PRIKAZ NOVIH ELEMENATA SIGURNOSTI U MOBILNIM SISTEMIMA

Milan Janković [1], Borislav Odadžić [2]
[1]Republička agencija za elektronske komunikacije RATEL Beograd,
[2]Tehnički fakultet „Mihajlo Pupin“ Zrenjanin

Sadržaj: *Tema ovoga radu usmerena je u pravcu pronalaženja rešenja za sigurnost transporta, servisa, mrežnog pristupa, privatnosti korisnika i naplate u bežičnom okruženju. Konvergentne mreže i mobilnost povećavaju nove izazove u odnosu na postojeće sisteme za autentifikaciju, autorizaciju i naplatu (AAA). U radu je dat prikaz postojećeg stanja autentifikacije za mobilne sisteme i sugerisana su njegova poboljšanja polazeći od sigurnosti i privatnosti integrisanih rešenja za korisnike. Uloga inteligentnih kartica i sigurnosnih paketa tokena takođe je prikazana kao i siguran i prilagođen sistem prenosa. Korišćenjem enkripcije na sloju voda podataka, uvođenjem inteligentnih kartica i sigurnih metoda za prenos ključeva može se znatno povećati sigurnost sistema i zaštita privatnosti.*

Ključne reči: *Autentifikacija, autorizacija i naplata (AAA*), *Udaljeni dial in servis za autentifikaciju (RADIUS), Konvergentne mreže, Upravljanje digitalnim pravima (DRM), Infrastruktura javnih ključeva (PKI), Rivest-Shamir-Adleman (RSA) algoritam, Modul za identifikaciju korisnika (SIM), Inteligentna kartica*

1. Uvod

Sve razvijenija i rasprostranjenija primena ICT tehnologija baziranih na kompjuterskom okruženju donosi nove izazove u odnosu na realizaciju telekomunikacionih servisa. Danas je konvergencija mreža sa korisničkim pristupom postala stvarnost, što znači da će se jedna mreža koristiti za isporuku različitih servisa: na primer za telefoniju, emitovanje i prijem TV programa, pristup Internetu itd. Fiksno mobilne konvergentne mreže sastavljene od mobilnih GSM/UMTS, bežičnih IEEE 802.11, IEEE 802.16, IEEE 802.20 i žičnih ili optičkih kablovskih ili xDSL mreža ukidaju granicu između telekomunikacionih, radiodifuznih i kompjuterskih mreža.

Zajednički servisi omogućavaju roming tako da se putem terminala može pristupiti servisima nezavisno od trenutno upotrebljavane mrežne tehnologije. Učesnici na tržištu transformišu se u operatore bežičnih servisa preko pristupnih mreža, telekomunikacioni operatori omogućavaju prenos podataka sa komutacijom paketa i

mobilne servise preko fiksne mreže, dok internet servisni operatori realizuju prenos govora koristeći IP protokol (VoIP) i video na zahtev (VoD) preko mobilnih mreža.

U bežičnom svetu se javljaju nove tehnologije, a naročito IEEE 802.11 porodica standarda drastično menja način na koji se korisnici prijavljuju na mreže. Najosnovniji zahtev za nove uređaje je sposobnost podrške bežičnog servisnog pristupa. Mobilni svet je predstavio mobilne sisteme 2^{+}G (GPRS), treće i četvrte generacije 3G/4G, koji omogućavaju stalnu IP povezanost i zajedno sa Wi-Fi pristupom daju stalnu bežičnu vezu. Pored komunikacionih uređaja kao što su laptopovi, telefoni danas i autobomili, kancelarijski aparati i kućni uređaji dolaze sa opremom za bežično povezivanje.

Zaštita korisničkih podataka je od ključnog značaja za sve komunikacije, a naročito za bežične, gde su napadi na privatnost mnogo jednostavniji. Sa jednostavnom bežičnom LAN (WLAN) karticom i odgovarajućim softverom moguće je uhvatiti, analizirati i potencijalno dešifrovati sadržaj bežičnog saobraćaja. Implementacija prvog WLAN enkripcijskog standarda (WEP). za zaštitu koji je trebao biti ekvivalentan elementima sigurnosti u fiksnoj mreži imala je ozbiljne nedostatke

Standardizacija globalnog sistema za mobilne komunikacije (GSM) uvela je A5 kriptografske algoritme, koji se danas mogu krekovati u realnom vremenu (A5/2) ili gotovo realnom vremenu (A5/1). Dalja bezbednosna pretnja je nedostatak međusobne autentifikacije između terminala i mreže. Samo se terminal autentifikuje a korisnik mora bezuslovno verovati mreži.

U mobilnom telekomunikacionom sistemu treće generacije (UMTS), primenjuje se snažna enkripcija u delu radio prenosa koja daje adekvatnu zaštitu dok se ne osigurava odgovarajuća zaštita pri prenosu preko jezgra mreže.

2. Prikaz postojećeg stanja metoda zaštite

Danas se na postojećim mrežama primenjuje AAA (Authentification, Authorisation, and Accounting) metod koji se je razvijen za pojedinačni tip mreže. Njegov razvoj doveo je do postojanja dva različita sistema, jednog za telekomunikacione i drugog za kompjuterske mreže. Oni definišu primenu AAA u globalnim sistemima za mobilne komunikacije GSM i UMTS a u domenu kompjuterskih mreža na osnovu RFC standarda organizacije IETF.

Kompjuterske mreže omogućavaju jedinstven AAA pristup, a aktuelna istraživanja su fokusirana na proširenje postojećih metoda koji bi trebalo da budu primenljive i za telekomunikacione servise. Predložena su proširenja protokola RADIUS (Remote Authentication Dial In User Service) i Diametar.

RADIUS je trenutni *de facto* standard za autentifikaciju korisnika na daljinu koji koristi UDP (User Datagram Protocol) kao transportni protokol. Autentifikacioni zahtevi su zaštićeni zajedničkim tajnim podacima između servera i klijenta, a klijent koristi *Hash* vrednosti koje su proračunate iz ove tajne vrednosti. Zahtevi se šalju u običnom tekstu osim u slučaju ako se radi o lozinki korisnika.

Protokol Diametar omogućava nadogradnju u odnosu na RADIUS pojačavajući bezbednost kroz kontrolisan prenos paketa uz pomoć transportnog protokola TCP (Transmission Control Protocol) i enkripcije transportnog sloja radi umanjenje posredničkih napada.

Oba metoda imaju različitu pozadinu, kod kompjuterske mreže cilj je osoba koja koristi kompjuter u fiksnoj mreži, dok kod mobilnih sistema usmerenje je na lični uređaj

u mobilnoj mreži. Prema tome, izazov za telekomunikacione operatore je da se unapredi i pojednostavi autentifikacija mreže u pravcu korisničke autentifikacije za pristup servisima. Većina telekomunikacionih kompanija su i operatori Internet servisa pa bi ovo predstavljalo prirodnu unifikaciju njihovih AAA sistema. Stim u vezi korišćen je generički pristup pri razvoju ekstenzionog protokola autentifikacije EAP (Extensible Authentication Protocol) Ova familija protokola ima potencijal da postane buduća zajednička platforma za autentifikaciju korisnika preko konvergentnih mreža. EAP je univerzalni autentifikacioni okvir koji je standardizovan od strane IETF, i koji uključuje sporazum o autentifikaciji i ključevima AKA (Authentication and Key Agreement) i modul pretplatničkog identiteta SIM (Subsciber Identity Module). EAP i AKA je standardni autentifikacioni metod za UMTS mreže.

Pored osnovnih razlika između komunikacionih i kompjuterskih mreža, mobilnost je ključno pitanje za oboje. Mrežnim servisima ne samo da bi trebalo da se pristupa preko mobilnih terminala, već bi trebalo da budu adaptirani na kvalitet usluge (QoS) koji se traži za mobilne/bežične sisteme. Unapređenja AAA metoda su od osnovnog značaja za mobilnost, jer treba da obezbede brz prenos, pouzdane i sigurne komunikacije na osnovu zaštite privatnosti i lakog korišćenja.

3. Autentifikacija pretplatnika u postojećim mrežama

U GSM mrežama, integrisani AAA se koristi za bilo koji tip korisničkog saobraćaja. Autentifikacija je samo jedan način da se korisnik potvrdi na mreži. Preciznije, korisnik se potvrđuje kroz PIN kod u odnosu na SIM karticu u mobilnom telefonu, zatim se uređaj potvrđuje na mreži.

U UMTS, autentifikacija uređaja je dvosmerna. Uređaj može proveriti autentičnost mreže uz pomoć ključeva koji se nalaze na SIM kartici. Integracija mobilne autentifikacije sa različitim spoljašnjim servisima nije do danas naročito raširena.

Telekomunikacione kompanije koriste svoje interne servise, koji mogu potvrditi pretplatnika na osnovu podataka koji dolaze iz mreže. Akreditacija može biti CallerID, privremeni međunarodni identitet mobilnog pretplatnika TIMSI (Temporary International Mobile Subcriber Identity) ili neki drugi podaci koji su transformisani *Hash* funkcijom.

Kontrola pristupa i autorizacija je više zadatak interne mreže. Bez značajnih proširenja, sadašnje mobilne mreže su više ostrva nego povezane mreže u oblasti AAA. Proizvođači opreme sada preporučuju različite IP multimedijalne podsisteme (IMS) za mobilne operatore da bi se omogućila integracija i servisi trećih strana (Third Party) u smislu konvergencije i da bi se omogućio prenos i isporuka multimedijalnih sadržaja preko sadašnjih mreža.

AAA protokoli koji su primenjeni u kompjuterskim mrežama bi trebalo da omoguće servis potvrđenim korisnicima. Trenutni pojedinačni protokoli upisa SSO (Single Sign On), kao što su RADIUS, Diametar ili Kerberos daju identitet korisnika trećim licima. SSO može koristiti digitalne sertifikate, infrastrukturu javnih ključeva (PKI) i ostale snažne metode enkripcije. Ali, nijedna od ovih rešenja nije u stanju da ponudi kompletno rešenje kao integrisani AAA na mobilnim mrežama. Kompjuterskim mrežnim protokolima nedostaje podrška za brzu mobilnost i pokretne klijente.

Sa uključivanjem jednostavne autentifikacije korisnika u mrežnim internim servisima u svetu telekomunikacija i SSO rešenjima koja omogućavaju različiti protokoli kompjuterskih mreža, jedinstveni AAA sistem treba da bude prihvatljiv za korisnike i da

poveća nivo bezbednosti servisa. U takvom sistemu, od ključnog značaja je bezbedno pohranjivanje ključeva i rukovanje otporno na zlonamernu manipulaciju. Smart kartice za skladištenje ključeva i njihovo generisanje ispunjavaju bezbednosne zahteve, ali je distribucija i upotreba smart kartica donekle komplikovana. Pošto većina korisnika poseduje mobilni telefon, SIM kartica je kandidat da postane primarna smart kartica koja se koristi za AAA.[2]

4. Zaštita u kovergentnim mrežama

Konvergentna mreža prenosi nekoliko tipova saobraćaja i omogućava jednostavnu razmenu informacija između različitih terminala, bez obzira na transportni medijum. Da bi se omogućio konvergentni AAA, istraživanja se kreću u različitim pravcima: stvaranje mogućnosti međusobnog spajanje bežičnih LAN (WLAN) i mobilnih mreža, unapređenje mrežne mobilnosti u bežičnim kompjuterskim mrežama, i smanjenje potreba za resursima u kriptografiji.

Mrežna konvergencija je najznačajnija u bežičnoj sredini, posto se pred njom nalazi niz različitih izmerenih vrednosti QoS na radio interfejsu, kao što su na primer, kašnjenje usled propagacije, varijacije kašnjenja signala, stepen greške bita BER, greške slobodnih sekundi, distrorzija, odnos signal/šum, trajanje prekida, verovatnoća prekida, vreme između prekida, protok i propusnost (throughput). Ovi parametri zavise od okruženja u kome se nalaze korisnik i terminal. U Tabeli 1 date su osnovne karakteristike ovih mreža. [4]

Pojačana potreba za sigurnošću je unapredila bezbednost bežičnih veza, što je dovelo do Wi-Fi zaštićenog pristupa WPA (WiFi Protected Access) i WPA2 kao i do implementacije IEEE 802.11i standarda. Ovaj standard ima za cilj inkorporaciju protokola EAP porodice, naročito što se tiče bezbednosti transportnog sloja TLS (Transport Layer Security) i SIM.

Tabela 1. *Poređenje mobilnih ćelijskih i WLAN mreža*

	Mobilna ćelijska mreža	WLAN bežična mreža
Pokrivenost	Teritorija države	Lokalno
Bezbednost	Na viskom nivou	Zavisi od podešavanja
Brzina prenosa	Niska	Visoka
Investicioni troškovi	Visoki	Niski
Trošak licence	Visok	Nema, nelicencirani opseg
Instaliranje	Teško	Lako
Podrška mobilnosti	Visoka	Slaba

Veliki broj celularnih operatora danas pruža mogućnost korišćenja WLAN servisa uz primenu univerzalnog metoda pristupa UAM (Universal Access Method) za autentifikaciju. UAM koristi metod autentifikacije na trećem sloju, tipični Web pretraživač, koji identifikuje klijente za pristup WLAN-u. Međutim sada rastu problemi višestrukih autentifikacija, koji su inače postojali i u GSM mrežama. Međutim proširenjem EAP-SIM metode na ovaj slučaj moguće je ostvariti autentifikaciju na zasnovanu na SIM kartici za uređaje koji poseduju SIM.

Drugi izazov predstavlja roming između operatora pristupa. Pošto se podaci između pristupnih tačaka prenose preko IP jezgra mreže, prirodno je koristiti mrežno zasnovane protokole kao što je RADIUS. U konvergentnim mrežama, gde korisnici mogu prelaziti između mobilnih mreža i WLAN- servisa, uobičajeni AAA sistem mora biti operativan da bi se osigurala ispravna operacija. Neki autori predlažu jedinstvenu šemu naplate (billing)), koja sugeriše upotrebu 802.1x na WLAN strani. WLAN konekcija mobilnih mreža je sugerisana kroz RADIUS server koji se koristi i za kontrolu pristupa u 802.1x.

Upotreba IEEE 802.1x standarda omogućava jednostavnu autentifikaciju, pošto su prethodno pokazani sertifikati i dogovori o ključevima na mobilnoj mreži, gde je korisnik već potvrđen. Sa upotrebom digitalnih sertifikata, sistem se približava željenom izgledu, gde se korisnik i operator servisa međusobno identifikuju. Pošto ovi sistemi identifikuju korisnika u odnosu na nekoliko servisa, privatnost je od primarne važnosti. Danas postoji moguće rešenje, [5] koje poseduje sigurnosnu šemu autentifikacije uz očuvanje privatnosti korisnika.

U cilju održavanja razumanog nivoa privatnosti, sistem bi trebalo da se bavi pitanjima privatnosti lokacije, anonimnosti konekcije i poverljivosti. Ove preporuke su zasnovan na slepim potpisima i *Hash* lancima. Upotreba *Hash*-a se preporučuje, pošto dobra *Hash* funkcija omogućava dobru osnovu za anonimni pristup a potrebe u odnosu na resurse su nisu previsoke za sadašnje mobilne uređaje, što se ponekad može desiti kod primene slepih potpisa RSA (Rivest-Shamir-Adleman) šeme. U određenim sredinama, GSM integrisane funkcije se takođe mogu koristiti.

Korisnik zadržava punu kontrolu nad akreditacijom autentifikacije prilikom sastavljanja i stvaranja posebnog paketa *tokena* autentifikacije. Početni pristup servisu se može postići prikazivanjem jedanog od ovih *tokena* nakon međusobne identifikacije između operatora servisa i korisnika. Na osnovu ovih *tokena*, nikakvi korisnički podaci se ne mogu pretraživati niti pratiti. Ukoliko uspe svaki od inicijalnih koraka identifikacije, razmena potrebnih akreditacija može biti nastavljena uz pomoć "sveže" dogovorenog ključa sesije. Osnova većine tehnika autentifikacije je prethodno dogovoreni ključ, koji je isporučen van opsega (out of band) do korisničke jedinice. Autentifikacija se može postići na primer u mobilnim telefonima ubacivanjem master privatnog ključa na SIM karticu prilikom aktivacije kartice [7]

Drugi pristup podrazumeva proširenje sadašnje mobilne mreže dodatnim elementima kojima bi se omogućio mrežno integrisani AAA i u Internet sredini. Neki autori predlažu uključivanje novog čvora, pod nazivom uslužni GPRS pristupni ruter. (Serving GPRS Access Router). Ovaj entitet deluje kao mrežni prolaz (Gateway) za WLAN saobraćaj za ulazak u GPRS mobilni sistem, i omogućava primenu GPRS signalizacije za kontrolu WLAN. Novi set protokola eliminiše potrebu za primenom signalizacije SS7 pored IP jezgra mreže. Ovo rešenje je superiorno u smislu brzine i opterećenja u poređenju sa RADIUS metodama koje su predložene ranije. Glavni nedostatak je potreba za posebnim uređajemi koji treba da rade u dvostrukom modu i da dele IP sloj, što je rešenje koje možda i nije praktično imajući u vidu više od 5 milijardi mobilnih telefona na tržištu.

5. Pravci razvoja do sigurnih komunikacija

Primena neke od raspoloživih vrsta kriptografije ne znači da će se obezbediti siguran pristup. Strane koje komuniciraju se moraju dogovoriti o ključevima koje koriste za enkripciju podataka. Pri tom je očigledno da enkripcioni ključ koji se koristi kao ključ sesije ne može biti poslat preko mreže kao običan tekst.

Da bi se omogućila enkripcija čak i za prvu poruku koja je po pravilu kritična, postoji nekoliko rešenja. Najjednostanije, koje se koristi u mobilnim mrežama je prethodno prikazan ključ koji se unapred dostavi mobilnom terminalu. Ovaj ključ se može upotrebiti kasnije za inicijalizaciju bezbednosne infrastrukture i može se koristiti kao master ključ u budućoj autentifikaciji.

U dinamičnijim sistemima upotreba prethodno prikazanih ključeva može izazvati poteškoće. Većina WLAN enkripcionih metoda podržava ovaj tip distribucije ključeva, gde se ključ prenosi na novu jedinicu nekim metodom koji je van opsega (out of band) na primer preko neke spoljašnje jedinice. Praktično svi privatni i mnogi korporativni WLAN-ovi koriste statičke ključeve, omogućavajući onome ko prisluškuje da uhvati veliku količinu saobraćaja i tako omogući lako dešifrovanje sadržaja. To znači da sistem koji poseduje tako osiguran pristupni medijum može biti lako kompromitovan. Ključevi koji ne zastarevaju mogu kompromitovati čak i najjaču enkripciju, pa se preporučuje obnavljanje ključeva s vremena na vreme.

Van sveta telekomunikacija teško je distribuisati ključeve unapred, tako da je to dovelo do izrade protokola razmene ključeva, koji pružaju zaštitu već od prve poruke i nije potrebna nikakav prethodno uspostavljeni tajni ključ. Najviše korišćeni protokol je Diffie-Hellman (DH) razmene ključeva, koji omogućava da dve strane koje se ne poznaju od ranije uspostavljaju zajednički tajni ključ preko nebezbednog komunikacionog kanala. Ovaj protokol ne autentifikuje međusobno čvorove ali omogućava razmenu podataka, koje mogu dekodirati samo učesnici. Maliciozni napadači mogu primeniti napad tipa „posrednik“. Pošto je problem dobro poznat od ranije, nekoliko modifikacija omogućava DH zasnovan na identitetu. Tako se koristi metod enkripcije zasnovan na hijerarniji identiteta, koja u suštini deluje kao sistem javnih ključeva, gde je kao javni ključ upotrebljen izabrani niz.

Infrastruktura javnih ključeva PKI (Public Key Infrastructure) može pomoći u odbrani u odnosu na posredničke napade. Kriptografija javnih ključeva se zasniva na ne-polinomialnim (Non Polynomial) vremenskim problemima, na primer primenom faktorizacije ili elipsoidnih krivih.

Formiraju se dva ključa, javni i privatni. Javni ključ se može poslati kao otvoreni tekst, jer se poruke koje se šalju preko javnog ključa mogu dekodirati jedino privatnim ključem, i obrnuto. Dvostruka priroda javnih ključeva omogućava međusobnu autentifikaciju korisnika, pošto se potpisi koji su napravljeni javnim ključevima mogu proveriti javnim ključem. Autentičnost poruka se garantuje, mada identitet čvora nije dokazan. Potpis dokazuje samo da je poruka kodirana od strane čvora, koji ima javni ključ entiteta koji možda želi da komunicira.

Identitet se može osigurati upotrebom sertifikata. Autorizacija sertifikata čuva javne ključeve i nakon provere identiteta vlasnika van opsega dokazuje se identitet potpisivanjem javnog ključa i korisničkih informacija sa sopstvenim ključem. Ovaj metod je potreban kod finansijskih transakcija i poslovnih operacija.

Sledeće bezbednosno pitanje za terminale je nedostatak bezbednog skladištenja. Upotreba smart kartica je rešenje za ovaj problem, ali podrazumeva dodatne hardverske zahteve. Nedostatak bezbednog skladištenja dobija sve više na značaju u šemama za upravljanje digitalnim pravima DRM (Digital Right Management). Većina DRM šema koristi softverska rešenja, ali se u poslednje vreme uvode i hardverska rešenja.

Svi ovi metodi autentifikacije, bezbedno skladištenje i upravljanje pravima podržavaju sigurnu razmenu podataka, ali ne štite privatnost korisničkih akreditacija, preferenci i profila. Ad hoc mreže, kao što su lične mreže PAN (Personal Area Networks) koje su dinamički konfigurisane otvorenije su za napade na privatnost. Prema tome, zaštita korisničkih akreditacija u bežičnoj sredini je jedan od osnovnih pravaca sadašnjih istraživanja.

6. Put do sigurne infrastrukture kontrole pristupa

Mobilnost i bežični pristup su uveli nove probleme u mreže u pogledu upravljanja korisnicima, u poređenju sa instalacijama fiksne mreže sa na primer, ograničenjima pristupa zasnovanim na portovima. Mrežni operatori žele da zaštite mrežu od štetnih napada, nekorektne naplate servisa određenom korisniku i da omoguće lak i otvoren pristup servisima.

Prvi korak u dobijanju pristupa enkriptovanoj mreži je dogovor o prvom ključu sesije. To je rešeno u koordiniranim mrežama kao što su mobilne mreže kroz prethodno predstavljene ključeve. Autentifikacija i kontrola pristupa je data od strane centralnih entiteta da bi se osigurala operativnost.

U kompjuterskim mrežama, koje se ne kontrolišu na takav način i koje obično nisu podržane centralnom autorizacijom, autentifikacijom i obračunom (AAA) za kontrolu konekcije su stvoreni različiti metodi. Osnovni metod je i dalje dogovor o enkripcionim ključevima na osnovnu prethodno prikazane tajne informacije. Tipični prethodno prikazani ključevi su lozinke za *Hash* proračun, koje se jednom šalju preko mobilnog telefona ili koje se daje na USB jedinici.

Postoji nekoliko rešenja za zaštitu podataka koji se prenose preko bežičnog linka. U privatnim mrežama, radno rešenje je bezbednost koja je zasnovana na prethodno predstavljenim ključevima. U korporativnim ili javnim mrežama, potrebno je robusnije rešenje. Način koji obećava najviše je integracija dogovora o ključevima sesija u AAA proces. Pošto operatori moraju identifikovati konektovanog korisnika, u tom postupku oslanjaju se na AAA infrastrukturu i sprovode enkripciju akreditacija korisnika kao osnovnu politiku. Kontrola pristupa medijuma na osnovu sertifikata i AAA sistema se prporučuju gde AAA poruke mogu nositi sertfikate koji su potrebni da se osigura razmena poruka.

Operacije javnim ključevima proizvode dosta mrežnog saobraćaja, pa se dogovoreni ključevi sesija moraju koristiti na najefikasniji način. Protokoli enkripcije koji su izrađeni za žične sredine, kao što je sigurnost transportnog sloja TLS (Transport Layer Security) ne podrazumevaju probleme koji su u vezi sa radio prenosom i ograničenjima mobilnih uređaja. U žičnoj sredini, proračunati trošak dogovora o ključevima se obično zanemaruje.

Ukoliko mobilni uređaj želi da izvrši međusobnu autentifikaciju sa operatorom servisa sa razmenom sertifikata, to može dovesti do velike količine podataka koja se prenosi preko radio interfejsa.

U sredinama sa ograničenim resursima, autentifikacija i upravljanje identitetom na osnovu prethodno podeljenih ključeva je i dalje najefikasnije rešenje. Neki autori predlažu produžetak TLS-a, koji omogućava upotrebu prethodno predstavljenih tajnih podataka umesto upotrebe asimetrične enkripcije. To je u skladu sa naporima da se potrebe za resursima zadrže na zahtevanom minimumu u mobilnim uređajima. Rešenje prethodno predstavljenog ključa je takođe došao kao predlog 3GPP foruma kao metod autentifikacije za bežične LAN operacije. Problem sa predloženim rešenjem je u tome što prethodno prikazani ključ ne omogućava odgovarajuću privatnost niti zaštitu identiteta u Internet konekcijama. Da bi se rešio ovaj problem, TLS metod razmene ključeva TLS KEM (TLS Key Exchange Method) omogućava zaštitu identiteta, minimalno potrebne resurse i punu kompatibilnost sa originalnom šemom protokola.

U UMTS mrežama, niz autentifikacijskih ključeva se šalje na mobilni uređaj u vektorskom obliku. U svetu kompjutera dobro rešenje je upotreba *Hash* funkcije za proračun novih ključeva sesija, zbog malog utroška energije.

Mobilni terminal može imati problem u komunikaciji, pošto višak saobraćaja podataka koji je rezultat dogovora o ključu može produžiti vreme konekcije na mrežni čvor. Sačuvani ključ sesije za upotrebu u novoj mreži je potencijalno rešenje u mobilnoj sredini, pošto ubrzava autentifikaciju čvora, pa se preporučuje šema, koja omogućava ponovnu upotrebu ključeva sesije. Na osnovu AAA infrastrukture, moguće je proslediti ključ novom odgovarajućem AAA serveru na zaštićenoj mreži i upotrebiti ga za autentifikaciju bez kompromitacije bezbednosti sistema. To može smanjiti odlaganje konekcije, i mogućnost neuspeha autentifikacije. Pošto se stari ključevi sesija mogu koristiti za autentifikaciju čvora prema novom AAA serveru, konekcija prema domaćem AAA više nije potrebna. Poruke se razmenjuju na sledeći način: prilikom slanja zahteva za autentifikaciju novoj mreži, čvor uključuje staru mrežnu adresu koju je imao. Strani agent se povezuje na novi lokalni AAA server i šalje zahtev za autentifikaciju. Novi AAA server se povezuje na stari slanjem poruke kojom se identifikuje korisnik. Stari AAA potvrđuje poruku proverom *Hash* vrednosti koja se tu nalazi, i stvara privremeni podatak za terminal i stranog agenta. Server sklapa odgovor AAA terminala, koji se sastoji od običnog privremenog podatka, šifrovanog privremenog podatka i ključa koji je poznat starom stranom agentu i terminalu. Zatim se kompletna poruka potpisuje i enkriptuje ključem koji koriste dva AAA servera. Kada je novi AAA primi, šifruje i pošalje poruku novom stranom agentu. Na osnovu običnog privremenog podatka, agent stvara ključ i šalje nazad odgovor, koji uključuje privremeni podatak koji je enkriptovan sa starim AAA. Nakon autentifikacije korisnika u odnosu na mrežu, korisnik može da počne da koristi servise.

Upotreba *Hash* funkcije se preporučuje za mobilno okruženje, jer daje bolje performanse mehanizmima zasnovanim na javnim ključevima. Mobilni IPv4 protokol koristi simetrične ključeve i *Hash* vrednosti u osnovi. Pošto je simetričnim ključevima teško upravljati, preporučuje se razmena ključeva na osnovu sertifikata, koja međutim zahteva više resursa. Da bi se smanjila potreba za resursima, preporučuje se kompozitna arhitektura. Procedura koristi sertifikate samo na mestima na kojima terminal ne podrazumeva procesuiranje algoritama javnih ključeva i ne podrazumeva skladištenje sertifikata.

Rezultati poređenja pokazuju da je *Hash* metoda najefikasniji za generisanje ključeva, ali ima slabosti u pogledu upravljanja. Takođe čista autentifikacija na osnovu sertifikata nije odgovarajuća za mobilnu sredinu. Delimična upotreba sertifikata i

autentifikacija na osnovu identiteta sa jakom upotrebom *Hash* funkcije može biti potencijalni put napred.

7. Primena inteligentnih SIM kartica u povećanju zaštite mobilnih sistema

Upotreba inteligentnih SIM kartica ima svoje mesto u rešavanju osnovnog problema bezbednosne infrastrukture jer čak i najbolje dizajnirani sistem je osetljiv na slabe lozinke. Kartica, koja predstavlja fizički entitet može mnogo lakše da se zaštiti u poređenju sa posedovanjem lozinke. Pametne kartice integrišu skladištenje podataka otporno na neovlašćen pristup i neophodne kriptografske funkcije. One se obično pokreću pomoću prethodno dodeljenog ključa i stvaraju Hash lanac, čije vrednosti mogu da se upotrebe kao tokeni za autentifikaciju.

Server za daljinsku autentifikaciju koristi iste funkcije da izračuna sledećeg člana. Ključ za enkripciju je izbor hash funkcija otporanih na koliziju. Dok su tokeni koje oni nude prilično bezbedni, problem sa inteligentnim karticama je što one predstavljaju novu jedinicu koja mora da bude prisutna kako bi se obezbedila bezbedna komunikacija, a terminali korisnika moraju da budu opremljeni odgovarajućim čitačima. Dodatni hardver ne samo da izaziva probleme intervorkinga, već je obično spor, kako to pokazuju sprovedena merenje [6]. Ovo postaje očigledno kada je veliki saobraćaj povezan sa asimetričnom enkripcijom: slanje poruke jedne reči sa standardnim TLS-om do inteligentne kartice je trajalo 10 sekundi. Za razliku od toga, modifikovanom TLS-KEM-u je trebalo 1.5 s.

Sistem neprimetne isporuke ključeva jednostavan za korisnika može da se kreira uz pomoć operatera mobilne telefonije i SIM kartica sa pojačanim mogućnostima enkripcije. SIM i USIM moduli upotrebljeni u GSM/UMTS su prilično moćne inteligentne kartice. Oni nude zaštićeno skladištenje sa mogućnošću upravljanja ključevima prutem radio komunikacija, dobar korisnički interfejs i standardnu arhitekturu.

Isporuka ključa mobilnog telefona za različite uređaje može da bude problematična, pošto mnogi uređaji nemaju SIM čitač kartica, ili nije pogodno da se SIM kartica prebacuje iz mobilnog telefona u drugi uređaj.

8. Zaključak

Enkripcija signala u transportu i autentifikacija uređaja biće predmet istraživanja još dugo vremena, koje treba da rezultira dovoljno bezbednim rešenjima sa trenutno raspoloživim i novim tehnologijama. Aktuelni predlozi se fokusiraju na ograničene mogućnosti mobilnih terminala i uvođenje tehnologija enkripcije za mobilne i bežične veze.

Distribucija ključeva između čvorova je rešena, osim prvog koraka, koji obično zahteva prenos van opsega (out-of-band). Rešenje za ovu inicijalnu distribuciju ključeva može da bude mobilni telefon sa integrisanom inteligentnom karticom i već postojećim komunikacionim mogućnostima.

Dok je autentifikacija uređaja dovoljno obrađena, identitet korisnika je teško dokazati. Lozinka zasnovana na znanju ili zahtev za PIN kodom nije rešenje koje korisnici smatraju jednostavno prihvatljivim. Aktuelni predlozi imaju tendenciju ka tome

da učine kompromis između iskustva korisnika i bezbednosti što može dovesti do rešenja sa smanjenom sigurnošću..

Dalja istraživanja bi trebalo da se fokusiraju na područje personalnih i kućnih mreže. Ove mreže čuvaju većinu ličnih privatnih podataka i sadržaja korisnika, bez obzira da li su kupljeni ili kreirani od strane korisnika. Trenutno ne postoji standardno rešenje za upravljanje pravima na sadržaj ili za kontrolu pristupa vlastitom sadržaju.

9. Literatura

[1] Jeong, K. C., Lee, T.-J., Lee, S., & Choo, H. (2006). Route optimization with AAA in network mobility. In *Computational Science and Its Applications — ICCSA 2006* (LNCS 3981)

[2] Kálmán,G., C howdhury, M.M.R.,& Noll, J. (2007). Security for ambient wireless services. In *Proceedings of the 65th IEEE Vehcular Technology Conference (VTC2007)*.

[3] Khara, S., Mistra, I. S., & Saha, D. (2006). An alternative architecture for WLAN/GPRS integration. In *Proceedings of the IEEE Vehicular Technology Conference, 2006, VTC 2006* (pp. 37-41).

[4] Lee, M., Park, S., & Jun, S. (2006). A security management framework with roaming coordinator for pervasive services. In *Autonomic and Trusted Computing* (LNCS 4158).

[5] Shi, M., & al. AAA Architecture and Authentication for Wireless LAN Raoming, *Springer series on Signal and Communications Technology ISBN 10 038728040-5, 2007*

[6] Lutei, H., Shi, W., An adaptive Encryption Protocol in Mobile Computing, *Springer series on Signal and Communications Technology ISBN 10 038728040-5, 2007*

[7] Vacca, R., J., Guide to Wireless Network Security, *Springer, ISBN 10 0 38795425-2*

Abstract: *Focus in this paper is towards solutions for securing transport, service access, user privacy, and accounting in wireless environments. . Converging networks and mobility raise new challenges towards the existing authentication, authorisation, and accounting (AAA) systems. We provides an overview over the state of the art in authentication for mobile systems and suggests extending AAA mechanisms, taking into account security and privacy of the users integrated solutions. The rolle of smart cards and other security tokens are shown and a secure and convenient transmission method. By using link layer encryption, smart cards, and secure key transfer methods the security and privacy protection can be greatly enhanced.*

Keywords: *Authentication, authorisation, and accounting (AAA)*, *Remote Authentication Dial in User Service (RADIUS), Converged Network, Digital Rights Management (DRM), Public Key Infrastructure (PKI), Rivest-Shamir-Adleman (RSA), Subscriber Identity Module (SIM), Smart Card*

OVERVIEW NEW ELEMENTS OF SECURITY IN MOBILE SYSTEM

Milan Janković, Borislav Odadžić