

ОДБРАМБЕНЕ БЕЗБЕДНОСНЕ ОПЕРАЦИЈЕ

*Универзитет у Крагујевцу
Лицеја Кнежевине Србије 1А 34000 Крагујевац*

Prof dr Igor Franc

Predavač / Digitalni forenzičar / Etički haker / Preduzetnik

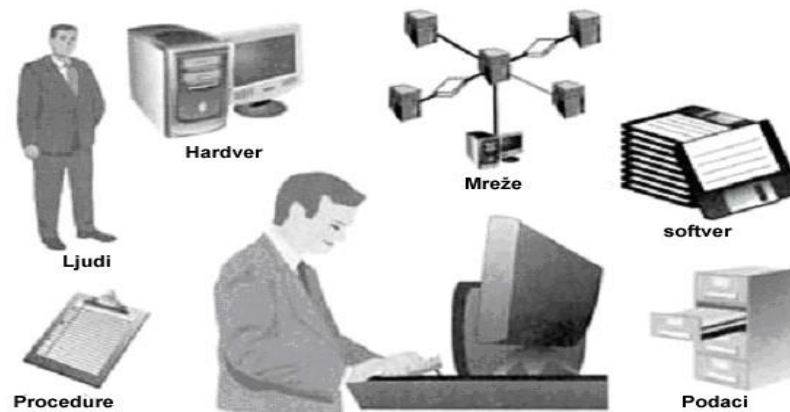


-
- Tim predavača
 - Komponente bezbednosti informacija
 - Kontrola pristupa mrezi
 - Sistemi zaštite
 - Višefaktorska autentifikacija
 - Kriptografija
 - Fizička bezbednost

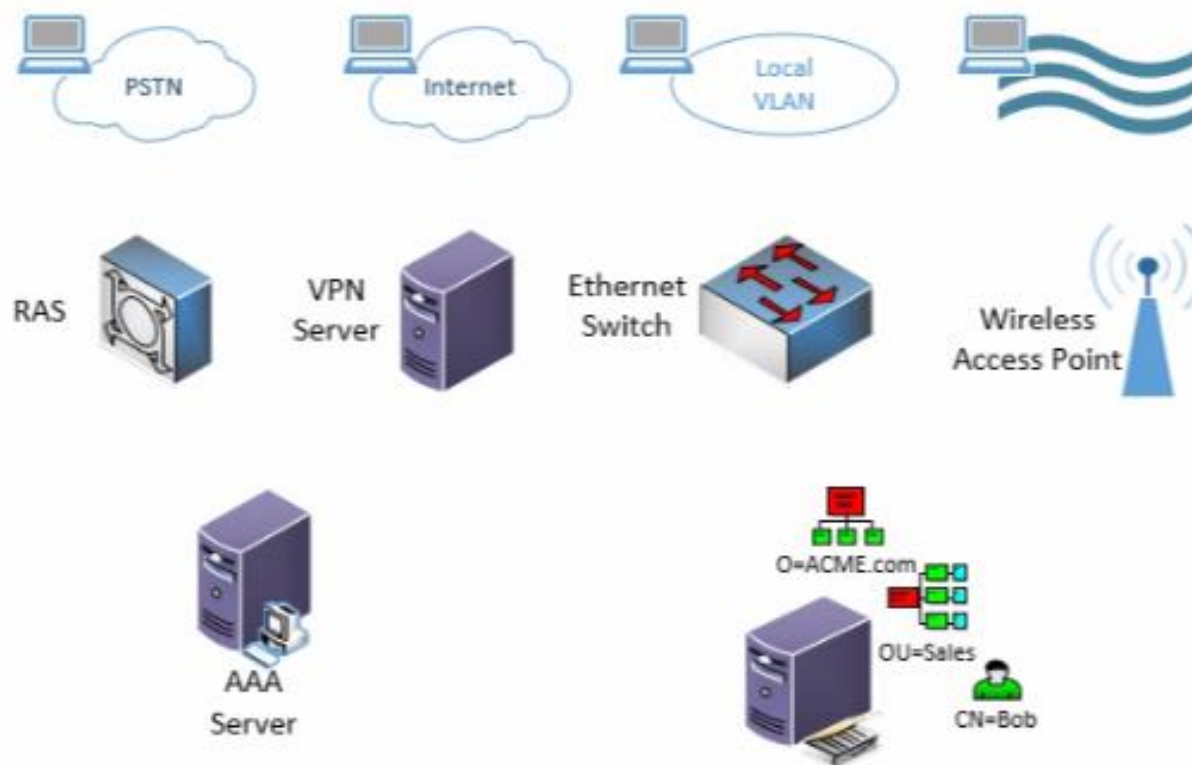
- Prof dr Igor Franc
- Uroš Babić – MCT instruktor
- Vladan Todorović
- Mikica Ivošević
- Aleksandar Mirković



- Informacioni sistem ne čini samo hardver računara; on je potpun skup softvera, hardvera, podataka, ljudi, procedura i mreže.



Kontrola pristupa mrezi





-
- Zastitni zidovi - firewall
 - Sistemi za detekciju/prevenciju upada
 - Lazni mamci – Honeypot
 - Višefaktorska autentifikacija
 - Menadžeri lozinki
 - Wi-Fi enterprise rešenja
 - Penetraciono testiranje
 - Klasifikacija i označavanje informacija
 - Dodatne kontrole

Zastitni zidovi - firewall

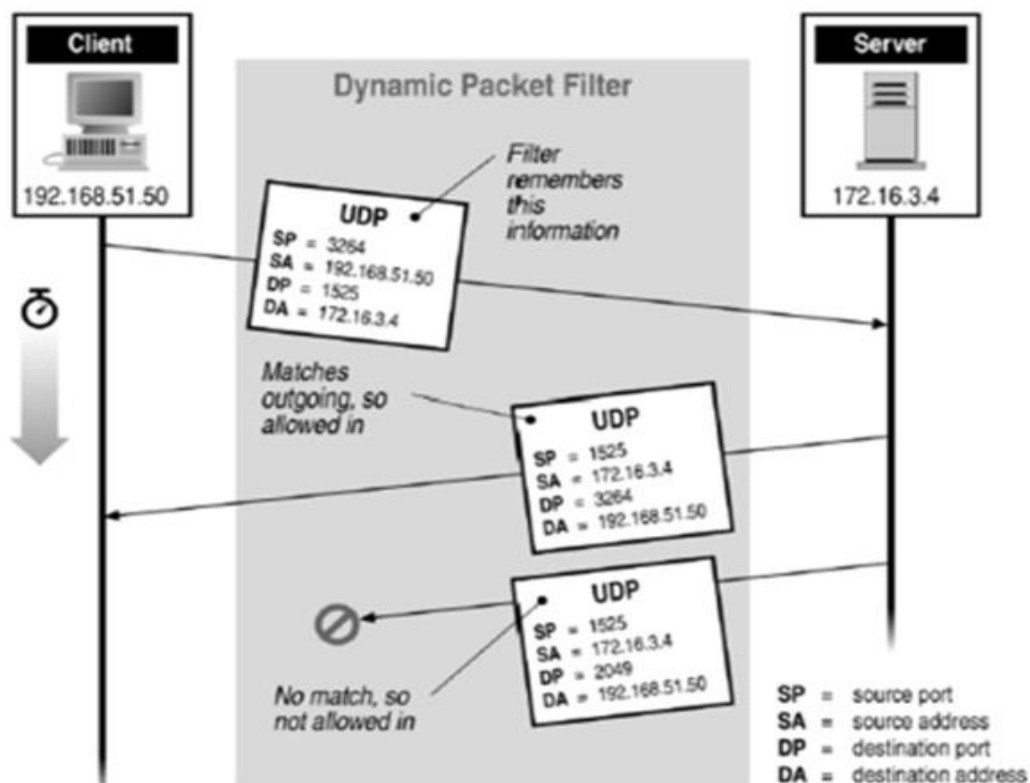


Mrežne barijere Firewall

- Softverski zaštitni zidovi (lokalni)
- Hardverski zaštitni zidovi (mrežni)
- Dinamičko ispitivanje paketa
- Nesigurni protokoli i portovi



Dinamičko ispitivanje paketa

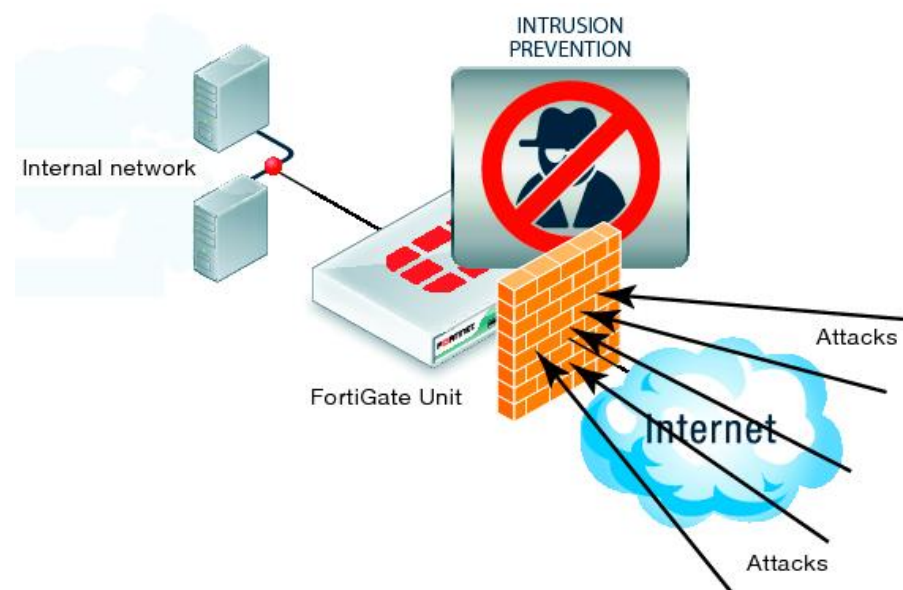


Nesigurni protokoli i portovi

- FTP (File Transfer Protocol) – port 21 i 20
- SFTP (Simple File Transfer Protocol) – port 115(tcp)
- TFTP (Trivial File Transfer Protocol) – port 69(udp)
- Telnet – port 23 (zamena sa sifrovanjem SSH – port 22)
- HTTP – port 80 (zamena https – port 143)
- NetBIOS – port 137,138 i 139 (microsoft)
- SNMP (Simple Network Management Protocol) v1 i v2 – port 161
- SMTP – port 25
- POPv3 – port 110
- IMAP – port 143



Sistemi za detekciju/prevenciju upada



Sistemi za detekciju/prevenciju upada

- Detekcija upada
- Sistemi za detekciju/prevenciju upada bazirani na hostu (HIDS/HIPS)
- Mrežni sistemi za detekciju/prevenciju upada (NIDS/NIPS)

Detekcija upada

- Ukoliko je upad detektovan dovoljno brzo, napadač je identifikovan, pre nego što nastupi oštećenje sistema. Naime, što je brže napadač detektovan, manji je stepen oštećenja, a sistem se brže oporavlja.
- Sistem sa efektivno sprovedenom detekcijom upada sprečava i deluje preventivno na napadača. Detekcija upada omogućava kolekciju informacija o tehnikama napada koje se mogu upotrebiti da se brzo ojača prevencija upada.

Lazni mamci - Honeypot

- Vrste laznih mamaca (low/high)
- Lokacije laznih mamaca
- Mreza laznih mamaca (Honeynet)



Vrste laznih mamaca

Types of Honeypots

Low Interaction

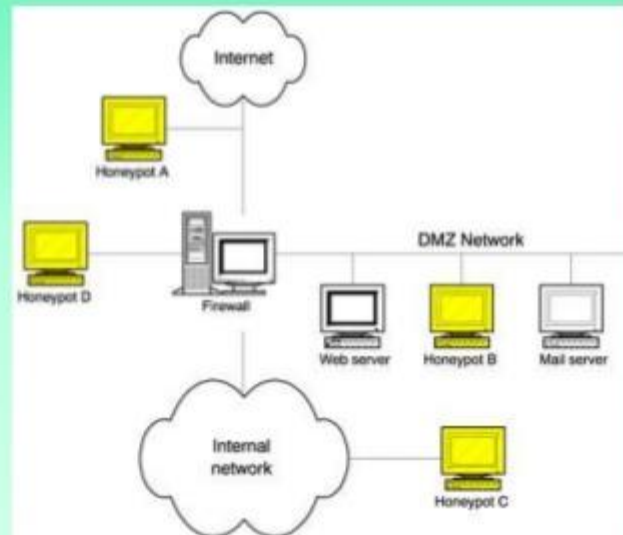
- Usually an image running on a physical machine
- Used for logging intruders, distracting script kiddies and stopping automated attacks
- Less flexibility and risk

High Interaction

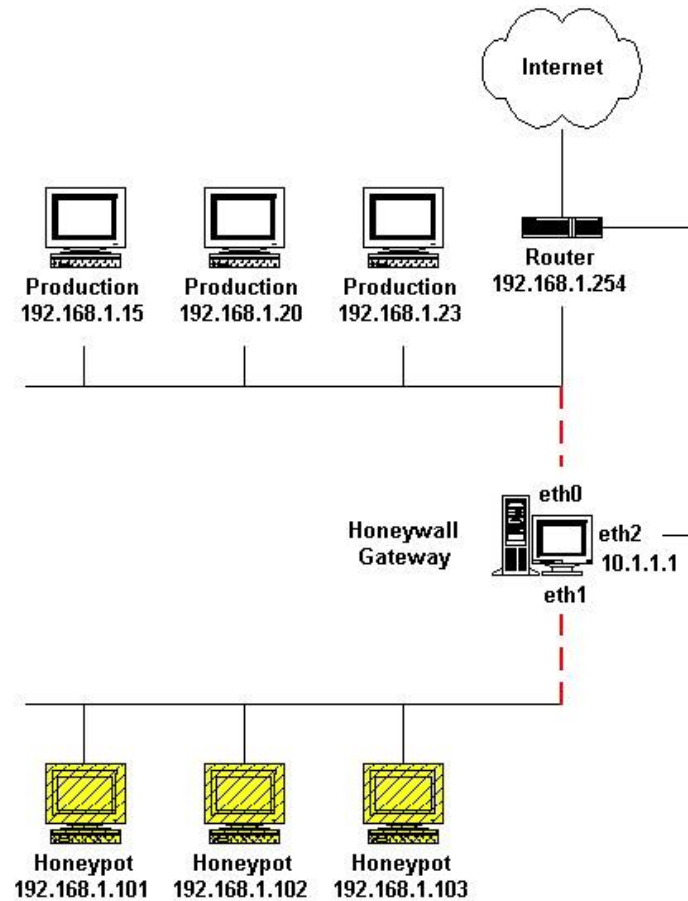
- Usually a physical machine
- Used for research purposes
- Highly Flexible in uses
- More risk

Location of Honeypots

- In front of the firewall
- Demilitarized Zone
- Behind the firewall (Intranet)

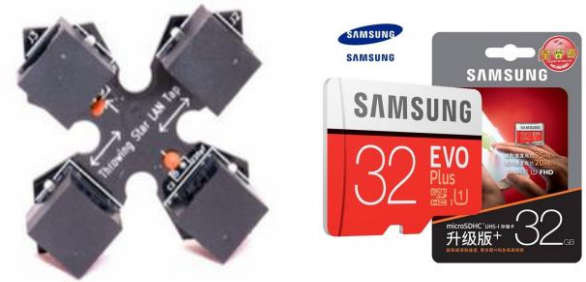
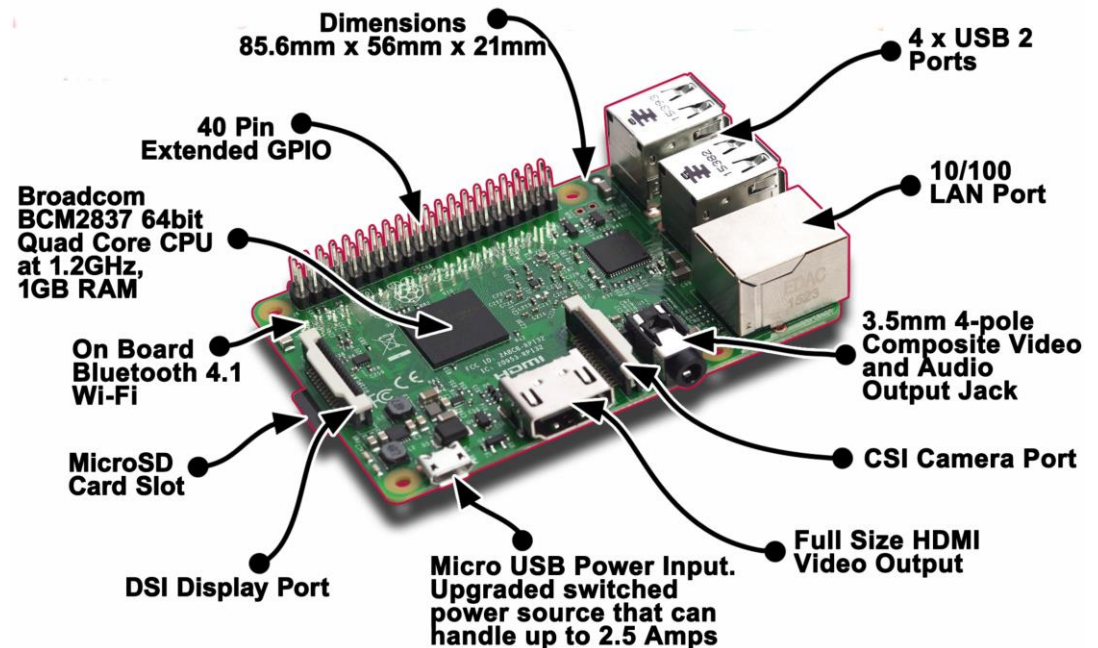


Mreza lazni mamaca Honeynet



Wireshark na Raspberry Pi 3

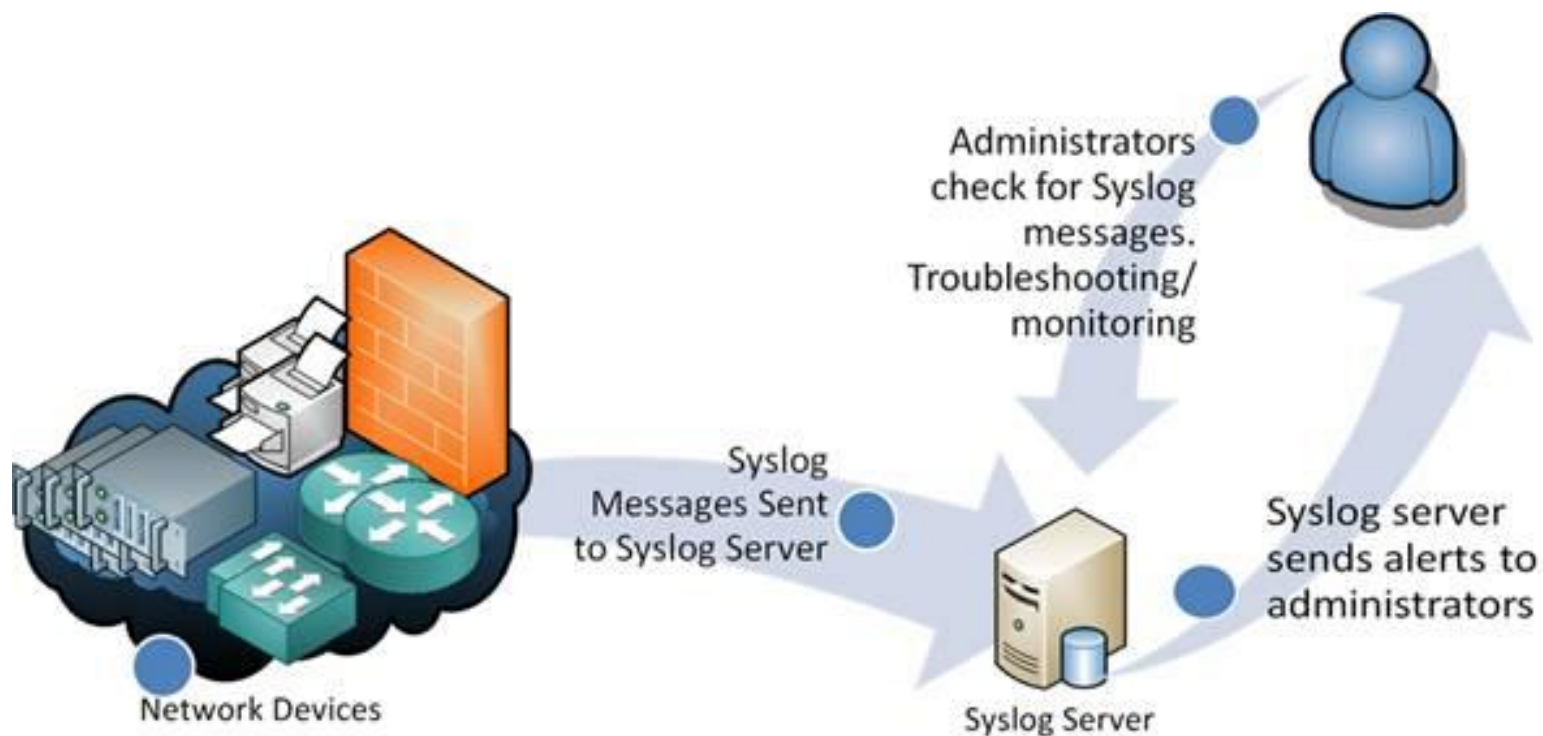
- Kali image arm
- VNC server
- Putty klijent



Nadzor mreže

- Logovanje aktivnosti na mrezi
- SIEM sistemi

Logovanje aktivnosti



Security information and event management - SIEM



Višefaktorska autentifikacija



Faktori autentikacije

- Nešto što korisnik zna (password, PIN...)
- Nešto što korisnik ima (smart kartica, mobilni...)
- Nešto što korisnik jeste (biometrija)
- Gde se korisnik nalazi (lokacija)
- Kako se korisnik ponaša (šta radi i kada)



Biometrijski sistemi zaštite

- Vrste biometrijskih sistema zaštite
- Top lista biometrijskih sistema zaštite
- Pokazatelji uspešnosti
- Prihvaćenost od strane korisnika
- Skener srca
- Skener hoda
- Biohakovanje

Vrste biometrijskih sistema zaštite



Iris Recognition



Retina Recognition



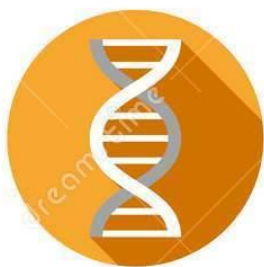
Face Recognition



Fingerprint Recognition



Voice Recognition



DNA Matching



Finger Geometry Recognition



Hand Geometry Recognition

Top lista biometrijskih sistema zaštite

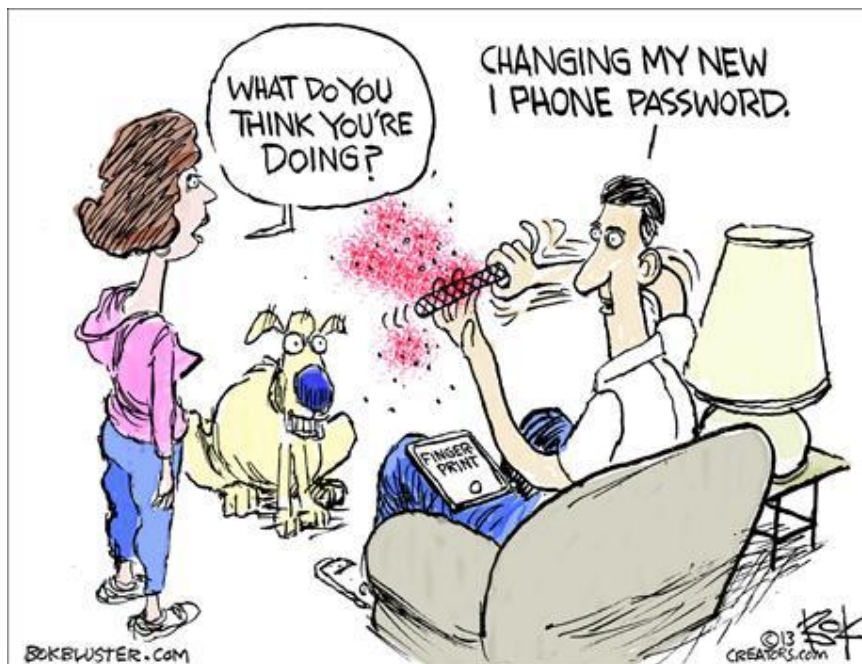
1. iris scan
2. retina scan
3. fingerprint recognition
4. hand recognition / geometry / topography
5. face recognition
6. voice recognition
7. signature recognition (potpis, pritisak olovke)
8. keystroke dynamics (dwell time - koliko dugo pritiska taster, flight time - koliko vreme je potrebno za prelazak sa tastera na taster)

Prihvaćenost od strane korisnika

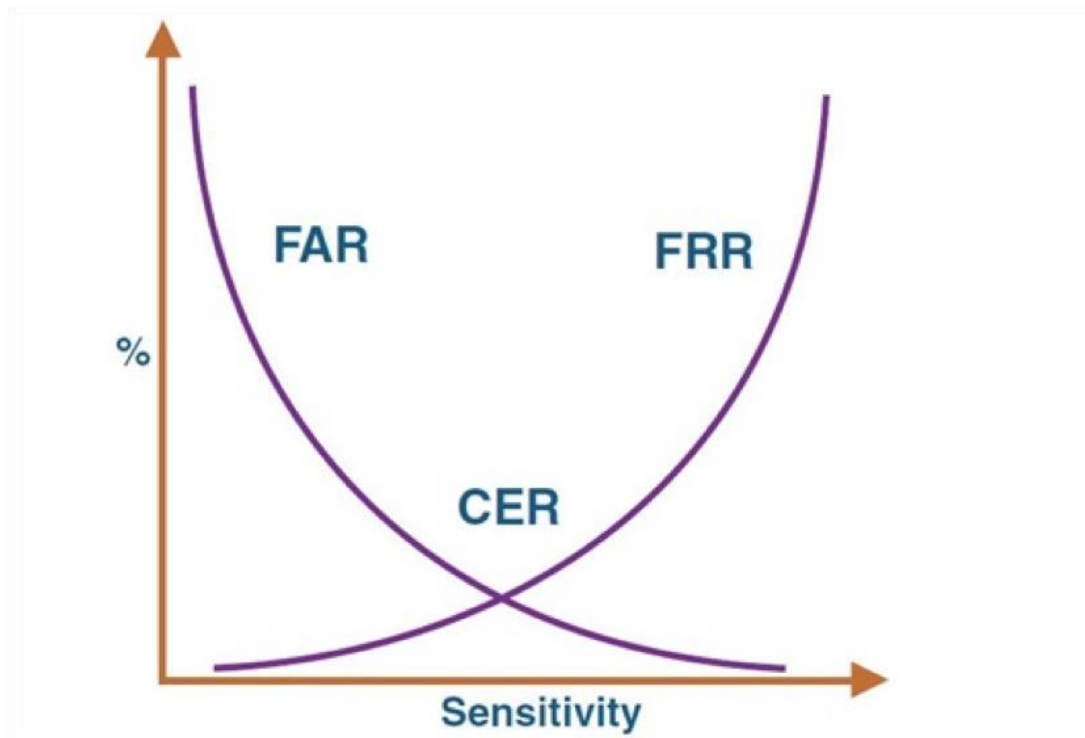
1. Behavior karakteristike

1. voice recognition
2. signature recognition
3. keystroke dynamics

2. Fizicke karakteristike



Pokazatelji uspešnosti

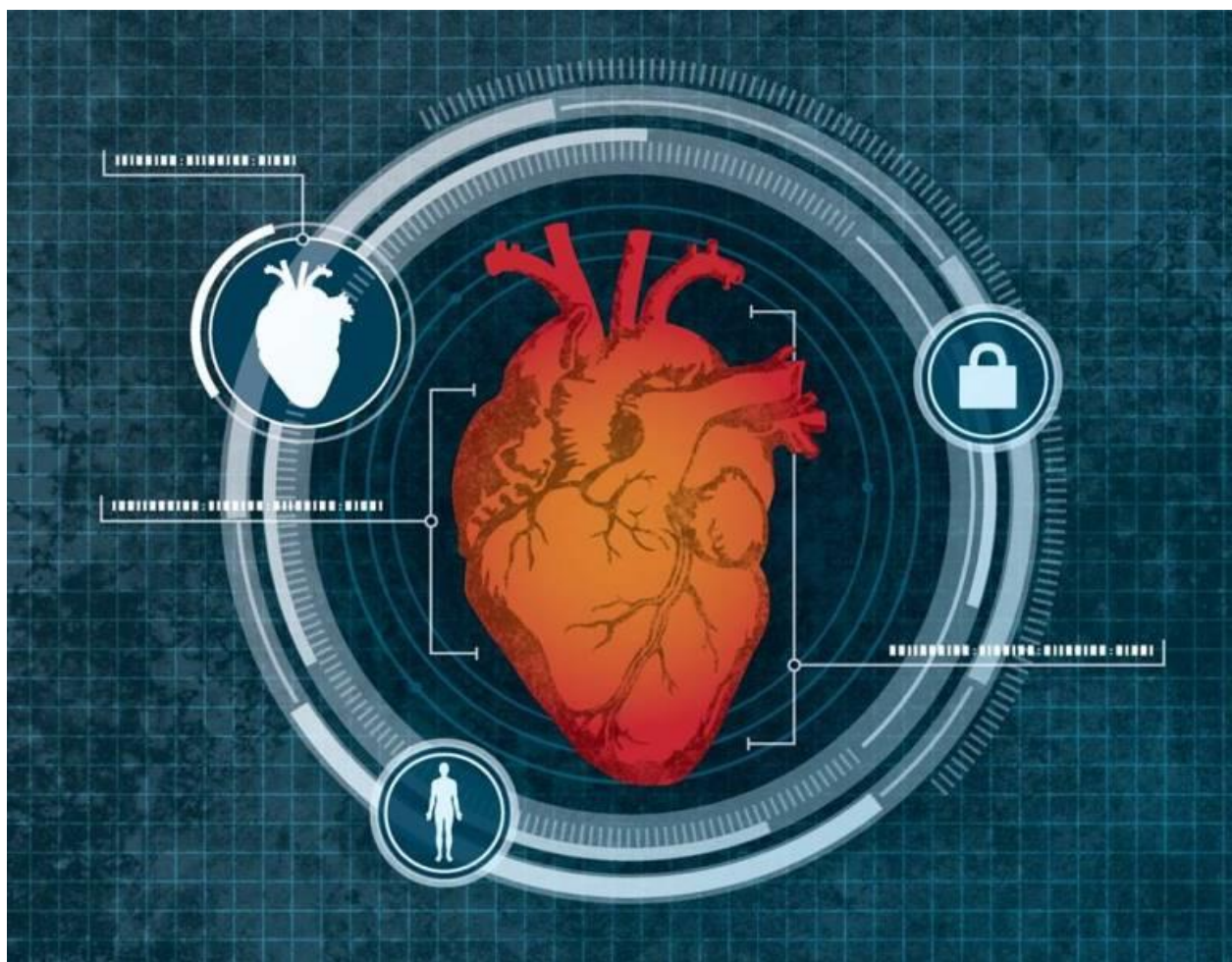


FRR (type 1) - false rejection rate
FAR (type 2) - false acceptance rate
CER – Crossover Error Rate

Skener hoda



Skener srca - Doppler radar



Biohakovanje



Mehanizmi za autentikaciju

- Tokens (hardver ili softver)
- Smart card (chip, memory)
- OTP (One Time Password)
- Multifactor authentication
- SSO (Single Sign-On)
- Kerberos protokol



Tokens



RSA SecurID SD600



RSA SecurID SID700



RSA SecurID SD200



RSA SecurID SID800



RSA SecurID SD520



BlackBerry with
RSA SecurID software token

Smart card



OTP - One Time Password

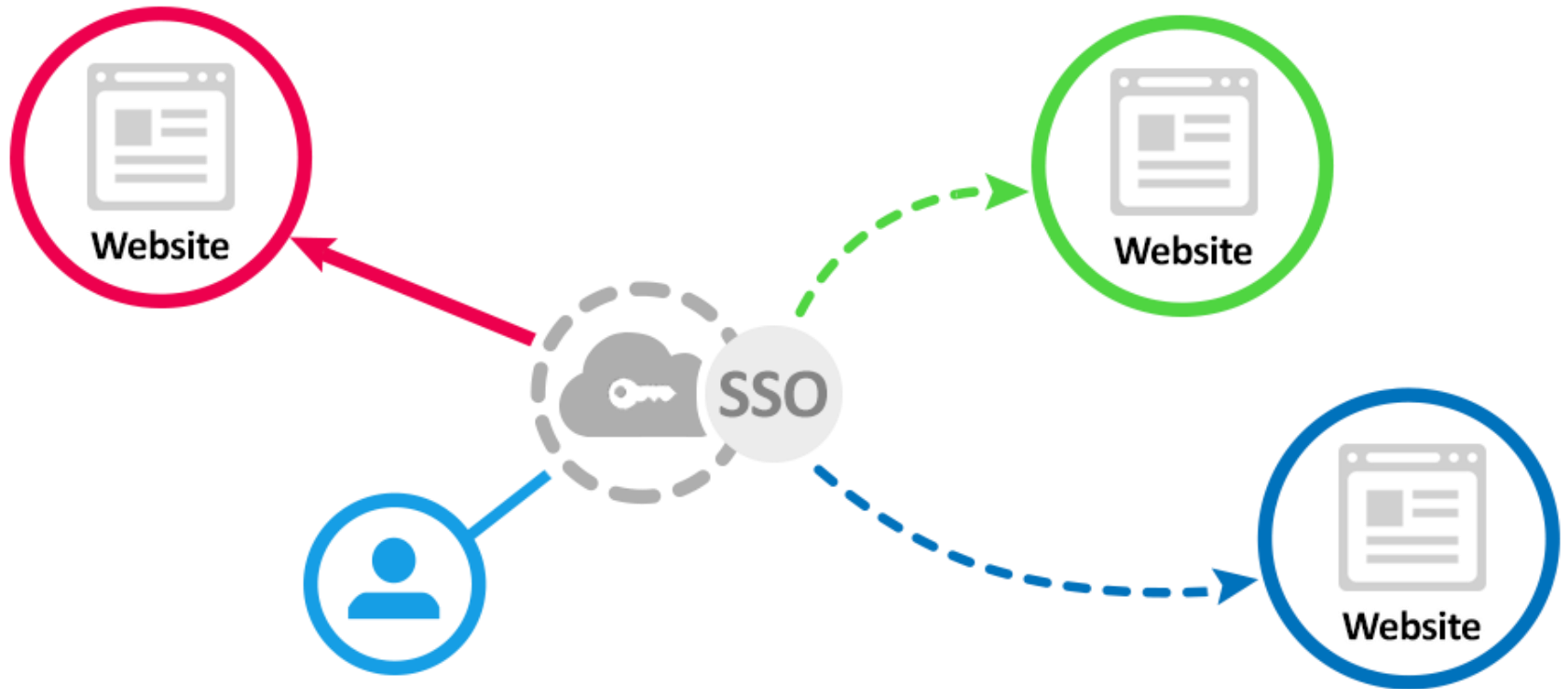
- TOTP – time based (uglavnom 60sec)
- HOTP – hash based (dogodaj)



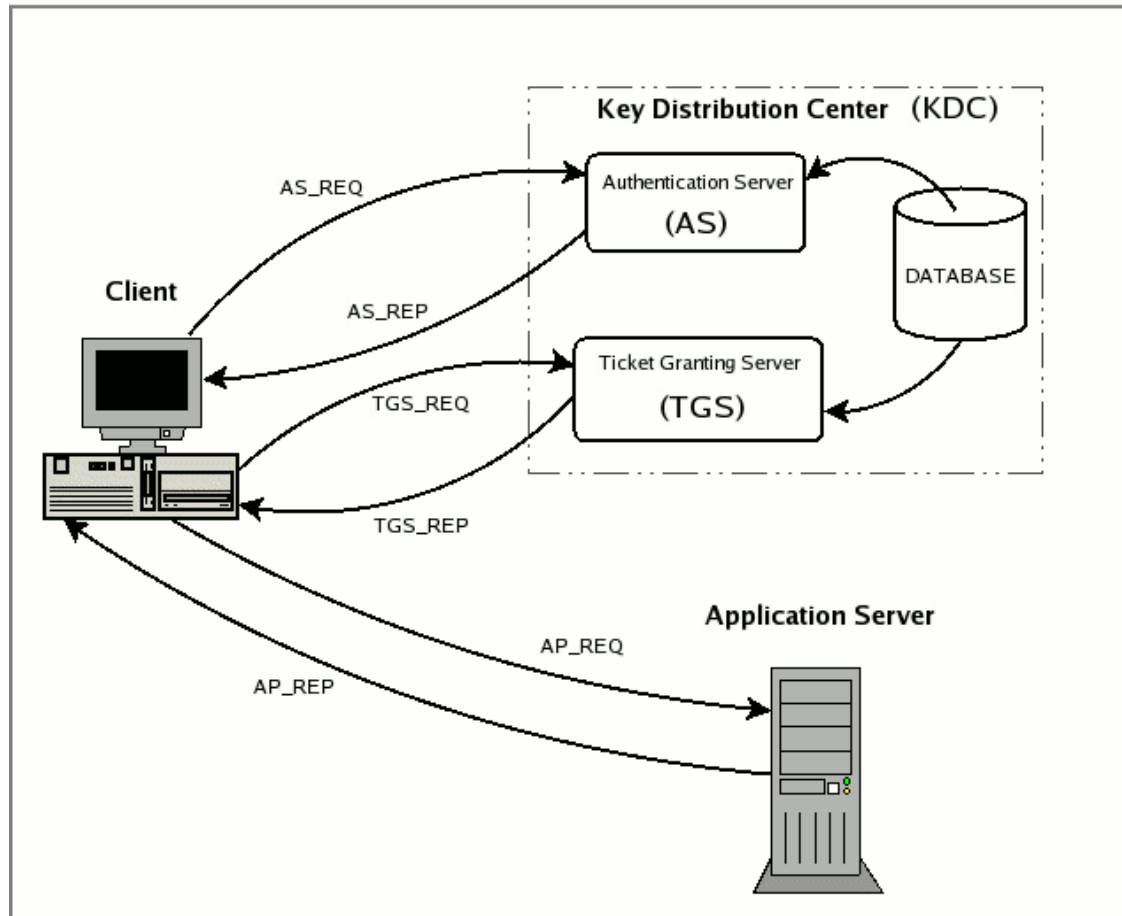
Multifactor authentication



SSO - Single Sign-On



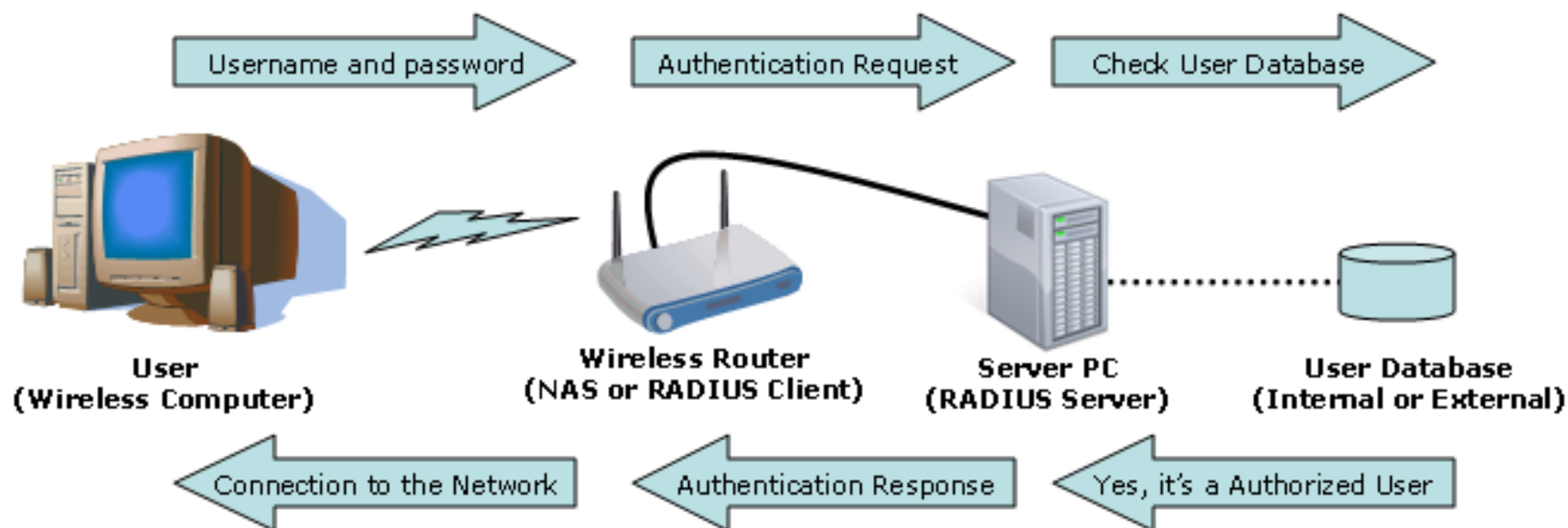
SSO - Kerberos



Menadžeri lozinki



Wi-Fi enterprise rešenja

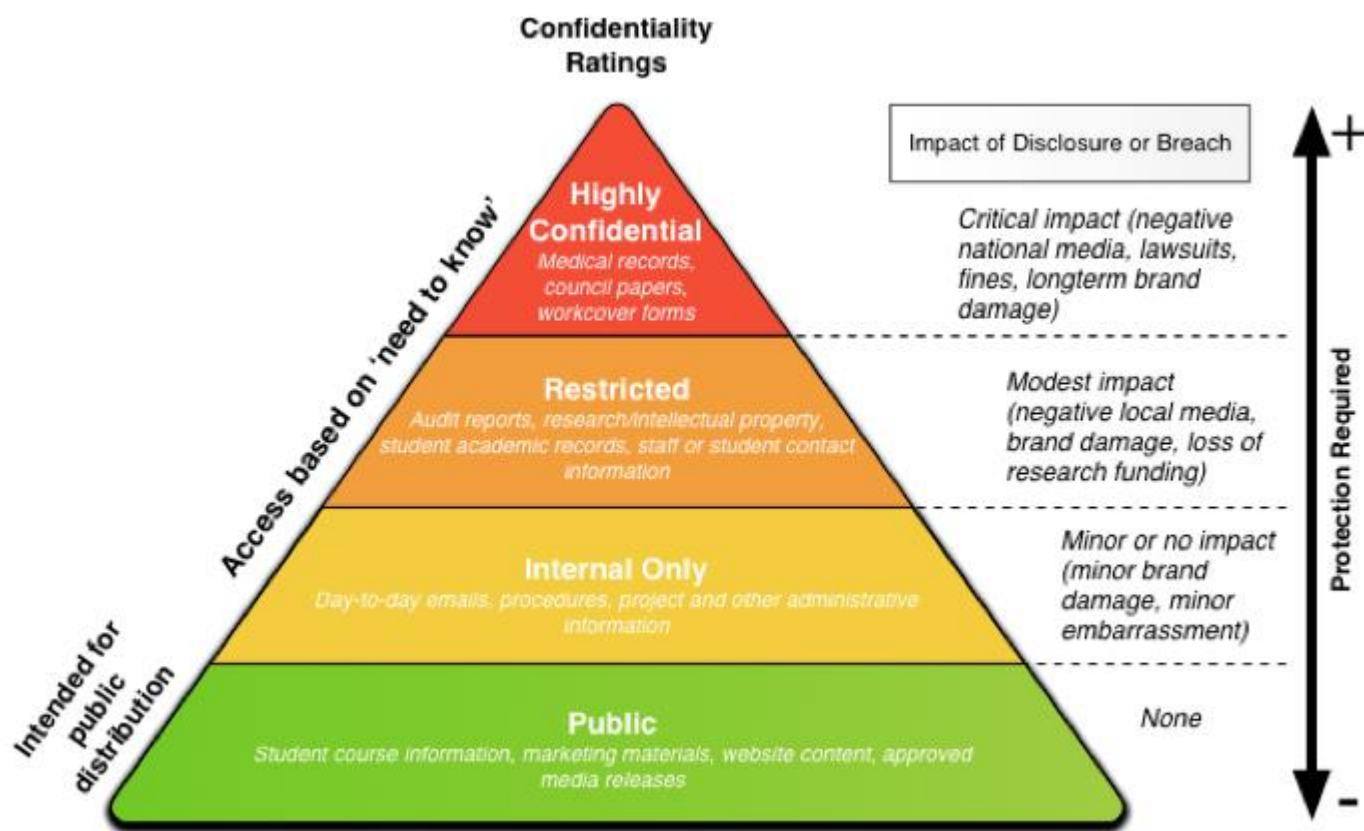


Penetraciono testiranje



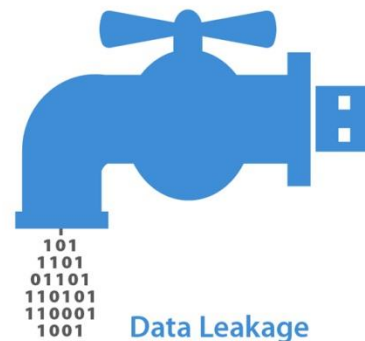
- Testiranje sistema na ranjivosti (Etičko hakovanje)
- Neophodna pismena saglasnost kompanije

Klasifikacija i označavanje informacija



Dodatne kontrole

- Podela dužnosti (separation of duties)
- Minimalne privilegije (least privilege)
- Obavezan odmor (mandatory vacations)
- Rotacija poslova (job rotation)
- Uvođenje DLP (Data Loss Prevention)



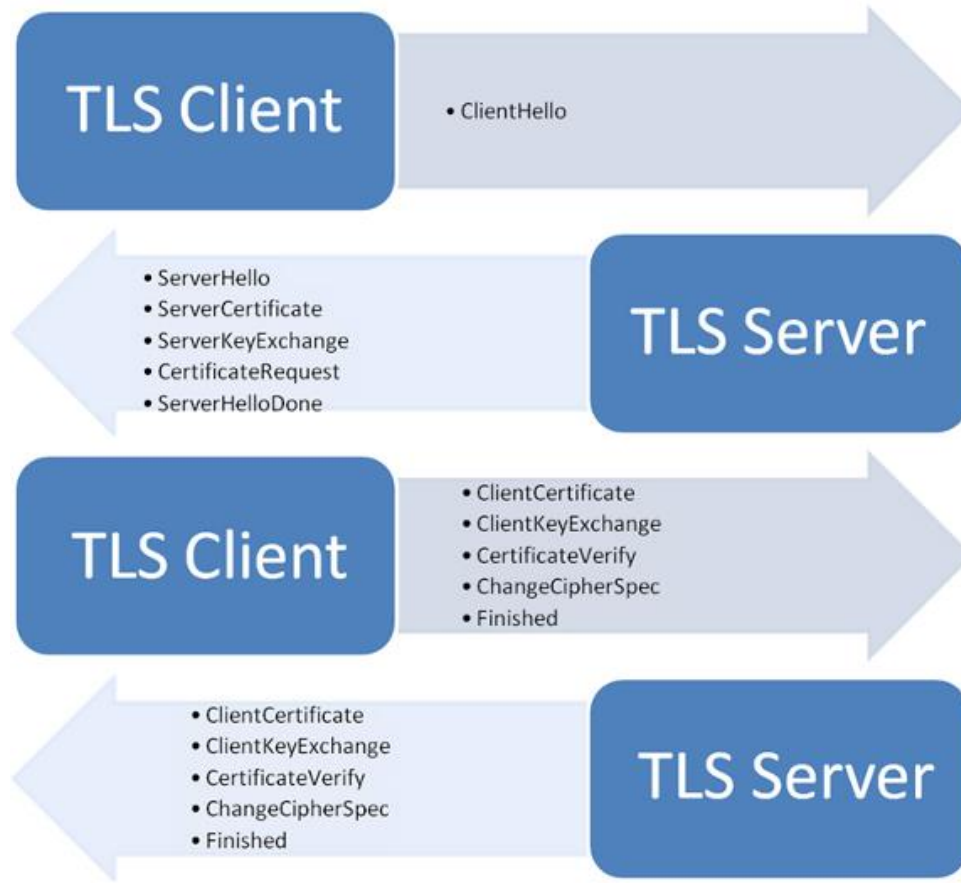


- Dugo u upotrebi još od vremena Julija Cezara
- Dve varijante: simetrična i asimetrična

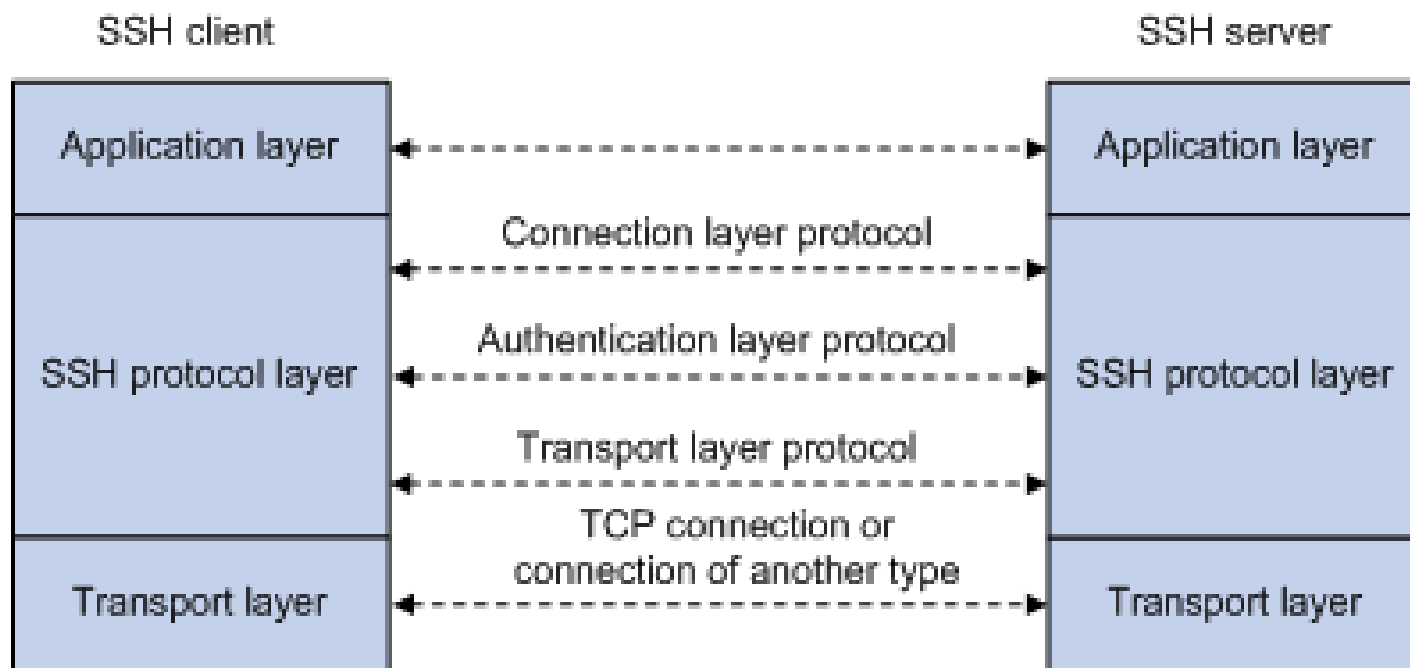
SSL



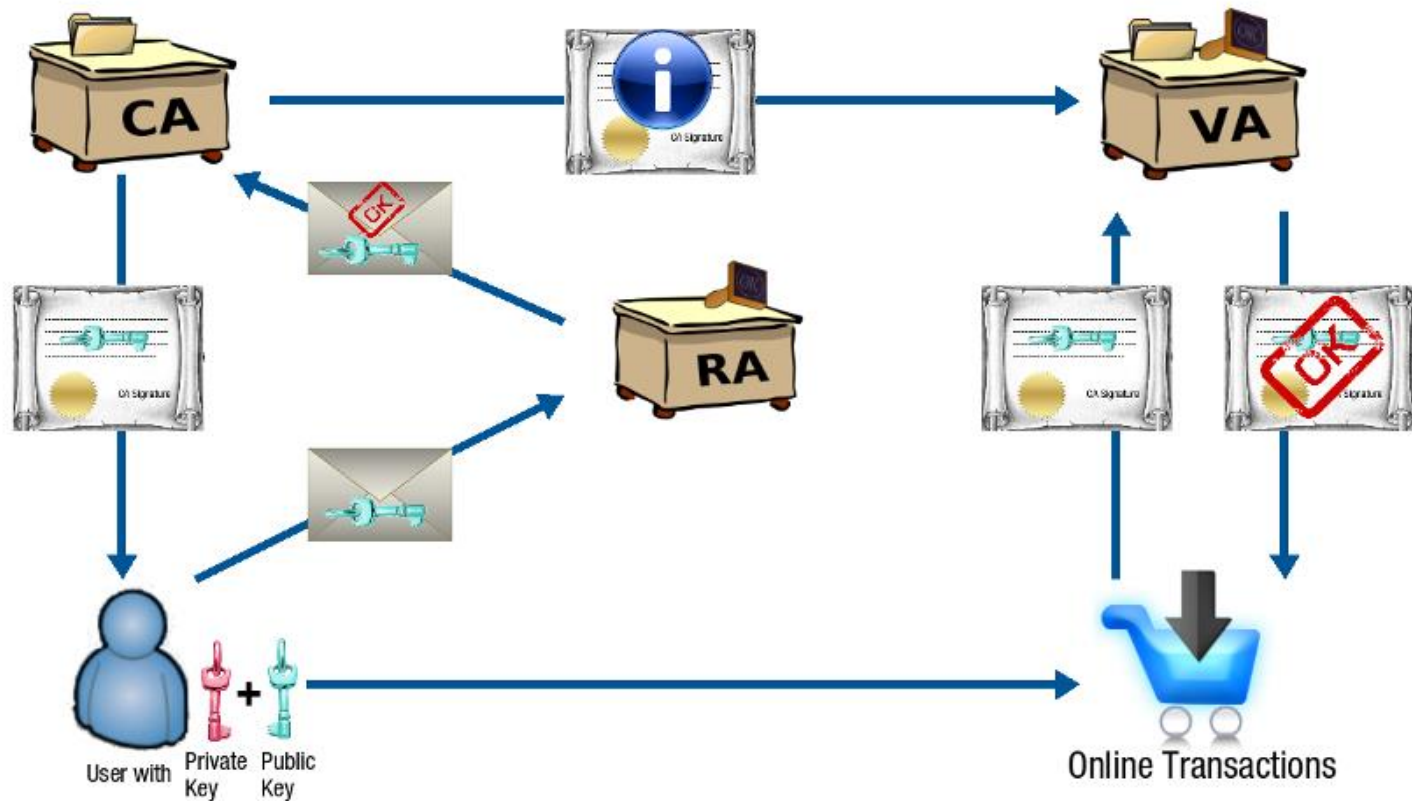
TLS



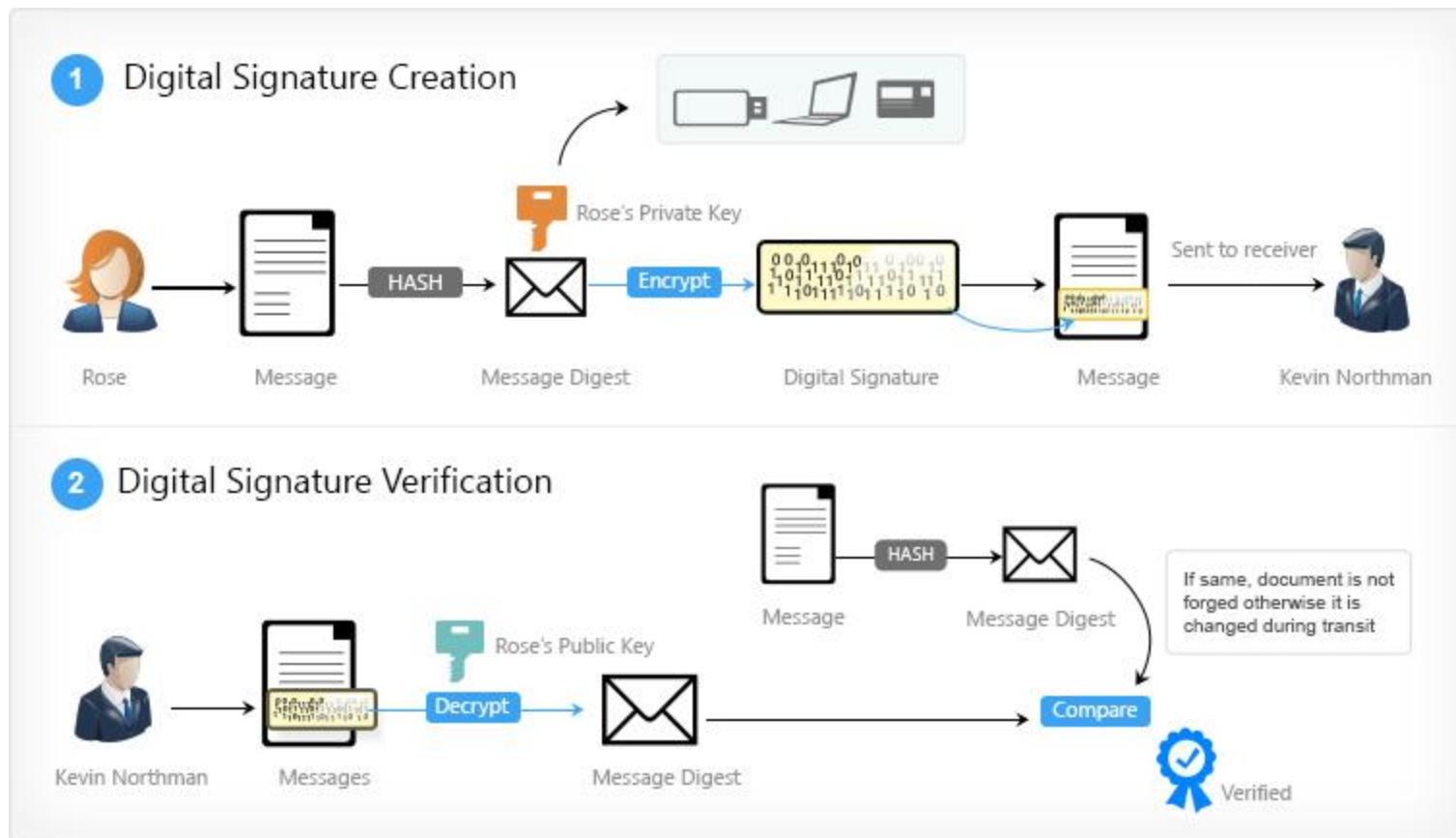
SSH



PKI

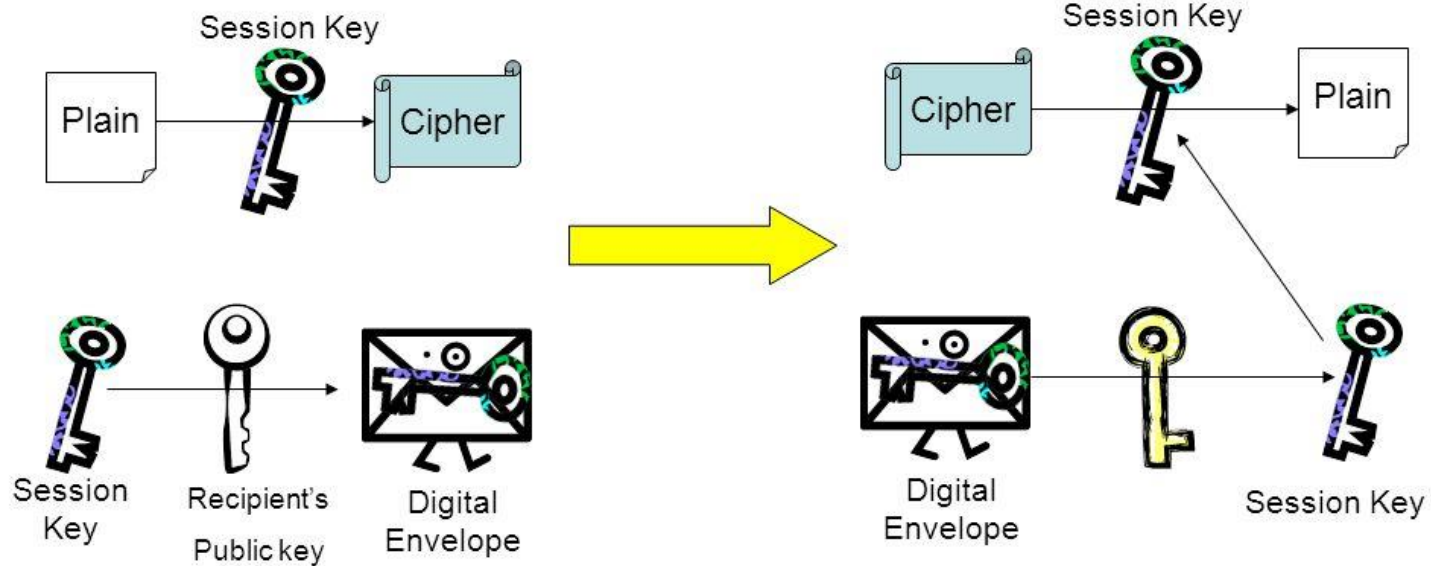


Digitalni potpis

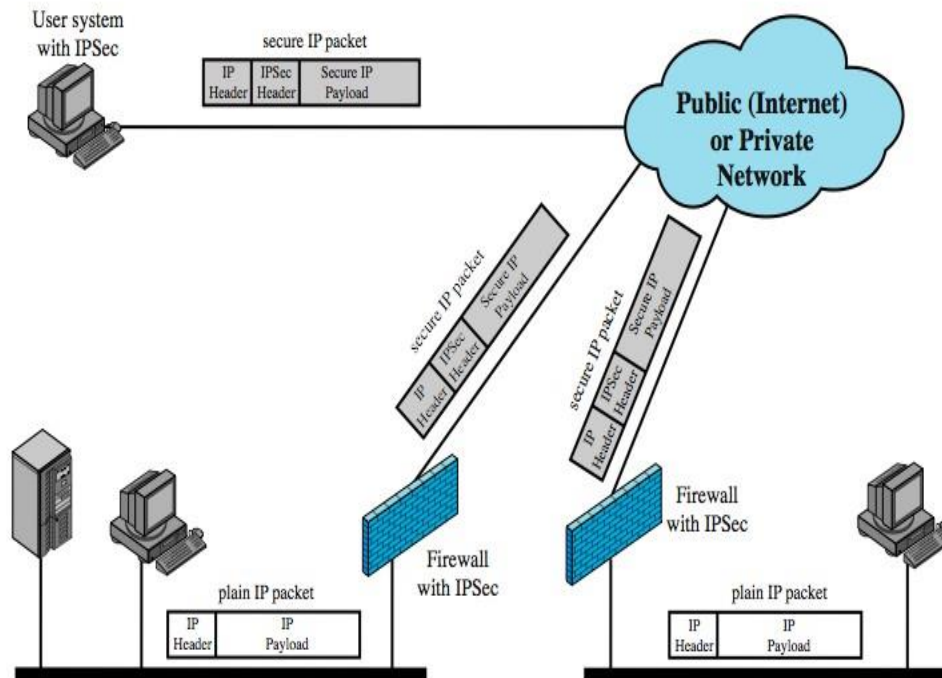


Digitalna koverta

Digital Envelopes



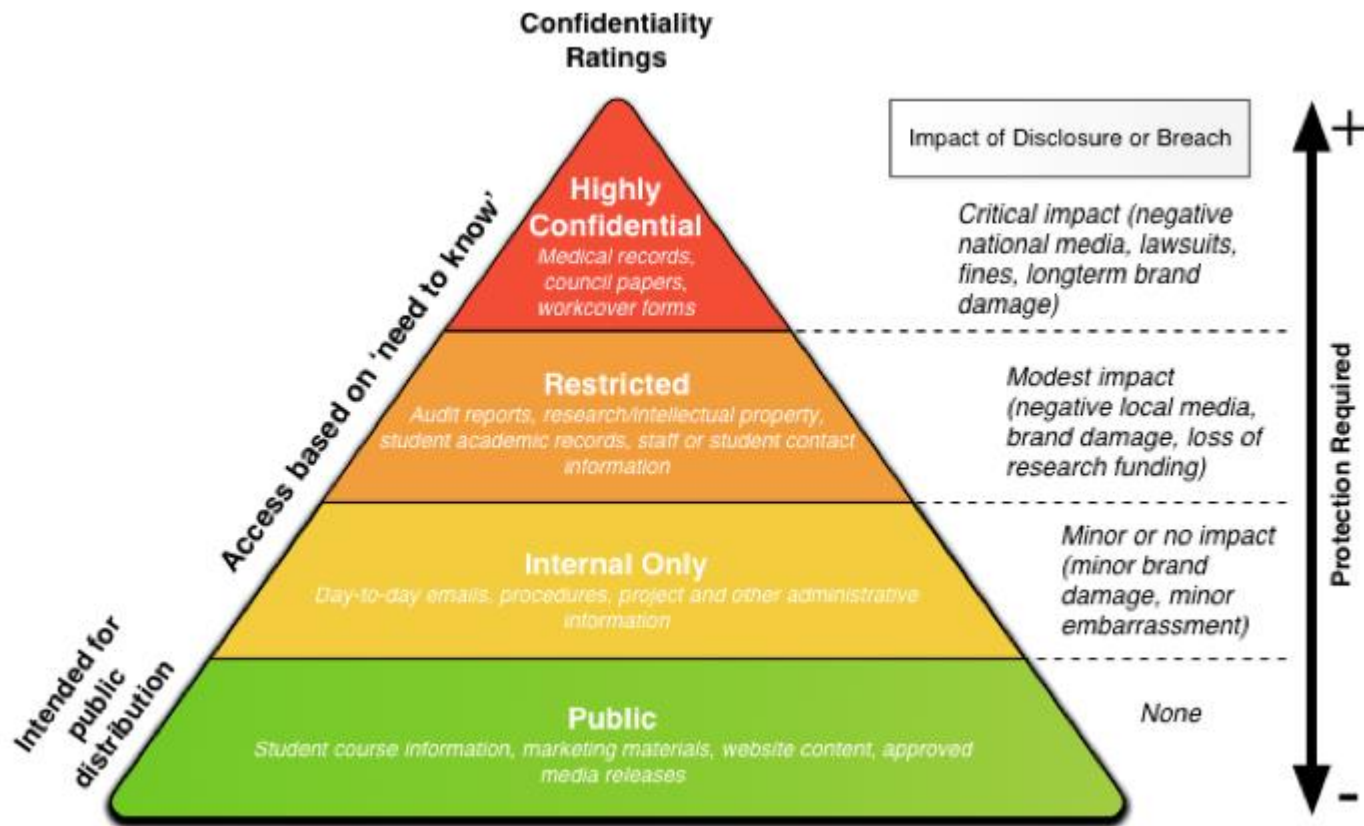
VPN (IPSec)



Hardening



Klasifikacija i označavanje informacija



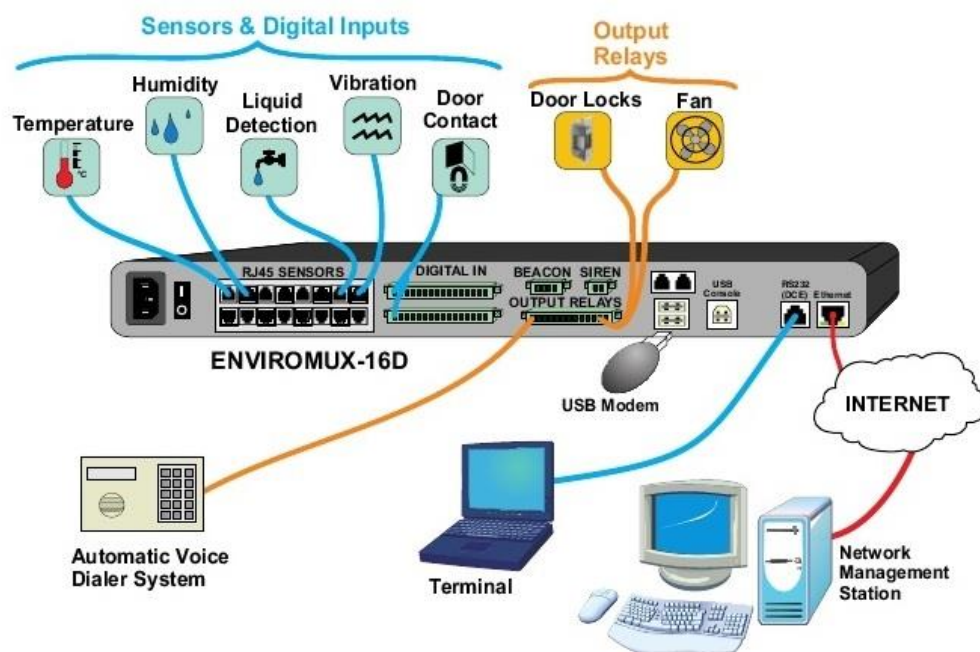
Fizička bezbednost

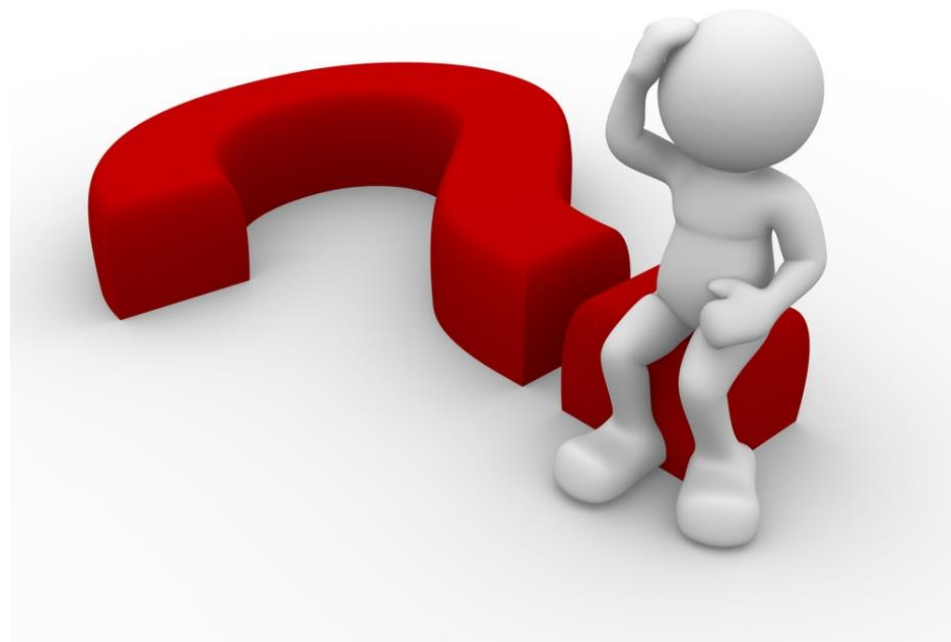
- Hardware locks (brave)
- Mantraps (dupla vrata)
- Video surveillance (CCTV)
- Fencing (ograda)
- Proximity readers (citaci sa udaljenosti)
- Access list (odstampana lista)
- Proper lighting (osvetljenje)
- Signs (znaci)
- Guards (strazari)
- Barricades (stubovi)
- Biometrics (biometrija)
- Protected distribution (kabliranje)
- Alarms (alarmi)
- Motion detection (senzori pokreta)



Bezbednost okruženja

- Environmental monitoring
- Kontrola temperature i vlažnosti
- HVAC
- Fire suppression
- EMI shielding





Kontakt podaci:

- Mail: ifranc@secitsecurity.com , ifranc@esigurnost.org
- Web: <http://secitsecurity.com> , <http://esigurnost.org>
- Twitter: <https://twitter.com/francigorbg>
- LinkedIn: <https://rs.linkedin.com/in/ifranc>