Sigurnost računalnih sustava

Mrežna sigurnost

- drugi dio (VPN, certifikati, TLS)

doc. dr. sc. Ante Đerek
doc. dr. sc. Stjepan Groš
izv. prof. dr. sc. Miljenko Mikuc
izv. prof. dr. sc. Marin Vuković

VPN

Virtualne privatne mreže

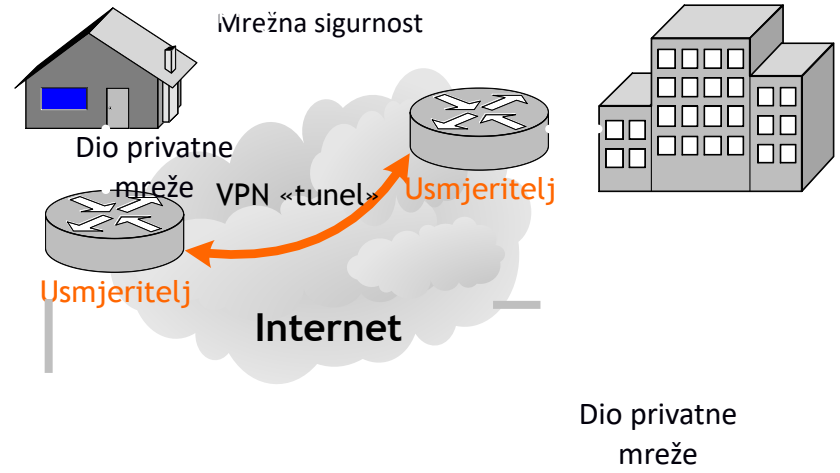
- Virtual Private Networks (VPN)
  - Pojam koji označava stvaranje privatnih mreža nad javnom infrastrukturom Interneta
  - Zamjena za nekadašnje iznajmljivanje linkova, modeme, i slično.
  - Nije specifičnost mrežnog sloja, ali je nužno prenositi IP pakete
- Rješenja za ostvarenje virtualnih privatnih mreža
  - PPTP – ne koristiti!
  - OpenVPN
  - WireGuard
  - IPsec (verzije 2 i 3) – standardni dio IPv6 (i IPv4), kompleksna konfiguracija
    - IPsec+L2TP
  - „Clientless VPN” - TLS

Protokol PPTP

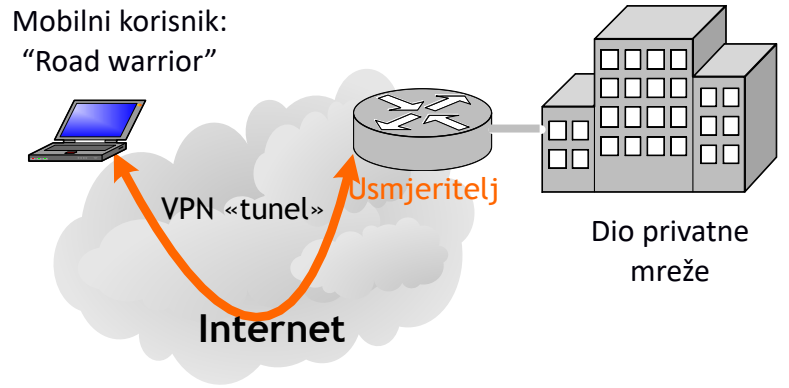
- Point-to-Point Tunneling Protocol – PPTP
  - Razvila tvrtka Microsoft 1999. godine
  - Vrlo jednostavan za podešavanje sa širokom podrškom
  - Najčešće se koristi za spajanje računala na korporativnu mrežu
- **Od 10. mjeseca 2012. Microsoft ne preporuča korištenje tog protokola**
  - Na Internetu postoji usluga probijanja šifre za bilo koju PPTP konekciju unutar jednog dana

Vrste VPN

- od točke do točke (*Site-to-site*)
  - između dva mrežna entiteta (na primjer usmjeritelja)
  - privatne i zaštićene mreže iza oba entiteta



- udaljeni pristup (*Remote Access*)
  - između uređaja i usmjeritelja
  - na udaljenoj lokaciji se ne nalazi zaštićena mreža



Osnove arhitekture IPsec (1)

- Rješenje na mrežnom sloju
- Služi za
  - povezivanje dviju ili više mreža (VPN)
  - povezivanje osobnih računala na korporativnu mrežu (engl. road-warrior)
  - povezivanje dva računala međusobno
- Može raditi u tunelskom i prijenosnom načinu rada
- Autentikacija putem certifikata, dijeljene tajne ili EAP-a
- Najčešće upotrebljavana je verzija 2 a najnovija je verzija 3

Osnove arhitekture IPsec (2)

- Protokol definira ponašanje krajnjih točaka i protokole za razmjenu upravljačkih informacija i podataka
- Ponašanje krajnjih točaka definirano bazama SPD i SAD
- Osnovni protokoli
  - IKE: Uspostava ključeva, implementira se u korisničkom načinu rada u vidu aplikacije
  - ESP: Encapsulating Security Payload
    Zaštita tajnost, integriteta i autentičnosti, impl. u jezgri operacijskog sustava
  - AH: Authentication Header
    Zaštita integriteta i autentičnosti, impl. u jezgri operacijskog sustava

Baze SPD i SAD (1)

- SPD (Security Policy Database) definira što se treba zaštititi
  - Način zaštite (tunel ili prijenosni način)
  - Sadrži selektore prometa
    - Selektor se sastoji od IP adrese/mreže, protokole, pristupe; za svaku stranu veze posebno
  - Navodi što treba učiniti s paketom koji odgovara
    - Blokirati, propustiti ili zaštititi
- SAD (Security Association Database) definira kako treba štiti
  - Sadrži odabrane kriptografske algoritme i ključeve

Baze SPD i SAD (2)

- Primjer ispisa SPD baze na Linux OS-u

```
172.16.228.0/24[any] 192.168.173.0/24[any] any
        out prio def ipsec
        esp/tunnel/161.53.65.225-161.53.65.11/require
        created: Nov 22 15:52:52 2010  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=17 seq=1 pid=16163
        refcnt=1

192.168.173.0/24[any] 172.16.228.0/24[any] any
        in prio def ipsec
        esp/tunnel/161.53.65.11-161.53.65.225/require
        created: Nov 22 15:52:52 2010  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=8 seq=0 pid=16163
        refcnt=1
```

Baze SPD i SAD (3)

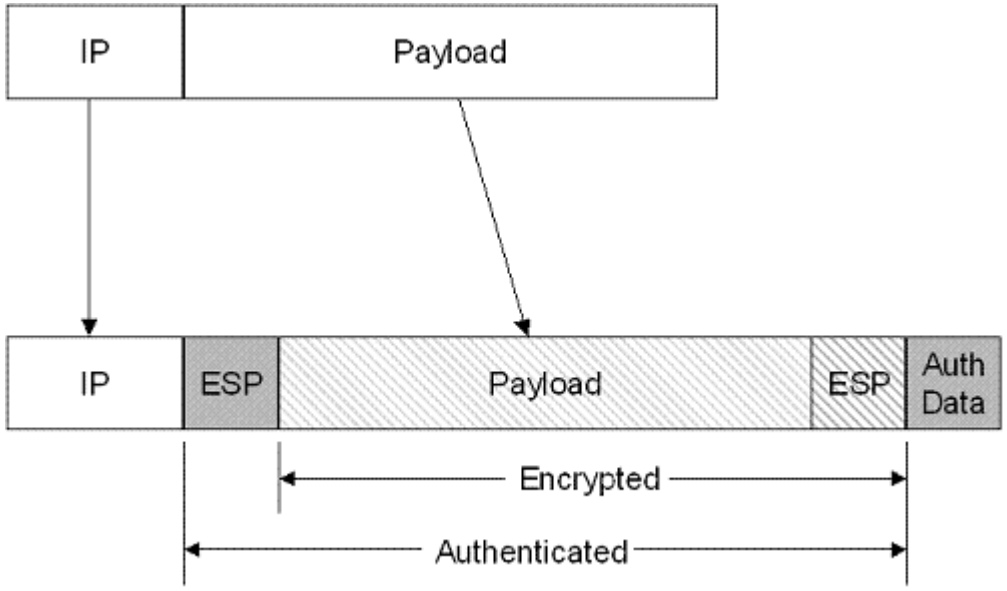
- Primjer ispisa SAD baze na Linux OS-u

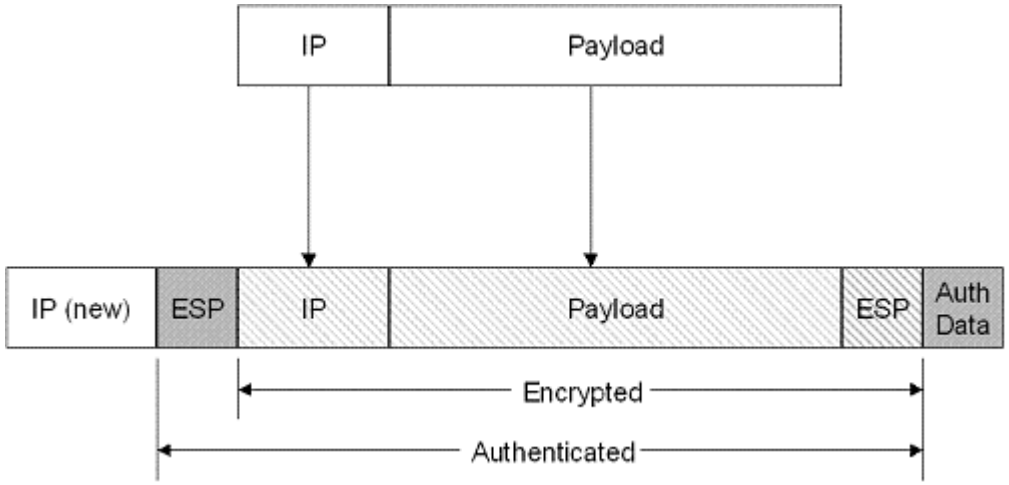
```
161.53.65.225 161.53.65.11
        esp mode=tunnel spi=15702(0x00003d56) reqid=0(0x00000000)
        E: 3des-cbc  31323334 35363738 39303132 31323334 35363738 39303132
        seq=0x00000000 replay=0 flags=0x00000000 state=mature
        created: Nov 22 15:52:52 2010           current: Nov 22 15:56:41 2010
        diff: 229(s)    hard: 0(s)      soft: 0(s)
        last:                           hard: 0(s)      soft: 0(s)
        current: 0(bytes)               hard: 0(bytes)              soft: 0(bytes)
        allocated: 0    hard: 0         soft: 0
        sadb_seq=1 pid=16330 refcnt=0

161.53.65.11 161.53.65.225
        esp mode=tunnel spi=15701(0x00003d55) reqid=0(0x00000000)
        E: 3des-cbc  31323334 35363738 39303132 31323334 35363738 39303132
        seq=0x00000000 replay=0 flags=0x00000000 state=mature
        created: Nov 22 15:52:52 2010           current: Nov 22 15:56:41 2010
        diff: 229(s)    hard: 0(s)      soft: 0(s)
        last:                           hard: 0(s)      soft: 0(s)
        current: 0(bytes)               hard: 0(bytes)              soft: 0(bytes)
        allocated: 0    hard: 0         soft: 0
        sadb_seq=0 pid=16330 refcnt=0
```

Protokol ESP

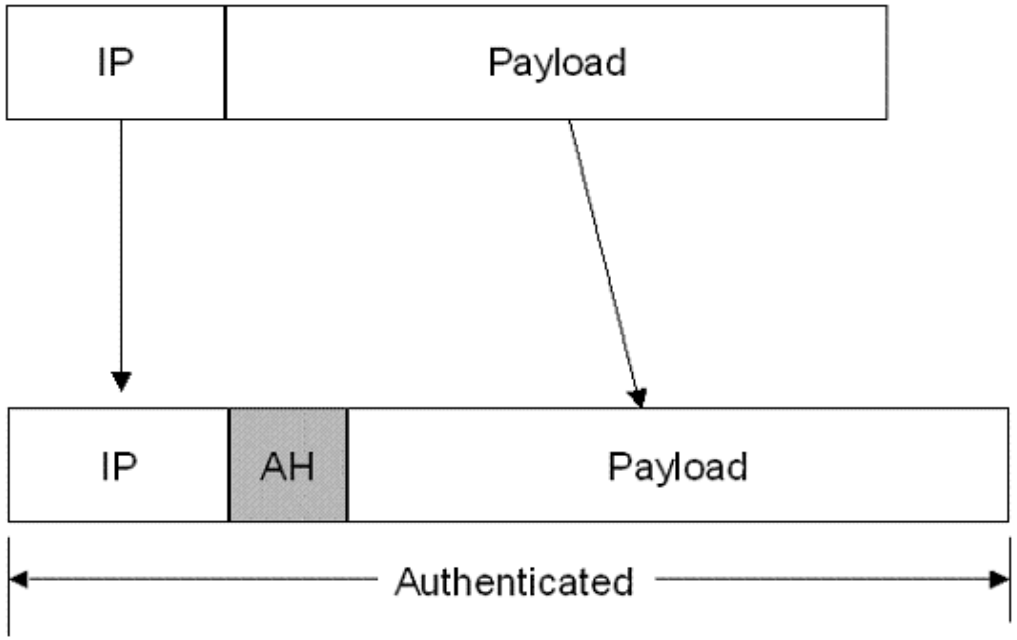
- Struktura zaglavlja paketa ESP (Encapsulating Security Payload) u prijenosnom (lijevo) i tunelirajućem (desno) načinu rada

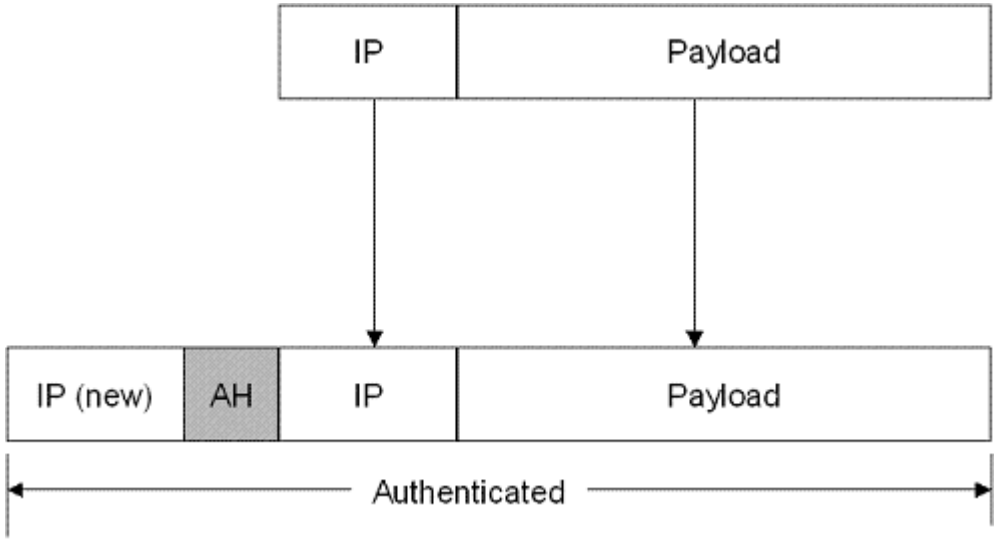




Protokol AH

- Struktura zaglavlja paketa AH (Authentication Header) u prijenosnom (lijevo) i tunelirajućem (desno) načinu rada



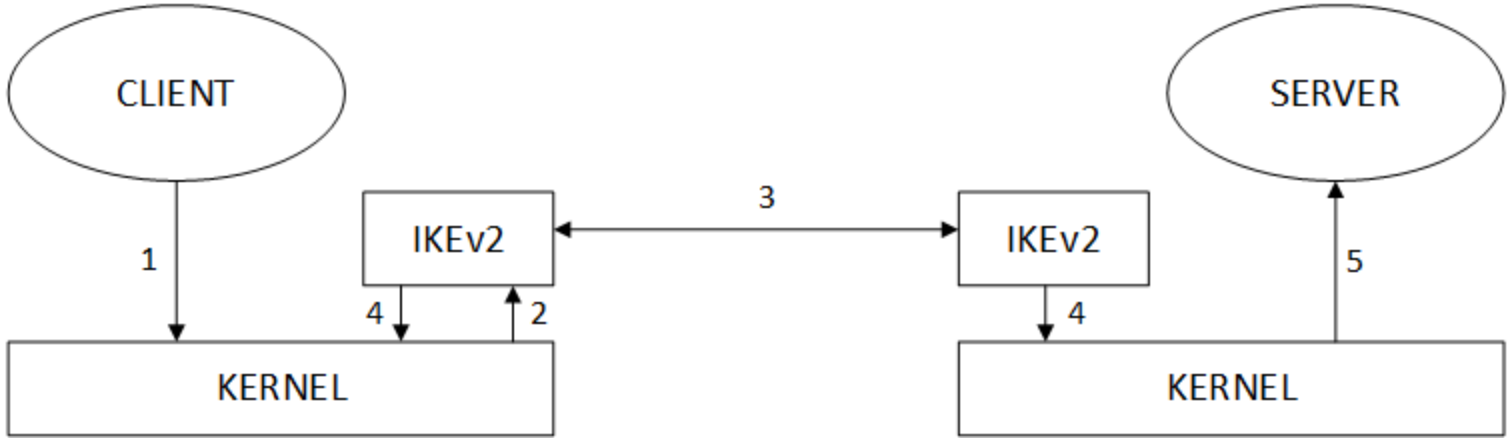


Protokol IKEv1 i IKEv2

- Skraćenica od Internet Key Exchange
- Zadaće protokola su
  - Autentifikacija partnera
  - Dogovor oko sigurnosnih asocijacija (engl. security associations, SA)
  - Periodička razmjena ključeva
- Razlike IKEv2 u odnosu na IKEv1
  - IKEv2 pojednostavljen u odnosu na IKEv1
  - Potrebno je manje razmjena paketa kako bi se uspostavila prva sigurnosna asocijacija
  - Uklonjena i jedna ranjivost u posebnom načinu rada

Primjer rada protokola IKE i ESP/AH

- Neka aplikacija na lijevom računalu želi pristupiti aplikaciji na desnom računalu
  - Prikazan je slijed komunikacije pod uvjetom da te dvije aplikacije nisu prethodno komunicirale



Nekriptirani VPN sustavi

- Ponekad se pod nazivom VPN-a nudi neka nezaštićena usluga
  - Pojedine usluge koje telekomi nude nisu kriptirani
- Primjer je MPLS usluga
  - MPLS je tehnologija slična na ATM-u koja IP adrese mijenja labelama
  - Labele su oznake fiksne veličine
  - U toj usluzi nema nikakvog kriptiranja te je IPsec ili nekakav sličan mehanizam i dalje nužan

Digitalni certifikati

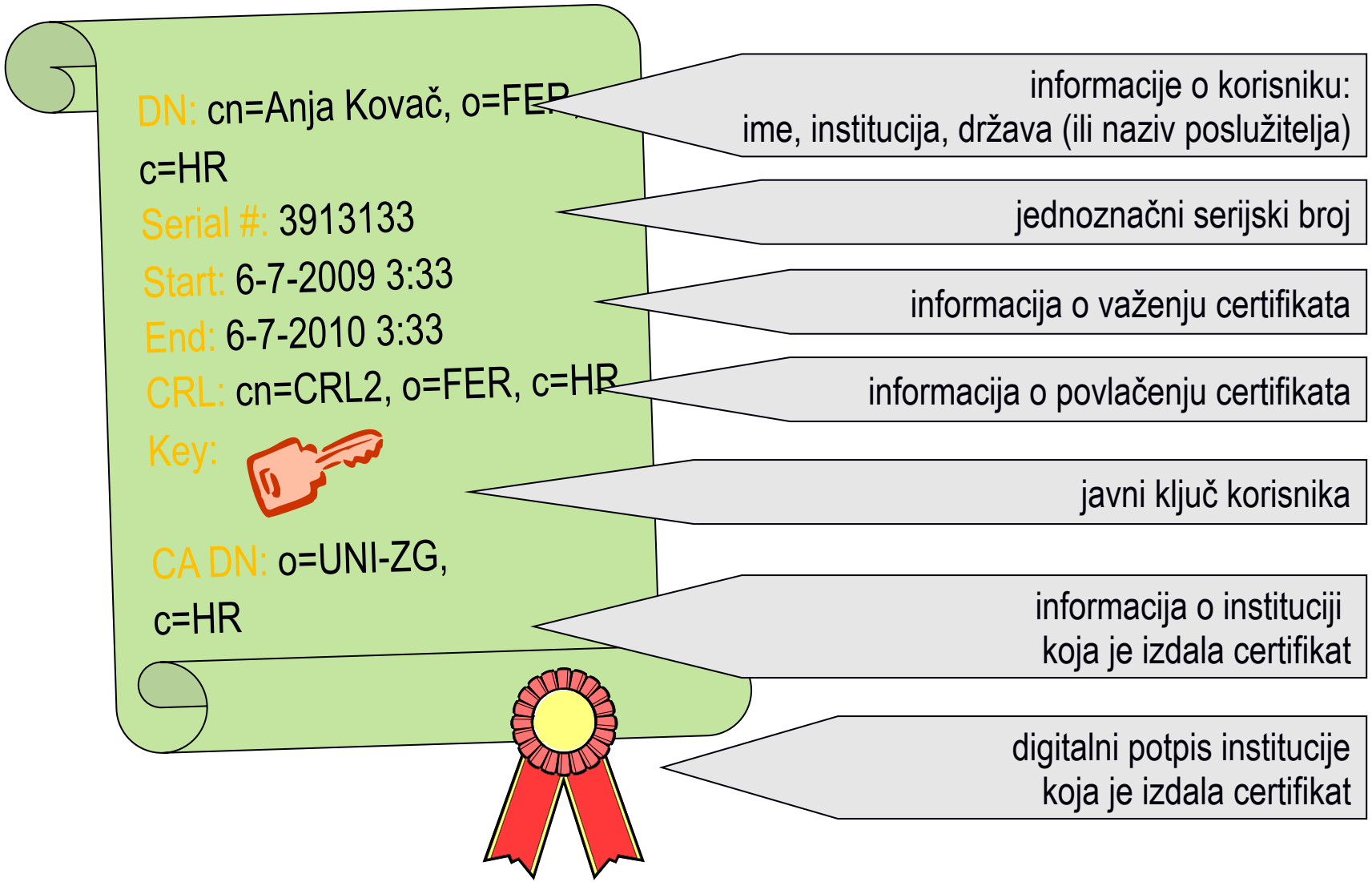
Digitalni certifikati

- Simetrične šifre: jedan tajni ključ (za šifriranje i dešifriranje)
- Asimetrične šifre: par ključeve, javni ključ dostupan svima, privatni ključ dostupan samo vlasniku:
  - Ima li privatni ključ samo odgovarajuća osoba — kriptografski uređaj
  - Kako povezati javni ključ sa osobom — digitalni certifikat
  - Vrijedi li nečiji javni ključ? Da li je opozvan? — lista opozvanih certifikata (CRL)
  - Tko izdaje i jamči za certifikat? — Certification authority (CA)
  - Identifikacija i autentikacija osobe — Registration authority (RA)
  - U koju svrhu se certifikat koristi — Certificate Policy - CP

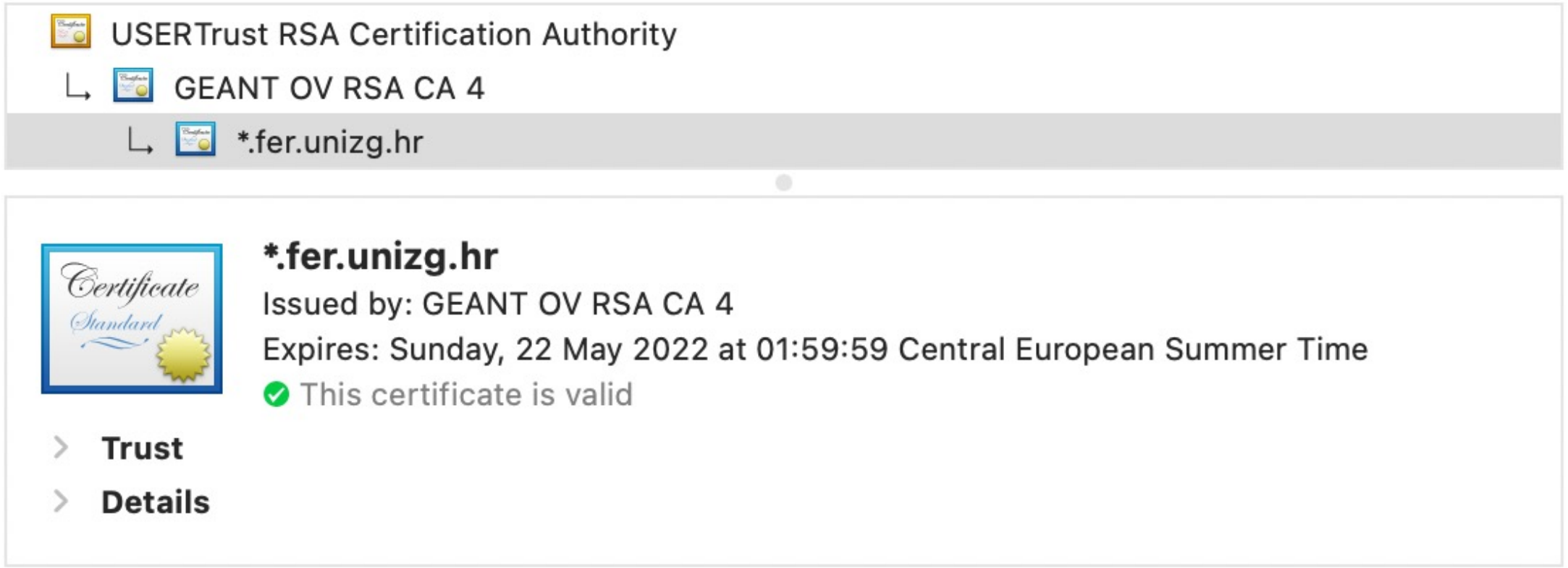
Digitalni certifikati

- Certifikat – digitalni objekt
  - Sadrži javni ključ i ostale informacije o subjektu, izdavatelju i valjanosti
  - Subjekt certifikata je naziv računala ili osobe kojoj certifikat pripada
  - Certifikat izdaje i digitalno potpisuje izdavatelj certifikata (CA, Certificate Authority)
- Standardi:
  - format X.509 - ISO, ITU-T
  - RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

Sadržaj osobnog certifikata



Sadržaj certifikata za web poslužitelj



Sadržaj certifikata

Subject Name	
Country or Region	HR
Postcode	10000
County	Grad Zagreb
Locality	Zagreb
Street Address	Unska 3
Organisation	Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva
Organisational Unit	CIP
Common Name	*.fer.unizg.hr
Issuer Name	
Country or Region	NL
Organisation	GEANT Vereniging
Common Name	GEANT OV RSA CA 4
Serial Number	00 9F 6E AB 25 65 BB F2 CC 7D 8C E0 15 6F 1A FC 4F
Version	3
Signature Algorithm	SHA-384 with RSA Encryption (1.2.840.113549.1.1.12)
Parameters	None
Not Valid Before	Thursday, 21 May 2020 at 02:00:00 Central European Summer Time
Not Valid After	Sunday, 22 May 2022 at 01:59:59 Central European Summer Time

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes: A6 05 99 6E EE 6E 2A F6 …
Exponent	65537
Key Size	2.048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	512 bytes: 5E 5A 3B 65 A1 53 11 20 …
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Digital Signature, Key Encipherment
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)

Sadržaj certifikata

Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	*.fer.unizg.hr
DNS Name	fer.unizg.hr
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.6449.1.2.2.79)
Qualifier ID #1	Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI	https://sectigo.com/CPS
Policy ID #2	(2.23.140.1.2.2)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl
Extension	Embedded Signed Certificate Timestamp List (1.3.6.1.4.1.11129.2.4.2)
Critical	NO
SCT Version	1
Log Operator	Google
Log Key ID	46 A5 55 EB 75 FA 91 20 30 B5 A2 89 69 F4 F3 7D 11 2C 41 74 BE FD 49 B8 85 AB F2 FC 70 FE 6D 47
Timestamp	Thursday, 21 May 2020 at 11:17:51 Central European Summer Time
Signature Algorithm	SHA-256 ECDSA
Signature	72 bytes: 30 46 02 21 00 98 A1 CF ...

Log Operator	Let's Encrypt
Log Key ID	DF A5 5E AB 68 82 4F 1F 6C AD EE B8 5F 4E 3E 5A EA CD A2 12 A4 6A 5E 8E 3B 12 C0 20 44 5C 2A 73
Timestamp	Thursday, 21 May 2020 at 11:17:51 Central European Summer Time
Signature Algorithm	SHA-256 ECDSA
Signature	72 bytes: 30 46 02 21 00 E8 15 0D ...
SCT Version	1
Log Operator	Sectigo
Log Key ID	6F 53 76 AC 31 F0 31 19 D8 99 00 A4 51 15 FF 77 15 1C 11 D9 02 C1 00 29 06 8D B2 08 9A 37 D9 13
Timestamp	Thursday, 21 May 2020 at 11:17:51 Central European Summer Time
Signature Algorithm	SHA-256 ECDSA
Signature	71 bytes: 30 45 02 21 00 D9 F5 21 ...
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	CA Issuers (1.3.6.1.5.5.7.48.2)
URI	http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt
Method #2	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://GEANT.ocsp.sectigo.com
Fingerprints	
SHA-256	6C B5 C9 D6 65 CF 7F 87 74 8B 8B D0 84 69 D0 01 C9 41 11 93 F7 FD 7D B5 F2 3A 75 B7 87 E5 28 D0
SHA-1	DF 5E 53 9B CC BB 7F 4F A9 FC EC BD 40 08 D3 C2 C6 78 F7 0C

CA certifikati

- Certifikati svih poznatih izdavatelja ugrađeni su u preglednike ili operacijski sustav (certificate store, keychain,…)

- Unutar organizacije je moguće kreirati vlastito certifikacijsko tijelo koje izdaje samopotpisani certifikat („self-signed certificate”)

Datoteke

- .CER/.CRT/.DER – binarni, DER kodirani certifikat (ili niz certifikata)
- .PEM – dodatno kodiran po Base64
  - počinje retkom "`-----BEGIN CERTIFICATE-----`"
- .PFX – PKCS#12, javni i privatni ključ (zaštićen lozinkom)

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

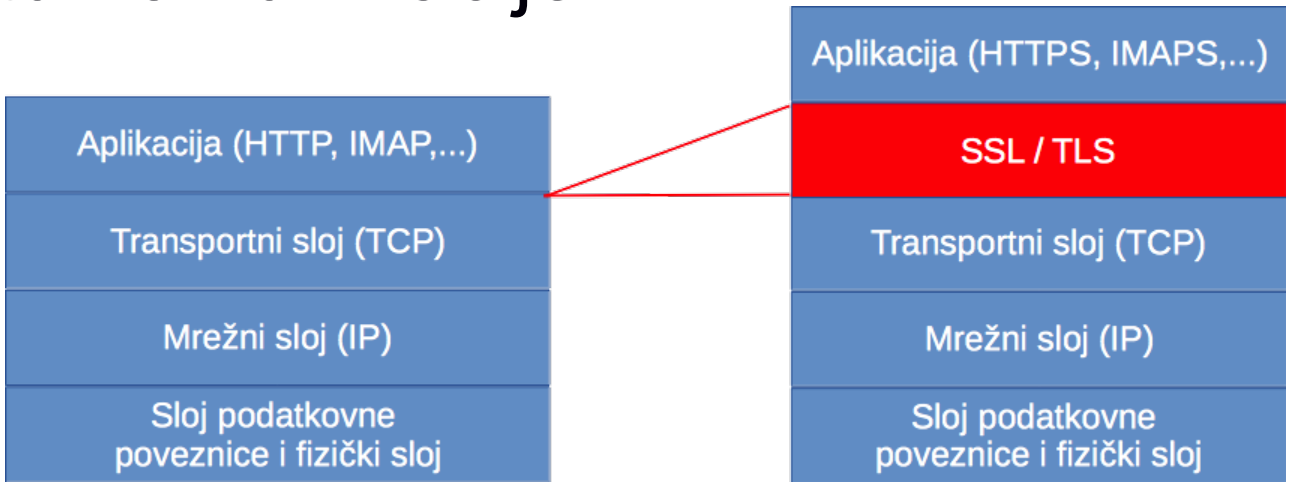
Valjanost certifikata

- Polja u certifikatu: „not valid before” i „not valid after”
- Za vrijeme roka valjanosti certifikat može biti opozvan
  - Gubitak ili kompromitacija privatnog ključa, promjena naziva ili imena, …
- *Certificate Revocation List* (CRL) – lista opozvanih certifikata
  - CRL je digitalni objekt s rokom valjanosti koji sadrži listu opozvanih certifikata te vrijeme i razlog opoziva (digitalno potpisan od strane CA)
  - u certifikatu su navedene adrese i načini pristupa CRL (https, ldap)
- OCSP - Online Certificate Status Protocol
  - OCSP stapling: poslužitelj, uz certifikat, dostavlja klijentu i vremenski ovjeren rezultat OCSP provjere od strane CA

Protokol TLS

Model prijetnje

- Protokol TLS služi za zaštitu komunikacije
- Pretpostavke:
  - Krajnje točke komunikacije su sigurne
  - Ostali sustavi mogu biti pod kontrolom napadača
  - Napadač ima potpunu kontrolu nad komunikacijskim kanalom
    - Može proizvoljno mijenjati pakete, ubacivati pakete, duplicirati, …
  - Eksplicitno ne brinemo o napadima uskraćivanja usluge
    - Napadač presiječe komunikacijski kanal, zaustavi komunikaciju, …
    - Protiv njih se je izuzetno teško nositi s dizajnom protokola



Povijest razvoja protokola SSL i TLS

Protokol	Godina	Opis/Napomena
SSLv1	?	Interno razvijen u tvrtki Netscape Communications. Nikad nije javno objavljen.
SSLv2	1995.	RFC6176 zabranjuje upotrebu ovog protokola zbog niza manjkavosti koje ga čine nesigurnim.
SSLv3	1996.	Više se ne smatra sigurnim. U pripremi je RFC da se njegova upotreba zabrani.
SSL v3.1/TLS 1.0	1. 1999.	Opisan u RFC2246, nije preporučeno korištenje
SSL v3.2/TLS 1.1	4. 2006.	Opisan u RFC4346, nije preporučeno korištenje
TLS 1.2	8. 2008.	Opisan u RFC5246. najčešće korištena verzija
TLS 1.3	8. 2018.	Opisan u RFC8446. Najnovija i trenutno najsigurnija verzija.

podrška za različite verzije na web poslužiteljima na Internetu: https://www.ssllabs.com/ssl-pulse/

Aplikacije koje koriste TLS

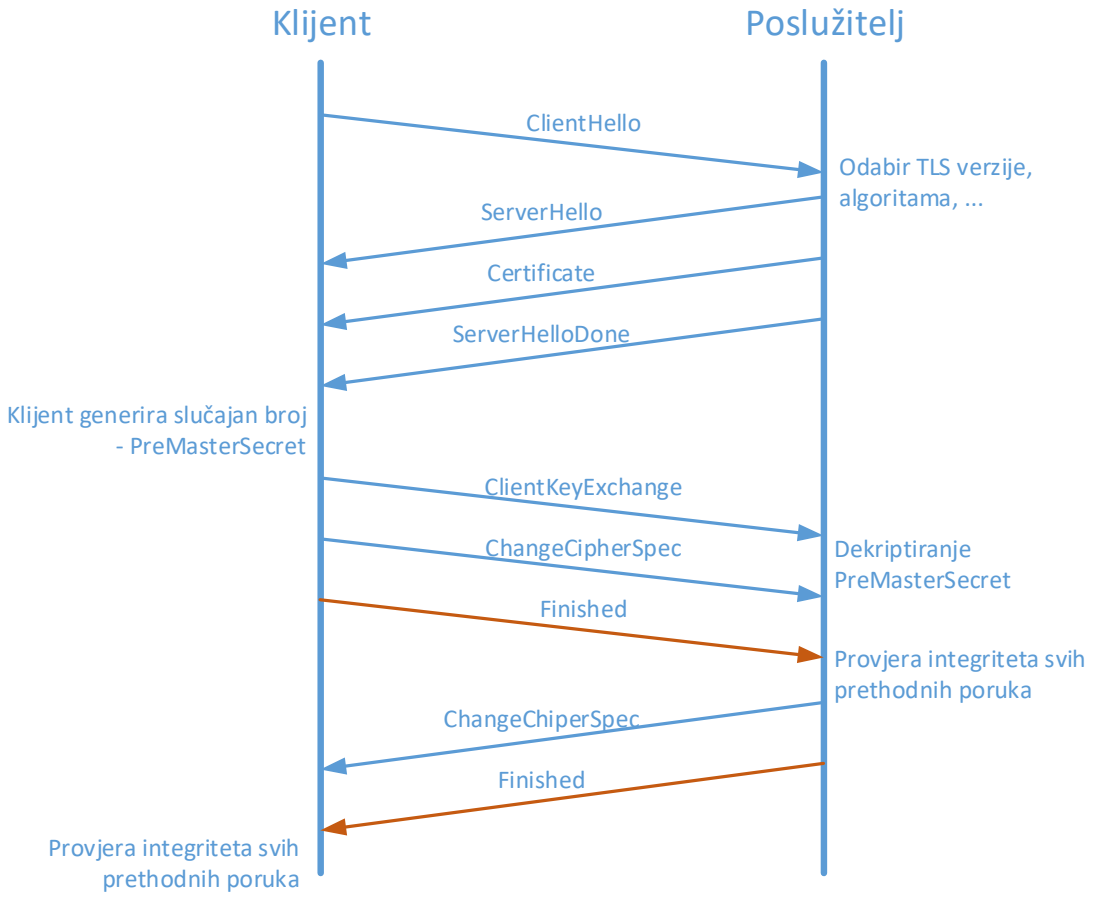
```
https     443     # http protocol over TLS/SSL
smtp       25     # STARTTLS keyword (RFC 2487)
ldaps     636     # ldap protocol over TLS/SSL (was sldap)
ftps-data 989     # ftp protocol, data, over TLS/SSL
ftps      990     # ftp protocol, control, over TLS/SSL
telnets   992     # telnet protocol over TLS/SSL
imaps     993     # imap4 protocol over TLS/SSL
imap4     143     # STARTTLS keyword (RFC 2595)
pop3s     995     # pop3 protocol over TLS/SSL (was spop3)
pop3      110     # STLS keyword (RFC 2595)
. . .
```

HTTP + TLS

- Najčešća upotreba TLS-a: HTTPS
  - Korisnik na klijentskoj strani (u pregledniku) zahtijeva dokument s URL koji sadrži https umjesto http
  - Preglednik prepoznaje SSL/TLS zahtjev i uspostavlja konekciju s poslužiteljem na TCP portu 443
  - Klijent inicira „handshake” korištenjem protokola „record” (u ovoj fazi se ne koristi šifriranje i provjera integriteta)

Osnovna funkcionalnost protokola

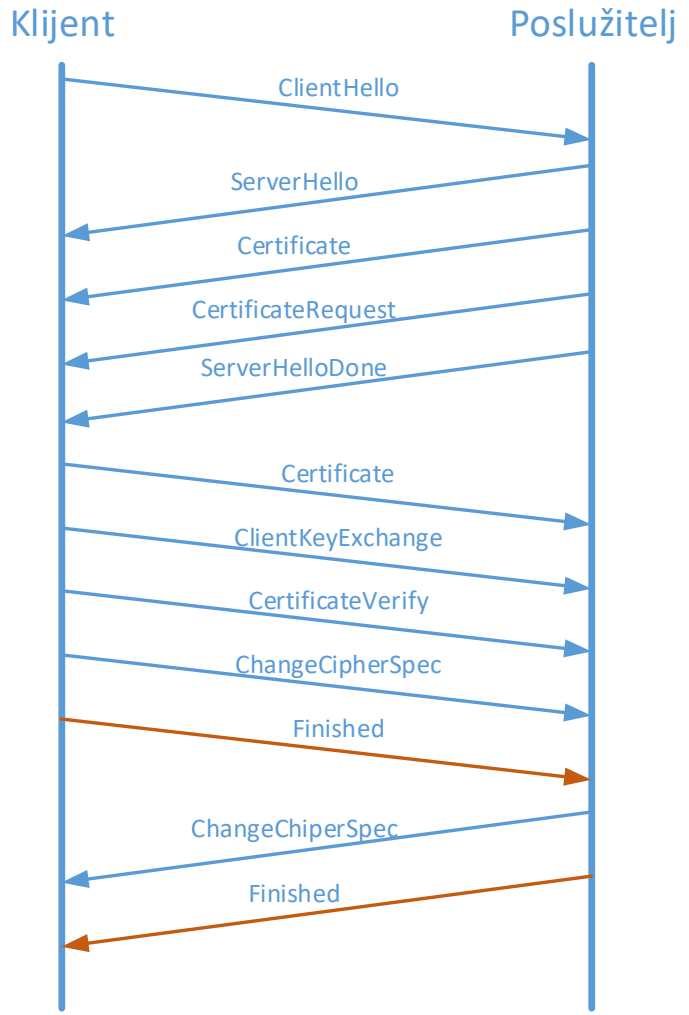
- Potvrda identiteta poslužitelja i zaštita tajnosti i autentičnosti komunikacije
- Izvršava se nad protokolom TCP
  - Postoji i varijanta nad protokolom UDP – DTLS (prvenstveno definiran zbog VoIP-a)
    - UDP varijanta je gotovo identična TCP varijanti



- Za one koji žele znati više: „„The Illustrated TLS Connection”: https://tls13.ulfheim.net

Autentifikacija klijenta i poslužitelja

- Protokol također omogućava autentifikaciju klijenta korištenjem certifikata
  (Certifikat sadrži javni ključ)



Presretanje protokola

- Za tvrtke je kriptirani mrežni promet problematičan
  - Narušavanje politika i pravila korištenja intraneta i Interneta, skidanje zlоćudnog koda, eksfiltracija podataka
  - U slučaju presretanja komunikacije zaštićene TLS-om klijenti dobivaju upozorenje (ili uočavaju nezaštićenu komunikaciju)
  - Moguće je kreiranje vlastitog CA i instaliranje na klijentska računala
  - Određeni Web preglednici imaju „pinned certificates” na temelju čega se može prepoznati presretanje komunikacije

Napadi na protokol (1)

- Heartbleed (CVE-2014-0160)
  - ranjivost OpenSSL implementacije (a ne protokola!)
  - napadač može dohvatiti osjetljive podatke iz memorije poslužitelja
- „SSL Stripping” – 29. srpanj 2009.
  - MITM napad s ciljem uklanjanja SSL/TLS protokola
  - Jedan način sprečavanja je korištenjem HSTS (RFC6797)
  - Teško „obranjivo” ako klijent prvi puta pristupa usluzi
- BEAST (CVE-2011-3389) – 23. rujan 2011.
  - Iskorištava se predvidivi IV u CBC načinu rada protokola TLS 1.0
  - Omogućava dešifriranje pojedinih dijelova paketa, najbitnije HTTP kolačića

Napadi na protokol (2)

- CRIME - Compression Ratio Info-leak Made Easy (CVE-2012-4929) – 13. rujan 2012.
  - BREACH (CVE-2013-3587) je varijanta CRIME napada
- POODLE (CVE-2014-3566) – 14. listopad 2014.
  - Padding Oracle On Downgraded Legacy Encryption
  - Napad na CBC implementaciju u SSL 3.0

Promjene u TLS 1.3

- TLS 1.3 je brži i sigurniji protokol od verzije 1.2
  - Uspostavu zaštićene veze moguće je ostvariti u jednom zahtjevu i jednom odgovoru (u TLS 1.2 su potrebne dvije takve razmjene)
- Uklonjene su zastarjele i nesigurne komponente protokola
  - SHA-1, RC4, DES, 3DES, DES-CBC, MD5, Arbitrary Diffie-Hellman groups — CVE-2016-0701, EXPORT-strength ciphers – Responsible for FREAK and LogJam

Preporuke za korištenje TLS protokola (1)

- Koristiti ključeve od minimalno 2048 bita za RSA ili 256 bita za ECDSA
- Samostalno generirati privatni ključ na sigurnom računalu
- Osigurati dobru pokrivenost računala za koja se koriste certifikati
  - Izbjegavanje upozorenja koja zbunjuju
- Ispravno podesiti lanac certifikata

Preporuke za korištenje TLS protokola (2)

- Ne koristiti SSLv2, SSLv3.0, TLS1.0 i TLS1.1
- TLS1.2 i TLS1.3 su bez poznatih ranjivosti
  - Sve bi trebalo nadograditi da pruža podršku za TLS 1.3
- Izbjegavati korištenje slabih kripto algoritama
  - Izbjegavati korištenje RC4
- Omogućiti „Forward secrecy” i koristiti kripto algoritme koji podržavaju taj način rada
- Onemogućiti kompresiju, pregovaranje koje inicira klijent

Napadi uskraćivanja usluge (DoS/DDoS)

Osnovno o napadima uskraćivanja usluge

- Nisu specifični za mrežni sloj
  - Bilo koje ograničeno sredstvo može biti cilj napada: pristupni link, memorija, CPU, disk, ...
  - Cilj napada može biti i nekakva pogreška u aplikaciji ili protokolu
- Obrana vrlo teška i ovisi o konkretnom napadu i specifičnostima samog napada
  - U određenim slučajevima nužna je suradnja s ISP-om
  - Dobro je planirati razne situacije unaprijed
- Posljedice napada mogu biti katastrofalne za žrtvu
  - Nedostupnost ima novčane i reputacijske posljedice

Povijesni razvoj

- Napadi uskraćivanjem usluge (engl. denial of service attacks) poznati su još iz 80-tih godina prošlog stoljeća
- Prvi DoS napad na Internetu zbio se u ljeto 1999. godine
- Od tada do danas DDoS napadi su postali način zarade te veliki problem za korisnike Interneta
  - DDoS as a Service – cca $40 za 2 sata napada od 220 Gbps
- DDoS: Distributed Denial of Service
  - Raspodijeljeni (distribuirani) napad uskraćivanjem usluge
  - Izvor napada su u pravilu prethodno kompromitirana računala (bot) organizirana u mrežu pod kontrolom napadača (botnet)
  - Mogu se koristiti i postojeće ranjivosti računala (ne nužno „zaraženih”)

Podjela mrežnih (D)DoS napada (1)

- Napadi preplavljivanja (engl. flooding attacks)
  - Lažirani i legitimni UDP promet, ICMP preplavljivanje, DNS preplavljivanje, VoIP preplavljivanje, itd.
- Preplavljivanje koje iskorištava karakteristike protokola (engl. protocol exploitation flooding attack)
  - TCP SYN preplavljivanje, TCP SYN-ACK preplavljivanje, ACK & PUSH ACK preplavljivanje, RST/FIN preplavljivanje, itd.

Podjela mrežnih (D)DoS napada (2)

- Reflektirajući napadi preplavljivanja (engl. reflection based flooding attacks)
  - Smurf/fragle attack
- Napadi preplavljivanja s pojačanjem (engl. amplification based flooding attacks)
  - DNS amplification, NTP amplification

Podjela aplikacijskih (D)DoS napada

- Reflektirajući/amplifikacijski napadi
  - Vrlo slični mrežnim DDoS napadima, ali ciljaju protokole viših slojeva (DNS, NTP, …)
- HTTP napadi
  - Slow request/response attacks
  - Asimetrični napadi
  - Napadači šalju upite koji značajno opterećuju poslužitelj
  - Session/request flooding request
  - Slanje velikog broja upita žrtvi

Pregled zaštita

- Zaštita na strani žrtve
- Zaštita na komunikacijskom putu do žrtve
  - Suradnja s ISP-om
  - Višestruko povezivanje na Internet
  - Usluge zaštite specijaliziranih tvrtki
- Djelovanje na strani napadača i C&C poslužitelja
  - Obavljaju policijske agencije i veliki proizvođači programske podrške (Microsoft)

Zaštita na mjestu žrtve

- Zaštita od napada vrlo specifična o konkretnoj situaciji
  - Nužno je dobro poznavanje vlastite infrastrukture i karakteristika napada
  - Nužno je uspostaviti dobar odnos sa svojim ISP-om
    - ISP može filtrirati promet na svojim usmjernicima
- Primjeri
  - Ako je napad temeljen na UDP-u moguće je blokirati UDP (pripaziti na DNS koji koristi UDP!)
  - Ako paketi dolaze izvan Hrvatske moguće blokiranje vanjskog prometa (vatrozid ili BGP)