

Primenjena kriptografija

Informaciona bezbednost

FAKULTET TEHNIČKIH NAUKA

V3



Sadržaj

- **Podsetnik**
- **Uvod**
- **Razmena ključeva**
- **Infrastruktura javnih ključeva**
- **Digitalni sertifikat**
- **Upravljanje ključevima**
- **Zaštita podataka u tranzitu**
- **Skladištenje osetljivih podataka**

...Podsetnik

- Na čemu se zasniva tajnost simetričnih/asimetričnih algoritama?
- Šta je predstavljalo najveći problem u komunikaciji između Alice i Boba?
- Kako da budemo sigurni da prilikom slanja poruke koristimo baš javni ključ one osobe kojoj je poruka namenjena?

Uvod

U prethodnom poglavlju je bilo reči o kriptografskim primitivama i načinu na koje one predstavljaju osnovu bezbednosti digitalnih podataka u modernim sistemima. Uvođenjem šifri, problem zaštite poverljivosti podataka je postao problem zaštite poverljivosti ključa. Međutim, kriptografske primitive kao takve nisu dovoljne za funkcionisanje poslovnih sistema. Iako predstavljaju osnovu, *identifikovano je nekoliko problema, poput distribucije javnih ključeva kao i zaštite kriptografskih ključeva tokom njihovog životnog ciklusa.*

U ovom poglavlju će biti adresirani prethodni problemi. Definisaće se mehanizmi za distribuciju ključeva, njihovo bezbedno skladištenje, kao i ostale faze u životnom ciklusu kriptografskog ključa. Na kraju će se prodiskutovati realne primene kriptografskih kontrola za zaštitu podataka, kroz analizu TLS protokol (engl. Transport Layer Security) i tehnika za skladištenje osetljivih podataka.

Razmena ključeva

- Prvi korak pri uspostavljanju sigurne komunikacije - razmena ključeva

Kako Alisa može da osigura da Bob koristi baš njen javni ključ kada šalje njoj poruku?

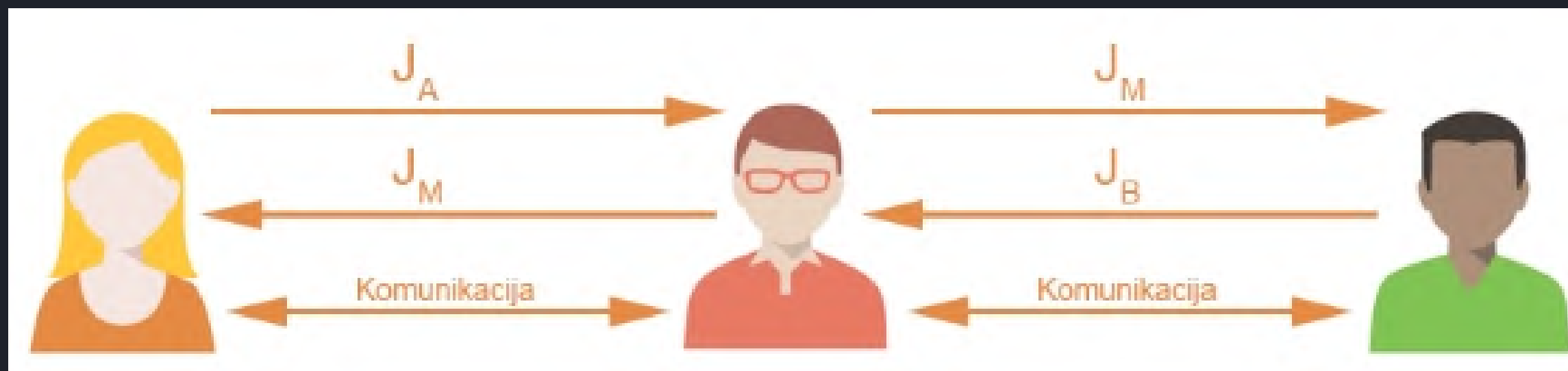
MAN IN THE MIDDLE

Prva opcija jeste da Alisa pošalje Bobu ključ, ali ovaj pristup nema zaštitu od čoveka u sredini (engl. Man in the Middle)



Razmena ključeva

Kako Alisa može da osigura da Bob koristi baš njen javni ključ kada šalje njoj poruku.



1. Alisa šalje svoj javni ključ Bobu;
2. Maliciozni subjekat, Marko, se ponaša kao proxy koji čita sav saobraćaj između Alise i Boba. U trenutku kada Alisa šalje svoj javni ključ J_A Bobu, Marko zaustavlja zahtev, čuva J_A kod sebe, i prosleđuje svoj javni ključ J_M Bobu;
3. Bob šalje svoj javni ključ Alisi, i Marko opet preuzima J_B kod sebe, a Alisi šalje J_M ;
4. Alisa želi da pošalje poruku Bobu, koristeći šifru koja uključuje Bobov, odnosno Markov javni ključ;
5. Marko presreće šifrat, dešifruje ga sa svojim privatnim ključem, čita poruku, šifruje je Bobovim javnim ključem i prosleđuje je dalje Bobu.

Razmena ključeva

SPOLJNI SERVIS ZA UPRAVLJANJE KLJUČEVIMA

Druga opcija bi bila da Alisa i Bob ne generišu svoje ključeve, već da koriste spoljni servis da generiše i distribuira ključeve



1. Alisa pravi zahtev za izradu ključeva, i dobija od servisa za upravljanje ključevima javni i privatni ključ;
2. Alisa želi da pošalje poruku Bobu, i upotrebom svog privatnog ključa je digitalno potpisuje;
3. Alisa kontaktira servis za upravljanje ključevima i traži Bobov javni ključ;
4. Alisa šifrue poruku sa Bobovim javnim ključem i prosleđuje mu šifrat;
5. Bob dobija šifrat, koji dešifruje sa svojim privatnim ključem;
6. Od servisa za upravljanje ključevima dobija javni ključ od Alise;
7. Putem Alisinog javnog ključa, Bob proverava validnost digitalnog potpisa;

Razmena ključeva

SPOLJNI SERVIS ZA UPRAVLJANJE KLJUČEVIMA

Ovakav pristup ima nekoliko problema:

1. Problem čoveka u sredini je i ovde prisutan, gde maliciozni subjekt stoji između servisa za upravljanje ključevima i učesnika komunikacije. Iako teži za sprovođenje, napad je i dalje moguć;
2. Problem može da bude i u performansama servisa, koji ne može da opsluži intenzivnu komunikaciju između više učesnika, zbog čega dolazi do gubitka dostupnosti;

Infrastruktura javnih ključeva

Infrastruktura javnih ključeva (engl. Public key infrastructure, PKI) predstavlja sistem koji vezuje javne ključeve za identitete subjekata kojim pripadaju.


PKI predstavlja grupu rola, polisa i procedura koje koriste ranije pomenute kriptografske primitive kako bi kreirali, upravljali, distribuivali, koristili, skladištili i opozivali **digitalne sertifikate** (engl. Digital certificate).

Digitalni sertifikat

Digitalni sertifikat predstavlja elektronski dokument koji sadrži sledeće podatke:

- Ko je izdao sertifikat (issuer)
- Kome je sertifikat izdat (subject)
- Kada je sertifikat izdat;
- Do kada je sertifikat validan;
- Javni ključ povezan sa sertifikatom i identitetom kom je sertifikat izdat;
- Digitalni potpis formiran od strane izdavaoca sertifikata
- Dodatne informacije (ekstenzije)

Naveden spisak nije potpun, i u zavisnosti od standarda uključuje određene dodatne informacije.

 **Certificate Information**

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.amazon.com

Issued by: Symantec Class 3 Secure Server CA - G4

Valid from 31. 10. 2016 **to** 1. 1. 2018

Digitalni sertifikat

Digitalni sertifikati su izdati od strane sertifikacionih tela (engl. Certificate Authority; CA). Pored toga što je ova informacija navedena u samom sertifikatu, sertifikat je digitalno potpisan od strane sertifikacionog tela koje je izdalo dati sertifikat. Koristeći javni ključ sertifikacionog tela, moguće je proveriti digitalni potpis koji stoji na sertifikatu kako bi se garantovalo da sertifikat nije menjan i da je stvarno izdat od strane datog sertifikacionog tela

U ovakvom sistemu postoje tri problema:

1. Kako doći do sertifikata nekog subjekta?
2. Kako doći do javnog ključa sertifikacionog tela kako bi se proverio digitalan potpis sertifikata?
3. Kako sertifikaciono telo zna da je sertifikat koji je izdat stvarno vezan za ispravan entitet?

Digitalni sertifikat

KAKO DOĆI DO SERTIFIKATA NEKOG SUBJEKTA?

Prvi problem je lako rešiv tako što se, prilikom uspostavljanja komunikacije sa datim subjektom, zatraži i njegov digitalan sertifikat. Ukoliko postoji čovek u sredini on može da proba da podmetne svoj sertifikat, slično kao što je opisan problem podmetanja ključa, ili može da izmeni sertifikat tako da stoji njegov javni ključ u sertifikatu. **Prvi problem se rešava tako što sertifikat ima identifikator koji je jedinstven, te bi razlikovanje identifikatora sertifikata koji je zatražen i onog koji je dobijen okinulo alarm. Drugi problem se rešava putem digitalnog potpisa, jer svaka izmena sertifikata menja heš sertifikata.**

KAKO DOĆI DO JAVNOG KLJUČA SERTIFIKACIONOG TELA KAKO BI SE PROVERIO DIGITALAN POTPIS SERTIFIKATA?

Drugi problem se rešava tako što sertifikaciono telo nudi svoj javni ključ upotrebom digitalnog sertifikata, koji je potpisan od strane drugog sertifikacionog tela. Ovako se formira stablo, čiji korenski čvor predstavlja korensko sertifikaciono telo (engl. Root CA), koje takođe ima sertifikat, potpisan od strane sebe samog (engl. Self-signed certificate).

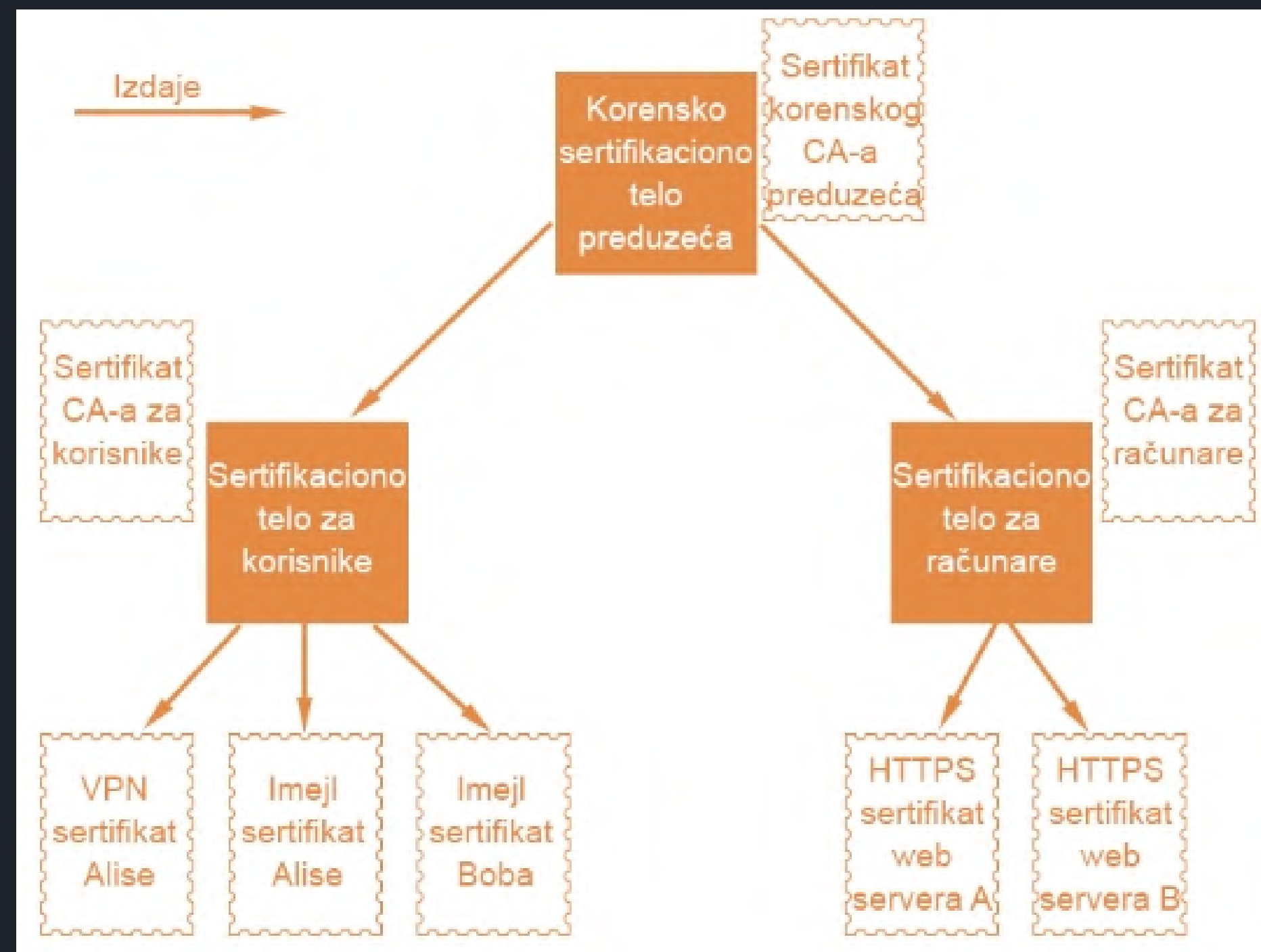
KAKO SERTIFIKACIONO TELO ZNA DA JE SERTIFIKAT KOJI JE IZDAT STVARNO VEZAN ZA ISPRAVAN ENTITET?

Kada je u pitanju intranet nekog preduzeća, problem je lako rešiv jer su sertifikati vezani za zaposlene i sisteme koji su pod direktnom kontrolom preduzeća. Međutim, postavlja se pitanje kako javno dostupni servisi dobijaju sertifikate, i generalno kako priča sertifikacionih tela radi na javnom internetu.

Digitalni sertifikat

HIJERARHIJA SERTIFIKATA

- **Korenskih sertifikacionih tela** na javnom internetu ima više, i glavna tri igrača predstavljaju **Symantec, Comodo i GoDaddy**. Ovo su preduzeća čiji poslovni model predstavlja održavanje infrastrukture javnih ključeva interneta. Plaćanjem ozbiljnije sume novca, ova korenska sertifikaciona tela mogu da izdaju sertifikat za sertifikaciono telo, odnosno sertifikat koji može da izdaje druge sertifikate. Sa druge strane, moguće je za manju sumu novca kupiti sertifikat koji nema mogućnost izdavanja sertifikata, ali se može koristiti za obezbeđivanja HTTPS protokola na veb-sajtu.

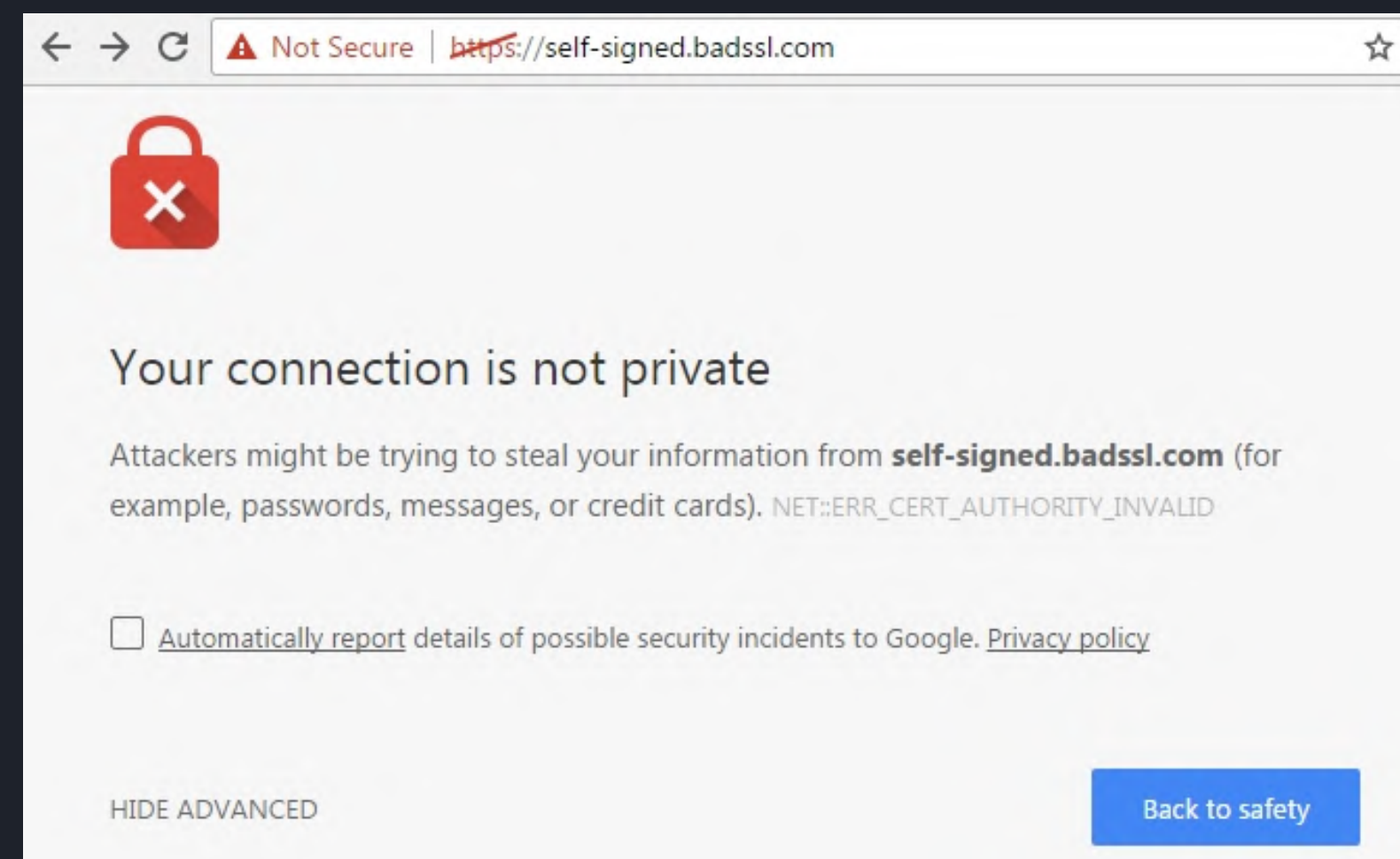


Digitalni sertifikat

HIJERARHIJA SERTIFIKATA

- Kako serveri sertifikacionih tela izdržavaju konstantne upite da li je neki sertifikat validan?

Sertifikati poznatih sertifikacionih tela interneta dolaze ugrađeni u operativni sistem, ili sam veb-čitač. Ako se ode na domen sa sertifikatom u čijem lancu se nalazi poznato sertifikaciono telo, smatra se da se može verovati sertifikatu. Ukoliko se učitava domen koji nema validan sertifikat, veb-čitač će blokirati saobraćaj i prikazati upozorenje



Digitalni sertifikat

NEISPRAVAN SERTIFIKAT

Sertifikat može da bude neispravan:

- ako je istekao
- ako nema validan digitalan potpis
- ako je izdat od strane sertifikacionog tela koje nije od poverenja
- ako je sertifikat povučen

- nevalidan vs povučen sertifikat?

Digitalni sertifikat

POVUČEN SERTIFIKAT

Razlozi za povlačenje sertifikata uključuju:

- Gubitak privatnog ključa koji odgovara javnom ključu koji se nalazi na sertifikatu, što je najčešći razlog;
- Nenamerno izdavanje sertifikata, kao posledica greške ili napada na sertifikaciono telo;
- Npropisno ponašanje vlasnika izdatog sertifikata;
- Naknadno otkrivanje neispravnosti zahteva za izdavanje sertifikata;

Tehike provere da li je sertifikat povučen:

1. upotreba listi za povučene sertifikate (**engl. Certificate revocation list; CRL**)
2. upotreba protokola za onlajn proveru statusa sertifikata (**engl. Online Certificate Status Protocol; OCSP**)

Digitalni sertifikat

OCSP ZAHTEV

1. Alisa i Bob imaju sertifikat izdat od strane Pere, koji predstavlja sertifikaciono telo
2. Alisa želi da komunicira sa Bobom i šalje mu svoj sertifikat
3. Bob šalje OCSP zahtev koji uključuje serijski broj Alisinog sertifikata, kako bi bio siguran da sertifikat nije povučen
4. Pera proverava svoju bazu podataka i gleda koji je status sertifikata sa datim serijskim brojem.
Pronalazi da je sertifikat validan i da nije povučen
5. Bob dobija odgovor, potpisan od strane Pere, koji tvrdi da je Alisin sertifikat ispravan
6. Bob, koji ima uskladišten Perin sertifikat, proverava digitalni potpis i uspostavlja komunikaciju sa Alisom

...Rezime

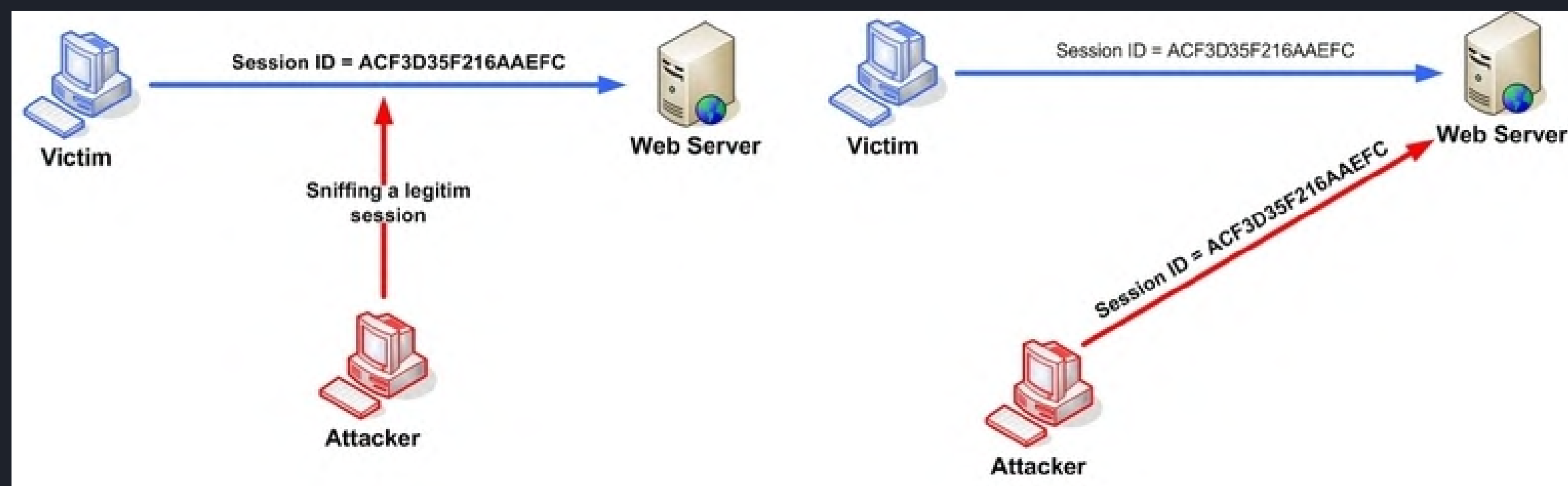
Komunikacije Alice i Boba...

- ☑ Problem razmene ključeva rešen pomoću sertifikata
- ☑ Utvrdili smo da su sertifikati validni
- ☑ Razmena poruka može da počne
- ☐ *Kako će običan korisnik da ostvari bezbednu komunikaciju putem interneta, ako ne poseduje sertifikat?*

Zaštita podataka u tranzitu

Šta se dešava ako jedno preduzeće nema svoj privatni i javni ključ. Primer za ovaj slučaj je komunikacija između veb-čitača i serverske aplikacije. Prosečan korisnik interneta ne poseduje sertifikat, već putem običnog veb-čitača komunicira sa raznim serverima putem **HTTP protokola**.

Ukoliko je saobraćaj između klijenta i servera izvršen putem HTTP protokola, sav saobraćaj koji se razmenjuje između ovih subjekata je vidljiv svakom napadaču koji osluškuje mrežu. Ako bi, putem besplatne WiFi mreže kafića, korisnik pristupao serveru preko HTTP protokola, vlasnik WiFi mreže bi, upotrebom alata poput WireShark, mogao da osluškuje sav saobraćaj i da uhvati sve podatke koji se razmenjuju, uključujući korisničke kredencijale, identifikator sesije, i druge osetljive podatke



Zaštita podataka u tranzitu

TLS PROTOKOL

Originalna zamisao oko upotrebe interneta se značajno razlikuje od današnje. Sam HTTP protokol je dizajniran tako da nudi visok nivo fleksibilnosti, dok bezbednost uopšte ne predstavlja zahtev. Zbog ograničenosti hardverskih resursa i količine protoka inicijalno nije bilo moguće ponuditi adekvatnu kriptografsku zaštitu internet saobraćaja, ali je taj problem davno rešen uvođenjem **SSL (engl. Secure Socket Layer) protokola**.

U novijim verzijama SSL protokol je preimenovan u **TLS (engl. Transport Layer Security)**, gde je SSL verzija 3.1 zapravo TLS verzija 1.0.

Zaštita podataka u tranzitu

TLS PROTOKOL

- TLS - Transport Layer Security
- Sloj u komunikaciji između browser-a i nekog remote servera

Komunikacija između veb-čitača i veb-servera obezbeđena dobro konfigurisanim TLS protokolom ima sledeća svojstva:

1. **Poverljivost**- obezbeđena upotrebom simetrične šifre. Server i klijent generišu jedinstven ključ za datu sesiju, upotrebom tajne informacije koja je dogovorena između ovih subjekata na samom početku komunikacije, upotrebom asimetrične šifre- (engl. Handshake)
2. **Integritet**- postiže se upotrebom heša
3. **Autentičnost**- najčešće jednosmerna, gde je server autentifikovan preko svog sertifikata

Zaštita podataka u tranzitu

HTTPS PROTOKOL

- HTTP komunikacija zasnovana na TLS protokolu se naziva **HTTPS (engl. HTTP over TLS)**.
- Kada korisnik, putem veb-čitača, pristupa veb-sajtu koji podržava HTTPS, vrši se handshake u sklopu kog veb-čitač i veb-server uspostavljaju HTTPS komunikaciju.
- Handshake se uspostavlja nakon TCP konekcije, a pre slanja HTTP zahteva. Sastoji se od nekoliko koraka, gde je suština odrediti koji kriptografski algoritmi su podržani, proveriti validnost sertifikata servera i generisati ključeve za simetrično šifrovanje poruka