# Internetin tietoturva - kuka on heikoin lenkki?

TkL Markus Peuhkuri

27.2.2008

## Luennon aiheet

- Turvallisuudesta
- Ohjeita, tapauksia
- Miten hyvät asiat menevät pilalle

## Otsikoita turvallisuudesta

- Slammer-mato sulki Davie-Besse ydinreaktorin ohjausverkon 2002
- Blaster-mato viivästytti sähkönsiirtoverkon mittaustietoja ja oli yksi osasyyllinen Koillis-Yhdysvaltojen sähkökatkoon 2003
- Panix.com[1] menetti piirinimensä hallinnan tammikuussa 2005. Asiakkaiden sähköposti ohjautui kolmannen osapuolen palvelimelle.
- Ryhmä varasti väärillä viivakoodeilla tavaraa 1,5 MUSD arvosta Wal-Mart-kauppaketjulta
- Murtautujalla oli pääsy T-Mobilen verkkoon 7 kk ajan ja pääsi käsiksi henkilötietoihin, valokuviin ja FBI:n dokumentteihin
- Englantilainen nainen ei voi nukkua, koska joku varasti aivotahdistimen kaukosäätimen, laitteen vaihtaminen vaatii uuden leikkauksen.
- Teho-osaston koneet osana botnettia: olivat käyttökelvottomia, ovet eivät avautuneet, tietoja ei pystytty syöttämään.
- Ainankin 218 621 856 henkilötietuetta hävinnyt Yhdysvalloissa 2005 alusta `http://www.privacyrights.org/ar/ChronDataBreaches.htm`

## Kuinka selvitän henkilön salasanan?

- Asenna koneeseen troijalainen tai valvontaohjelma
  - − netbus, back orifice, bo2k
  - \+ salakuuntelu, -katselu, tiedostojen selailu
  - \- antivirusohjelmat tunnistavat
    ⇒ täytyy koodata itse
- Salakuuntele (langatonta)verkkoa nykyään vaikeampaa, mutta sopivia laitteita löytyy verkkoliitäntään asennettaviksi.
- Asenna koneeseen näppäilyt tallentava laite: tallentaa 64Ki näppäilyä, USD90

[1] Iso internet-operattori New Yorkissa

- Hanki TEMPEST-laitteisto
  - . . . tai, osta lahjaksi langaton näppäimistö

## . . . tai kysy vain!

- Vetoa ongelmaan – haluan vain auttaa: (keskiviikkoiltana)
- Huijaa aloittelevaa työntekijää

**h** Tietoturvaosastolta Mika terve, tervetuloa taloon! Oletko saanut jo opastuksen tietoturva-asioista?

**u** En vielä.

**h** No, käydään sitten läpi perusasioita:

**. . .** *keskustelua*

**h** . . . salasanasta vielä, siinä pitää olla sekä isoja ja pieniä kirjaimia että numeroita. Onko salasanassasi niitä?

**u** Ei, se on vain tyttönimeni “pienranta”.

**h** Et olisi saanut sanoa sitä, mutta se ei ole kovin hyvä. Parempi olisi lisätä siihen vaikka kuukausi ja vuosi, esimerkiksi “PienrantaHel03”

**u** Joo, vaihdan sen. Osaan tehdä sen.

**. . .** *keskustelua*

**h** Etköhän pärjäile, hyvää työntekoa.

## Miten ihmistä huijataan?

- Vastavuoroinen auttaminen
- Auktoriteetti
- Sääli
- “Tiimipelaaja” — auta kaveria pulassa
- Ahneus
- Luottamusta pienin askelin

## Turvaongelmat

**Protokollaongelmat** protokollien suunnittelussa ei riittävää painoa turvaominaisuuksiin

- IP-lähdereititys
- FTP-protokolla

**Ohjelmistovirheet** syötteen olettaminen

- ohjelmointivirheet (puskureiden ylivuodot yms.)
- virheellinen toteutus protokollasta (esim. ICMP redirect)
- mitään *ei pidä olettaa* käyttäjältä tai verkosta tulevasta datasta
- sovellusten yhteistoiminta

**Konfigurointivirheet** oletuskonfiguraatio pielessä

- ominaisuudet tärkeämpiä kuin turvallisuus
- yleensä valitetaan “miksi tämä ei toimi”
  ⇒ oletusasetukset liian sallivia

## Haittaohjelmat

**Virus** leviää toisten ohjelmien, dokumenttien tai verkkosivujen välityksellä (2007 lopussa yli 500.000 tunnettua, joista puolet löydettiin vuoden 2007 aikana. Vuodessa tuli siis enemmän viruksia kuin vuosina 1986 – 2006. )

- tuhoaa tiedostoja, jopa laitteistoja
- muuntaa tiedostoja
- heikentää suorituskykyä

**Mato** leviää itsenäisesti järjestelmästä toiseen verkon yli

- voi heikentää myös verkon suorituskykyä
- CodeRed, Slammer

**Troijan hevonen** näennäisesti hyödyllinen ohjelma tai dokumentti jolla on salainen toimintatapa

- voi esimerkiksi mahdollistaa murtautumisen koneeseen

- Kukin tyyppi voi
  - paljastaa tietoja, esim. lähtettämällä tiedostoja sähköpostise
  - tarkkailla käyttöä, esim. tallentaa salasanoja
  - mahdollistaa murtautuminen, esim. avaamalla takaportin
- Haittaohjelma voi olla myös *räätälöity* murtautumaan ainoastaan tiettyyn järjestelmään tai paljastamaan yksittäisen käyttäjän tietoja. Tälläistä haittaohjelmaa eivät normaalit virustorjuntaohjelmat välttämättä tunnista. Tämä on eräs tapa teollisuusvakoiluun.
- Yhä useammin osa järjestäytynyttä rikollisuutta

## Nykyiset uhkakuvat

- Virustehtailu muuttunut ammattimaiseksi
- Ennen: huomion tai maineen herättämistä
- Nyt: koneen ottaminen haltuun
  - salasanojen seuranta
  - luottokortti- ja pankkitietojen saaminen
  - haittaohjelmien levittäminen
  - ei aiheuta vahinkoa, välttää havaitsemista: loinen
- Kaapatut koneet muodostavat botnetin
- Drive-by-downloads: 1 websivu 1000:sta yrittää saastuttaa koneen

## Palomuurit

- Palomuuri eroittaa kaksi *eri turvapolitiikkaa* noudattavaa aluetta
  - yrityksen sisäinen verkko vs. Internet
  - myös yrityksen sisäisessä verkossa esim. osastojen välillä
- Yksikerroksinen palomuuri
  - yksi kone kahden verkon välissä
  - yksinkertainen konfigurointi, virheet vakavia
- Monikerroksinen palomuuri

  - palomuuritoiminnallisuus hajautettu useiden laitteiden välille
  - neutraaliverkko (DMZ) erotettavien verkkojen välillä
- Konekohtainen ohjelmistopalomuuri
  - ohjelmisto tarkkailee koneen liikennettä
  - mahdollistaa ohjelmapohjaisen valtuutuksen: ainoastaan nimetyt ohjelmat saavat liikennöidä tietyllä tavalla verkkoon
    ⇒ hienojakoinen turvallisuus
    ⇒ estää haittaohjelmia
  - turvallisuus riippuu koneen turvallisuudesta: esim. troijalainen voi kytkeä palomuurin pois päältä ennenkuin liikennöi verkkoon. Helppoa koneissa, jossa ei ole erillistä pääkäyttäjää (koti-windowssit), mahdollista myös paremmissa järjestelmissä, mikäli on paikallinen turva-aukko.

## Palomuurit

- Läpinäkyvyysvaatimus

  > The introduction of a firewall and any associated tunneling or access negotiation facilities *MUST NOT* cause unintended failures of *legitimate* and *standards-compliant* usage that would work were the firewall not present.[1]

- Tuottaa helposti "kova ulkoa, pehmeä sisätä"-suojauksen
  ⇒ *kun* hyökkääjä saa ohitetua palomuurin, ei enää vaikeuksia
- Sisäisten järjestelmien päivittämisellä ei aina pidetä kiirettä

## Kolme askelta tietoturvaan

1. Käyttöjärjestelmä ajan tasalle
   - kaikista järjestelmistä löytyy virheitä
     ⇒ säännöllisesti tarkistettava tietoturvapäivitykset
2. Virustorjuntaohjelmisto
   - ei tarpeen, mikäli sovellusohjelmat *virheettömiä*
   - kaupallisissa ohjemissa 20-30 virhettä/KLOC: Mozilla 1.7 1600 KLOC[2]
3. Palomuuri käyttöön
   - ei tarpeen, mikäli järjestelmä ja palvelut turvallisia ja *virheettömiä*

## Kuinka turvallisuus rakentuu

- Turvallisuus on prosessi, ei tuote
  - uusia turvallisuusongelmia tulee
  - ympäristö muuttuu: verkko, sovellukset, käyttäjät
- Turvallisuus riippuu heikoimmasta lenkistä

| käytäjä | sovellukset | OS | laitteisto | verkko | palomuuri |
|---|---|---|---|---|---|

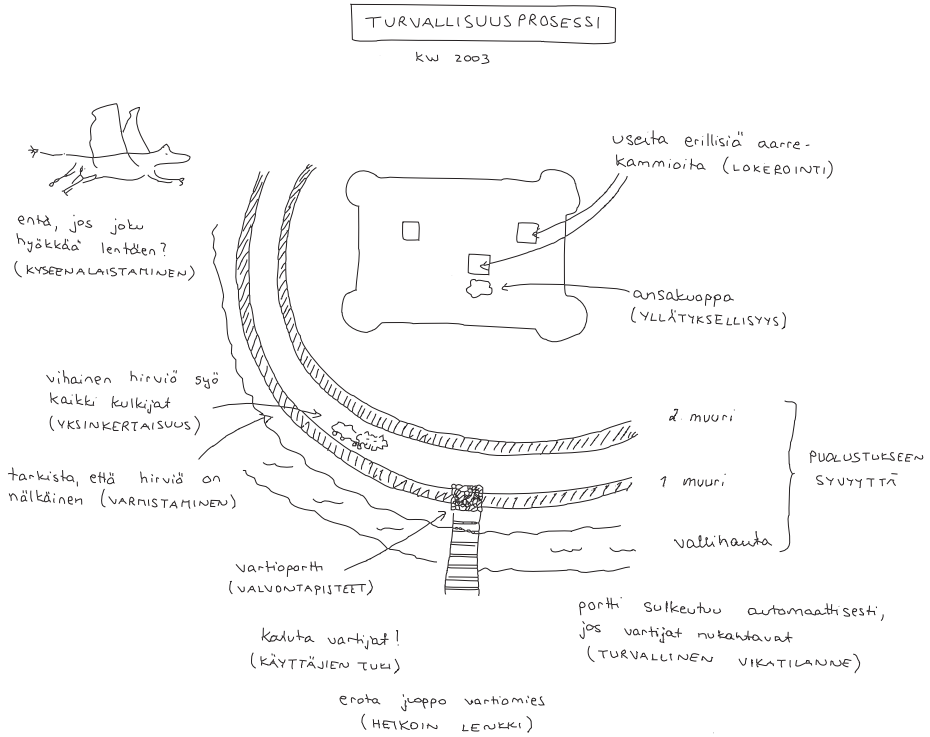
  Ei ole mitään merkitystä sillä, käytetänkö 40- vai 128-bittistä salausta tai 512- tai 2048-bittisiä RSA-avaimia, jos salasanan saa arvattua, kysyttyä käyttäjältä tai salakuunneltua koneesta.

[2]Kilo Lines of Code: tuhansia ohjelmakoodirivejä

## Kuinka parantaa turvallisutta?

- Lisätään tekniikkaa
  - lisää monimutkaisuutta
  - järjestelmät jäykkiä ⇒ kierrettäviä
  - luotetaan turvajärjestelmiin liikaa
  + lisää liikevaihtoa
- Vaaditaan parempi tunnistus
  - lisää monimutkaisuutta
  - virheellisten estojen määrä kasvaa
- Koulutetaan käyttäjiä
  + motivoitunut käyttäjä erinomainen suoja
  - aina on onnistuttu hämäämään joitakin jonkinaikaa
  - jos turvajärjestelmä estää työnteon, se kierretään
- Parannetaan prosesseja
  + toiminnan laatu paranee
  - työlästä: pitää miettiä miksi näin tehdään

## Turvallisuus organisaatiossa




## Turvallisuus ↔ vaarattomuus

- Security ↔ safety
- Järjestelmän vaarattomuutta tutkittaessa voidaan hyvin harvinaiset tapaukset jättää huomioimatta
- Turvallisuudessa pitää huomioida myös epätodennäköisiä yhteensattumia
  – hyökkääjä pyrkii saamaan järjestelmän nurin

  - menetelmä voi olla täysin arvaamaton
- Väärien positiivisten ja negatiivisten suhde oltava järkevä
- Absoluuttien turvallisuus tuhon alku (Titanic, Enigma)

## Turvallisuuden viisi askelta

1. Mitä haluan suojata?
2. Mitkä ovat riskit?
3. Kuinka hyvin turvaratkaisu suojaa riskeiltä?
4. Mitä muita riskejä turvaratkaisu aiheuttaa?
5. Mitä kustannuksia ja kompromisseja ratkaisusta aiheutuu?

## Riskien arviointi: yleisesti ihmiset

- Aliarvioivat usein ottamansa riskit
- Yliarvioivat riskit
  - joihin eivät voi vaikuttaa
  - harvinaiset
  - huomiota herättävät, uutisoidut
  - personoidut riskit

## Turvallisuuden arviointi

- Kulu-tuottoarviointi
  - turvallisuus ei saa maksaa enempää kuin suojattava kohde
  - päällekkäiset hyödyt
  - vaikea arvioida turvattomuudesta tulevia kuluja tai turvallisuuden tuottoja
    $\Rightarrow$ käytännössä hankintojen kuluarviointi
- Lait, säätelyt ja julkisuus
  - lait asettavat minimivaatimuksia turvallisuudelle
  - yleisesti hyväksytyt periaatteet
  - maineen menettäminen

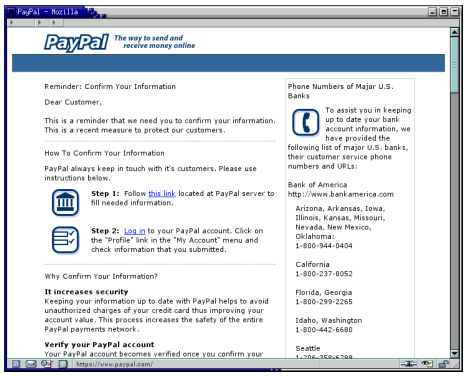
## Pankkikorttien kloonaus: lukija

## Lukija paikoillaan

## PIN-kamera esitekotelossa

## PIN-kamera toimintavalmiina

# Mistä tietää kuka siellä vastaa




# Katsotaas viestiä tarkemmin (HTML)

- Status-kenttää vaihdetaan 25 ms välein

```
var boodschap = 'https://www.paypal.com/';
function dgstatus()
{
      window.status = boodschap;
        timerID= setTimeout("dgstatus()", 25);
}
```

- Linkissä onkin IP-osoite

```
Follow <a href="http://210.78.22.113/verify.html">this
link</a> located at PayPal server to fill needed information.
```

- PayPal on Kaliforniassa

```
Domain Name: PAYPAL.COM

Administrative Contact, Technical Contact:
   Inc., PayPal  (36270680P)         hostmaster@PAYPAL.COM
   1840 Embarcadero Rd.
   Palo Alto, CA 94303
   US
   408-376-7400 fax: 650.251.1101
```

- `www.paypal.com` on myös

```
www.paypal.com has address 64.4.241.32
OrgName:    PayPal
OrgID:      PAYPAL
Address:    303 Bryant Street
City:       Mountain View
StateProv:  CA
PostalCode: 94041
Country:    US

NetRange:   64.4.240.0 - 64.4.255.255
CIDR:       64.4.240.0/20
```

- Ilmeisesti päivityspalvelin (`210.78.22.113`) ulkoistettu Kiinaan?

```
inetnum:      210.78.22.64 - 210.78.22.128
netname:      SHJITONG-CN
```

```
descr:        JiTong Shanghai Communications Co.,Ltd
address:      Room 1001,Lekai Builing,Shangcheng Road,
address:      Pudong Xin district,Shanghai
country:      CN
```

## Muita vedätyksiä

- Näytetty linkki ja “oikea” linkki eivät vastaa toisiaan

```
...secure server
<a href="http://www.scam.example/">
https://www.paypal.com</a>...
```

- Melkein sama nimi
  - www.PayPaI.com
  - www.PayPa1.com
  - www.paypal-secure.com
  - homomorfismi: `www.p&#1072;ypal.com`
- http://www.paypal.com:secure.information.update@10.12.80.5/
- http://www.paypal.com%01:secure@10.12.80.5/
- Monia vastaavia huijauksia toteutettu eri yrityksille, tyypillisesti pankeille
- Ensimmäiset suomenkieliset

  > Toivoen ymmartamyksen ja kannatuksen Teidan puolelta.
  > Kunnioittaen,
  > Hallinto

## Toinen phishing-hyökkäys

- `From: ITviikko Digilehti <itviikko.digilehti@sanoma.fi>`
- Rekisteröintilinkki

```
Rekisteröidy Digilehden lukijaksi
<A href="http://www.webstudio.fi/itviikko/esittely.html"
target=_top>tästä</A>
```

Ei `itviikko.fi`?

```
domain:   webstudio.fi
descr:    SOPRANO COMMUNICATIONS OY
```

- Sähköpostin lähettäjä:

```
Received: from mail pickup service by mail.swelcom.fi
   with Microsoft SMTPSVC; Thu, 20 Jan 2005 12:50:28 +0200
```

Ehkä murrettu palvelin, ei **itviikko.fi**?

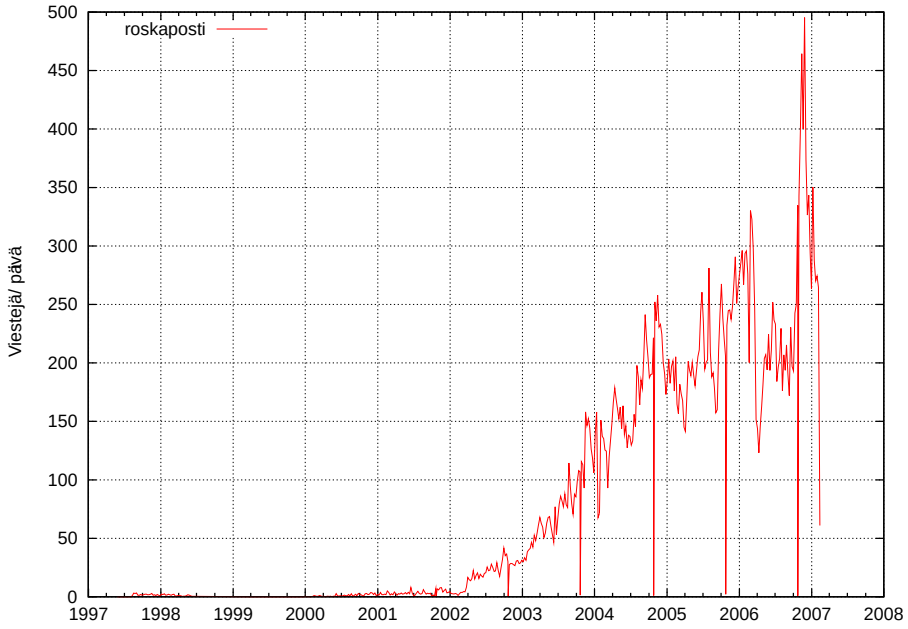
```
domain:   swelcom.fi
descr:    SWelcom Oy
```

## Toinen phishing-hyökkäys

- Web-osoite osoittaa jonnekin muulle ja jokin kolmas osapuoli on lähettynyt joku kolmas osapuoli
  ⇒ Phishing-hyökkäys?

Viesti oli kuitenkin “oikea” (varmistettu ITViikon toimituksesta), vaikka siinä oli kaikki phishing-hyökkäyksen merkit. Tavallisen käyttäjän on hyvin vaikea eroittaa “oikeat” ja “huijaus”sähköpostit; teknisesti ei välttämättä mitään eroa.

## Roskaposti – kiusasta ongelmaksi




## Roskapostin torjunnasta

- Tekninen ratkaisu ei ole lopullinen
  - verkkoliikennettä
  - prosessointia
  - suodattimet ja järjestelmät kierrettävissä
- Ratkaisu saatava polittiselta tasolta
  - pääosa spämmistä on peräisin Yhdysvalloista
  - suurin osa tulee nykyään Kiinan ja Korean kautta
  - oikeuslaitoksen uhka ainoa “todellinen” hidaste
    ⇒ follow the money

## Yhteenveto

- Turvallisuus on monen asian summa
- Hyökkäykset muuttuvat ja muttavat pelin sääntöjä
- Turvallisuus on aina valinta ja kompromissi
- Tekniset järjestelmät kierrettävissä
  ⇒ huolehdittava siitä, että järjestelmä ei romahda

# Viitteet

[1] N. Freed. *Behavior of and Requirements for Internet Firewalls*, October 2000. RFC 2979. URL:`http://www.ietf.org/rfc/rfc2979.txt`.