Varne komunikacije

Varnostni mehanizmi na Internetu

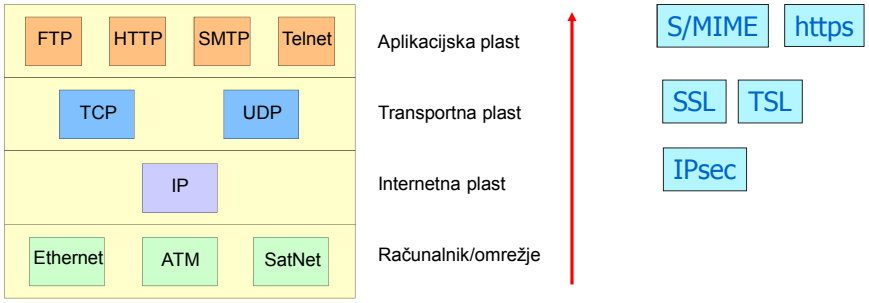
Varne komunikacije po Internetu

- **Plasti** in protokoli
- Varnost na **omrežni plasti**
  - IPsec
  - VPN
- Varnost na **transportni plasti**
  - SSL
  - TSL
- Varnost na **aplikacijski plasti**
  - varna elektronska pošta
    - S/MIME
    - PGP

Plasti in protokoli

osnovni internetni protokoli:

dodani varnostni protokoli:



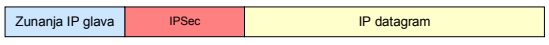
IPsec

IP Security (IPsec) omogoča varovanje na omrežni plasti.

IPsec deluje na dva možna načina:

- IPsec transportni način ohranja glave IP paketov nespremenjene, šifrira se samo vsebina paketa
- IPsec tunelski način dodaja novo glavo IP paketom, stara glava in vsebino paketa pa se prenašata v šifrirani obliki. Varovana komunikacija poteka med parom prehodov (gateway to gateway), ki jih naslavljajo dodane glave IP paketov.

Transportni način

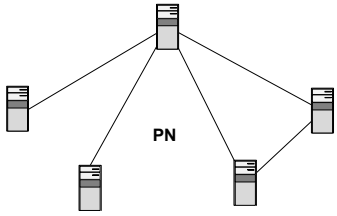


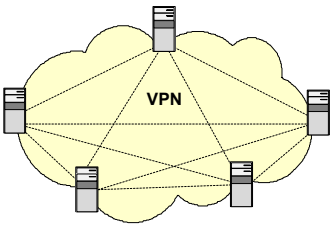
Tunelski način

VPN

VPN je navidezno zasebno omrežje (Virtual Private Network)

- Povezave v navideznih zasebnih omrežjih so dinamične in navidezne. Potekajo kot tuneli po javni TK infrastrukturi.
- Varno komunikacijo zagotavlja tunelski protokol, na primer IPsec.





Svetovni splet

- Svetovni splet = WWW (World Wide Web) je porazdeljen informacijski sistem. Sestavlja ga množica spletnih strani na strežnikih, ki so povezani v Internet.
- HTTP (Hypertext Transfer Protocol) je protokol za prenos spletnih strani med spletnim strežnikom in brskljalnikom. HTTP deluje na aplikacijski plasti. HTTP deluje podobno kot FTP in SMTP:
  - prenaša datoteke podobno kot FTP
  - sporočila med strežnikom in klientom so podobna kot pri SMTP,
  - HTTP prenaša sporočila direktno, SMTP pa po principu shrani in pošlji naprej
- HTML (Hypertext Markup Language) je programski jezik, ki ga uporabljamo za opis spletnih strani. HTML uporablja samo ASCII znake, kar omogoča največjo možno prilagodljivost.

Varna komunikacija po spletu

- SSL (Secure Socket Layer) je razvil Netscape za varno komunikacijo med spletnim klientom in strežnikom. SSL podpira preverjanje identitete strežnika. V komunikaciji se za vsako sejo ustvari varni kanal. SSL zagotavlja varno komunikacijo na transportni plasti.
- TLS (Transport Layer Security) je standardizirana (IETF) zamenjava za SSL.
- TLS_v1 in SSL_v3 sta si zato zelo podobna, razlike so sicer zelo majhne, vendar nista interoperabilna

SSL, TLS

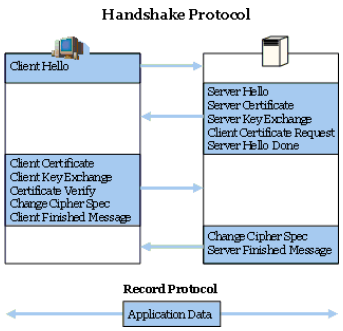
- SSL in TLS imata dve plasti: handshake in record
  - **Handshake** protokol določa vrsto sporočil za dogovor varnostnih parametrov, ki se bodo uporabili za podatkovni prenos v seji.
  - Klient in strežnik dogovorita uporabo varnostnih mehanizmov ob izmenjavi prvih sporočil: Client Hello , Server Hello

    Poziv klienta= Client Hello:
    ClientVersion 3,1
    ClientRandom[32]
    SessionID: None (new session)
    Suggested Cipher Suites:
    TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA Suggested Compression Algorithm: NONE

    Odgovor strežnika = Server Hello:
    Version 3,1
    ServerRandom[32]
    SessionID: bd608869f0c629767ea7e3ebf7a63bdcffb0ef58b1b941e6b0c044acb6820a77
    Use Cipher Suite:**TLS_RSA_WITH_3DES_EDE_CBC_SHA**
    Compression Algorithm: NONE

SSL, TLS

- Strežnik pošlje digitalno potrdilo z javnim ključem, ki služi za avtentikacijo strežnika in za šifriranje sporočil. Klient tako lahko preveri tudi ujemanje imena strežnika. Strežnik zahteva avtentikacijo klienta (opcija).
- Klient na zahteva pošlje svoj certifikat in za tem še z javnim ključem strežnik šifrirano sporočilo ki omogoča generacijo glavnega ključa. Klient podpiše izvleček vse komunikacije in s tem omogoči lastno avtentikacijo = Certificate verify. Klient potrdi, da bo nadaljna komunikacija potekala šifrirano z dogovorjenimi parametri.
- Strežnik obvesti klienta, da bo nadaljna komunikacija šifrirana v skladu z dogovorom
- **Record protokol** obdeluje podatkovni niz aplikacijske plasti. Podatkovni niz se razdeli na označene podatkovne bloke in obratno združuje v pravi vrstni red. Sledi lahko kompresija blokov, za tem pa šifriranje blokov. Verodostojnost podatkov se preverja z računanjem MAC.



Varna komunikacija po spletu

- https ni poseben protokol, pač pa pomeni da HTTP poteka preko varne transportne plasti: SSL, TLS !
- S-HTTP (Secure Hypertext Transfer Protocol) je poseben protokol, ki deluje na aplikacijski plasti. Namesto ustvarjanja varnega kanala kot pri SSL se pri S-HTTP šifrira vsako sporočilo posebej. S-HTPP podpira dvosmerno preverjanje identitete.

Elektronska pošta

- SMTP je protokol za izmenjavo elektronske pošte med poštnimi strežniki (Simple Mail Transfer Protocol)
- SMTP modul (strežnik) sprejme sporočilo o naslovu prejemnika in ga preko FTP pošilja SMTP modulu naslovljenega strežnika. Ko se identificira naslov prejemnikovega poštnega strežnika, se poštno sporočilo usmerja po internetnem protokolu (TCP/IP).
- Na strani prejemnikovega strežnika se poleg SMTP uporablja še dodatni protokol, ki omogoča delovanje uporabnikovega poštnega nabiralnika:
  - POP3 (Post Office Protocol ver.3) ali
  - IMAP (Internet Message Access Protocol)
- Uporabnik elektronske pošte uporablja SMTP protokol za pošiljanje in POP3 ali IMAP za sprejemanje poštnih sporočil.
- MIME (Multipurpose Internet Mail Extension) je dodatni protokol za izmenjavo podatkov, ki niso v ASCII formatu. MIME določa nabor funkcij za pretvorbo v ASCII in obratno.

Varna elektronska pošta

- PEM (Privacy Enhanced Mail) je standard za varno elektronsko pošto. PEM določa način šifriranja pri izmenjavi e-pošte. PEM uporablja CA certifikate.
- MOSS (MIME Object Security Service) je zamenjava standarda PEM, ki nudi povezavo med poštnimi naslovi in certifikati. MOSS omogoča tudi varno izmenjavo priponk v elektronski pošti.
- S/MIME (Secure/Multipurpose Internet Mail Extentions) je varna izboljšava standarda za format elektronske pošte MIME.
  - S/MIME uporablja X-509 infrastrukturo javnih ključev
  - S/MIME je zelo prilagodljiv in omogoča uporabo različnih simetričnih in asimetričnih šifrirnih postopkov
- PGP (Pretty Good Privacy) zagotavlja
  - tajnost s šifriranjem sporočil
  - avtentičnost z digitalnim podpisom