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

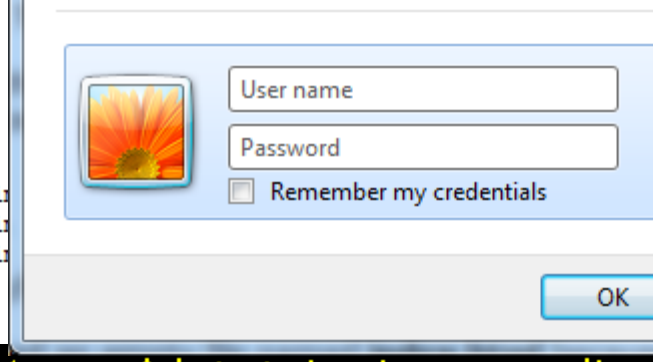
  (*CIA = confidentiality, integrity, availability*)

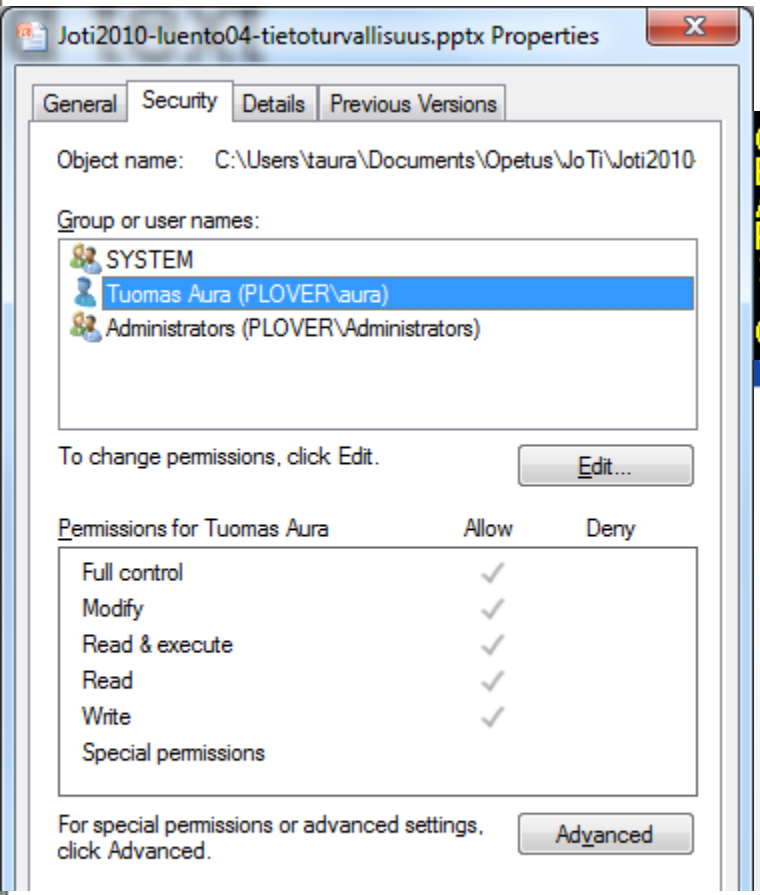
- Uhkia:
  - Tietomurrot, salakuuntelu
  - Väärentäminen, luvaton muokkaus
  - Palvelunesto: kaataminen, ylikuormitus

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)

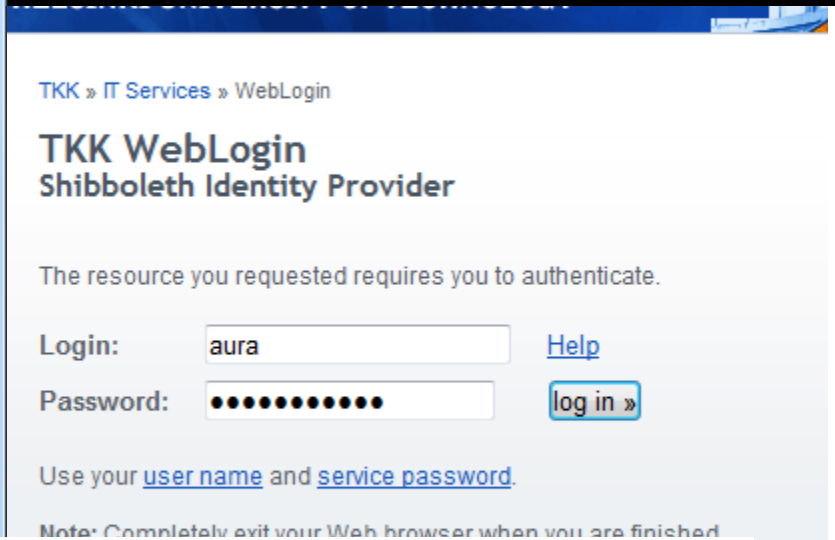
```
vipunen joti 11 % ls -la
total 12856
drwxr-xr-x   2 aura     users       4096 Feb  8 23:45 .
drwxr-xr-x   3 aura     users       4096 Jan 18 02:43 ..
-rw-r--r--   1 aura     users          4 Feb  8 23:45 a
-rw-r--r--   1 aura     users        344 Jan 17 21:39 esimerkki.html
-rw-r--r--   1 aura  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



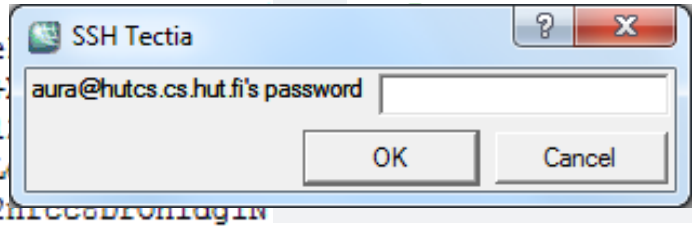



```
C:\Users\taura>runas /user:Administrator regedt
Enter the password for Administrator:
Attempting to start regedt as user "PLOVER\Admini
RUNAS ERROR: Unable to run - regedt
1326: Logon failure: unknown user name or bad pas

C:\Users\taura>
```




```
vipunen ~ 1 % cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIEAoo2GzkiJmvpTgrRtuVbFyPxCfiToe
8oVkR4DOzZ5Wa743EnCWsyKLj02ZEnDK6r6dZowrMSuQ/tg+M93KVMW42m8VaNuZ+
k8uC57yTuzItt7gmdvsqv0OgrO1sxmj+Jdb51WzJaf7Uqt3mc= rsa-key-200811
ssh-dss AAAAB3NzaC1kc3MAAAEBAIYSt9WWY8dqB65u6mVrKYusvbIhXRzfaKEEL
UVfuz51jIl1nXiHSOumBPeBh8AqEh8TkoZeCiB1YDQn071aWZNY5k+tarOCPmpsH2
Ob5Ke33QW2nSplql3uHJPqO/gVmCRhILaAPKM3zGgA3QCZPw84koOXiBtGp3inKFW9p3ZHf9ANiRbT5
cnM/DFrsO3rtg8nCg+3QECPIxznEB+UxkK4d/5sV9Nsierug5cPYvrT0UKYaxzNidazzkaNjozbiT0u
```



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

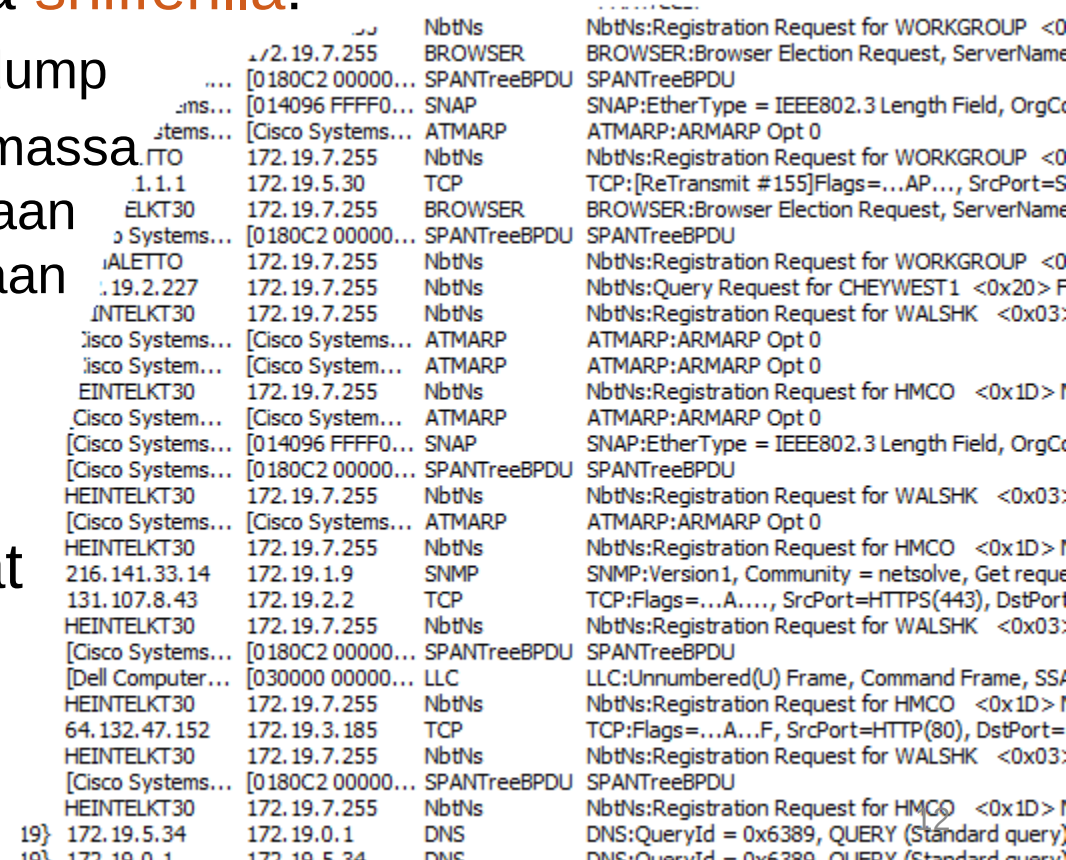
Uhka-analyysi

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

UHKIA JA HYÖKKÄYKSIÄ VERKOSSA

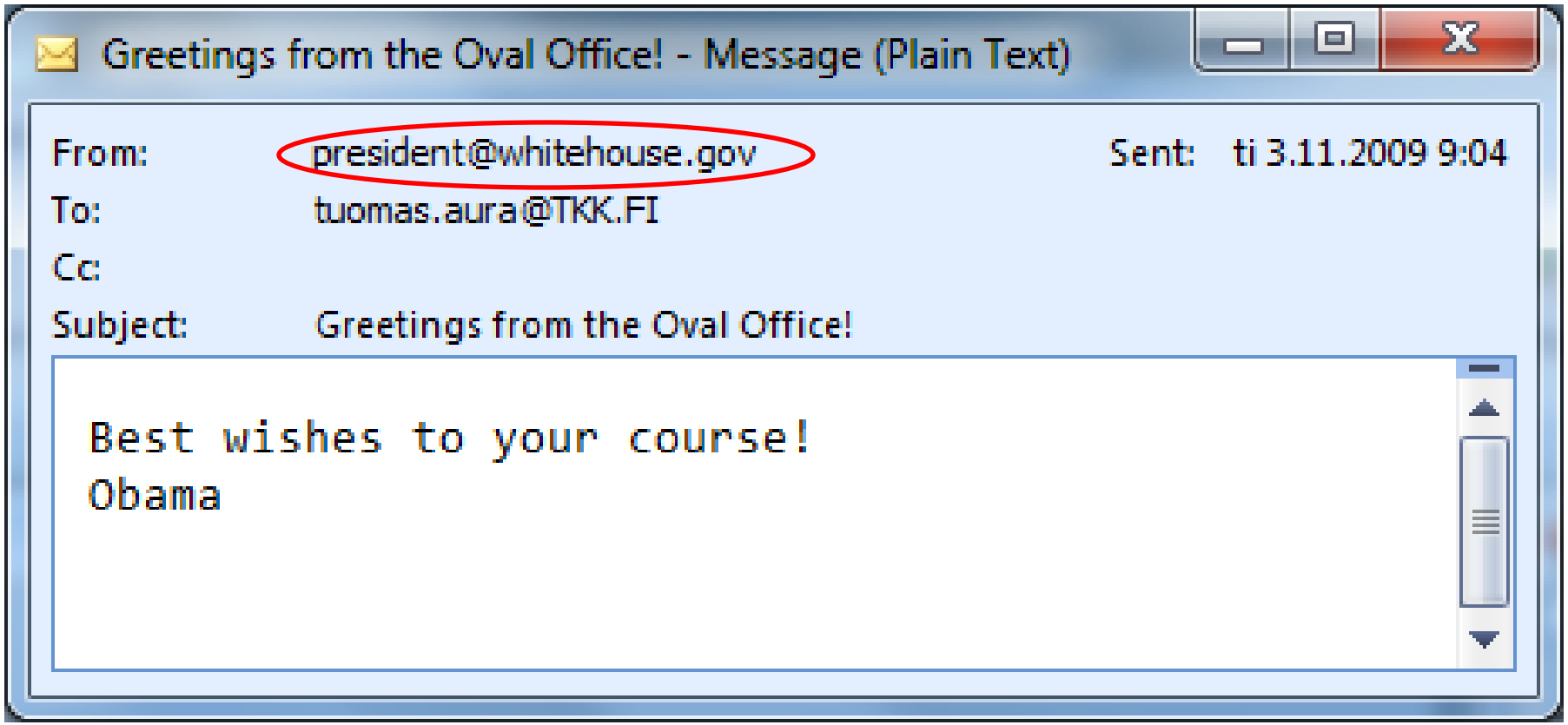
Salakuuntelu

- 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



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);
}
```

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

- Ohjelmistovirheet mahdollistavat tietokoneiden kaappaamisen ja haittaohjelmien leviämisen

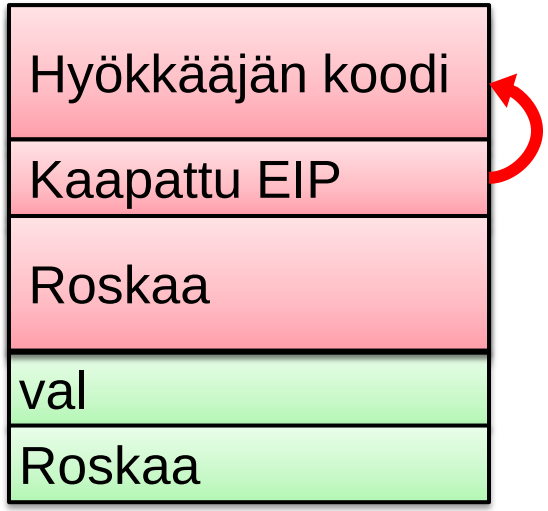
Ohjelmistovirheet

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

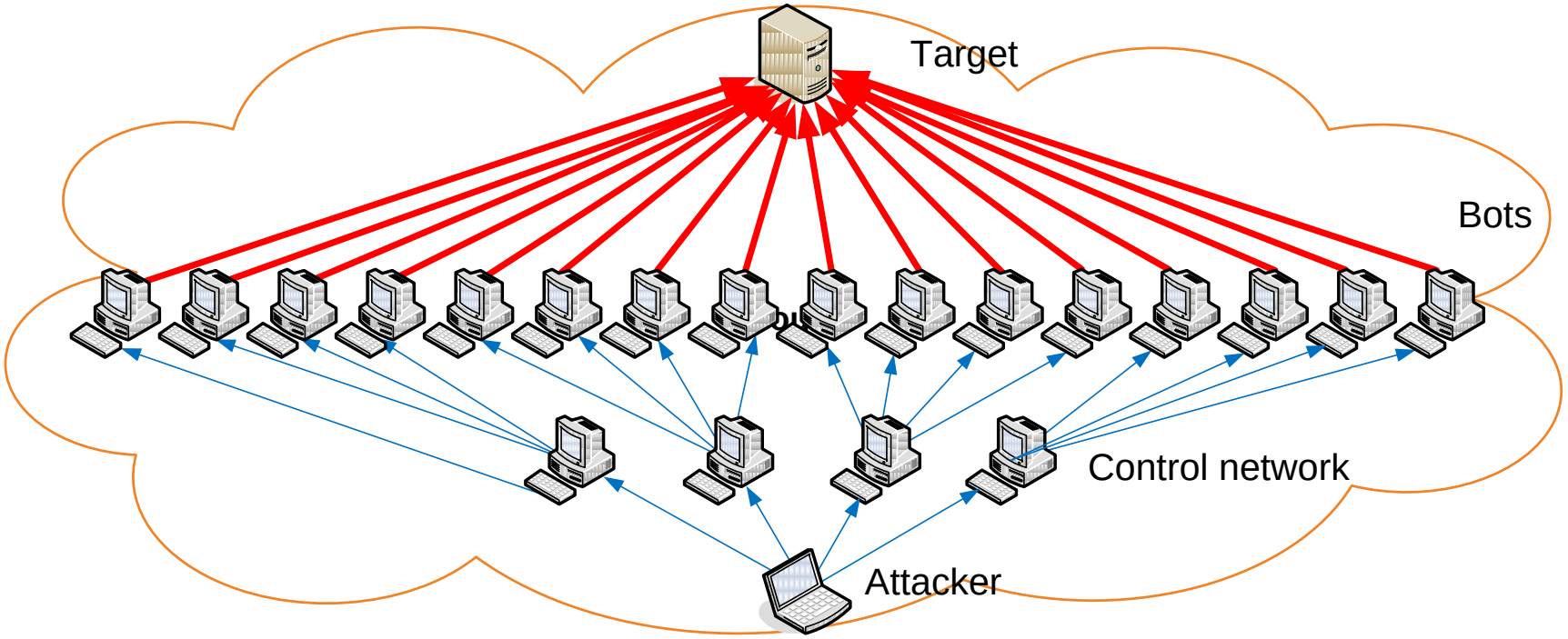
- Virukset ja madot leviävät itsestään
- Troijalainen on viattomalta näyttävä ohjelma, joka kätkee haittaominaisuuksia
- Rootkit kätkeytyy koneelle
- Vakoiluohjelma etsii ja lähettää tietoa koneelta hyökkääjälle
- Ennen haittaohjelmat olivat harrastajien tekemiä, nykyään ammattirikollisten
  - Eivät 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 webbisivut
  - 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

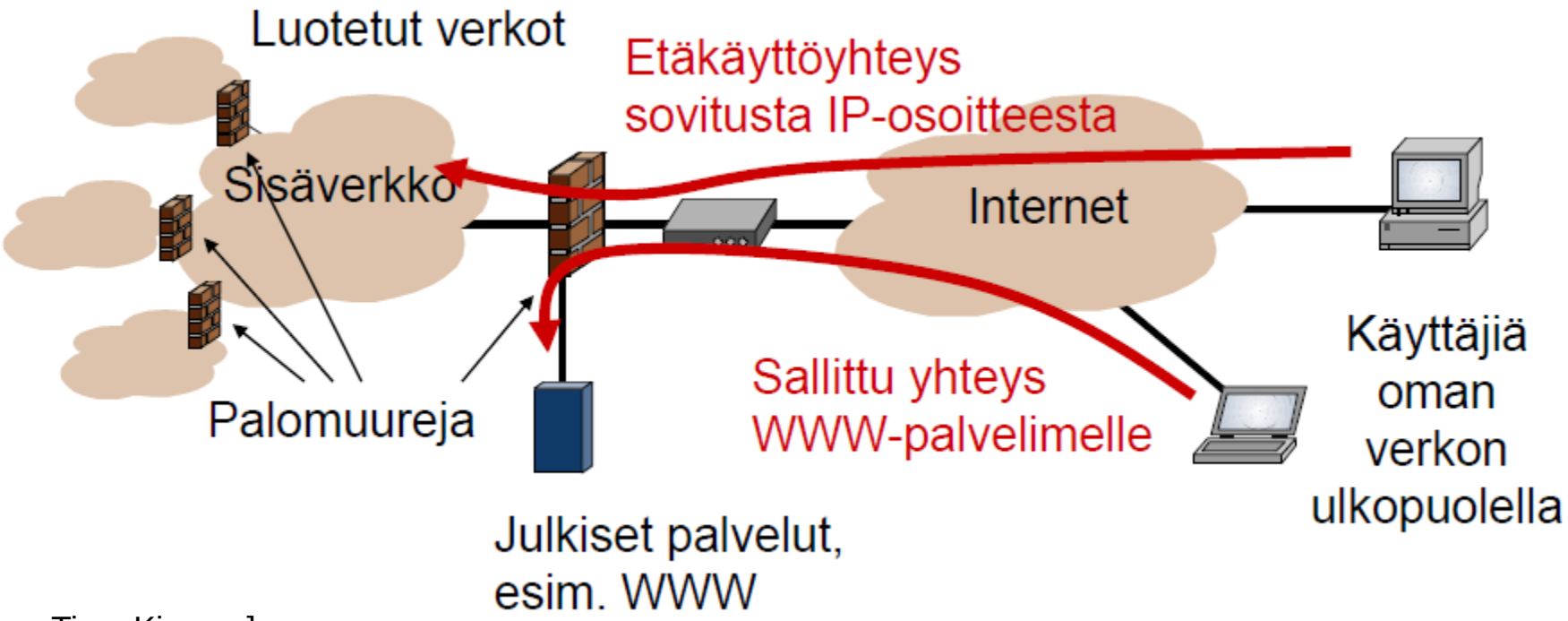
- Hyökkääjä voi estää rehellisiä asiakkaita käyttämästä palvelua ylikuormittamalla palvelimen tai verkon
- Hajautetussa palvelunestossa hyökkääjällä on botnet



TIETOVERKKOJEN TURVARATKAISUJA

Palomuuri

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

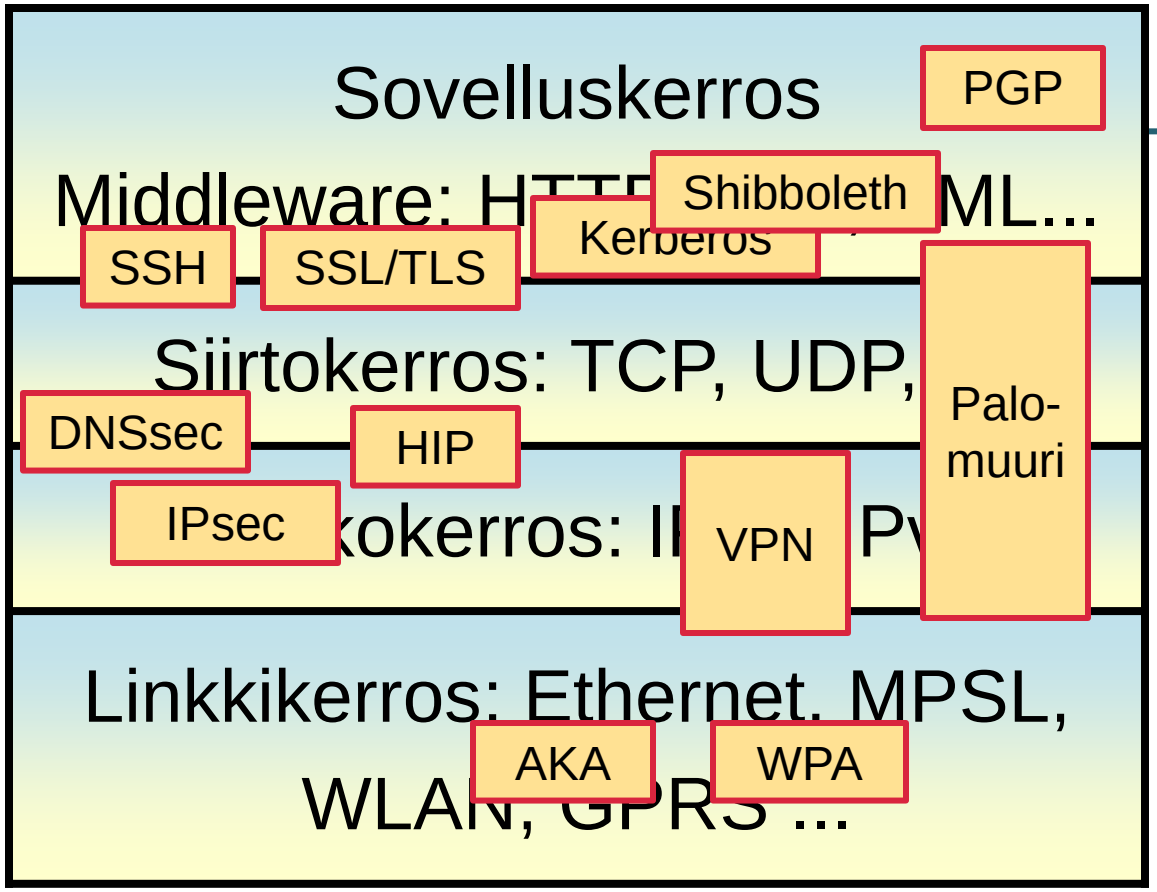


[Kuva: Timo Kiravuo]

Salaustekniikat

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

Tietoturvaprotokollat



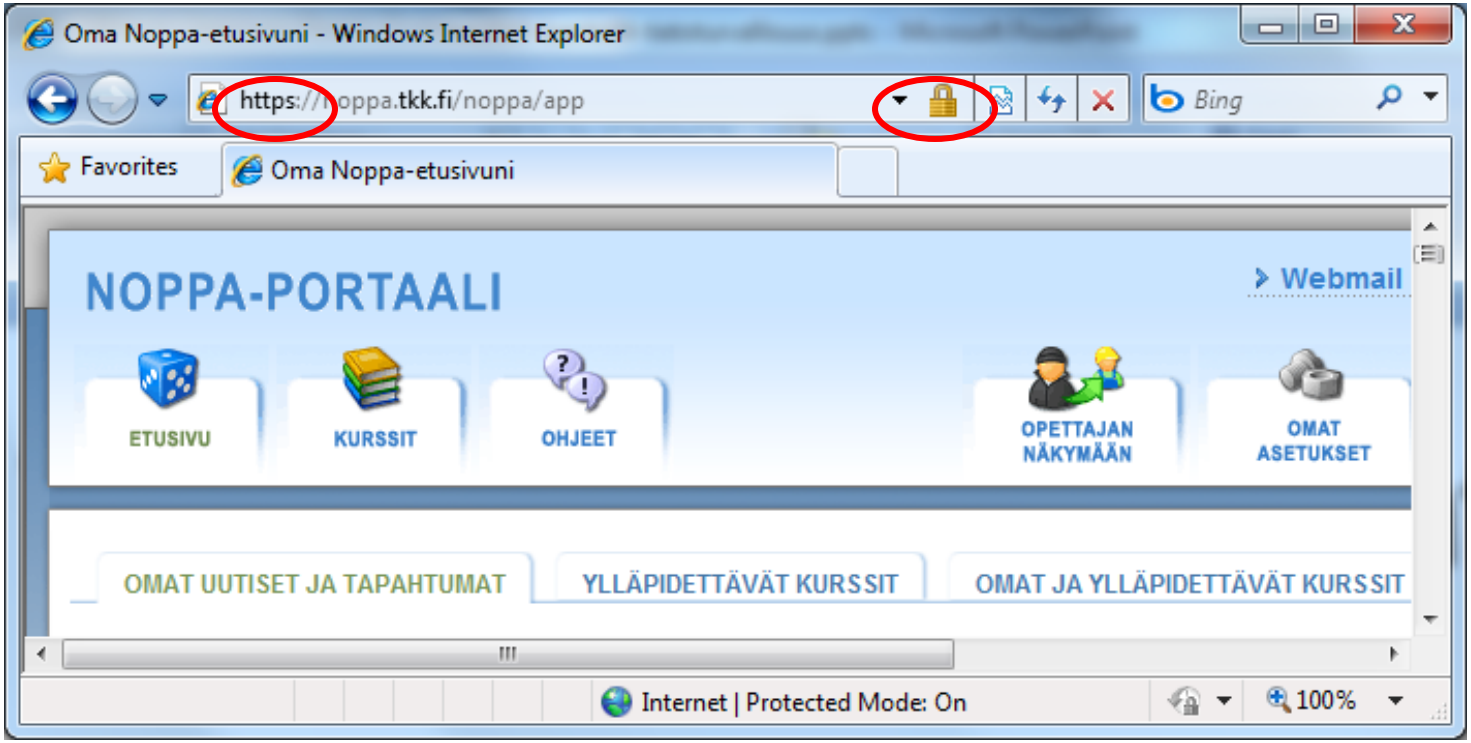
Sovellusten turvallisuus, esim. sähköinen kaupankäynti

Tiedonsiirron luottamuksellisuus ja ja eheys

Verkko-infrastrustuurin luotettavuus

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