Aplikacija za evidentiranje prisustva

MSc završni rad

Autor: Malik Koljenović, BSc IT

Odsjek za računarstvo i informatiku

Elektrotehnički fakultet

Mentor: prof. dr. Saša Mrdović

Sarajevo, juni 2018

Abstract This thesis addresses the problem of large scale electronic attendance taking in university setting by presenting an Android based attendance taking application, based on immutable and non repudiable location proofs backed by RSA cryptography, utilizing NFC and HCE for ease of use, emulating NFC Forum Tag Type 4 it is also compatible with existing reader infrastructures. It also presents a general overview of the utilized techologies and select implementation details.

Apstrakt Ova teza tretira problem masovnog elektronskog bilježenja prisustva u univerzitetskom okruženju izradom prijedloga aplikacija bazirane na Android platformi korištenjem neizmjenjivih i neporecivih vremensko-lokacijskih dokaza osiguranih korištenjem RSA kriptografije, te NFC i HCE tehnologija u cilju jednostavnosti upotrebe; emulirajući NFC Forum Tag Tip 4 kompatibilna je sa postojećim infrastrukturama čitača. Dat je i opšti pregled korištenih tehnologija i izdvojenih implementacijskih detalja.

MSC Primary 68P25; Secondary 94A60;

Keywords: NFC - near-field communication, HCE - host card emulation, security, Android, attendance, RSA, cryptography, NDEF, NTAG, geolocation, location proofs

Sadržaj

Popis slika

Popis tablica

Pojmovnik

ATTN repozitorij potpisanih prisustva spremljen na LAPI.

BUMP približavanje mobilnih uređaja, otvara jednosmjerni komunikacijski kanal u smijeru od slave (S) prema master (M) uređaju.

CERT javni dio korisničkog kriptografskog ključa.

DEVICE korisnički Android uređaj.

HCE *(en. Host card emulation)* softverska arhitektura koja omogućava virtualnu emulacija elektronskog identiteta.

ISO/IEC 14443 Tip A standard fizičkog sloja NFC komunikacijskog protokola.

KEYS jedinstveni set korisničkih RSA ključeva dužine 2048 bita.

LAPI Logit API, Python serverska aplikacija, komponenta LAPP platforme.

LAPP Logit višekomponentna aplikacijska platforma.

M *(en. master)* - Android UI komponenta pokrenuta na uređaju koji bilježi prisustvo.

NDEF vrsta standardizovanog paketa korištena za NFC komunikaciju između uređaja.

NDEFMSG NDEF poruka koja sadrži vremensko-lokacijski dokaz potpisan od strane korisnika.

S *(en. slave)* - Android komponenta koja se izvršava u pozadini na uređaju čije se prisustvo bilježi.

SPIM *(en. SPacetIME)* - lokacijski dokaz (JSON objekat, struktura podatka).

SSO *(en. Single Sign On)* - politika autentifikacije korištenjem jedinstvenog repozitorija.

NFC Forum Tag standardizovani format NFC taga.

UI Android komponente LAPP platforme.

1 Uvod

Prodor digitalnih računara i komunikacijskih tehnologija u sve sfere ljudskog života i djelovanja, te dramatično povećanje broja korisnika interneta u posljednjoj deceniji nametnulo je mnoštvo novih društvenih i tehničkih izazova. Društveni izazovi najbolje su uočljivi kroz višedecenijsku debatu o privatnosti i vlasništvu nad ličnim podacima, samim time zadiru duboko u diskusiju o ljudskim pravima i identitetu sa jedne i često suprostavljenim komercijalnim interesima sa druge strane. Ukoliko se u tom kontekstu posmatra aktuelna EU uredba o zaštiti podataka[1] (*en. GDPR*) postaje jasno da su digitalna tehnologija i komunikacije postale integralni dio društvene i emocionalno-psihološke realnosti[2], do te mjere da se digitalni tragovi smatraju dijelom nepovredivog identiteta osobe. Iz navedenog je jasno da se radi o institucionalizaciji jedne potpuno nove društveno-tehnološke paradigme unutar pravnih okvira Europske unije.

Sa tehničke strane, dostignuća na poljima kriptografije, teorije mreža i novih komunikacijskih tehnologija, te njihova široka prihvaćenost otvorila su mogućnosti izrade računarskih sistema spremnih da odgovore na novonastale društvene izazove u okviru opisane nove paradigme. Pomenuti računarski sistemi kao dodatno izvršno okruženje imaju društveno-pravnu realnost te se u tim okvirima izvršavaju masovno, dobrovoljno, distribuirano i interaktivno[3] van centralizovanog računarskog izvršnog okruženja u smislu Von Neumannove arhitekture. Opisani sistemi mogu se okarakterisati kao sistemi potpomaganja (*en. assist*), npr. kriptografski računarski sistem u domenu autentifikacije i autorizacija u novoj paradigmi postmatra se kao sistem računarski-potpomognutog povjerenja, ekvivalentno višem nivou apstrakcije.

Registri u kontekstu društvenih institucija su elementarni mehanizam sistema povjerenja, sigurnosne karakteristike takvih institucionalnih registara stoga čine osnov istraživačkog interesa u domenu institucionalne sigurnosi. Napredni elektronski registri izrađeni korištenjem kriptografskih tehnika i savremenih komunikacijskih protokola za prikupljanje i obradu podataka omogućavaju poboljšanje njihovih sigurnosnih osobina, otvarajući nove načine primjene i stvarajući uslove za viši nivo društvenog razvoja i institucionalne efikasnosti, uz to pružaju i adekvatan odgovor na novonastale društvene izazove. Stoga, ukoliko se obezbijede i ispoštuju preduslovi izrade sigurnog sistema, evidenciju prisustva u kontekstu naprednog elektronskog registara treba posmatrati i kao vremensko-prostorni dokaz određenog događaja, ovaj rad usmjeren je na izradu jednog takvog sistema računarski-potpomognutog povjerenja u obliku institucionalnog registra elektonske evidencije prisustva.

2 Postavka problema

Projektni zadatak ovog završnog rada je izrada aplikacije na Android platformi sa pripadajućom udaljenom komponentom, koje u cjelini treba da omoguće evidentiranje prisustva nastavnim aktivnostima na Elektrotehničkom fakultetu u Sarajevu. U skladu sa zadatim funkcionalnim zahtjevima, a iz razloga olakšanog korištenja i praktičnosti upotrebe neophodno je iskoristiti beskontaktne komunikacijske mogućnosti savremenih mobilnih telefona u vidu NFC komunikacijskog protokola.

Također neophodno je osigurati korisnike aplikacije od mogućih zloupotreba korištenjem dostupnih kriptografskih metoda i tehnologija, te stvoriti neophodne uslove za sticanje povjerenja u širi sistem bilježenja prisustva putem neporecivosti i neizmjenjivosti prethodno unesenih podataka. Poželjna mogućnost je jednostavna integracija sa postojećim sistemima, prvenstveno onim autentifikacijskim i autorizacijskim, te planiranje arhitekture za buduća proširenja u vidu omogućavanja integracije sa infrastrukturnim hardverskim čitačima i TAG karticama.

Potrebno je dokumentovati proces izrade i opisati korištene tehnologije, sa posebnim osvrtom na korištene kriptografske metode i tehnologije, te identifikovati otvorena pitanja na polju elektronskih registara prisustva, mogućnosti i izazove koje oni predstavljaju uz rješenja koja navedena aplikacija nudi u datom kontekstu.

3 Prijedlog rješenja

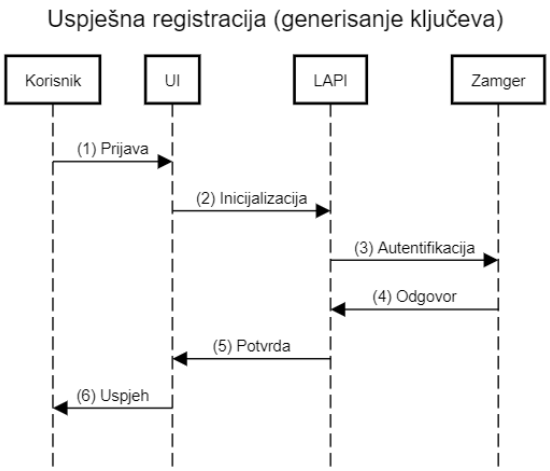
U skladu sa datim zahtjevima predložena je izrada aplikacijske platforme pod nazivom Logit (LAPP), opisane u nastavku, sa detaljnim tehničkim detaljima u narednim poglavljima. Uzimajući u obzir data ograničenja, te funkcionalne i nefunkcionalne zahtjeve određeno je da se korisnička aplikacija izradi na Android platformi sa podrškom za Android API nivo počevši od nivoa 19 (4.4 KitKat), to je najniži nivo koji omogućava korištenja naprednih NFC i kriptografskih funkcionalnosti te osigurava dobru pokrivenost potencijalne korisničke baze sa ukupnom adopcijom od preko 90% za navedenu ili višu verziju[4]. Za uspješan rad aplikacije neophodno je da korisnički uređaj podržava i NFC funkcionalnosti, prema prognozama analitičke kuće IHS Technology, do 2020. godine svaki treći uređaj imati će podršku za NFC.[5]

3.1 Logički model rješenja

Priloženi dijagrami interakcije osnovnih funkcionalnosti Logit platforme i pripadajući opis imaju za cilj stvoriti opštu sliku sistema, te tako olakšati praćenje tehničkog modela rješenja datog u nastavku. Tehnički model opisuje dosta detaljniju sliku funkcioniranja sistema i može služiti kao svojevrstan uvod u kod platforme.

3.2 Tehnički model rješenja

Uvodi se dodatno pojam lokacijskog dokaza[6] koji u širem smislu u kontekstu podređenog korisnika (en. slave), obuhvata kriptografski potpisan korisnički identitet, korisnički uređaj, vrijeme i GPS lokacijske podatke korisničkog uređaja. Za svrhu

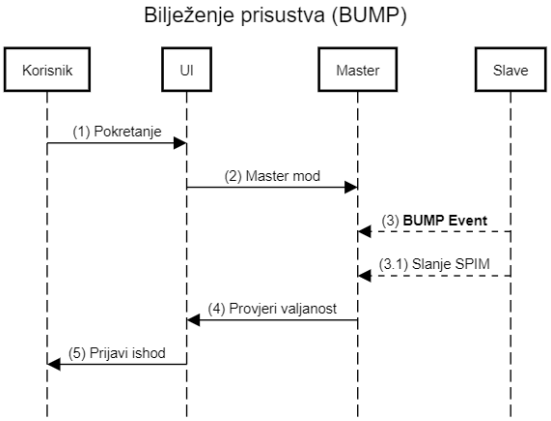


Slika 3.1: Dijagram interakcije - uspješna registracija korisnika i generisanje ključeva

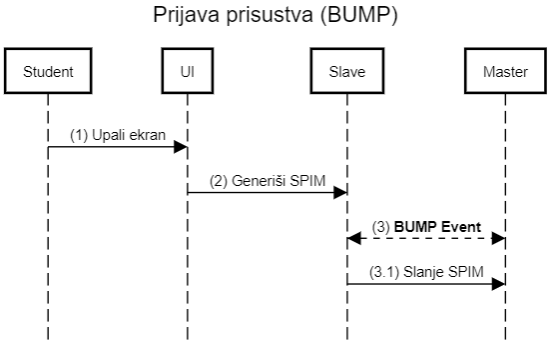
osiguranja jedinstvenosti identiteta i vjerodostojnosti potvrde lokacijskih dokaza odabrano je korištenje RSA asimetrične enkripcije, gdje se pri uspješnoj autentifikaciji generiše jedinstveni set ključeva za korisnički uređaj, privatnom dijelu ključa nije moguće pristupiti izvan aplikacije (SEC1), niti je moguće eksportovati ključ (SEC2), a u određenom vremenskom period može postojati samo jedan valjan set ključeva za jednog korisnika jer se raniji ključevi ne uzimaju u obzir ukoliko postoji noviji set (SEC3), sprječavajući tako replikaciju identiteta na više uređaja.

Pored Android komponente aplikacije (UI) izrađena je i serverska aplikacija u programskom jeziku Python (LAPI), čija je namjena posredovanje u komunikaciji sa autentifikacijskim agentom (ZAMGER), te pohranjivanja i održavanje javnih korisničkih kriptografskih ključeva (CERT) i njihovo povezivanje sa autentifikacijskim podacima korisnika, pored toga služi i kao repozitorij za potpisana prisustva (ATTN). Na ovu komponentu se može gledati kao na integrisani namjenski repozitorij korisničkih certifikata i domenski repozitorij neporecivih i neizmjenjivih lokacijskih dokaza (SPIM).

Budući da na Elektrotehničkom fakultetu u Sarajevu postoji SSO (en. Single-Sign On) politika autentifikacije, u serverskoj komponenti (LAPI) je implementiran auten-



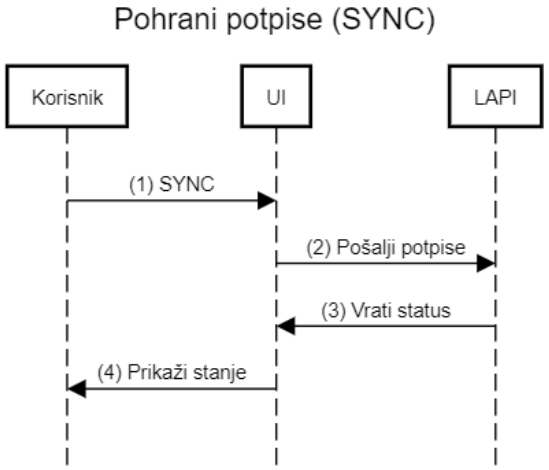
Slika 3.2: Dijagram interakcije - bilježenje prisustva studenata (Master BUMP)



Slika 3.3: Dijagram interakcije - prijava prisustva studenta (Slave BUMP)

tifikacijski posrednik koji prilikom prvog pokretanja aplikacije prijavljuje korisnika koristeći postojeće pristupne podatke, tom prilikom u slučaju uspješne prijave generiše se i jedinstveni set RSA ključeva dužine 2048 bita (KEYS), koji se pohranjuju na korisničkom uređaju (DEVICE), a javni dio, tj. certifikat (CERT) se pohranjuje i u repozitorij ključeva (LAPI) sa poveznicom na korisnički identitet, kasnije se ti certifikati koriste za provjeru valjanosti potpisa lokacijskih dokaza (SPIM).

Da bi se osigurala jednostavnost korištenja aplikacije odabrana je implementacija HCE emulacijskog načina rada NFC komunikatora koji omogućava korisniku da izvrši komunikaciju sa drugim uređajem bez potrebe da pokreće aplikacijski prozor na svom



Slika 3.4: Dijagram interakcije - pohranjivanje potpisa na LAPI (SYNC)

uređaju, dovoljno je da upali ekran svoj uređaja i prinese ga master (M) uređaju koji prikuplja potpise, u ovom slučaju drugoj instanci Logit aplikacije na kojoj je pokrenuta aktivnost za prikupljanje potpisa (LAPP).

Približavanjem mobilnih uređaja (BUMP) otvara se jednosmjerni komunikacijski kanal u smijeru od slave (S) prema master (M) uređaju korištenjem ISO/IEC 14443 Tip A komunikacijskog protokola pri čemu se emulira NFC Forum Tag tipa 4 i putem NDEF Aplikacije prenosi jedna NDEF poruka (NDEFMSG) koja sadrži vremensko-lokacijski dokaz potpisan od strane korisnika, nadalje u tekstu označen kao SPIM (en. spime)[7].

Po primitku poruke nadređeni uređaj (en. master) koji osluškuje da mu se pridruže podređeni uređaji (en. slave) i ima pokrenutu Logit aplikaciju, tu poruku sprema u lokalni repozitorij potpisa ukoliko ona zadovolja uslove da očitana slave GPS lokacija nije udaljena više od 50 metara od očitane master GPS lokacije (VK1 - validacijski kriterij #1), te da podešena razlika satova master i slave uređaja nije veća od 300 sekundi (VK2), bez da nad SPIM objektom vrši ikakve izmjene, ukoliko SPIM objekat ne zadovoljava date validacijske kriterije odbija se i ispisuje se odgovarajuća poruka na master ekranu. Moguće je naknadno klikom na validacijsko dugme (ACTVAL) u korisnič-

kom interfejsu izvršiti provjeru svih prikupljenih potpisa tokom jedne sesije (SESS), tom prilikom se, ukoliko postoji mrežna veza; svi potpisi pošalju Logit serveru (LAPI) na provjeru i vraća se stanje valjanosti potpisa za sve proslijeđene SPIM objekte.

Ukoliko master (M) želi da pohrani SPIM objekte iz jedne sesije (SESS) na Logit server (LAPI), klikom na sinhronizacijsko dugme u interfejsu (ACTSYNC), on vrši dodatno potpisivanje svakog SPIM objekta svojom komponentom privatnog ključa (MPRK), tako što potpiše hash (SHA256) vrijednost SPIM objekta (AID) sa dodatim svojim jedinstvenim master korisničkim imenom (MUSER) i jedinstvenim identifikatorom sesije (SID) i dodatno generiše SHA256 vrijednosti tih potvrda (CID), nakon čega objedinjuje sve CID vrijednosti i dodatno ih potpisuje svojim MPRK, sve te vrijednosti šalje Logit server (LAPI) na pohranjivanje, ovakvom procedurom se obezbjeđuje neporecivost i neizmjenjivost SPIM i SESS objekata, jer onemogućava izmjene pojedinačnih SPIM objekata, te brisanje ili dodavanje objekata u finaliziranoj sesiju (SESS) od strane malicioznih aktera bez da naruši integritet SHA256 vrijednosti.

Uzmimajući u obzir bitnost rješenja i visoku vjerovatnoću svakodnevne primjene kod ciljane korisničke grupe, te izazove koje takav slučaj korištenja predstvalja omogućena je i direktna e-mail komunikacija za prijavu grešaka ili slanje prijedloga sa glavnog korisničkog interfejsa (ACTBUG). Kako se radi o slojevitom i kompleksnom softverskom rješenju za više detalja referirati se na izvorni kod priložen u dodatku.

4 Pregled korištenih tehnologija

Android API https://developer.android.com/about/dashboards/

4.1 NFC - Near-field communication

android.nfc.cardemulation - added in API level 19

4.2 NDEF - NFC Data Exchange Format

4.3 HCE - Host card emulation

https://developer.android.com/guide/topics/connectivity/nfc/hce https://nelenkov.blogspot.com/201
embedded-secure-element-in.html https://nelenkov.blogspot.com/2012/08/android-
secure-element-execution.html https://nelenkov.blogspot.com/2012/08/exploring-google-
wallet-using-secure.html UICCs are actually smart cards that can host applications, and as such are one form of a SE. However, since the UICC is only connected to the basedband processor, which is separate from the application processor that runs the main device OS, they cannot be accessed directly from Android. All communication needs to go through the Radio Interface Layer (RIL) which is essentially a proprietary IPC interface to the baseband. there is currently no standard way to communicate with the UICC SE through the RIL

The Single Wire Protocol (SWP) is a specification for a single-wire connection between the SIM card and a near field communication (NFC) chip in a cell phone. It is currently under final review by the European Telecommunications Standards Institute

(ETSI).[1][2] ETSI TS 102 613 V.11.0.0 - UICC-CLF Interface; Part 1: Physical and data link layer characteristics (Release 11) ETSI TS 102 622 V.12.1.0 - UICC-CLF Interface; Host Controller Interface (HCI) (Release 12) https://en.wikipedia.org/wiki/Single$_{W}ire_{P}rotocolThisisthec$

NFC and the SE are tightly integrated in Android, and not only because they share the same silicon, so let's say a few words about NFC. NFC has three standard modes of operation: reader/writer (R/W) mode, allowing for accessing external NFC tags peer-to-peer (P2P) mode, allowing for data exchange between two NFC devices (Android Beam) card emulation (CE) mode, which allows the device to emulate a traditional contactless smart card

https://randomoracle.wordpress.com/2014/08/12/fakeid-android-nfc-stack-and-google-wallet-part-i/

https://randomoracle.wordpress.com/2013/12/02/nfc-card-emulation-and-android-4-4-part-i/

HCE je inicijalno bio direktno nakacen na eSE, kasnije je i i sam Google presao na host emulaciju, razlog za ugradnju SE cipa je bio jer telekom operateri nisu dopustili Googlu pristup njihovom SE, naknadno je google kupio taj njihov projekat ISIS, koji je izgleda na kraju i napusten.

Turning the screen on enables card-emulation mode on Android devices by default. (Note it is not necessary to unlock the screen, similar to how payments can be executed by tapping the point-of-sale terminal.) When the phone is introduced to the NFC field of the smartcard reader in this state, Windows smart-card service registers it as a card-present event. Appearance of a new card triggers a discovery process, to determine what type of card the user has introduced. End goal is picking a suitable smart-card driver. Because applications using smart-card operate in terms of higher level of abstractions such as certificates and cryptographic keys, drivers are required to translate these into low-level commands that each type of card understands. During the discovery process, the PC will exchange traffic over NFC with the secure element, to query its features. Driver discovery fails. This is not surprising– the "card" in question is used for contactless payments. It does not im-

plement any of the standard card edges built into Windows 7/8 (PIV and GIDS) and neither does the answer-to-reset (ATR) identifier returned by the secure element Because no driver is located, the higher level application– in this case Windows logon– also fails in its attempt to locate credentials on the card, displaying the error in the last screenshot. https://randomoracle.wordpress.com/2012/11/25/your-android-phone-is-also-a-smartcard/

The first post in this series described the permissions model for accessing the Android secure element from its contact interface. (Not to be confused with access from contactless aka NFC interface, which is open to any external device in NFC range.) This model can be viewed as a generalization of standard Android signature-based permissions— in fact for Gingerbread it was a vanilla signature permission based on matching the certificate used for signing NFC service.

Starting with ICS, there is an explicit whitelist of allowed signing certificates. Any user application signed with one of these keys can obtain access to the secure element, and more broadly to administrative actions involving the NFC controller such as toggling card emulation mode. https://randomoracle.wordpress.com/2013/01/19/using-the-secure-element-on-an-android-device-23/

4.4 Kriptografske tehnologije

https://www.kaspersky.com/blog/secure-element/22408/

4.5 Android

4.5.1 GPS Geolokacija

Treba provjeravati geo spoof

5 Izdvojeni detalji implementacije

5.1 Podatkovni i kriptografski primitivi

5.1.1 SPIM paket

5.1.2 SESS paket

5.2 NFC komunikacijski protokol

5.3 LAPI komunikacijski protokol

6 Zaključak

Dodaci

A Korisničko uputstvo

B LAPI model podataka

C Logit API Dokumentacija

Bibliografija

[1] EU, "Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)," 2016.

[2] J. R. Searle, S. Willis, *et al.*, *The construction of social reality*. Simon and Schuster, 1995.

[3] V. Cahill, E. Gray, J. M. Seigneur, C. D. Jensen, Y. Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. Di Marzo Serugendo, C. Bryce, M. Carbone, K. Krukow, and M. Nielsen, "Using trust for secure collaboration in uncertain environments," *IEEE Pervasive Computing*, vol. 2, no. 3, pp. 52–61, 2003.

[4] "Android statistics dashboard." - https://developer.android.com/about/dashboards/index.html. Pristupano: 2017-09-01.

[5] "Nfc world - adoption statistics." - https://www.nfcworld.com/2014/02/12/327790/two-three-phones-come-nfc-2018/, 2014. Pristupano: 2017-09-11.

[6] R. Khan, S. Zawoad, M. M. Haque, and R. Hasan, "Who, when, and where? location proof assertion for mobile devices," in *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 146–162, Springer, 2014.

[7] B. Sterling and L. Wild, *Shaping things*. The MIT Press, 2005.