METODI I NAPADI NA DISTRIBUCIJU SIMETRIČNIH I ASIMETRIČNIH KRIPTOLOŠKIH KLJUČEVA

Brkić Bogdan[1], Miroslav Ćajić[2]

Sadržaj - U ovom radu biće analizirane metode distribucije kriptoloških simetričnih i asimetričnih ključeva, kao i napadi koji se mogu desiti tokom same distribucije. Razmotrićemo načine distribucije ključeva kada u sistemu ne postoji treća stana od povjerenja, kao i slučajeve kada se povjerenje zasniva upravo na postojanju treće strane.

Ključne riječi - simetrična i asimetrična kriptografija, distribucija kriptoloških ključeva, napad

I. DISTRIBUCIJA I UPRAVLJANE KRIPTOLOŠKIM KLJUČEVIMA

Upravljanje kriptološkim ključevima se bavi sigurnim generisanjem, distribucijom i čuvanjem ključeva. Sigurnost metoda upravljanja ključevima je od ekstremnog značaja. Kada je ključ jednom generisan on mora ostati tajan da bi se izbjegle situacije kao što je impersonalizacija. Kada je riječ o infrastrukturi sa javnim ključevima, u praksi se najviše napada dešava na nivou upravljanja ključevima, a vrlo rijetko se dešavaju napadi na same algoritme. Učesnici u PKI sistemima moraju biti sposobni da generišu ključeve. Takođe moraju imati mogućnost da publikuju svoj javni ključ i da im budu dostupni javni ključevi ostalih korisnika u sistemu, za šta se koriste sertifikati. Ukoliko dođe do kompromitacije ili gubitka nečijeg privatnog ključa ostali učesnici moraju biti upozoreni. U suprotnom, napadač će ukradenim privatnim ključem moći dešifrovati sve poruke koje su šifrovane odgovarajućim javnim ključem ili će moći vršiti neovlašteno digitalno potpisivanje. Korisnicima mora biti omogućeno da na siguran način čuvaju svoje ključeve i učine ih nedostupnim osim za legitimnu upotrebu.

Ključevi imaju ograničen životni vijek. Najvažniji razlog za ovo je zaštita od kriptoanalize. Svaki put kada se ključ upotrijebi generišu se šifrati. 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 / 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 za privremene ključeve koji se koriste 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. Simetrični i privatni ključevi su po svojoj prirodi tajni ključevi.

[1] Bogdan Brkić dipl.ing.inf.-master, Ministarstvo finansija Republike Srpske, Trg Republike Srpske 1, 78000 Banja Luka, tel.: +387 65/567-941, e-mail: bbogdan@teol.net

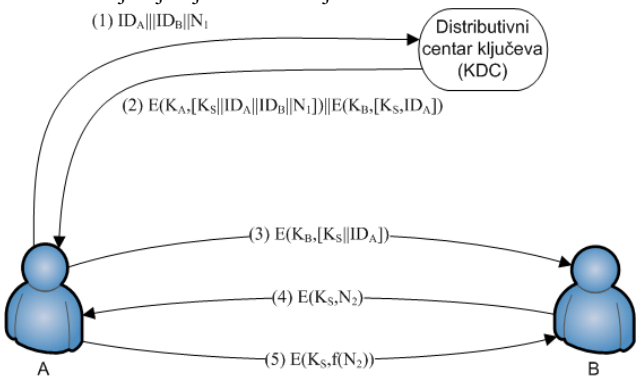
[2] Miroslav Ćajić dipl.ing.inf.-master, MikroByte doo, Vesa Rackovića 16, 73220 Rogatica, tel.: +387 65/631-675, fax: 387 58/417-517, e-mail: info@mikrobyte.com

II. DISTRIBUCIJA KLJUČEVA U SIMETRIČNOJ KRIPTOGRAFIJI

Da bi simetrično šifrovanje i dešifrovanje sa druge strane funkcionisalo, obe strane moraju da posjeduju isti ključ. Ovdje se javlja problem distribucije ključeva. 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.

A. Distributivni centar ključeva (Key Distribution Center - KDC)

Ovakav način razmjene ključeva podrazumijeva da svaka strana u komunikaciji dijeli jedinstveni ključ sa distributivim centrom.



sl. 1. Scenario distribucije ključeva

Pretpostavimo da A želi da komunicira sa B, ali nemaju zajednički ključ već samo imaju po jedan zajednički ključ sa distributivnim centrom. Komunikacija će se uspostaviti upravo posredstvom KDC distributivnog centra ključeva.

- Strana A generiše identifikator N_1 koji služi za jednokratnu upotrebu (može biti slučajan broj ili vremenska oznaka, a služi da bi spriječila maskiranje), i šalje ga zajedno sa svojim identifikatorom ID_A (npr. mrežna adresa od A) i identifikatorom ID_B, a sve to je šifrovano zajedničkim ključem korisnika A i KDC-a, K_A.
- KDC odgovara i šalje jednokratni ključ K_S, ID_A, ID_B, N_1 šifrovane ključem K_A i šalje podatke koje će A proslijediti prema B a to su K_S, ID_A šifrovano ključem K_B. Sada i A i B posjeduju sesijski ključ K_S, a B zna da je A inicirao komunikaciju.
- B šalje šifrovani identifikator N_2 šifrovan sesijskim ključem K_S i čeka odgovor od A, a to je $f(N_2)$ šifrovan sesijskim ključem K_S. Ovim se B obezbjeđuje od mogućnosti falsifikovanja poruke u trećem koraku.

U daljnjem tekstu E predstavlja šifrovanje, a D dešifrovanje. 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. Tokom komunikacije između dvije strane poželjno je da se sesijski ključevi ne upotrebljavaju dugo i da se generišu novi.

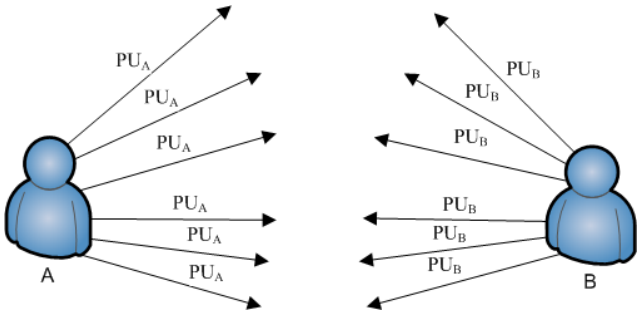
III. DISTRIBUCIJA JAVNIH KLJUČEVA U ASIMETRIČNOJ KRIPTOGRAFIJI

Postoji nekoliko tehnika za distribuciju javnih ključeva u asimetričnoj kriptografiji:

- javno objavljivanje
- javno dostupan direktorijum
- autoritet za javne ključeve (Public-Key Authority)
- sertifikati

A. Javno objavljivanje

Kao što im i samo ime govori javni ključevi trebaju biti javno dostupni. Ako postoji neki opšte prihvaćeni i široko rasprostranjeni asimetrični algoritam, kao što je RSA, dovoljno je da svaki učesnik pošalje javni ključ strani sa kojom želi da komunicira.



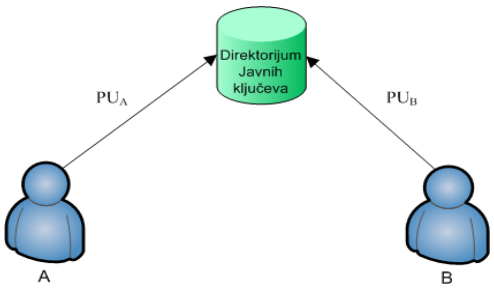
sl. 2. Nekontrolisana distribucija javnih ključeva

Ovakav način razmjene ključeva je veoma jednostavan ali ima i nedostatke. Bilo ko može da se predstavi kao osoba A i pošalje svoj javni ključ, navodeći drugu stranu na pomisao da će šifrovane poruke razmjenjivati sa osobom A. Ovakav način razmjene ključeva ne obezbjeđuje povezanost javnog ključa sa njegovim vlasnikom.

B. Javno dostupan direktorijum

Veći stepen sigurnosti u odnosu na javno objavljivanje postiže se korištenjem javno dostupnog direktorijuma. Održavanje i distribucija javnog direktorijuma je u nadležnosti nekog entiteta od povjerenja ili neke organizacije. Ovakva šema uključuje sledeće elemente:

- entitet održava direktorijum i unosi slogove sa sadržajem (ime, javni ključ) za svakog učesnika
- svaki učesnik registruje javni ključ lično ili nekim sigurnim metodom autentifikacije
- učesnik može zamijeniti javni ključ kada to odluči bilo da je razlog kompromitacija ili dugačak period upotrebe
- učesnici mogu elektronskim putem pristupiti direktorijumu

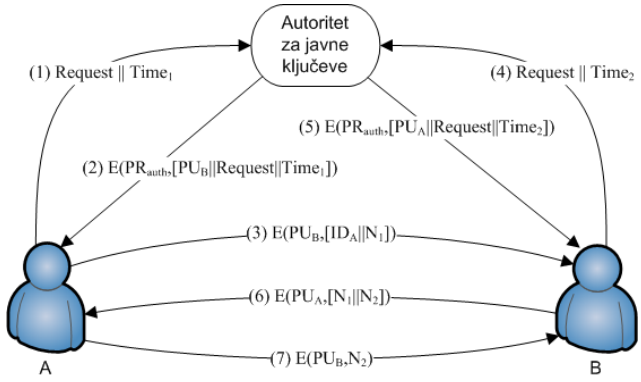


sl. 3. Publikovanje javnog ključa u direktorijum

Ovakav način distribucije je sigurniji od javnog objavljivanja, ali je još uvijek ranjiv. Ako napadač uspije u namjeri da pribavi ili rekonstruiše privatni ključ entiteta koji je u posjedu direktorijuma, može doći do kompromitacije bilo kog učesnika u sistemu. Drugi problem koji se javlja je mogućnost krivotvorenja javnih ključeva u direktorijumu od strane napadača.

C. Autoritet za javne ključeve (Public-Key Authority)

Ovaj sistem je sličan prethodnom s tim što svaki učesnik poznaje javni ključ autoriteta, a privatni ključ autoriteta je dostupan isključivo njemu samom.



sl. 4. Scenario distribucije javnih ključeva

Razmjena ključeva između dva učesnika se odvija na sledeći način:

1. A šalje vremenski označenu poruku autoritetu u kojoj se nalazi i zahtjev za javnim ključem od B
2. autoritet odgovara šaljući javni ključ od B i originalan zahtjev, a sve je šifrovano privatnim ključem autoriteta PR_{auth}
3. A šalje poruku prema B i šifruje je javnim ključem korisnika B PU_B, a u poruci se nalaze identitet učesnika A i jednokratna vrijednost N_1
4. kao i u prvom koraku B šalje vremenski označenu poruku autoritetu u kojoj se nalazi i zahtjev za javnim ključem od A
5. autoritet odgovara šaljući javni ključ od A PU_A
6. B šalje poruku koja se sastoji od N_1 i N_2, a šifrovana je upotrebom PU_A (N_2 je generisao B i samo njemu je poznata)
7. A iz N_1 i N_2 uzvraća šaljući N_2 a šifrovano je upotrebom PU_B, pa je B siguran da je poruku primio baš od A

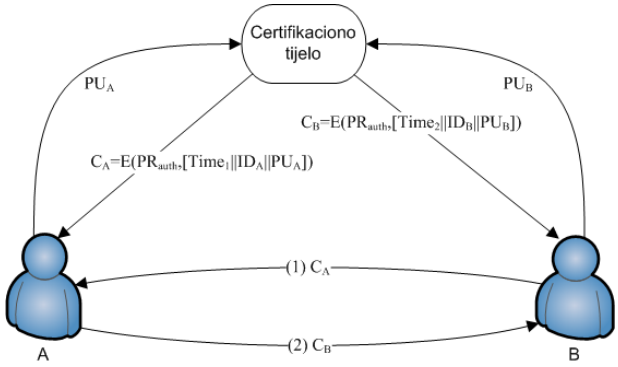
D. Sertifikati

Poboljšanje prethodnog metoda se postiže upotrebom sertifikata. Autoritet nekada može biti usko grlo u cijelom sistemu, jer se za svaki javni ključ mora podnijeti zahtjev prema autoritetu. Alternativni pristup prethodnom rješenju je upotreba sertifikata. Korištenjem sertifikata nekom učesniku je moguće dostaviti vlastiti

javni ključ na način kao da je to učinio autoritet. Sertifikat se sastoji od javnog ključa i identifikacije vlasnika tog ključa. Ovi podaci su potpisani od strane "treće strane", u koju svi učesnici u sistemu imaju povjerenje - sertifikaciono tijelo. Korisnik na siguran način prezentuje svoj javni ključ autoritetu i nakon toga dobija sertifikat koji se može javno objaviti. Svako kome je potreban javni ključ ovog korisnika može preuzeti njegov sertifikat. Svi učesnici mogu provjeriti da li je sertifikat kreiran od strane autoriteta.

Za ovakav način razmjene ključeva moraju biti ispunjeni sledeći zahtjevi:

- svaki učesnik može pročitati sertifikat da bi odredio javni ključ i ime vlasnika sertifikata
- svaki učesnik može utvrditi da je sertifikat izdat od strane sertifikacionog tijela i da nije krivotvoren
- samo sertifikaciono tijelo može izdavati i reizdavati (update) sertifikate



sl. 5. Razmjena sertifikata

Izdavanje sertfifikata započinje tako što svaki zainteresovani učesnik šalje svoj javni ključ i zahtijeva izdavanje sertfikata. Autentifikacija mora biti u ličnom kontaktu ili nekom drugom sigurnom metodom. Za nekog učesnika A autoritet izdaje sertifikat u obliku:

$$C_A = E(PR_{auth}, [T||ID_A||PU_A])$$

gdje su PR_{auth} privatni ključ autoriteta i T vremenska oznaka. A zatim može proslijediti sertifikat nekom drugom učesniku koji čita taj sertifikat i verifikuje sledeće:

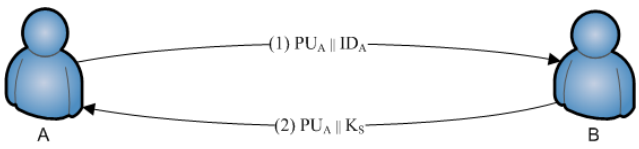
$$D(PU_{auth},C_A)=D(PU_{auth},E(PR_{auth},[T||ID_A||PU_A]))=(T||ID_A||PU_A)$$

Sertifikat je moguće dešifrovati samo javnim ključem autoriteta, što garantuje da je baš taj autoritet izdao sertifikat. Ova šema je postala opšteprihvaćena i formalizovana je kroz standard X.509.

IV. DISTRIBUCIJA TAJNIH KLJUČEVA KORIŠTENJEM KRIPTOGRAFIJE SA JAVNIM KLJUČEM

Kriptografija javnog ključa nije pogodna za razmjenu poruka tj. šifrovanje i dešifrovanje veće količine podataka. Zato se pribjegava tehnici razmjene tajnih ključeva korištenjem kriptografije sa javnim ključevima.

A. Jednostavna distribucija tajnog ključa

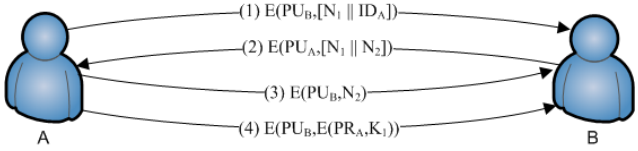


sl. 6. Jednostavna distribucija tajnog ključa

- učesnik A generiše par ključeva $\{PU_A,PR_A\}$ i šalje poruku korisniku B koja se sastoji od PU_A i ID_A
- B generiše sesijski ključ K_S, šifruje ga javnim ključem PU_A i šalje ga učesniku A
- A dolazi do sesijskog ključa $K_S = D(PR_A, E(PU_A, K_S))$; sada samo A i B poznaju sesijski ključ K_S
- A uništava ključeve PU_A, PR_A, a B uništava ključ PU_A
- A i B mogu sigurno razmjenjivati šifrovane poruke upotrebom sesijskog ključa K_S
- po završetku komunikacije sesijski ključ se uništava

Ovakva razmjena ključeva nije bezbjedna zbog "man-in-the-middle" napada. Napadač C može da presretne prvi korak, generiše svoj par ključeva $\{PU_C, PR_C\}$ i komunikaciju A-B pretvori u A-C i C-B .

B. Distribucija tajnih ključeva sa povjerljivošću i vjerodostojnošću



sl. 7. Distribucija tajnih ključeva sa povjerljivošću i vjerodostojnošću

Distribucija se odvija na sledeći način:

- učesnik A koristi javni ključ učesnika B da bi poslao svoju identifikaciju ID_A i jednokratnu vrijednost N_1
- učesnik B uzvraća i šalje poruku koja se satoji od N_1 i N_2, a šifrovana je sa PU_A
- A šalje poruku N_2 šifrovanu ključem PU_B
- sada su i A i B sigurni u identitet druge strane i A može generisati K_S i poslati ga učesniku B kao $M = E(PU_B, E(PR_A, K_S))$, a B do sesijskog ključa dolazi računajući $K_S = D(PU_A, D(PR_B, M))$

V. DIFFIE-HELLMANOV ALGORITAM ZA RAZMJENU KLJUČEVA

D-H algoritam se zasniva na činjenici da je teško izračunati broj α^{ab} ukoliko su poznati brojevi α^a i α^b. Postupak razmjene ključeva se odvija na sledeći način:

- dva korisnika izaberu slučajan broj α
- korisnik A izabere slučajan broj a i izračuna α^a i pošalje ga korisniku B
- korisnik B izabere slučajan broj b i izračuna α^b i pošalje ga korisniku A
- zajednički tajni element je αab koji korisnik A dobije kao $(\alpha^b)^a$, a korisnik B izračunavanjem $(\alpha^a)^b$.

Ovaj algoritam nije otporan na "man-in-the-middle" napad. Napadač, Ted, može da presretne αa i umjesto toga Bobu pošalje α^{a1} i presretne α^b i umjesto toga Alisi pošalje α^{b1}. Sada Ted i Alisa imaju zajednički element α^{ab1}, a Ted i Bob zajednički element α^{a1b}. Pošto Ted i dalje presreće komunikaciju, Alisa je uvjerena da komunicira sa Bobom, ali komunicira sa Tedom. I Bob je uvjeren da komunicira sa Alisom, ali komunicira sa Tedom.

Rješenja za ovaj problem mogu biti:

- šifrovanje DH razmjene simetričnim ključem
- šifrovanje DH razmjene javnim ključem
- digitalno potpisivanje DH vrijednosti privatnim ključem

VI. ZAKLJUČNA RAZMATRANJA

Za simetrično šifrovanje i dešifrovanje predložen je "model distributvnih centara ključeva". 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.

U nastavku ovog rada razmotrena su dva osnovna aspekta kriptografije javnog ključa: distribucija javnih ključeva i upotreba kriptografije javnog ključa za distribuciju tajnih ključeva.

Najbolji rezultati u distribuciji sesijskih ključeva postižu se upotrebom hibridnog-troslojnog modela tj. upotrebom distributivnih centara ključeva koji sa svakim korisnikom dijele zajednički tajni master-ključ koji se upotrebljava za distribuciju sesijskih ključeva, i upotrebom asimetrične kriptografije za distribuciju zajedničkih master-ključeva. Na ovaj način se izbjegava degradacija performansi u sistemima u kojima se često mijenja sesijski ključ, a koja nastaje usljed činjenice da je šifrovanje/dešifrovanje sesijskog ključa asimetričnim alogiritmima sporo. Ovim se postiže da se spore operacije kao što su asimetrično šifrovanje sesijskog ključa zamijene sa dvije: simetričnim šifrovanjem sesijskog ključa upotrebom master-ključa i asimetričnim šifrovanjem master-ključa. Prva može biti i veoma frekventna ali je istovremeno i brza, a druga je spora ali i veoma rijetka.

LITERATURA

[1] A.Menzes, P.van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[2] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, 1996.

[3] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, 2005.

[4] Carlisle Adams, Steve Lloyd, "Understanding PKI: Concepts, Standards and Deployment Considerations", Addison Wesley, 2002.

[5] Steve Burnett, Stephen Paine, "RSA Security's Official Guide to Cryptography", RSA Press, 2001.

[6] Andrew Nash, William Duane, Celia Joseph, Derek Brink, "PKI Implementing and Managing E-Security", RSA Press, 2001.

ABSTRACT

In this paper methods of symetric and asymetric cryptologic keys distribution and attacks on this methods will be analised. We will consider ways of keys distribution in cases with or without trusted third party.

METHODS AND ATTACKS ON THE DISTRIBUTION OF SYMETRIC AND ASYMETRIC CRYPTOLOGIC KEYS

Bogdan Brkić, Miroslav Ćajić