DISTRIBUCIJA KRIPTOLOŠKIH KLJUČEVA U MOBILNIM UREĐAJIMA POD ANDROID OPERATIVNIM SISTEMOM
CRYPTOLOGY KEYS DISTRIBUTION IN MOBILE DEVICES UNDER ANDROID OPERATION SYSTEM

Miroslav Ćajić, MikroByte doo, Vese Rackovića 16, 73220 Rogatica
Mladen Veinović, Univerzitet Singidunum, Bulevar Zorana Đinđića 44, Novi Beograd
Bogdan Brkić, Ministarstvo finansija Republike Srpske, Trg Republike Srpske I, 78000 Banja Luka

Sadržaj — U ovom radu razmatran je način razmjene tajnih simetričnih ključeva između mobilnih uređaja koji rade pod Android operativnim sistemom. Tajni ključevi su suštinski element zaštićenih komunikacijakoje se zasnivaju na simetričnim kriptografskim algoritmima. U radu je analizirano standardno sigurnosno rješenje za distribuciju ključeva, diskutovane su slabosti ovakvog rješenja i predložena je njihova modifikacija u cilju povećanja povjerljivostu u cjelokupan bezbjedonosni sistem. Predloženo rješenje je opisano na nivou protokola. Za analizu je odabrana Android platforma zbog toga što je otvorena za dogradnju i realizaciju sopstvenih rješenja.

Ključne riječi — distribucija kriptoloških ključeva, android operativni sistem, simetrični algoritam

Abstract — In this paper, the way of exchanging of secret symmetric keys between mobile devices that operate under the Android operating system has been discused. Secret keys are an essential element of protected communications that are based on symmetric cryptographic algorithms. The paper analyzed the standard security solution for the distribution of keys, such weaknesses are discussed and solutions proposed modification to increase the confidentiality of the entire security system. The proposed solution is described at the level of protocol. For the analysis was selected Android platform because it is open for extension and implementation of their own solutions.

Key words — cryptographic key distribution, android operating system, symetric cipher

1. UVOD

Operativni sitem predstavlja ključnu vezu između korisničkih aplikacija i hardvera uređaja na kom se izvršava. Osobine dobro projektovanog operativnog sistema ogledaju se u prilagođenosti korisniku i korisničkom interfejsu, korisničkim aplikacijama, kao i dostupnosti korisničkim podacima. Prilagođenost operativnog sistema za korisnike mobilnih uređaja u velikoj mjeri doprinijela je poboljšanju njihovih funkcionalnosti. Potreba za usavršavanjem upravljivosti mobilnih telefona dovela je do toga da su proizvođači primjenjuju sasvim novu, sveobuhvatnu i programski otvorenu platformu koja će velikom broju korisnika pružiti ugodan i efikasan rad.

U ovom radu analizira se zaštićeni prenos podataka za mobilne telefone čiji se rad zasniva na Android arhitekturi. Android je upravljčki 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]. Arhitektura Android platforme definiše njenu funkcionalnost i ulogu. U početku je razvijana samostalno od strane Google-a, da bi se poslije pridružila u **OHA** (**O**pen **H**andset **A**lliance). 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
- Hardverski referentni sloj
- Open Source biblioteke
- Run Time
- Dalvik virtual machine
- Application framework

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 (*sourc*e) 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.

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.

2. DISTRIBUCIJA I UPRAVLJANE KRIPTOLOŠKIM KLJUČEVIMA

Upravljanje kriptološkim ključevima podrazumjeva sigurnosno generisanje, distribucija i čuvanje ključeva. Sigurnosna metoda upravljanja ključevima je od ekstremnog značaja za cjelokupan bezbjedonosni sistem. Jednom generisan kriptološki ključ mora ostati tajan, odnosno, mora se izbjeći situacija kao što je impersonalizacija. U kriptološkoj infrastrukturi, veliki broj napada se dešava na nivou upravljanja ključevima, dok se napadi na same algoritme dešavaju vrlo rijetko. Učesnici u kriptografskim sistemima moraju biti sposobni da generišu ključeve, odnosno, moraju biti dostupni korisnicima u komunikaciji. U slučaju da dođe do kompromitacije ili gubitka ključa on strane X, ostali učesnici u komunikaciji moraju biti blagovremeno upozoreni. U suprotnom, napadač će ukradenim ključem moći dešifrovati sve poruke koje su šifrovane tim. Takođe, korisnicima mora biti omogućeno da na siguran način čuvaju svoje ključeve i učine ih nedostupnim osim za legitimnu upotrebu.

Pošto ključevi imaju ograničen životni vijek, najvažniji razlog za nihovo periodično mijenjanje je zaštita od kriptoanalize. Svaki put kada se ključ upotrijebi generiše se šifrat određene dužine i veličine. Skupljanjem ovakvih šifrata napadač prikuplja podatke neophodne za kriptoanalizu. Iz tog razloga, ključevi trebaju da imaju ograničen životni vijek. Ukoliko vlasnik ključa posumnja da je napadač dobavio ključ treba da razmotri prestanak korištenja kompromitovanog ključa i generiše novi ključa tj. par ključeva. Istraživanja u kriptoanalizi dovode do otkrivanja potencijalnih slabosti i napada, pa se svakih nekoliko godina povećava preporučena minimalna dužina ključeva za pojedine algoritme. Npr. za RSA algoritam trenutno se preporučuje minimalna dužina ključa od 512 bita. Ovo se odnosi na privremene ključeve čiji je vremenski indeks upotrebe jedan ili nekoliko dana. Preporučena dužina ključeva za dužu upotrebu je minimalno 1024 bita. Napomenimo da, ključeve možemo podijeliti na: simetrične, javne i privatne ključeve, a samo su simetrični i privatni ključevi su po svojoj prirodi tajni ključevi.

Za dešifrovanje poruke strana B mora posjedovati validnu kopiju alata koji je strana A koristila za šifrovanje, ali i ključ kojim je poruka šifrovana. Problem distribucije ključeva je prisutan kroz cijelu istoriju kriptografije. Bez obzira koliko je u teoriji kriptografski algoritam siguran, povjerljivost njegovog mehanizma može ugroziti problem distribucije ključa. Pitanje distribucije ključa može se činiti trivijalnim, ali on je za pouzdan kriptografski sistem najslabija karika. Ako dvije osobe žele razmjenjivati podatke u bezbjednosnom okruženju, moraju se pouzdati u treću, osobu C, koja će im dostaviti ključ, koji u ovom slučaju postaje slabija karika u lancu bezbjednosti u odnosu na ove dvije. Iako postoje tvrdnje da je problem distribucije kriptoloških ključeva nerješiv problem, sredinom sedamdesetih godina prošlog vijeka otkriveno je pouzdano rješenje. Pošto je računarska tehnologija preobrazila primjenu kriptografskih algoritama, ipak je najveću revoluciju u kriptografiji dvadesetog vijeka izazvao razvoj tehnika za svladavanje problema distribucije ključeva. To se otkriće smatra najvećim kriptografskim ostvarenjem još od izuma monoalfabetske metode [7] kriptovanja (jedne od najranijih metoda kriptovanja poruka) prije dvije hiljade godina.

3. MODEL BEZBJEDNOSNOG RJEŠENJA U KOMUNIKACIJI

Za uspješno funkcionisanje simetričnog šifrovanja s jedne i dešifrovanja sa druge strane, osnovni preduslov je da strane u komunikaciji moraju posjedovati isti ključ. Samim tim, ovdje se javlja problem distribucije ključeva između strana u komunikaciji. Da bi tajnost komunikacije između svaka dva korisnika u grupi od N korisnika bila zagarantovana, svaki učesnik mora da posjeduje N-1 ključ za komunikaciju sa ostalim korisnicima. To nas dovodi do ukupno N(N-1)/2 ključeva. Za grupu od npr. 1000 korisnika potrebno je približno 500000 ključeva, a svaki korisnik bi morao da posjeduje 999 ključeva. Ovakav sistem bi bio vrlo nepraktičan i težak za održavanje. Na osnovu analize

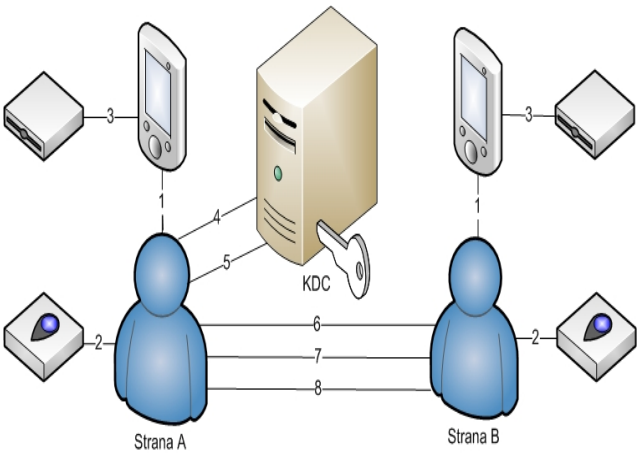
Android arhitrkture može se zaključiti da pomenuti model predstavlja standardni scenario kada je u pitanju prijem podataka u mobilni uređaj. Model koji je analiziran u ovom radu odnosi se na zaštitu govornog kanala koji se uspostavlja između dva ili više korisnika.

Ovaj scenario je ograničen samo na simetrični kriptografski sistem [8]. 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, predajene strane B kao i od **KDC**-a (**K**ey **D**istribution **C**enter). 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** (**G**enerisani **N**iz **K**ljučeva). 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** (**I**ndex **U**potrebljenih **K**ljučeva) 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 sihronizovao 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 Ks i identifikatori za IDa i IDb koji je šifrovan njihovim zajedničkim ključem Ka, kao i podatke koje će A strana proslijediti prema B strani.
6. Strana A prosljeđuje podatke prema strani B, a to su Ks i identifikator od IDb koji je šifrovani ključem B strane.
7. Sada i A i B strane posjeduju sesijski ključ Ks, 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 Ks i čeka odgovor od strane A. Kada dobije odgovor od strane A, a to je fNa koji je šifrovan sesijskim ključem od Ks, stana B je obezbjeđena od mogućnosti modifikovanja poruke u narednom koraku. Vrijeme potrebno za sihronizovanje komunikacionih strana zavisi do kvaliteta komunikacionog kanala.



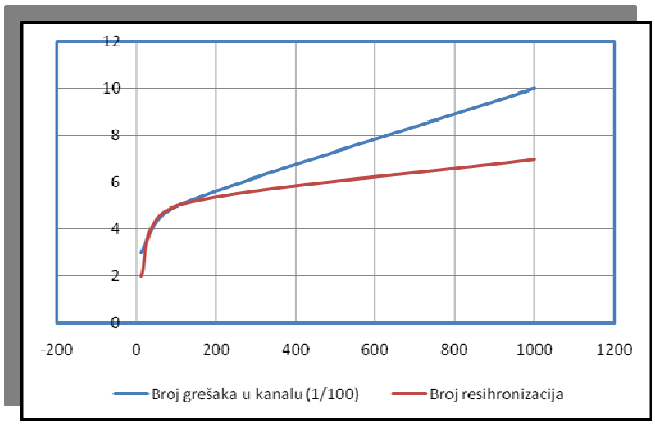
Slika br.1. Model distribucije ključeva u Android operativnom sistemu

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.

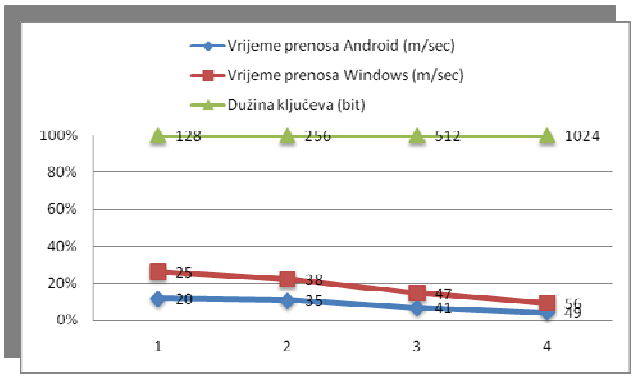
Na osnovu brzine prenosa podataka u komunikacionom kanalu, broja grešaka i broja resihronizacija izvrešna je analiza karakteristike komunikacionog kanala. Analizirane su različite vrijednosti brzine prenosa podataka na osnovu kojih je napravljen dijagram.

Povećenjem 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 sihronizaciji 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. Uticaj kompleksnost algoritma na Android i Windows operativni sistem.

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] S.Singh, TheC ode Book, Doubleday of New York, 1999.

[8] Osnovi bezbednosti i zaštite informacionih sistema Milan Milosavljević i Gojko Grubor, *Univerzitet Singidunum*, 2006.

[9] Modeli sigurnosnog rješenja za mobilne uređaje zasnovanih na Android operativnom sistemu, Miroslav Ćajić i Bogdan Brkić, *Telfor 2009.*

[10] Metodi i napadi na distribuciju simetričnih i asimetričnih kriptoloških, Bogdan Brkić i Miroslav Ćajić, *Telfor 2009.*

[11] Kriptografska zaštita podataka za Android arhitekturu,Mladen Veinović, Miroslav Ćajić i Bogdan Brkić, *Sinergija 2010, prihvaćeno za objavu.*

[12] http:// android.git.kernel.org

[13] http://android-developers.blogspot.com

[14] http://code.google.com

[15] http://developer.android.com

[16] http://source.android.com