Internetin tietoturva - kuka on heikoin lenkki?

Markus Peuhkuri

2004-02-26

Luennon aihe

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

Kuinka selvitän henkilön salasanan?

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

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

. . . tai kysy vain!

- Vetoa ongelmaan – haluan vain auttaa: (keskiviikkoiltana)

h Ylläpidosta Mika terve; tietomurron takia palvelimet joudutaan asentamaan uudelleen — tiedostot ovat käytettävissä taas maanantaina.

u Ei tule mitään! Minun pitää saada suunnitelma valmiiksi perjantaihin menessä asiakkaalle tai tulee firmalle isot sakot.

h Joo, joo. Arvaa oletko ainoa joka sanoo noin? Itselläni on *hauska* viikkonloppu tiedossa.

u Mikä oli nimesi? Kukas on esimiehesi? Soitan hänelle, niin saa pistää asiat tärkeysjärjestykseen.

h Huoh. . . No joo, voin koettaa saada tiedostosi väliaikaispalvelimelle, mutta sitä varten tarvitsen tunnuksesi ja salasanasi.

u Mitäs. . . ? Eihän ylläpito koskaan kysy salasanaa? Kuka oikein olet?

h Hei, koetan vain saada ne tiedostosi sinulle! Jos annat salasanasi, voin kopioida sinun tiedostosi nopeasti — toinen vaihtoehto on kopioida koko palvelin; saat tiedostot maanantaina.

u Njaa...

h Odotas hetki, käyn hakemassa paperisi… Työntekijänumerosi on 24671 ja eka salasanasi on ollut “changeme98”.

u Äh. Ok. Salasana on “Uuponen02”.

h Hyvä. Tiedostosi ovat näkyvissä puolen tunnin kuluttua.

- 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”
  $\Rightarrow$ oletusasetukset liian sallivia

Haittaohjelmat

Virus leviää toisten ohjelmien tai dokumenttien välityksellä (2001 lopussa yli 60.000 tunnettua, joista ainoastaan muutamia satoja on tavattu levinneinä “villinä”.)

- 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.

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
    $\Rightarrow$ hienojakoinen turvallisuus
    $\Rightarrow$ 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.
- 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
  $\Rightarrow$ *kun* hyökkääjä saa ohitetua palomuurin, ei enää vaikeuksia

Kolme askelta tietoturvaan

(www.tietoturvaopas.fi)

1. Käyttöjärjestelmä ajan tasalle
   - kaikista järjestelmistä löytyy virheitä
     $\Rightarrow$ säännöllisesti tarkistettava tietoturvapäivitykset
2. Virustorjuntaohjelmisto
   - ei tarpeen, mikäli sovellusohjelmat turvallisia
3. Palomuuri käyttöön
   - ei tarpeen, mikäli järjestelmä turvallinen

Kuinka turvallisuus rakentuu

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

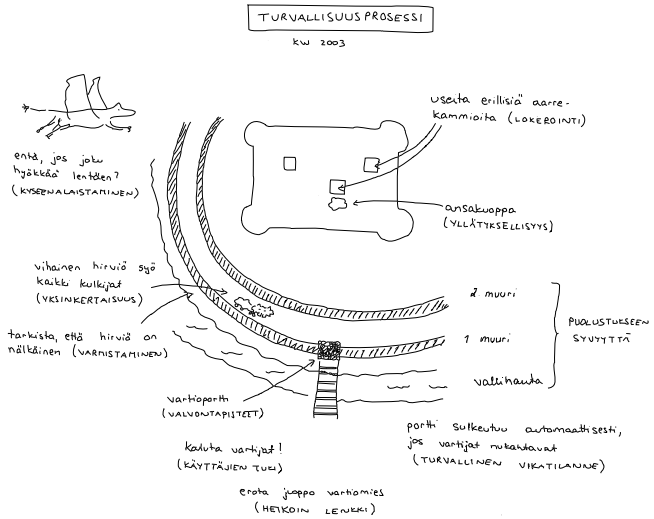
käytäjä	sovellukset	OS	laitteisto	verkko	palomuuri

  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.

Kuinka parantaa turvallisutta?

- Lisätään tekniikkaa
  - lisää monimutkaisuutta
  - järjestelmät jäykkiä $\Rightarrow$ kierrettäviä
  + lisää liikevaihtoa
- Vaaditaan parempi tunnistus
  - lisää monimutkaisuutta
  - virheellisten estojen määrä kasvaa
- Koulutetaan käyttäjiä
  + motivoitunut käyttäjä erinomainen suoja
  - aina on onnistuttu hämäämään joitakin jonkinaikaa

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?

Lentokoneturvallisuus

	pinsetit kielletään	tulitikut kielletään
1	estää koneen kaappaaminen pinseteillä uhkaamalla	estää koneen vahingoittaminen tulipalolla
2	kaappaaja nyppii lentoemännän ripset	kaappaaja sytyttää läjän lehtiä palamaan (747:ssä noin 250 kg paperia + yli 100 l väkevää alkoholia)
3	vähentää riskin mahdollisuutta	vähentää riskin mahdollisuutta
4	-	-
5	tarkempi tarkastus, matkustajan ärtymys (käsilaukun siivoaminen ennen lentomatkaa yms.)	tarkempi tarkastus, matkustajan ärtymys, tupakoinnin väheneminen

Kumpi on parempi lobbaaja: Pinsetin käyttäjät ry. vai tupakkateollisuus?

Arvioi riskejä

- Aseta eläimet vaarallisuusjärjestykseen (kuolemantapauksia Yhdysvalloissa)
  - hai
  - koira
  - käärme
  - peura
  - sika
- Todennäköisin kuolinsyy 2000-2003 (Yhdysvalloissa)
  - diabetes
  - junaonnettomuus
  - lentokoneonnettomuus
  - maaliikenneonnettomuus
  - murha
  - salamanisku
  - terrori-isku
  - tulva

- Todennäköisin kuolinsyy 2000-2002 (Suomessa)
  - kurkunpää-, henkitorvi-, keuhkosyöpä
  - diabetes
  - influenssa
  - keuhkokuume
  - astma
  - maaliikennetapaturmat
  - vesikuljetustapaturmat
  - tapat. kaatumiset ja putoamiset
  - hukkumistapaturmat
  - myrkytystapat. pl. alkoholimyrkytys
  - itsemurhat
  - murhat, tapot, muu tahall. pahoinpit.

Ja vastaus on..

- Aseta eläimet vaarallisuusjärjestykseen (kuolemantapauksia Yhdysvalloissa, kokonaismäärä/vuosi)
  1. peura (135)
  2. koira (18)
  3. käärme (15)
  4. sika (?)
  5. hai (0,6)
- Todennäköisin kuolinsyy 2000-2003 (Yhdysvalloissa vuosittain)
  1. diabetes (68 000)
  2. maaliikenneonnettomuus (41 000)
  3. murha (15 600)
  4. terrori-isku (1 000)
  5. lentokoneonnettomuus (631)
  6. junaonnettomuus (530)
  7. tulva (139)
  8. salamanisku (87)

- Todennäköisin kuolinsyy 2000-2002 (Suomessa, 1/100 000)
  1. keuhkokuume (41)
  2. kurkunpää-, henkitorvi-, keuhkosyöpä (32)
  3. itsemurhat (21)
  4. tapat. kaatumiset ja putoamiset (18)
  5. diabetes (9,2)
  6. maaliikennetapaturmat (7,2)
  7. myrkytystapat. pl. alkoholimyrkytys (3,4)
  8. hukkumistapaturmat (2,7)
  9. murhat, tapot, muu tahall. pahoinpit. (2,7)
  10. astma (1,8)
  11. vesikuljetustapaturmat (1,2)
  12. influenssa (1,2)
- Yleensä ihmiset
  - aliarvioivat usein ottamansa riskit
  - yliarvioivat riskit, joihin ei voi vaikuttaa

Pankkikorttien kloonaus: lukija

Lukija paikoillaan

PIN-kamera esitekotelossa

PIN-kamera toimintavalmiina

Yleiset päätason piirinimet (gTLD)

- Alunperin Internet Yhdysvaltain sisällä käytettäväksi
  ⇒ USA-keskeiset määrittelyt

  .gov USA:n hallituksen organisaatiot (esim. `fbi.gov`, `whitehouse.gov`)

  .mil USA:n armeijan käyttöön (esim. `af.mil`)

  .edu pääasiassa yhdysvaltalaiset yliopistot (esim. `mit.edu`, `harward.edu`)

- Myöhemmin laajennettu kansainväliseksi [2]

  .com kaupallisille yrityksille, nykyään erittäin laajaksi paisunut, noin 21 miljoonaa piiriä (esim. `sun.com`, `whitehouse.com`)

  .net alunperin verkko-operaattoreille tarkoitettu, nykyään sisältää mitä tahansa (esim. `uusitupa.net`), noin 3,6 miljoonaa

  .org erilaisia organisaatioita, jotka eivät sovellu muihin ryhmiin – tai ole saaneet `.com`-piiriä (esim. `eff.org`, `debian.org`, `amnesty.org`, `metso.org`), noin 2,6 miljoonaa

  .int kansainvälisille, valtioiden välisillä sopimuksilla perustetuille organisaatioille (esim. `un.int`, `itu.int`, `nato.int`, 47 kappaletta)

- Uudet, 2001-02 voimaan tulleet piirinimet (tilanne 2003-01-09, lukumäärät osin 2002-09-31)

  .aero lentoyhtiöiden käyttöön – Societe Internationale de Telecommunications Aeronautiques SC, (SITA); 2.600 kpl

  .biz yritystoimintaa varten – JVTeam, LLC; 770.000

  .coop yhteistoiminnallisille yrityksille – National Cooperative Business Association, (NCBA): satoja

  .info rajoittamton – Afilias, LLC, 950.000

  .museum museot – Museum Domain Management Association, (MDMA): 600 kpl 2. tason piirinimiä

  .name yksityishenklöille 3. tasolla `john.doe.name` – Global Name Registry, LTD: 86.000

  .pro "ammattilaiset", esim. `johnDoe.med.pro` – RegistryPro, LTD; ei vielä toiminnassa

Piirinimien hankkiminen

- Yleiset päätason piirinimiet
  - useita rekisteröijiä
  - hinnat vaihtelevat
  - lista `http://www.icann.org`
  - ensin varannut saa nimen, prosessi "kiristyksen" estämiseksi

  Alunperin `.com`, `.net` ja `.org` piirinimien jako oli InterNIC:n yksinoikeus. Tämä varma (USD 35/vuosi/nimi) tulonlähde herätti kovasti kritiikkiä ja vuoden 1999 alusta lähtien on ollut muitakin rekisteröijiä.

- Maakohtaiset piirinimet
  - eri maissa erilaisia käytäntöjä

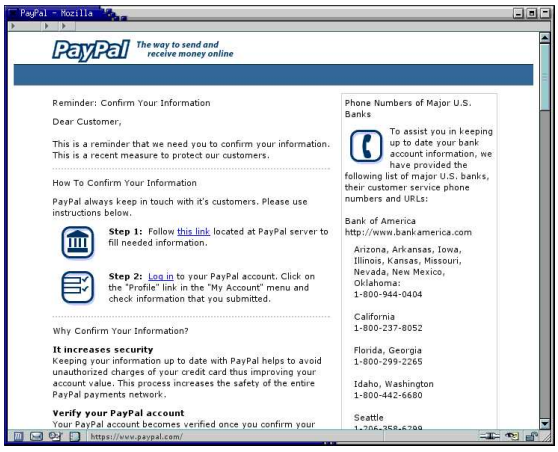
    Suomi, fi ennen varsin tiukat säännöt, nyt jälkivalvonta: " *hakija vastaa itse siitä, ettei haettu verkkotunnus oikeudettomasti perustu toisen tavaramerkkiin tai nimeen.*" `http://www.ficora.fi/suomi/`

    Japani, jp yrityksen tulee toimia Japanissa ja transliteroinnin oltava oikein

    Tuvalu, tv (470.000)

    Tonga, to "ostettu" maakoodi, vapaasti rekisteröitävissä (2.500)

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

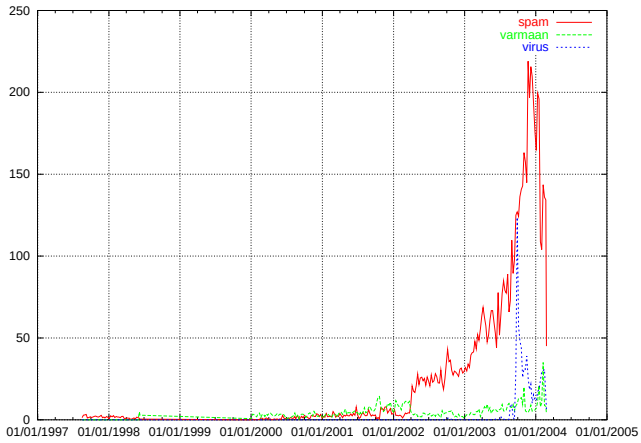
- Näytetty linkki ja “oikea” linkki eivät vastaa toisiaan

```
...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
- 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

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
  - oikeuslaitoksen uhka ainoa “todellinen” hidaste

Yhteenveto

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

Viitteet

[1] N. Freed. Behavior of and Requirements for Internet Firewalls. Request for Comments RFC 2979, Internet Engineering Task Force, October 2000. (Informational). URL:`http://www.ietf.org/rfc/rfc2979.txt`.

[2] J. Postel. Domain Name System Structure and Delegation. Request for Comments RFC 1591, Internet Engineering Task Force, March 1994. (Informational). URL:`http://www.ietf.org/rfc/rfc1591.txt`.