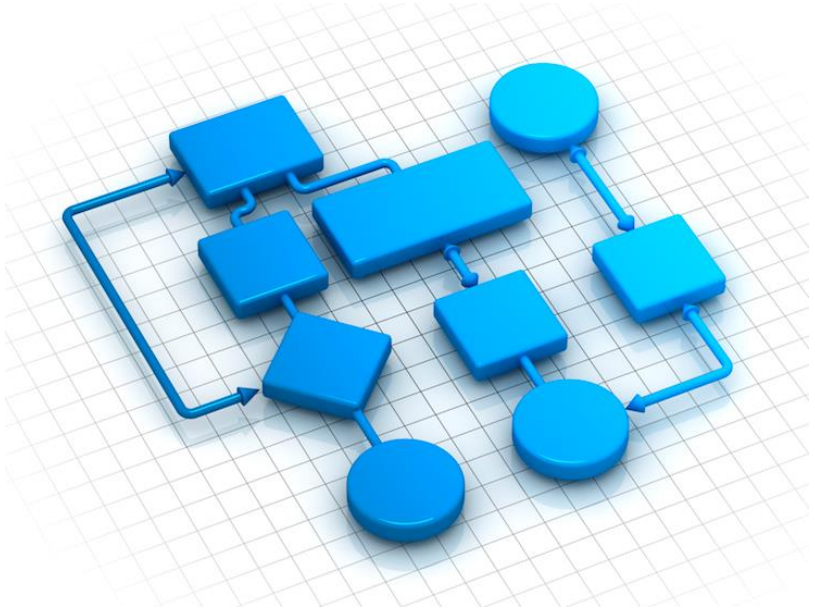
<RSA> Sigurnost informacijskih sistema </RSA>

<AES> predavanja </AES>

<CISSP> Sigurnosni protokoli </CISSP>



Summary

- Uvod u protokole
- Komponente sigurnosnih protokola
- Primjeri sigurnosnih protokola u IT

Lekcija 1. Uvod u protokole

- Šta su protokoli?
- Problemi sa protokolima
- Primjer greške u protokolu
- Idealan protokol
- Primjeri

Šta su protokoli?

- Protokol je niz precizno definisanih koraka koji definišu pravila unutar nekog sistema.
  - Protokol nije nešto što je usko vezano za informacijske tehnologije
    - Ponašanje unutar aerodroma, vožnja automobila, polaganje ispita i sl.
- Sigurnosni protokol je niz koraka koji osiguravaju zaštitu informacijskih resursa
  - Uglavnom se misli na zaštitu podatke
- Sigurnosni protokoli u IT-e su usko vezani za pravila komunikacije između korisnika unutar informacijskih sistema
  - Većina implementacija je vezana za mrežu

Problemi sa protokolima

- Vrlo je teško predvidjeti sve moguće scenarije i implementirati ih u protokol
- Potencijalni problemi nisu vidljivi u datom trenutku
- Greške i propusti se teško mogu primjetiti
- Mnoge ozbiljne implementacije imaju svoje poznate i manje poznate propuste
- Uglavnom se radi o vrlo kompleksnim implementacijama
- Protokol konceptualno može izgledati jednostavno
- Zavisnost od različitih tehnologija
  - Softver i hardver
- Veliki broj sigurnosnih problema je nastao zbog greške u protokolu
  - Potrebna je konstantno vršiti monitoring i raditi provjere
- Open source zajednica je vrlo dobro rješenje

Primjer problema u protokolu...

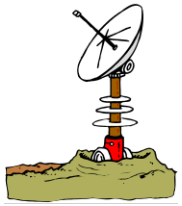
Ruski
MIG

Angola

SAAF
Impala
K

2. E(N,K)

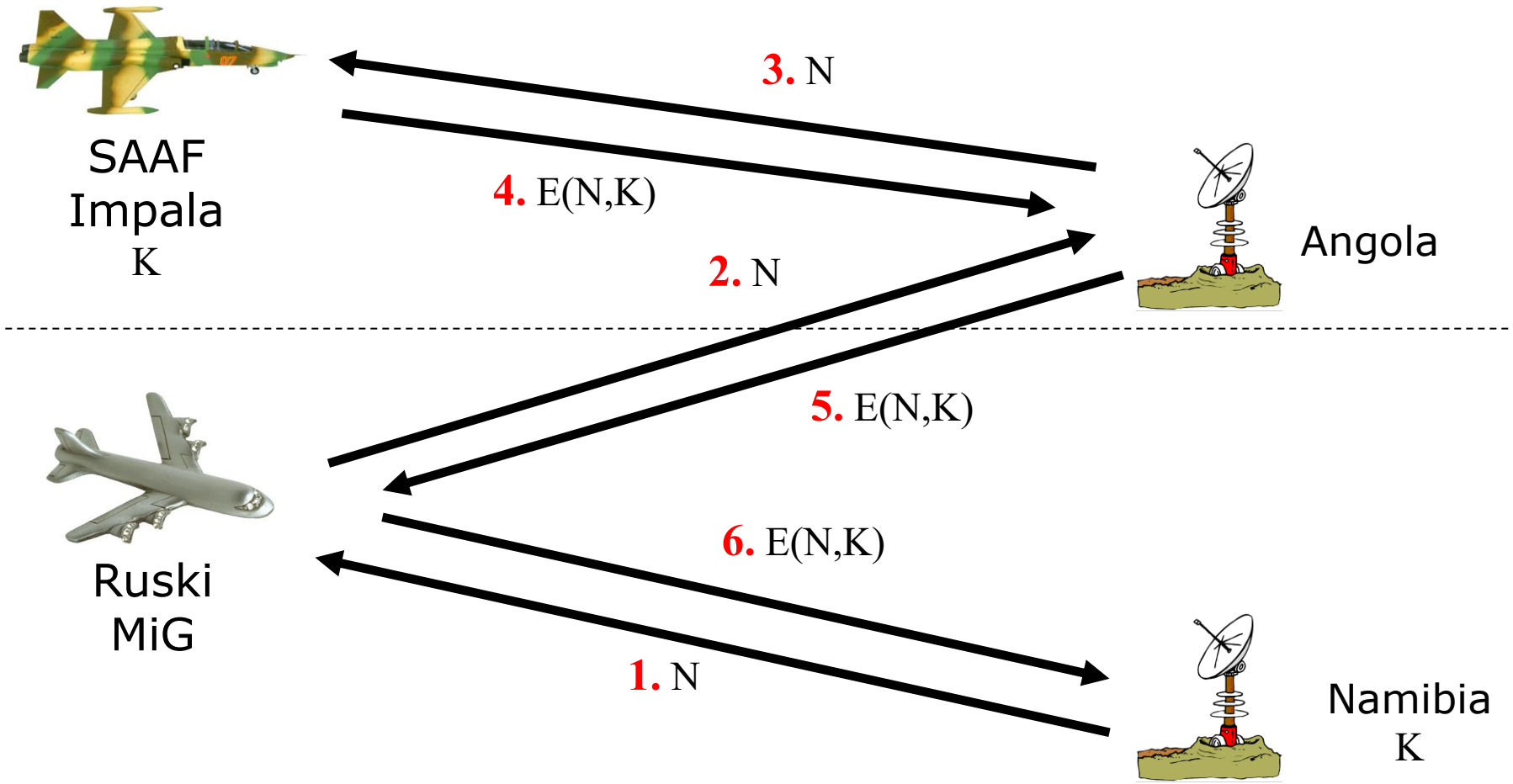
1. N



Namibia
K

IFF protokol - Identify Friend or Foe

...primjer problema u protokolu



IFF propust (MiG in the Middle)

Idealan protokol

- **Sveobuhvatan**
  - Zadovoljiti sve sigurnosne zahtjeve
  - Zahtjevi trebaju biti vrlo precizno definisani
- **Efikasan**
  - Minimalni zahtjevi po pitanju procesiranja pojedinih dijelova
  - Minimalni zahtjevi po pitanju mrežnog prometa
- **Robustan**
  - Radi i u slučajevima napada
  - Otporan na izmjene u sistemu
- **Jednostavan**
  - Lagan za implementaciju, korištenje, nadogradnju, prilagođavanje i fleksibilan
- Vrlo je teško zadovoljiti sve navedene elemente

Primjer 1: Provjera ulaska u vojni bazu

1. Provucite karticu kroz čitać
2. Unesite PIN
3. PIN ispravan ?

   Da? Ulazak je dozvoljen

   NE? Akcija straže

Primjer 2: Bankomat

1. Ubacite karticu
2. Unesite PIN
3. PIN ispravan ?

   Da? Dozvoljen pristup novčanim transakcijama

   Ne? Akcija bankomata (uzimanje kartice, drugi pokušaj i sl.)

Lekcija 2. Komponente sigurnosnih protokola u IT

- Kontrola pristupa
- Enkripcija
- Upravljanje ključevima
- Integritet sadržaja

Kontrola pristupa

- Osnova svakog sigurnosnog protokola jeste „Access control“
- Sastoji se iz dvije komponente:
  - Autentifikacija
  - Autorizacija
- Autentifikacija jeste provjera identiteta korisnika, servisa, resursa...
  - Nije baš tako jednostavno
- Autorizacija
  - Provjera prava pristupa pojedinim resursima

Enkripcija

- Kombinacija različitih metoda pretvaranja čitljivog teksta u nečitljiv i obrnuto
- Osnova svih sigurnosnih protokola
  - Primjena izlazi mnogo izvan tog opsega
- Kriptografija
  - Simetrična
  - Asimetrična
- Stenografija
  - Sakrivanje sadržaja

Upravljanje ključevima

- Proces koji je usko vezan za kriptografiju
- Rješava problem distribucije ključeva između učesnika u komunikaciji
- Skoro svaki sigurnosni protokol u IT ima ovu komponentu
- Obično se osigurava kombinacijom simetrične i/ili asimetrične enkripcije
- Termini kao što su:
  - https
  - Session key
  - Diffie-Hellman
- ...usko su vezani za ovu problematiku

Integritet sadržaja

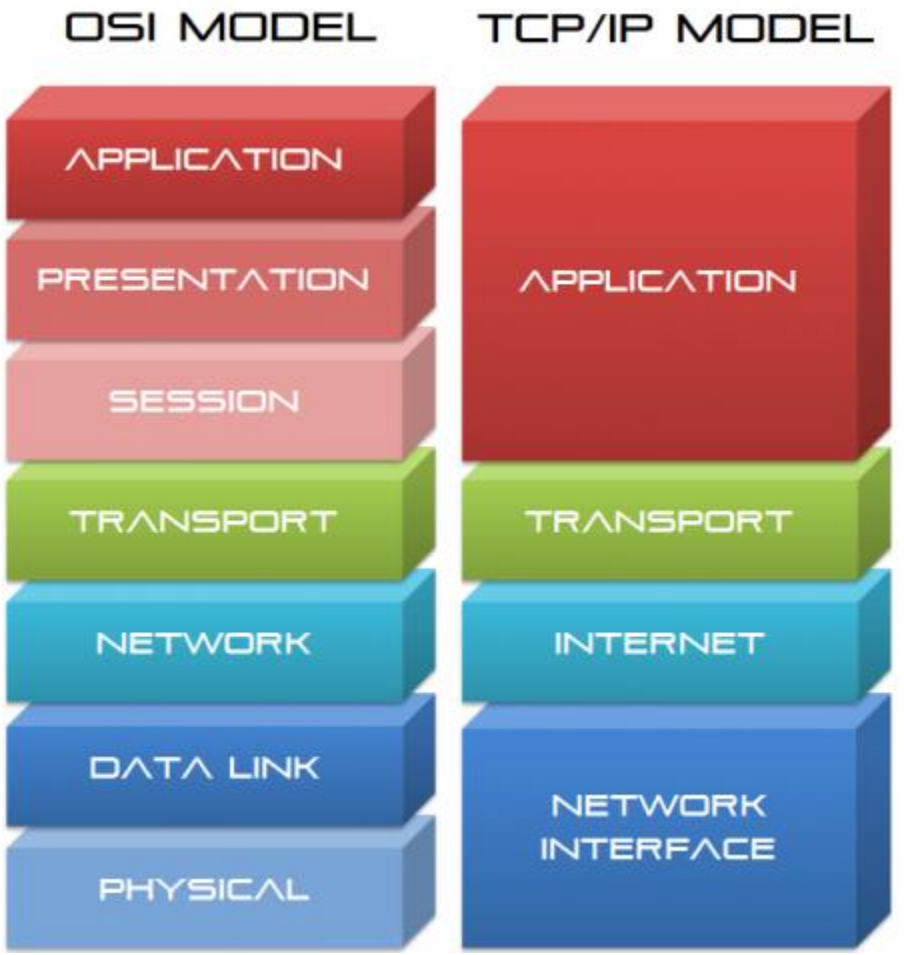
- Integritet je bitan u komunikaciji
- Koncept akcija, vrijednosti, metoda i principa u cilju osiguranja integriteta
  - Da li je došlo do promjene izvornog sadržaja – autentičnost poruke
  - Da li komuniciramo sa pravom osobom – autentičnost osobe
  - Ko je garant komunikacije – certified authority
- Jedan od izazova na koje dizajneri protokola trebaju odgovoriti jeste integritet
- Napadi kao što su:
  - Man in the middle
  - ARP poisoning
  - Session hijacking

Lekcija 3. Primjeri sigurnosnih protokola u IT

- TCP/IP
- SSH
- SFTP
- TLS/SSL
  - HTTPS
- IPSec/PPTP
- ...

TCP/IP

- Glavni komunikacijski protokol
- Kompletan internet leži na njegovim temeljima
- Sigurnost nije bila primarna u trenucima razvoja

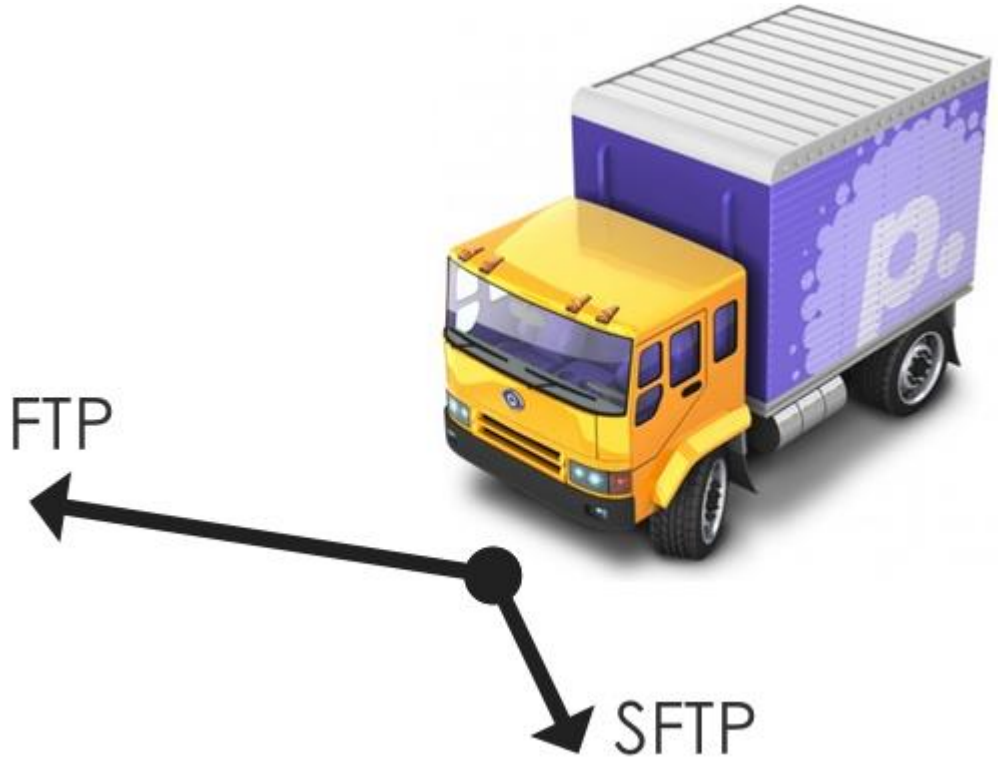


SSH - Secure Shell

- Primjena kriptografije u nesigurnim mreženim okruženjima
- Primarno je konzolni interfejs
- Prijava na udaljenje računare sa ciljem administracije
- Linux
- Zamjena za Telnet

SFTP

- Tradicionalni FTP protokol nije siguran
  - Clear tekst format
  - Fajlovi su vidljivi u transportu i na serveru
- Secure File Transfer Protocol rješava ove probleme
  - Primjena kriptografije
- Postoje konzolne i GUI implementacije

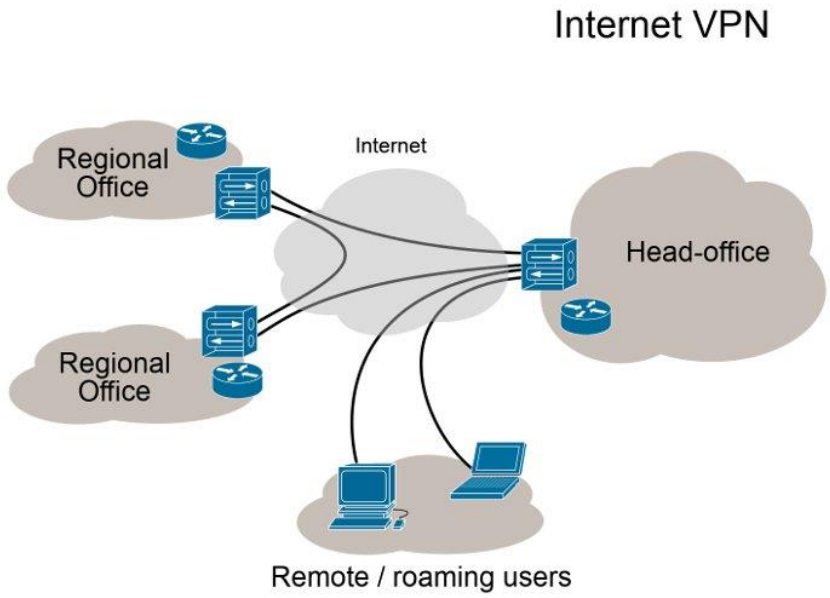


TLS/SSL

- Kriptografski protokoli za osiguranje sigurne komunikacije
  - Uglavnom se koristi na internetu
  - SSL je starija verzija
  - TLS je SSL nasljednik
- Zasniva se na asimetričnoj enkripciji

IPSec/PPTP

- Ova dva protokola se koriste za uspostavu VPN saobraćaja
- VPN omogućava proširenje internih LAN mreža preko interneta
  - Udaljeni pristup resursima unutar LAN okruženja
- Kreira se enkriptovani tunel između dvije tačke u komunikaciji
- Danas se VPN koristi i za anonimno surfanje internetom



Pitanja