



Aalto-yliopisto  
Teknillinen korkeakoulu

# Tietoturvan perusteet

Tuomas Aura

T-110.2100 Johdatus tietoliikenteeseen  
kevät 2010

# Luennon sisältö

Tällä viikolla:

1. Tietoturvallisuus
2. Uhkia ja hyökkäyksiä verkossa
3. Tietoverkkojen turvaratkaisuja

Ensi viikolla: salausmenetelmät ja SSL

# **TIETOTURVALLISUUS**

# Tietoturvan käsitteitä

- **Tietoturvan** tarkoitus on suojata järjestelmää **pahoilta asioilta**, jotka joku tekee **tahallaan**
  - Turvallisuus vs. luotettavuus?
- **Uhka** = paha asia, joka voi ehkä tapahtua
- **Hyökkäys** = joku toteuttaa uhkan tahallaan
- **Haavoittuvuus** = järjestelmän ominaisuus, joka helpottaa höykkäystä

# CIA-malli

- Tietoturvan tavoitteita:
  - Tiedon **luottamuksellisuus**
  - Tiedon **eheys**
  - Tiedon ja palvelujen **saatavuus**

*(CIA = confidentiality, integrity, availability)*
- Uhkia:
  - Tietomurrot, salakuuntelu
  - Väärentäminen, luvaton muokkaus
  - Palvelunesto: kaataminen, ylikuormitus

# Pääsynvalvonta

- Tavoite: vain valtuutetut käyttäjät pääsevät käyttämään tietoa tai palvelua
- Pääsynvalvonta = todentaminen + valtuuttaminen
- Käyttäjän todentaminen tapahtuu esimerkiksi salasanalla
- Valtuuttaminen tapahtuu katsomalla käyttäjän oikeudet esimerkiksi pääsynvalvontalistasta (ACL)

```
vipunen joti 11 % ls -la
total 12856
drwxr-xr-x  2 aura  users  4096 Feb  8 23:45 .
drwxr-xr-x  3 aura  users  4096 Jan 18 02:43 ..
-rw-r--r--  1 aura  users    4 Feb  8 23:45 a
-rw-r--r--  1 aura  users   344 Jan 17 21:39 esimerkki.html
-rw-r--r--  1 aura  users 810892 Jan 18 02:40 joti2010-luento01-miten-internet-toi
-rw-r--r--  1 aura  users 3082752 Jan 18 02:39 joti2010-luento01-miten-internet-toi
-rw-r--r--  1 aura  users 3082752 Jan 18 02:39 joti2010-luento01-miten-internet-toi
```

User name: 
Password: 
 Remember my credentials
OK

Joti2010-luento04-tietoturvaluisuus.pptx Properties
General Security Details Previous Versions
Object name: C:\Users\taura\Documents\Opetus\JoTi\Joti2010
Group or user names:
SYSTEM
Tuomas Aura (PLOVER\aura)
Administrators (PLOVER\Administrators)
To change permissions, click Edit.
Permissions for Tuomas Aura
Full control Allow
Modify Allow
Read & execute Allow
Read Allow
Write Allow
Special permissions Deny
For special permissions or advanced settings, click Advanced.

```
C:\Users\taura>runas /user:Administrator regedt
Enter the password for Administrator:
Attempting to start regedt as user "PLOVER\Admini
RUNAS ERROR: Unable to run - regedt
1326: Logon failure: unknown user name or bad pas
C:\Users\taura>
```

TKK » IT Services » WebLogin
TKK WebLogin
Shibboleth Identity Provider
The resource you requested requires you to authenticate.
Login: aura
Password:
log in »
Use your user name and service password.

- Suvilehto Jyry
- Ylä-Jääski Antti
- Muut ylläpitäjät
- Nimi ▲
- Adolfsson Soili
- Aura Tuomas
- Luukkainen Sakari
- Siekinen Matti
- Suoranta Sanna
- Suvilehto Jyry

```
vipunen ~ 1 % cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIEAoo2GzkiJmvpTgrRtuVbFyPxCfiToe
8oVkr4DOz25Wa743EnCWsyKLj022EnDK6r6dZowrMSuQ/tg+M93KVMW42m8VaNuZ+
k8uC57yTuzItt7gmdvsqv0OgrO1sxnj+Jdb51WzJaf7Uqt3mc= rsa-key-200811
ssh-dss AAAAB3NzaC1kc3MAAAEBAIYSt9WWY8dqB65u6mVrKYusvbIhXRzfaKEEL
UVfuz51jI11nXiHSOumBPeBh8AqEh8TkoZeCiB1YDQn071aWZNY5k+tarOCPmpsh2hrc
Ob5Ke33QW2nSplql3uHJPqO/gVmCRhILaAPKM3zGgA3QCZPw84koOXiBtGp3inKFW9p3ZHf9ANiRbT5
cnM/DFrsQ3rtq8nGg+3OECPIxznEB+UxkK4d/5aV9Naijeruq5cPYvrT0UKYaxzNidazzkaNiozbiT0u
```

SSH Tectia
aura@hutcs.cs.hut.fi's password
OK Cancel

# Tietoturvan suunnittelu

- Organisaation tai järjestelmän tietoturvan suunnittelu:
  - Tunnistetaan **suojattava tieto-omaisuus**
  - Tunnistetaan **uhat**: fyysiset, tietotekniset ja sosiaaliset
  - Tehdään **riski-analyysi**: vahinkojen suuruus ja todennäköisyys
  - Päätetään **suojauksen tavoitteet**
  - Päätetään **suojauksen keinot**: tekniset suojaukset, prosessit, vastuut ja resurssit
- Suunnittelun tulos: **tietoturvasäännöt**



# Tietoturvasäännöt

- Tietoturvasäännöissä on
  - Suunnitelma tietoturvan **tekniselle toteutukselle**
  - **Prosessit henkilöstölle** normaali- ja poikkeustilanteisiin
  - Suojausten perustelut
- Turvatilannetta on **valvottava**
  - Suojauksia päivitetään uhkien muuttuessa
- Sääntöjen pitää olla realistisia:
  - Liian hankalia sääntöjä ei noudateta
  - **Tietoturva ei saa estää organisaation ja työntekijöiden keskittymistä varsinaisiin työtehtäviin**
  - Turvallisuudesta tulee helposti vallankäytön väline

# Uhka-analyysi

- Esimerkki: **opintorekisteri**
  - Mitä suojeltavaa tietoa?
  - Mitä uhkia,  
kuka on hyökkääjä?
  - Uhkien priorisointi?
- Käytitkö ensin CIA-mallia?  
Riittääkö se?
- Muistitko sisäpiirin uhkat?

WebOodi v2.8

TKK

Aura Anssi Tuomas,  
39057P

Etusivu

- [-] Kurssien haku
  - Hakutermeillä
  - Opetusohjelmista
- [-] Omat opinnot
  - Ilmoittautumiset
  - Suoritusotot
  - Ei aktiiviset
  - Suoritusote
  - HOPS
- [-] Muut toiminnot
  - Henkilötiedot
  - Asetukset
  - Opintojaksojen kysyntä
  - HOPSeissa
  - Tutkintorakenteet
- [-] Opinto-oppaat
  - Opintokohteet
  - Opetustapahtumat
  - Opasraportti
  - Oppaiden ylläpito
- [-] Kurssipalautteet
  - Omat palautteet
  - Omien kurssien hallinta

Linkit

Ohje

Omat opinnot

10

Omat opinnot

Jos joku...

Tilaa suoritukset

Piilotetut kurssit

Ilmoittautumiset

Suoritusotot

Suoritusotot

Suluissa...

+ Tunnistaminen

[-] TKT-19

[-] Xv-

[-] Tkl-19

+ XI-

+ ZD

+ ZD

+ XL-

[-] DI-197

+ XD

+ §D

+ XA

+ XY-

+ §F3

+ XM

+ XH

# **UHKIA JA HYÖKKÄYKSIÄ VERKOSSA**

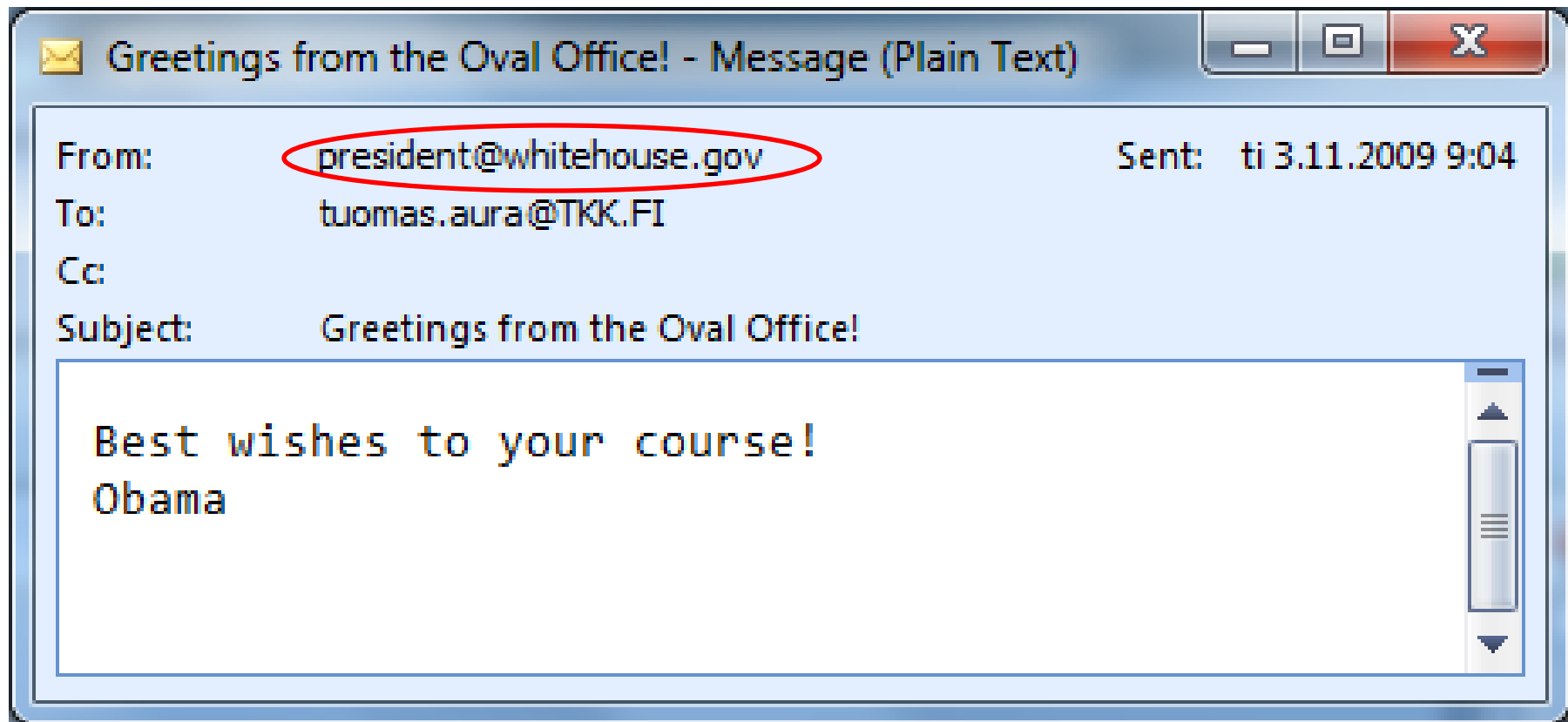
# Salakuuntelu

- Rikkoo tiedon **luottamuksellisuuden**
- Suuri osa Internet-yhteyksistä on suojaamattomia
  - SMTP, Hotmail, Yahoo Messenger, Facebook, Aalto
- Paketteja voi nauhoittaa **snifferillä**:
  - Wireshark, Netmon, tcpdump
  - Kuuntelijan pitää olla samassa paikallisverkossa asiakkaan kanssa tai reitillä asiakkaan ja palvelimen välillä
  - Kenen langatonta verkkoa käytät?
- Hyökkääjää kiinnostavat **tunnukset ja salasanat**

172.19.7.255	NbtNs	NbtNs:Registration Request for WORKGROUP <0x1D> M
172.19.7.255	BROWSER	BROWSER:Browser Election Request, ServerName=...
[0180C2 00000...]	SPANTreeBPDU	SPANTreeBPDU
[014096 FFFF0...]	SNAP	SNAP:EtherType = IEEE802.3 Length Field, OrgCo...
[Cisco Systems...]	ATMARP	ATMARP:ARMARP Opt 0
172.19.7.255	NbtNs	NbtNs:Registration Request for WORKGROUP <0x1D> M
172.19.5.30	TCP	TCP:[ReTransmit #155]Flags=...AP..., SrcPort=S...
172.19.7.255	BROWSER	BROWSER:Browser Election Request, ServerName=...
[0180C2 00000...]	SPANTreeBPDU	SPANTreeBPDU
172.19.7.255	NbtNs	NbtNs:Registration Request for WORKGROUP <0x1D> M
172.19.7.255	NbtNs	NbtNs:Query Request for CHEYWEST1 <0x20> F...
172.19.7.255	NbtNs	NbtNs:Registration Request for WALSHK <0x03>...
[Cisco Systems...]	ATMARP	ATMARP:ARMARP Opt 0
[Cisco System...]	ATMARP	ATMARP:ARMARP Opt 0
172.19.7.255	NbtNs	NbtNs:Registration Request for HMCO <0x1D> M
[Cisco System...]	ATMARP	ATMARP:ARMARP Opt 0
[014096 FFFF0...]	SNAP	SNAP:EtherType = IEEE802.3 Length Field, OrgCo...
[0180C2 00000...]	SPANTreeBPDU	SPANTreeBPDU
172.19.7.255	NbtNs	NbtNs:Registration Request for WALSHK <0x03>...
[Cisco Systems...]	ATMARP	ATMARP:ARMARP Opt 0
172.19.7.255	NbtNs	NbtNs:Registration Request for HMCO <0x1D> M
172.19.1.9	SNMP	SNMP:Version1, Community = netsolve, Get requ...
172.19.2.2	TCP	TCP:Flags=...A..., SrcPort=HTTPS(443), DstPort=...
172.19.7.255	NbtNs	NbtNs:Registration Request for WALSHK <0x03>...
[0180C2 00000...]	SPANTreeBPDU	SPANTreeBPDU
[030000 00000...]	LLC	LLC:Unnumbered(U) Frame, Command Frame, S...
172.19.7.255	NbtNs	NbtNs:Registration Request for HMCO <0x1D> M
172.19.3.185	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80), DstPort=...
172.19.7.255	NbtNs	NbtNs:Registration Request for WALSHK <0x03>...
[0180C2 00000...]	SPANTreeBPDU	SPANTreeBPDU
172.19.7.255	NbtNs	NbtNs:Registration Request for HMCO <0x1D> M
172.19.5.34	DNS	DNS:QueryId = 0x6389, QUERY (Standard query)
172.19.5.34	DNS	DNS:QueryId = 0x6389, QUERY (Standard query)

# Väärennetyt viestit

- Esimerkki: sähköposti



# Sähköpostin väärentäminen

```
C:>telnet smtp.kolumbus.fi 25
220 emh05.mail.saunalahti.fi ESMTP Postfix
ehlo nowhere.net
250-emh05.mail.saunalahti.fi
250-PIPELINING
250-SIZE 280000000
250-8BITMIME
mail from: president@whitehouse.gov
250 2.1.0 ok
rcpt to: tuomas.aura@tkk.fi
250 2.1.5 ok
data
354 End data with <CR><LF>.<CR><LF>
From: president@whitehouse.gov
To: tuomas.aura@tkk.fi
Subject: Greetings from the oval office!

Best wishes to your course!
Obama
.
250 2.0.0 ok: queued as 9935A27D8C
```

# Ohjelmistovirheet

Puskurin ylivuoto:

```
#define BUFLen 4

void vulnerable(char *input) {
    wchar_t buf[BUFLen];
    int val;

    val = MultiByteToWideChar(
        CP_ACP, 0, input,
        -1, buf, sizeof(buf));
    printf("%d\n", val);
}
```

Edellisen funktion pinokehys
Paluuosoite
buf
val
Roskaa

Oikea tapa laskea kohdepuskurin koko: `sizeof(buf) / sizeof(buf[0])`

- Ohjelmistovirheet mahdollistavat tietokoneiden kaappaamisen ja haittaohjelmien leviämisen

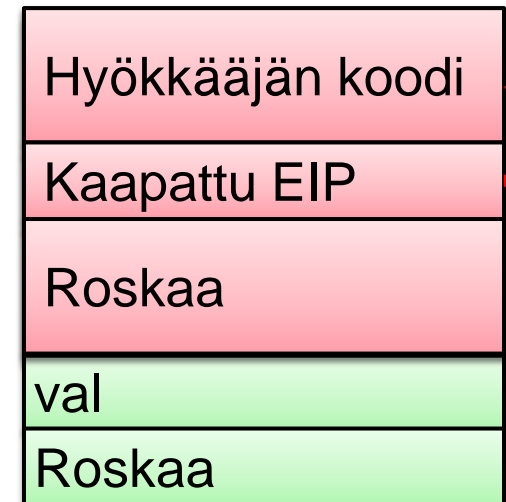
# Ohjelmistovirheet

Puskurin ylivuoto:

```
#define BUFLen 4

void vulnerable(char *input) {
    wchar_t buf[BUFLen];
    int val;

    val = MultiByteToWideChar(
        CP_ACP, 0, input,
        -1, buf, sizeof(buf));
    printf("%d\n", val);
}
```



Oikea tapa laskea kohdepuskurin koko: `sizeof(buf) / sizeof(buf[0])`

- Ohjelmistovirheet mahdollistavat tietokoneiden kaappaamisen ja haittaohjelmien leviämisen



# Haittaohjelmat

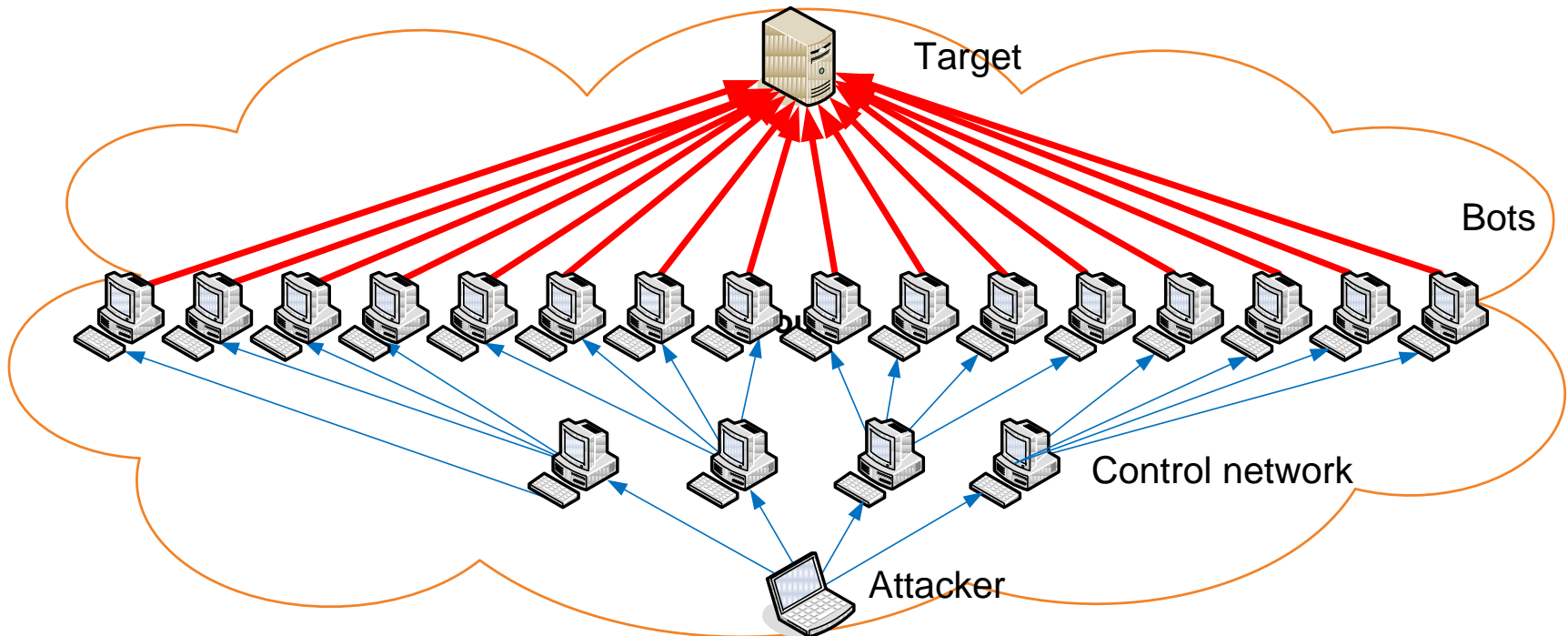
- **Virukset ja madot** leviävät itsestään
- **Trojialainen** on viattomalta näyttävä ohjelma, joka kätkee haittaominaisuuksia
- **Rootkit** kätkeytyy koneelle
- **Vakoiluohjelma** etsii ja lähettää tietoa koneelta hyökkääjälle
- Ennen haittaohjelmat olivat harrastajien tekemiä, nykyään ammattirikollisten
  - Eivät enää halua herättää huomiota
  - **Botnet**-verkkojen palveluita myytävänä
  - Käyttökohteita: **kalastelu ja roskapostin lähetys**

# Tunnusten kalastelu

- Rikolliset hankkivat huijaamalla tietoonsa **pankkitunnuksia** ja muita käyttäjätunnuksia ja salasanoja
  - Väärennetyt sähköpostit
  - Väärennetyt verkkosivut
  - Näppäinpainalluksia nauhoittavat haittaohjelmat
- **Uudet haittaohjelmat muuttavat pankkisiirtoja lennosta**
  - Myös suomalaisia pankkeja vastaan, kertakäyttösalasana ei auta!
  - Voiko samalle PC:lle ladata verkosta pelejä ja käyttää pankkiasiointiin?

# Palvelunesto

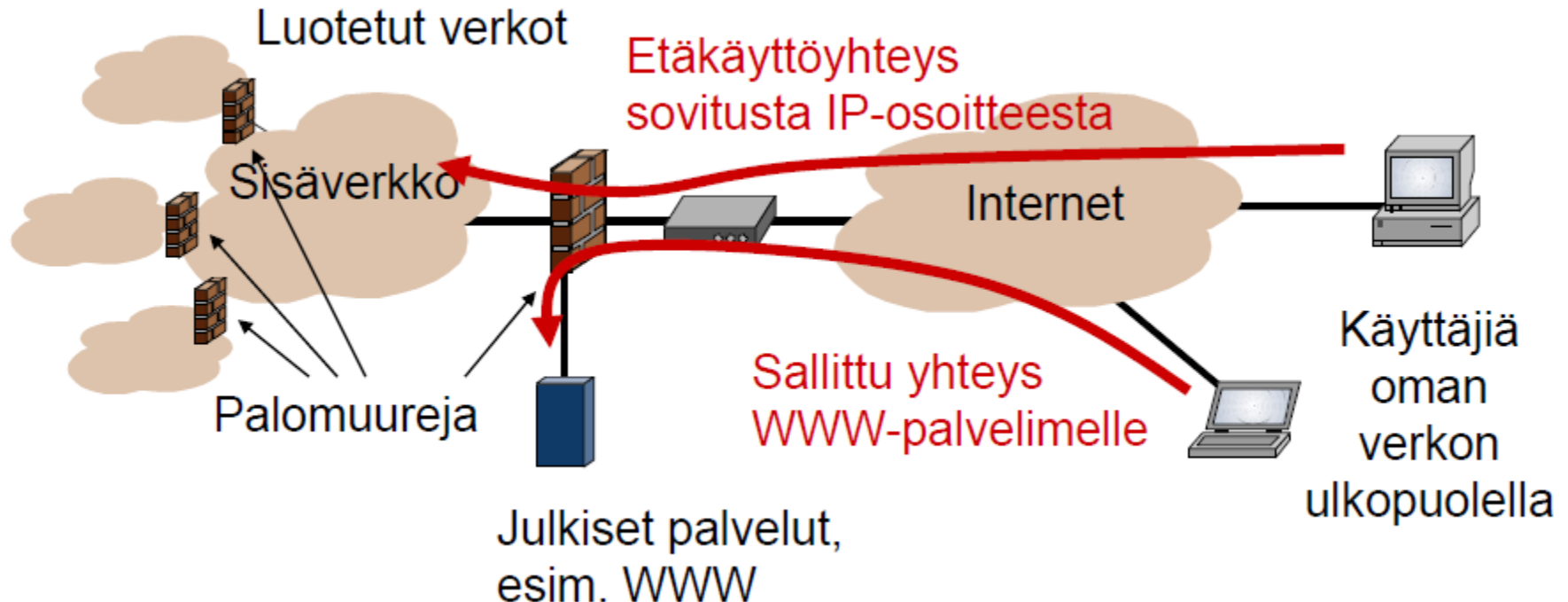
- Hyökkääjä voi estää rehellisiä asiakkaita käyttämästä palvelua **ylikuormittamalla palvelimen tai verkon**
- Hajautetussa palvelunestossa hyökkääjällä on botnet



# **TIETOVERKKOJEN TURVARATKAISUJA**

# Palomuuuri

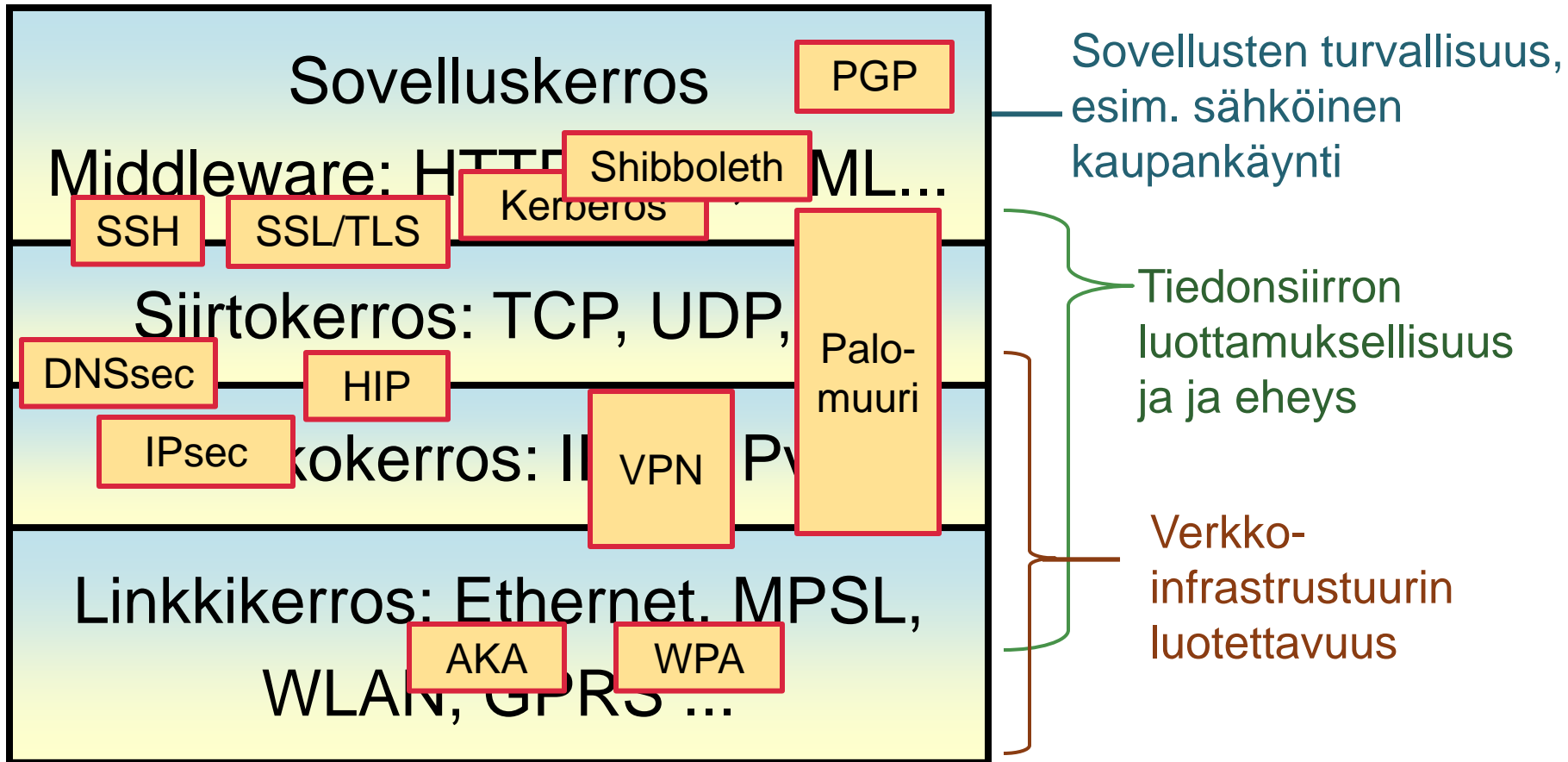
- Palomuuuri suodattaa Internetistä sisäverkkoon tulevaa liikennettä:
  - Vähentää havoittuvuutta rajapintoja pienentämällä
  - toteuttaa tietoturvasääntöjä



# Salaustekniikat

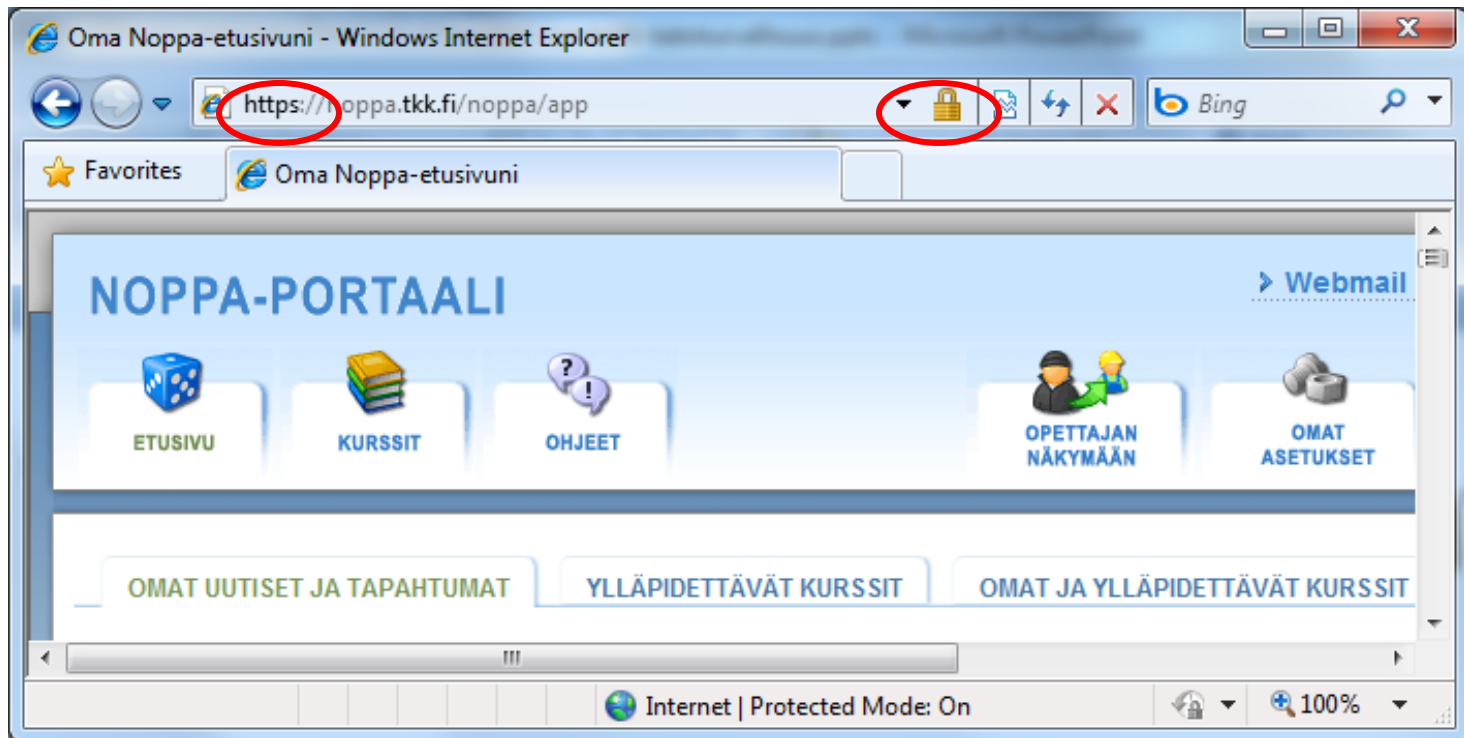
- **Salaus** (salakirjoitus) suojaa tiedon luottamuksellisuutta
- **Sähköinen allekirjoitus** suojaa tiedon eheyttä
- Palvelujen saatavuutta ei voi varmistaa salaustekniikoilla

# Tietoturva-protokollat



# SSL

- Ensi viikolla:





# Kurssin luennot

- **Aloitus: Miten Internet toimii**, Tuomas Aura
- **Web 2.0 ja uudet sovellustekniikat**, Tancred Lindholm
- **Sovelluskerros: WWW, email, socket API**, Tancred Lindholm
- **Tietoturvan perusteet**, Tuomas Aura
- **Salaustekniikat**, Tuomas Aura
- **Kuljetuskerros, TCP**, Matti Siekkinen
- **Verkkokerros, IP**, Matti Siekkinen
- **Linkkikerros, Ethernet ja WLAN**, N.N.
- **Tiedonsiirron perusteet**, N.N.
- **Puhelinverkot**, Antti Ylä-Jääski
- **Soluverkot**, Antti Ylä-Jääski
- **Tele- ja tietoverkon laskutus**, Sakari Luukkainen
- **Liiketoiminta verkkoympäristössä**, Sakari Luukkainen
- **Yhteenveto/kertaus**, Antti Ylä-Jääski ja Tuomas Aura