšati korištenje i mogućnost automatizacije pomoću jednog centralnog mjesta. Takva rješenja nam omogućuju korištenje jednog uređaja za upotrebu u plaćanju, identifikaciji te mnogim drugim stvarima. Neki od centralnih mjesta su mobilni telefoni te beskontaktne kartice koje se nalaze u džepu većine današnjeg stanovništva.

Kontrola ulaza je jedan od poslova koji se od antičkih civilizacija prepuštalo da obavlja čovjek. Vrata koja su koristila mehanizme ključa i brave nisu dopuštale odstupanje od te norme. Tek pojavom kartica s magnetskom trakom došlo je do promjena. Takve kartice dopuštale su da se svakoj osobi dodijeli jedinstveni identifikator. Pomoću čitaća kartica koje su sadržavale spremeljene identifikatore moglo se dopustiti ulaz samo određenim osobama i ujedno voditi evidencija pristupa. Jedna od mana ovakve tehnologije je što korisnik treba karticu dovesti u direktan kontakt s čitaćem te mogućnost jednostavnog repliciranja informacija spremljenih na njima.

Tehnologije kao što su radio-frekvencijska identifikacija (**RFID**) ,nastala 1983. godine, te beskontaktna tehnologija niže frekvencije (**NFC**), nastala 2003. godine, dozvoljavaju udaljenu komunikaciju između čitaća i kartice ili oznake. U današnje vrijeme zamijenile su upotrebu kartica s magnetskom trakom zbog veće sigurnosti i u slučaju RFID-a mogućnosti za praćenjem položaja kartice ili oznake korištenjem komunikacije velikih frekvencija.

Danas se najčešće za kontrolu ulaza koristi beskontaktna tehnologija niže frekvenicije zbog raširenosti u mobilnim telefonima i u slučaju studentske akademske zajednice Republike Hrvatske u njihovim akademskim iskaznicama, što ne zahtjeva uvođenjem posebnih oznaka kao u slučaju radio-frekvencijske komunikacije.

2. Opis problema

Sustav za kontrolu ulaza treba se sastojati od nekoliko dijelova:

- Softverskog dijela za autentifikaciju
- Hardverskog dijela za očitavanje NFC kartica
- NFC kartice
- Mehaničke brave za otvaranje ulaza

Potrebno je pronaći adekvatni uređaj na kojem bi se izvršavala autentifikacija te uređaj za čitanje kartica. Oba uređaja trebaju biti kompaktni, laki za montiranje i neinvanzivni.

Proces kojim bi sustav trebao raditi je:

- Korisnik prilaže NFC karticu u bliski domet čitaća
- Čitać čita identifikacijsku informaciju s NFC kartice
- Čitać šalje informaciju uređaju za autentifikaciju
- Uređaj pomoću programa koji se izvodi na njemu radi autentifikaciju korisnika
- Program zapisuje evidenciju o čitanju
- Uređaj vraća čitaću informaciju ima li korisnik autorizaciju za otvaranje ulaza
- Čitać ovisno o odgovoru uređaja otvara mehaničku bravu ili signalizira korisniku da nema pristup

3. Korišteni razvojni alati

3.1. GNU/Linux

GNU/Linux je operacijski sustav temeljen na Linux jezgri i GNU programskoj potpori te je temeljen na principima otvorenog koda. Jezgra je nastala 1991. godine od strane Linusa Torvaldsa. Razvijana je po uzoru na UNIX operacijski sustav. GNU je sloj iznad jezgre koji se sastoji od skupa programskih paketa koji omogućuju da zadnji aplikacijski sloj cijelog operacijskog sustava funkcionira.

GNU/Linux danas pokreće većinu poslužiteljskih računala, mobilnih telefona, ugrađenih sustava i sve više osobnih računala. Raznovrsnost i rasprostranjenost ovog operacijskog sustava nam omogućuje da razvijamo aplikacije koje će se izvršavati na što više uređaja.

Operacijski sustav dolaze putem različitih distribucija. Neke od pupularnih su: Debian, Ubuntu, SUSE, Red Hat Enterprise Linux te onih namjenjenih za slabija i manja računala poput Raspbiana temeljenog na Debianu.

Za razvoj ovog rada korištena je distribucija Ubuntu zbog svoje dobre programske i korisničke podrške. Za konačnu implementaciju i izvršavanje se koristi Raspbian koji se pokreće na Rapberry Pi-u.

3.2. Python 3 (3.6.7)

3.3. Vim

Vim je tekstualni editor koji zbog svoje velike mogućnosti proširenja i efikasnosti kod pisanja programa je savršeni alat za razvijanje programskih rješenja. Neke od njegovih glavnih značajka su:

- dosljedno, više razinsko stablo poništavanja
- širok sustav nadogradbi

- podrška za stotine programskih jezika i datotečnih formata
- snažna pretraga i promjena teksta
- mogućnost integracija s mnogo alata

3.4. Git

3.5. Raspberry Pi

4. Beskontaktna tehnologija niže frekvencije (NFC)

Beskontaktna tehnologija niže frekvencije, (eng. *Near field communication*) ili skraćeno NFC je vrsta beskontaktne komunikacije između uređaja poput mobilnih telefona i beskontaktnih kartica. Beskontaktna komunikacija dozvoljava komunikaciju na male udaljenosti bez potrebe da uređaji dolaze u neposredni doticaj.

NFC dozvoljava uređaju, koji služi kao čitać, tj. ispitivač, proizvodi aktivno radio frekvenciju što mu dozvoljava da komunicira s ostalim NFC kompatibilnim uređajima ili karticama. Pasivni uređaji poput beskontaktnih kartica i oznaka, imaju spremljenu informaciju te tu informaciju razmjenjuju s čitaćima, ali ne dozvoljavaju čitanje informacija drugih uređaja. Kod komunikacije dva aktivna uređaja postoji obostrana komunikacija slanja i primanja informacija.

Integracija beskontaktnih tehnologija u kreditne, putničke i kuponske kartice dozvoljava korisnicima da obavljaju plaćanja, ukrcavanje na javni prijevoz i razmjenu informacija preko jednostavnog približavanja kartica. Također postoji mogućnost integracije više usluga preko mobilnih telefona te tako eliminirati korištenje različitih kartica za različite usluge.

U današnje vrijeme sve više poduzeća implementira beskontaktne tehnologije u svoje usluge, uključujući implementacije virtualnih kartica koje dozvoljavaju plaćanjem na kartičnim terminalima pomoću mobilnih telefona.

4.1. Povijest

Beskontaktna tehnologija niže frekvencije postoji na temeljima radio-frekvencijske identifikacije (RFID). NFC je podset RFID-a s kraćim dometom zbog sigurnosnih razloga.

2004. godine Nokia, Sony i Philips zajedno su formirali NFC Forum. Njihov zjednički cilj je bio promoviranje sigurnosti, jednostavnosti korištenja i popularnosti

beskontaktne tehnologije niže frekvencije. Zaduženje Foruma je održavanje standarda koji dozvoljava da tehnologija može funkcionirati između sva uređaja. Ako netko želi proizvesti NFC uređaj potrebno je sljediti standarde postavljene od strane NFC Foruma. To osigurava da korisnik sa bilo kojim NFC uređajem može komunicirati s nekim drugim NFC uređajem.

Iako je NFC Forum formiran 2004. godine, prve specifikacije za NFC oznake su se pojavile 2006. godine. NFC oznake su mali objekti koji sadrže informacije koje NFC čitaći mogu pročitati. Informacije na oznakama se u većini slučajeva mogu samo čitati, ali postoje i oznake u koje se mogu upisati nove ili promijeniti stare informacije.

Prvi mobilni telefon koji je sadržavao NFC sposobnosti je bila Nokia 6131 NFC predstavljena 2006. godine. Sazrijevanjem tehnologije dolazile su i nove specifikacije koje su osim podržavanja plaćanja dozvoljavale i razmjenu slika, videa i ostalih informacija. Danas je NFC tehnologija dostupna na većini mobilnih uređaja, od telefona, pametnih satova do integracije u automobile.

4.2. Tehnološki standard

Kada se razvijaju NFC uređaji potrebno je pratiti NFC standarde. Standardi postoje da sve vrste NFC uređaja mogu međusobno komunicirati kako oni dizajnirani u prošlosti tako i u budućnosti. Postoje dvije vrste glavnih specifikacija za NFC tehnologiju:

- ISO/IEC 14443 koja definira identifikacijske kartice koje spremaju informacije, poput NFC oznaka
- ISO/IEC 18000-3 koja definira radio-frekvencijsku identifikacijsku komunikacijsko NFC uređaja

ISO/IEC 18000-3 je internacionalni standard za sve uređaje koji komuniciraju bežično na frekvenciji 13.56MHz. Uređaji trebaju biti na minimalnoj udaljenosti od 4cm prije nego dolazi razmjene informacija. Ovi standardi opisuju način na koji čitać i NFC oznaka s koje se čita trebaju komunicirati međusobno.

Čitać šalje signal oznaki. Ako su uređaji dovoljno blizu jedan drugom oznaka postaje napajana preko signala čitaća. To dozvoljava da oznaka bude malena i bez potrebe da sadrži bateriju ili svoj vlastiti izvor napajanja.

Ta dva uređaja kreiraju visoko frekvencijsko magnetsko polje između zavojnica uređaja. Jednom kada je polje uspostavljeno, dolazi do konekcije i razmjene informacija između čitaća i oznake. Čitać šalje prvu poruku oznaci kako bi doznao vrstu komunikacije koju oznaka koristi, tip A ili tip B. Kada oznaka odgovori čitać šalje prvu

naredbu koja mora odgovarati specifikaciji.

Oznaka nakon primitka naredbe provjerava je li ona ispravna. Ako nije, oznaka ne odgovara. U protivnom odgovara s zahtjevanom informacijom. Kod nekih komunikacija poput kartićnih plaćanja dolazi do uspostave sigurnog komunikacijskog kanala i sve informacije poslane su enkriptirane.

NFC oznake rade na principu da u jednom trenutku mogu samo primati ili slati informacije, dok čitaći mogu primati informacije i slati naredbe istovremeno. Naredbe se šalju s čitaća preko mofulacijskog faznog podrhtavanja (eng. *phase jitter modulation*) (PJM) kako bi modificirao okružujuće polje i poslao signal. Oznaka odgovara koristeći induktivnost kako bi poslala naboj preko svojih zavojnica.

Prateći ove specifikacije osiguravamo da svi NFC uređaji mogu međusobno komunicirati.

4.3. Sigurnosni problemi

Korisnici NFC tehnologije se naravno pitaju koji su sigurnosni rizici pogotovo oni koji ju koriste za kartična plaćanja. Jesu li njihove informacije sigurne i otporne na krađu? U nastavku su neki od sigurnosnih problema koji se mogu pojaviti i kako NFC tehnologija ih sprječava.

4.3.1. Prisluškivanje

Prisluškivanje se dešava kada osoba prati komunikaciju između čitaća i oznaka. Nije potrebno pratiti svaki signal da bi se prikupila privatna informacija. Postoje dvije metode kako spriječiti prisluškivanje:

- udaljenost na kojoj NFC radi. Kako NFC radi na maloj udaljenosti prisluškivanje se može desiti na jako malom području.
- Sigurni kanali. Kada je uspostavljen sigurni kanal, sve informacije koje se razmjenjuju su enkriptirane i samo ovlašćeni uređaji ih mogu dekriptirati. Potrebno je samo provjeriti koriste li čitaći sigurne kanale.

4.3.2. Korupcija i manipulacija podataka

Korupcija i manipulacija se dešavaju kada osoba manipulira informacijama koje se šalju čitaću ili posreduje informacijama tako da budu iskvarene i beskorisne kada dođu

do čitaća. Kako bi se spriječila korupcija i manipulacija koriste se sigurni kanali. Neki uređaji mogu prepoznati takve napade i spriječiti ih prije nego što se dogode.

4.3.3. Presretanje

Presretanje je slično manipulaciji podataka. Kod presretanja postoji posrednik koji čita, mijenja sve informacije koje se razmjenjuju između čitaća i oznake. Ovakva vrsta napada je složena za izvesti i rijeđe se dešava. Kako bi se spriječio jedan uređaj mora djelovati aktivno, a drugi pasivno. To znači da jedan šalje, a drugi prima informacije umjesto da oba šalju i primaju informacije.

4.3.4. Krađa

Ako dođe do krađe mobilnog telefona ili kartice kradljivac može lako oponašati osobu te tako dobiti pristup plaćanjima i ulazima. Zato je potrebno upotrijebiti dodatne mjere sigurnosti kao postavljanje sigurnosnih lozinka na svoje mobilne uređaje ili u slučaju kartica i oznaka prijaviti krađu svim administratorima sustava kod kojih je ta kartica ili oznaka zabilježena.

5. Arhitektura i dizajn sustava

6. Zaključak

Zaključak.

LITERATURA

Kontrola ulaza korištenjem beskontaktnih kartica

Sažetak

Sažetak na hrvatskom jeziku.

Ključne riječi: Ključne riječi, odvojene zarezima.

Title

Abstract

Abstract.

Keywords: Keywords.