

KRIPTOGRAFSKA ZAŠTITA PODATAKA ZA ANDROID ARHITEKTURU

Mladen Veinović

Univerzitet Singidunum
Bulevar Zorana Đinđića 44, Novi Beograd
Telefon: +381 11 31 21 349
Fax: +381 11 31 21 563
e-mail: mveinovic@singidunum.ac.rs

Miroslav Čajić

MikroByte doo
Vese Rackovića 16, 73220 Rogatica
Telefon: +387 65 631 675
Fax: +387 58 417 517
e-mail: miroslavcajic@gmail.com

Bogdan Brkić

Ministarstvo finansija Republike Srpske
Trg Republike Srpske I, 78000 Banja Luka
Telefon: +387 65 567 941
Fax: +387 51 339 686
e-mail: bbogdan@teol.net

Sažetak - U ovom radu izvršena je detaljna analiza Android tehnologije. Predstavljani su modeli bezbjednog rješenja za tajni prenos podataka između dva mobilna uređaja koji rade pod Android operativnim sistemom. Razmatrana su standardna rješenja distribucije ključeva i predložena je njihova modifikacija u cilju postizanja većeg stepena bezbjednosti i povjerenja u ukupan bezbjedonosni sistem. U predloženom rješenju podrazumeva se primjena sopstvenog kriptografskog algoritma.

Ključne riječi: Android arhitektura, vlastiti algoritam, kriptografski sistem, generator ključeva.

Abstract -This work was performed detailed analysis of the Android technology. Presented models of security solutions for the secret transfer of data between two mobile devices that operate under the Android operating system. Considered the standard solutions proposed distribution of keys and their modification in order to achieve a greater degree of security and confidence in the overall security system. The proposed security solution with its own cryptographic algorithm.

Key words: Android architecture, own algorithm, cryptographic system, keys generator.

1. UVOD

Svakodnevna upotreba mobilnog telefona dovela je do povećane potrebe kako za fleksibilnošću tako i za razvojem novog operativnog sistema sa nizom pogodnosti za olakšavanje rukovanja uređajem. Pretpostavka je da će u narednih nekoliko godina, zbog širenja broja ovih mobilnih uređaja, njihov broj premašiti broj fiksnih telefonskih aparata. Neke od osobina operativnog sistema koji se koristi za mobilne uređaje su:

- prilagodljivost korisniku,
- korisnički interfejs,
- korisničke aplikacije,
- integracija više uređaja u jednom,
- upravljivost uređajem i
- baza podataka.

Upotreba operativnog sistema za mobilne uređaje u velikoj mjeri je doprinijela poboljšanju funkcionalnosti samih uređaja. Potreba za usavršavanjem upravljivosti mobilnih telefona dovela je do toga da su proizvođači za svaki novi hardver telefona pravili i odgovarajući softver. Nova serija određenog tipa telefona zahtijevala je reviziju već postojećeg ili izradu nove verziju softvera.

U ovom radu se analizira zaštićeni prenos podataka za mobilne telefone čiji se rad zasniva na Android arhitekturi. Android je upravljački program namjenjen mobilnim uređajima, koji se sastoji se od operativnog sistema, međuslojeva i ostalih ključnih programa. Jezgro Androida čini Linux Kernel, verzija 2.6., što omogućava sistemu povećanu bezbjednost kao temelj stabilnosti sistema. Odlikuje se sistemom za upravljanje memorijom i procesima kao i mrežnim uslugama [1,2]. Odabrani operativni sistem je pogodan za realizaciju zaštićenih aplikacija i to za organizacije od opšteg interesa kao što su vojne i civilne bezbjednosne organizacije. Ove organizacije iz bezbjedonosnih razloga uvijek imaju interes za realizaciju vlastitih kriptografskih rješenja. Za realizaciju vlastitih, ili za modifikaciju postojećih rješenja zaštite neophodan je uslov koji se odnosi na dostupnost izvornog (*source*) kôda. Pored kriptografskih algoritama posebna pažnja je posvećena distribuciji kriptoloških ključeva. Činjenica je da je u korektno realizovanim rešenjima ukupna bezbjednost svedena na bezbjednost i kvalitet kriptoloških ključeva koji se primjenjuju u konkretnom kriptološkom rješenju. U ovom radu razmatrana su standardna rješenja distribucije ključeva i predložena je njihova modifikacija u cilju postizanja većeg stepena bezbjednosti i povjerenja u ukupan bezbjedonosni sistem.

2. ANALIZA ANDROID ARHITEKTURE

Arhitektura Android platforme definiše njenu funkcionalnost i ulogu. U početku je razvijana samostalno od strane Google-a, da bi se poslije pridružila u **OHA (Open Handset Alliance)**. Jedan dio Android operativnog sistema je razvijan privatno od strane različitih programera i naziva se *Cupcake*. Cupake je naziv za dopunu sistema koji nije zvanično potvrđen od Google-a [3,4,5,6]. Android je sastavljen od nekoliko bitnih i zavisnih dijelova kao što su:

- **Linux kernel** operativni sistem - omogućava komunikaciju na nivou hardvera, upravlja memorijom, kontroliše procese, vrši optimizaciju aplikativnog softvera za mobilne uređaje.
- **Hardverski referentni dizajn** - opisuje niz sposobnosti kako bi bila obezbjeđena softverska podrška potrebna za mobilne uređaje.

- **Open Source biblioteke** – koriste se za razvoj aplikacija, uključujući SQLite, WebKit, OpenGL, i Media Manager.
- **Run Time** - koristi se za izvršavanje i dominantnih Android aplikacija, uključujući Dalvik virtualni mašine kao i osnovne biblioteke za pružanje specifične Android funkcionalnosti. Run Time je osmišljen kako bi se ostvarila efikasnost u radu memorije pri upotrebi mobilnih uređaja.
- **Dalvik virtual machine** - vrši optimizaciju softvera za mobilne uređaje
- **Application framework** - vrši prezentaciju usluga aplikativnom sloju, omogućava ponovnu upotrebu i zamjenu komponenti uključujući Window Manager, Content Providers, Location Manager, telefoniranje i peer-to-peer servise.

Jedan od uslova za uspješno implementirano rješenje bezbjednog modela predstavlja i njegova jednostavnost upotrebe. Osnovni zadatak dobro projektovanog rješenja je da krajnji korisnici u radu što manje osjećaju prisustvo kriptografskog sistema. To podrazumijeva jednostavnost posla koji obavljaju, statičnost postojećih funkcija i minimum vremenskog perioda potrebnog za obavljanje konkretnog poslovnog zadatka. Model implementacije bezbjedonosnog rješenja komunikacionog kanala obezbeđuje odličan metod za zaštitu osjetljivih podataka koji se prenose od predajne do prijemne strane. Usložnjavanjem modela dovodi se do pada nivoa performansi kao i otežavanjem konkretne upotrebe predloženog sigurnosnog rješenja.

Osnovni Android proces model u sebi nema intergisane kriptografske mehanizme. Bezbjednost ovog modela zavisi od mogućnosti implementacije sopstvenog rješenja na bazi već provjerenih i dostupnih kriptografskih algoritama. Kao sveobuhvatna i dostupna razvojna platforma Android pruža programerima niz mogućnosti na osnovu kojih mogu nadograditi svoj bezbednosni mehanizam upotrebom DES, 3DES, AES ili nekog drugog kriptografskog rješenja.

3. MODEL BEZBJEDNOSNOG RJEŠENJA U KOMUNIKACIJI

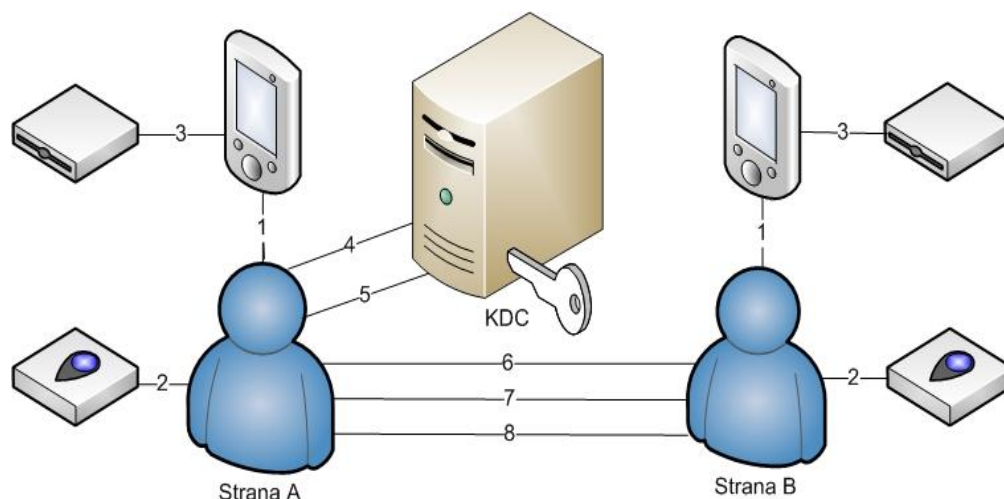
Na osnovu analize Android arhitrkture može se zaključiti da pomenuti model predstavlja standardni scenario kada je u pitanju prijem podataka u mobilni uređaj. Model koji je analiziran u ovom radu odnosi se na zaštitu govornog kanala koji se uspostavlja između dva ili više korisnika.

Ovaj scenario je ograničen samo na simetrični kriptografski sistem [7]. Jedna od karakteristika ovog modela je sigurnosna nadogradnja prilikom procesa prijavljivanja korisnika na uređaj, kao i način distribucije ključeva. Komunikacioni kanal se sastoji od prijemne strane A, predajne strane B kao i od **KDC-a (Key Distribution Center)**. Sve strane u komunikaciji posjeduju isti komunikacioni element koji je, u ovom slučaju, externi memorijski disk. Ovaj komunikacioni element strana A i strana B koriste radi ostvarenja komunikacije sa KDC-om. Prilikom odabira zaštićenog načina komuniciranja, korisnik umjesto sigurnosne lozinke i korisničkog imena treba da ostavi određeni biometrijski dokaz. To može biti otisak prsta, skenirana zjenica oka ili govorna komanda. Umjesto ove biometrijske kontrole moguće je koristiti neki drugi akreditiv kao što je smart kartica ili slično. Svaki učesnik u razgovoru koristi isti spoljašnji nosač podataka na kom je smješten **GNK (Generisani Niz Ključeva)**. Za svaku započetu iteraciju koristi se jedan ključ koji se nakon završene komunikacije odbacuje na određeni način. Odbacivanje se može vršiti fizičkim brisanjem tog ključa ili uvođenjem indeksa upotrebe za svaki pojedinačni ključ. Sledeći redni ključ za šifrovanje je sledeći ključ koji je na redu u nizu ključeva. Pošto je

jednom upotrebljen ključ za šifrovanje odbačen, na osnovu izvještaja **IUK** (Index Upotrebljenih Ključeva) sigurnosni servis se pozicionira na sledeći ključ. U slučaju totalne ili djelimične upotrebljenosti ukupnog broja ključeva, svaki korisnik ponovo dobija novu spoljašnju memorijsku jedinicu sa novim GNK. Ukoliko se komunikacija proširi na više novih korisnika koji posjeduju validnu externu memorijsku jedinicu, generator IUK može se resetovati na određenu vrijednost koja je zajednička za sve korisnike u komunikaciji. Vrijednost na osnovu koje se resetuje generator ključeva ne smije se ponoviti. U slučaju gubitka externe memorijske jedinice od strane jednog korisnika, potrebno je sve jedinice koje sadrže GNK u potpunosti zamijeniti drugim jedinicama. Ako se biometrijski podaci na osnovu kojih se vrši akreditovanje korisnika nalaze na ovoj memorijskoj jedinici i sa njih se vrši akreditovanje korisnika, u slučaju gubitka ili oštećenja iste, nije potrebno vršiti zamjenu ostalih jedinica. Razlog tome je što se neovlašćeni korisnik na osnovu svojih biometrijski parametara ne može validno predstaviti sistemu i samim tim nije u mogućnosti da ispravno koristi mobilni uređaj [8,9].

Protokol komuniciranja kroz šifrovani kanal bio bi sledeći:

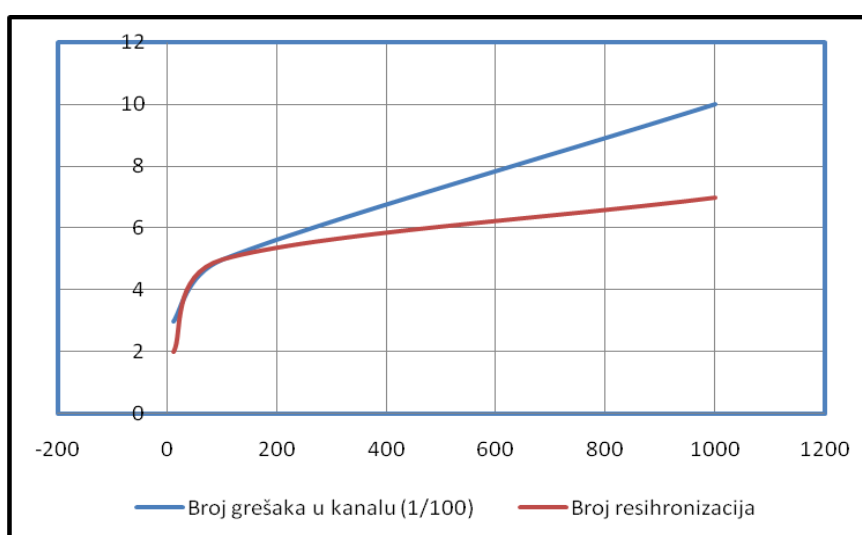
1. Korisnik šalje zahtjev za upotrebu EM (Externa Memorija).
2. Na osnovu svojih biometrijskih parametara korisnik se prijavljuje u sistem.
3. Ukoliko je biometrijski dokaz validan, uspostavlja se interni komunikacioni kanal između EM i telefona korisnika. Spoljašnja memorija je fizički povezana na mobilni uređaj tako da je smanjena mogućnost presretanja i modifikovanja podatka.
4. Da bi se komunikacioni kanal sinhronizovao potrebno je da sigurnosni servis korisnika A dobije određenu vrijednost na osnovu IUK-a, koji zajedno sa svojim identifikatorom šalje prema KDC. Podaci koji se šalju prema KDC-u su šifrovani zajedničkim ključem od korisnika A i KDC a koji se nalazi na EM.
5. Na osnovu podataka od strane A, KDC odgovara tako što šalje podatke prema strani A, a to su jednokratni ključ K_s i identifikatori za IDa i IDb koji je šifrovan njihovim zajedničkim ključem K_a , kao i podatke koje će A strana proslijediti prema B strani.
6. Strana A prosljeđuje podatke prema strani B, a to su K_s i identifikator od IDb koji je šifrovani ključem B strane.
7. Sada i A i B strane posjeduju sesijski ključ K_s , a strana B zna da je strana A inicirala komunikaciju.
8. Strana B počinje da šalje šifrovani identifikator Nb koji je šifrovan sesijskim ključem od strane K_s i čeka odgovor od strane A. Kada dobije odgovor od strane A, a to je fNa koji je šifrovan sesijskim ključem od K_s , strana B je obezbjeđena od mogućnosti modifikovanja poruke u narednom koraku. Vrijeme potrebno za sinhronizovanje komunikacionih strana zavisi do kvaliteta komunikacionog kanala.



Slika br.1. Model distribucije ključeva u Android operativnom sistemu

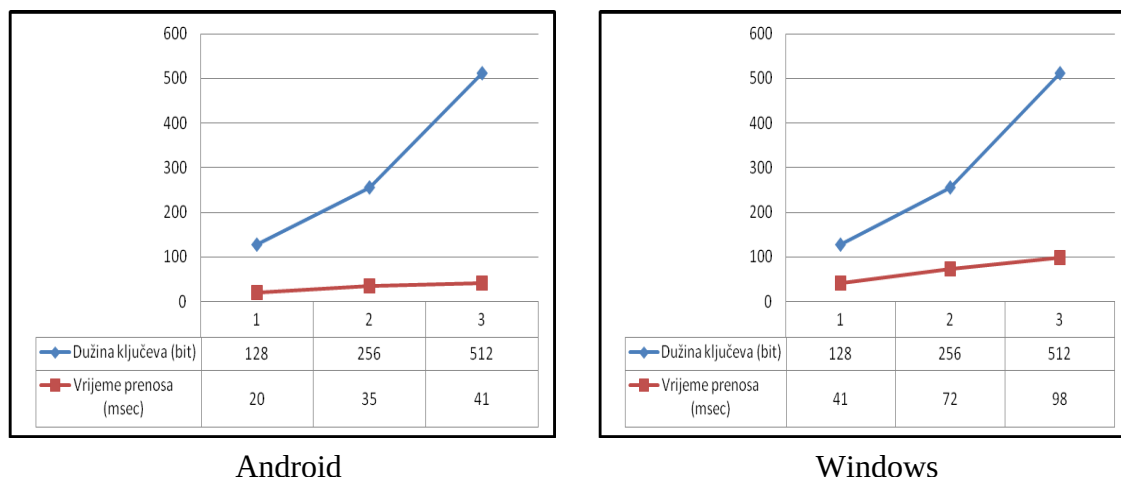
Tokom komunikacije između dvije strane poželjno je da se sesijski ključevi ne upotrebljavaju dugo i da se generišu novi na osnovu vrijednosti iz EM. Moguće je uspostaviti hijerarhiju KDC-ova pa korisnici iz različitih grupa mogu da komuniciraju tj. razmijene sesijske ključeve. Di bi to bilo moguće KDC-ovi između sebe na prethodno opisan način ostvaruju komunikaciju i razmjenjuju sesijske ključeve. Za veće mreže, umjesto jednog centra moguće je koristiti više distributivnih centara u hijerarhiji tako da svaki opslužuje manje domene ili mreže. Predložena metoda je centralizovanog karaktera.

Na osnovu brzine prenosa podataka u komunikacionom kanalu, broja grešaka i broja resihronizacija izvršena je analiza karakteristike komunikacionog kanala. Analizirane su različite vrijednosti brzine prenosa podataka na osnovu kojih je napravljen dijagram. Povećanjem brzine prenosa dolazi do broja grešaka koje se javljau prilikom prenosa podataka. Takođe, povećanjem brzine prenosa povećava se i broj resihronizacija između strana u komunikaciji. U analizi nije posmatrano dozvoljeno kašnjenje za kriptološku sinhronizaciju.



Dijagram br. 1. Analiza karakteristika komunikacionog kanala

Na kompleksnost algoritma koji se koristi u kriptološkoj sinhronizaciji utiče dužina ključa, period važenja ključeva kao i broj ključeva koji se koristi. Analizom je utvrđeno da je za prenos podataka u Android operativnom sistemu potrebno kraće vrijeme u odnosu na Windows operativni sistem. Test je rađen sa tri ključa različite dužine a otvoreni tekst je bio veličine 100 KB. Rezultati testa su prikazani u narednim dijagramima.



Dijagram br.2. Kompleksnost algoritma

4. ZAKLJUČAK

Bezbjednosno rješenje može se posmatrati kao komunikacioni sistem, gdje se informacija koja je generisana na predajnoj strani dostavlja željenom odredištu, odnosno, prijemnoj strani poruke. Poruka se šalje kroz otvoreni prostor i izložena je mogućim napadima koji se odnose na presretanje i modifikaciju podatka. Ključni element predstavlja način distribucije kriptoloških ključeva između strana u komunikaciji. Zadatak ovako formiranog sigurnosnog modela jeste poštovanje osnovnih principa bezbjednosti. Upotrebom vlastitog kriptografskog rješenja dobijamo potpuno nov, vlastiti proizvod, sa vlastitim rješenjem. Android platforma programerima pruža mogućnost izrade novog sigurnosnog servisa koji će u potpunosti biti prilagođen za potrebe određenih institucija čije se poslovanje bazira na tajnom prenosu podataka. Realno je očekivati da ćemo u narednih nekoliko godina imati kriptološke sisteme koji čine pouzdan i siguran sistem za prenos podataka, na bazi domaćeg rješenja.

LITERATURA

- [1] Android A Programmers Guide, J.F. DiMarzio, *Mc Graw Hill*, 2008.
- [2] Android Application Development, Rick Rogers, John Lombardo, Zigurd Mednieks, and Blake Meike, *O'Reilly*, 2009.
- [3] Android Essentials, Chris Haseman, *Apress*, 2008.
- [4] Applied Cryptography, Bruce Schneuer, 2en Edition, *WileyPublishing*, 2007.
- [5] Professional Android Application Development, *Reto Meier, WROX*, 2008.
- [6] Thoughts on Google Android, B. Smith, *Spectrum Data Technologies*, 2008.

- [7] Osnovi bezbednosti i zaštite informacionih sistema Milan Milosavljević i Gojko Grubor, *Univerzitet Singidunum*, 2006.
- [8] Modeli sigurnosnog rješenja za mobilne uređaje zasnovanih na Android operativnom sistemu, Miroslav Ćajić i Bogdan Brkić, *Telfor* 2009.
- [9] Metodi i napadi na distribuciju simetričnih i asimetričnih kriptoloških, Bogdan Brkić i Miroslav Ćajić, *Telfor* 2009.
- [10] [http:// android.git.kernel.org](http://android.git.kernel.org)
- [11] <http://android-developers.blogspot.com>
- [12] <http://code.google.com>
- [13] <http://developer.android.com>
- [14] <http://source.android.com>