# Zabezpečenie údajov a komunikácie v OS Linux

- Základné pojmy
  - Nedôveryhodná sieť a ochrana komunikácie
  - Symetrické šifrovanie
  - Asymetrické šifrovanie
  - Digitálny podpis
  - Infraštruktúra verejného kľúča (PKI)
- GNU Privacy Guard (GPG)
- Tunelovanie komunikácie pomocou protokolu SSH
  - Lokálne presmerovanie portov
  - Vzdialené presmerovanie portov
  - Dynamické presmerovanie portov

# Nedôveryhodná sieť

- Riziko, že obsahuje nedôveryhodné uzly:
  - Nemáme nad nimi kontrolu,
  - Môžu sledovať premávku, vykonávať útoky, a pod.
- Je mimo správy administrátora.
- Spravidla za hraničným smerovačom, prípadne firewall-om.
- Príklad: Internet, verejná sieť WiFi.
- Potreba ochrany údajov:
  - v pokoji (at rest) – uložené na dátovom úložisku,
  - v pohybe (in transit) – prenášané cez sieť.

# Ochrana komunikácie

- Šifrovanie - ukrytie obsahu správ pred potenciálnym útočníkom
  - Symetrické šifrovanie,
  - Asymetrické šifrovanie.
- Autentifikácia – overenie identity komunikúcich strán
  - Zdieľané tajomstvo (heslo),
  - Asymetrická kryptografia (kľúčový pár).
- Integrita – zabezpečenie proti nevyžiadanej zmene obsahu správy počas prenosu.

# Symetrické šifrovanie

- Použitie rovnkého kľúča pre šifrovanie aj dešifrovanie
- Komunikujúce strany sa musia bezpečne dohodnúť na kľúči (kritická je výmena kľúča medzi nimi)
- Je potrebné zvoliť kľúč, ktorý je náročné uhádnuť
- Sila symetrického kľúča – 128-bitový kľúč znamená 2^128 možných kľúčov

# Nevýhody symetrického šifrovania

- Útočník môže získať kľúč pri výmene medzi účastníkmi komunikácie

- Ťažko škálovateľné
  - Pri n komunikujúcich je nutné použiť n(n-1)/2 kľúčov, aby komunikácia každého s každým bola zabezpečená a privátna.

# Asymetrické šifrovanie

- Použitie dvoch typov kľúča (pár kľúčov)
  - Jeden na šifrovanie iný na dešifrovanie
- Verejný kľúč
  - Príjímateľ správy ho poskytne ostatným
  - Odosielateľ ním zašifruje správu
- Privátny kľúč
  - Odosielateľ ho nepozná
  - Pomocou neho je možné dešifrovať správu, zašifrovanú verejným kľúčom,
  - Má ho iba prijímateľ správy

# Digitálny podpis

- Výpočet jedinečnej hodnoty pre dokument
  - Funkcia many-to-one = hash funkcia
  - Slúži na overenie pravosti dokumentu
- Výsledok aplikovania hash funkcie
- Hash funkcia musí spĺňať dve podmienky:
  - Dva dokumenty nesmú mať rovnaký výsledok výpočtu hash funkcie
  - Z výsledku nesmie byť možné získať pôvodný dokument

# Infraštruktúra verejného kľúča (PKI)

- Množina pravidiel, postupov, technických a organizačných opatrení spojených s:
  - vytvorenie,
  - správa,
  - použitie,
  - šírenie,
  - ukladanie,
  - rušenie,

  Šifrovacích kľúčov a digitálnych certifikátov.

# Gnu Privacy Guard

- GnuPG je nástroj, ktorý umožňuje zvýšiť bezpečnosť v systéme.
  - Príkaz `gpg`
- Pre zabezpečenie komunikácie medzi komunikujúcimi stranami, je potrebné aby ho využívali obe strany.
- Pomocou GnuPG je možné realizovať kroky popísané v PKI

# GPG: Vytvorenie a správa kľúča

- prepínače
  - `--gen-key`
    - Vytvorenie kľúča, predvolené nastavenia
  - `--full-gen-key`
    - Voľba možného spôsobu použitia kľúča
    - Voľba veľkosti kľúča
  - `--edit-key`
    - CLI pre správu kĺúča
    - `help, fingerprint`
    - `disable, enable`
    - `passwd, addkey`

# GPG: Výmena kľúča

- prepínače
  - `--list-key`
    - zoznam verejných kľúčov
  - `--export`
    - exportovanie verejného kľúča
  - `--import`
    - importovanie verejného kľúča
  - `--armor`
    - exportovanie do formatu ASCII armor

# GPG: Zašifrovanie, dešifrovanie súboru

- prepínače
  - `--encrypt`
    - zašifrovanie súboru pomocou páru kľúčov
    - asymetrické šifrovanie
  - `--decrypt`
    - dešifrovanie súboru
  - `--symmetric`
    - symetrické šifrovanie súboru

# GPG: Podpísanie a overenie podpisu

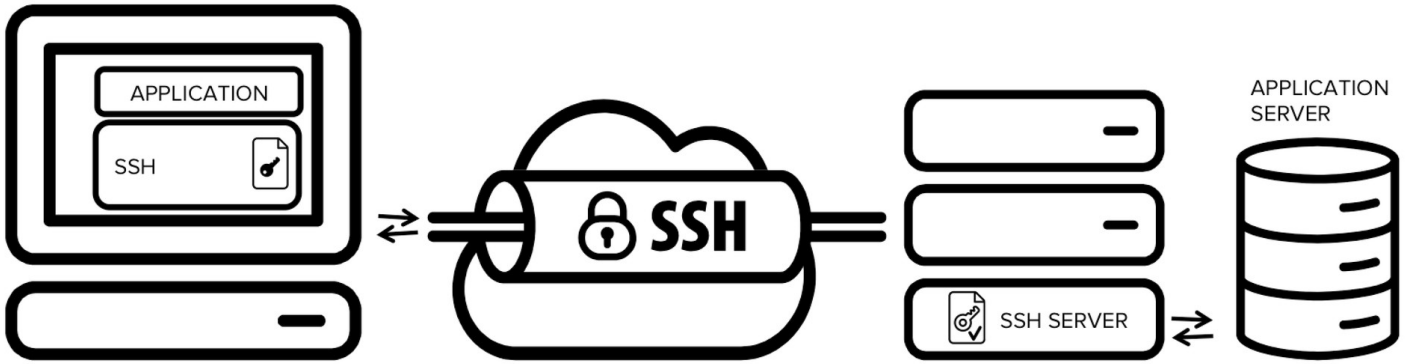
- prepínače
  - `--sign`
    - podpísanie a zašifrovanie súboru
  - `--clearsign`
    - podpísanie súboru bez zašifrovania
  - `--detach-sign`
    - oddelenie podpisu pri podpisovaní
  - `--verify`
    - overenie podpisu

# Tunelovanie premávky

- Vytvorenie bezpečného (šifrovaného) spojenia (“tunela”) pre komunikáciu cez nedôveryhodnú sieť.
- Možnosť zabezpečiť ľuvovoľnú komunikáciu pretekajúcu cez “tunel”.
  - Napríklad: vzdialený prístup, protokoly bez podpory šifrovania a pod.
- Protokol SSH podporuje vytvorenie “tunela” prostredníctvom presmerovania portov.

# Presmerovanie portov pomocou SSH

- Presmerovanie komunikácie cez zabezpečené SSH spojenie – tzv. “SSH tunel”.
- Potrebný prístup na dostupný SSH server.




https://www.ssh.com/ssh/tunneling/

# SSH: lokálne presmerovanie portov

```
ssh –L [ladresa:]lport:host:port login@ssh.server
```

- Spojenia na daný lokálny TCP port sú presmerované na daný cieľový host a port cez server “ssh.server”,
- Spojenie medzi lokálnym strojom a serverom “ssh.server” je zabezpečené prostredníctvom protokolu SSH,
- Privilegované porty môže presmerovať iba “root”.

# SSH: vzdialené presmerovanie portov

`ssh –R [radresa:]rport:host:port login@ssh.server`

- Spojenia na daný TCP port na vzdialenom hostovi (serveri) sú presmerované na daný cieľový host a port na lokálnej strane,
- Vytvorený “socket” na vzdialenej strane štandardne počúva na lokálnom rozhraní.
  - Možnosť zmeniť parametrom `radresa`,
  - Nastavenie parametra `GatewayPorts`.

# SSH: dynamické presmerovanie portov

```
ssh –D [ladresa:]lport login@ssh.server
```

- Špecifikuje lokálne dynamické presmerovanie na úrovni aplikácií,
- Spojenia na daný lokálny TCP port sú presmerované cez server “ssh.server”,
- Cieľ presmerovania je špecifikovaný aplikačným protokolom.
  - Podporované protokoly: SOCKS4, SOCKS5,
  - SSH pracuje ako SOCKS proxy.

# Literatúra a zdroje

Manuálové stránky:

- man gpg
- man ssh
- man sshd
- man ssh_config

GnuPG manual:

- https://www.gnupg.org/gph/en/manual.html

GnuPG Commands - Examples

- http://www.spywarewarrior.com/uiuc/gpg/gpg-com-4.htm

GPG Tutorial

- https://futureboy.us/pgp.html

SSH tunely

- https://www.ssh.com/ssh/tunneling/