Samlink

Tietoturvallisempia sovelluksia

Sovelluskehitys ja -arkkitehtuuri
Kontakti.net
15.2.2006

TTRY
Tietoturva ry - www.tietoturva.fi

Jari Pirhonen – iki.fi/japi
Turvallisuuspäällikkö, CISSP, CISA
Samlink – www.samlink.fi

Samlink lyhyesti

- **Vähittäispankkitoiminnan IT-palvelujen ja tukipalvelujen toimittaja**
- **Liikevaihto 51,6 M€ ja liikevoitto 2,4 M€ (2004)**
- **Henkilöstö noin 270 henkilöä**
- **Informaatioteknologian ja pankkitoiminnan syvällinen tuntemus**
- **Monipankkijärjestelmien toimittaja**
- **Palveluprosessien erikoistuntemus**
- **Projektinhallintaosaaminen**

Peruspankkipalvelut

Verkkopalvelut

Johdon raportointi ja viranomaisraportointi

Laskenta- ja taloushallinnon palvelut

Asiakashallinta-järjestelmät

Infrastruktuuripalvelut

Suurimmat asiakkaat: Säästöpankit, Aktia, Paikallisosuuspankit, Suomen Hypoteekkiyhdistys

Samlinkin asiakaspankeilla on yhteensä

- **lähes 1,1 miljoonaa asiakasta, joita palvellaan yhteensä yli 460 konttorissa**
- **noin 250 000 Internet-pankkipalvelujen käyttäjää**

Tietoturva ry lyhyesti

- Tietoturva-ammattilaisten yhdistys
- Edistää tietoturvallisuutta, tietoturvatietoutta, jäsentensä ammattitaitoa sekä hyvien tietoturvatapojen noudattamista
- Järjestää tietoturvan CISSP-ammattisertifikaatin koulutusta ja tutkintotilaisuuksia
- Järjestää seminaareja, keskustelutilaisuuksia ja yritysvierailuja
- Tietoturvayhteistyötä

Lisätietoa:
www.tietoturva.fi
info@tietoturva.org

Liity jäseneksi:
www.tt-tori.fi

Suomen suurin turvallisuusalan yhdistys

- 750 henkilöjäsentä
- 40 yritysjäsentä
- Suomessa yli 150 CISSP-sertifioitua ammattilaista
- Tietotekniikan liiton jäsenyhdistys

TTRY
Tietoturva ry - www.tietoturva.fi

29.1.2006 Jari Pirhonen

Lähtökohta

- Sovellusturvallisuus on (taas) huomion kohteena
  - mainframe-maailmassa fokuksena – mihin unohtui?
- Sovelluspuolella toistetaan ”perinteiset” tietoturvavirheet
  - reaktiivisuus
  - tarkastetaan valmiin tuotoksen hyvyys
  - ongelman syyt tiedetään, mutta tyydytään oireiden hoitoon
  - tietoturvatuotteilla paikataan sovellusongelmia
- Tietoturvahaasteet lisääntyvät entisestään
  - monimutkaisuus
  - verkottuminen
  - uudet tekniikat
- Erään kaupallisen systeemityömallin arviointi
  - TKK Dipoli Turvallisuusjohdon kolutuksen tutkielma
  - saatavilla kotisivuiltani

29.1.2006 Jari Pirhonen

Samlink

Gartner

Tutkimusyhtiö Gartner varoittaa, että ohjelmisto-ongelmien aiheuttamat vuosittaiset häiriöajat kolminkertaistuvat 15 prosenttiin vuoteen 2008 mennessä niiden firmojen osalta, jotka eivät suhtaudu tietoturvaan ennaltaehkäisevästi rakentaessaan ja ostaessaan ohjelmistoja.

Syyt toimintakatkoksiin:
- 40% sovellusvirhe
- 40% ihmisen tekemä virhe
- 20% laitevika

Kypsyystasot SSE-CMM

5. Optimoitu	Tietoa kerätään automaattisesti prosessin optimoimiseksi
4. Hallittu	Prosessia mitataan ja parannetaan tulosten perusteella
3. Määritelty	Prosessi on määritelty, sitä noudatetaan ja kehitetään
2. Toistettava	Projektit ovat toistettavissa. Pääpaino projektinhallinnassa ja -seurannassa
1. Lähtötaso	Ei prosessia.

Tutkimus: @stake

- 45 businesskriittistä sovellusta
  - räätälöityjä, kaupallisia ja middleware tuotteita
  - $3,5 miljardin liikevaihto

⇒ yhteensä 500 tietoturvaongelmaa
⇒ ~10 tietoturvaongelmaa per sovellus

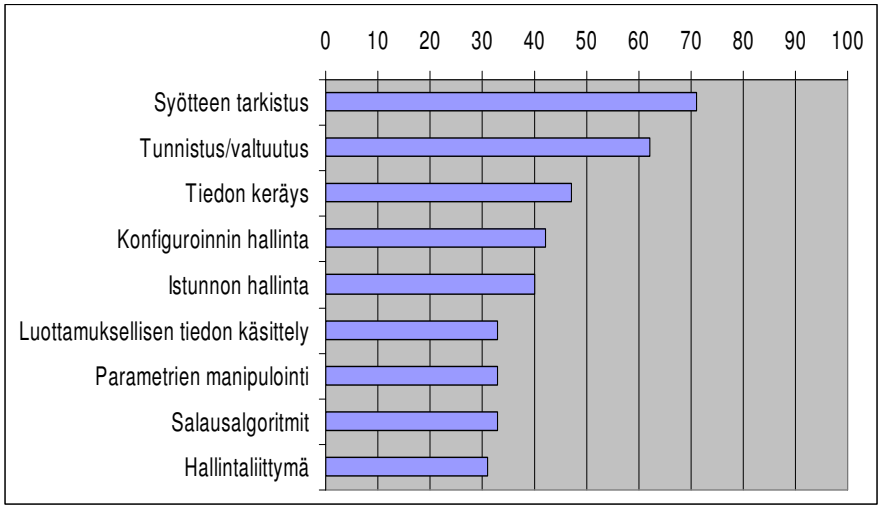
⇒ 70% kaikista tietoturvaongelmista suunnitteluvirheitä
⇒ 45% vakavista tietoturvaongelmista suunnitteluvirheitä

⇒ hyvät sovellustalot erottuvat hyvien ja turvallisten suunnittelu, koodaus ja käyttöönottotapojen ansiosta
  ⇒ työkaluilla, tuotteilla ja ohjelmointikielillä ei suurta merkitystä

http://www.netsourceasia.net/resources/atstake_app_unequal.pdf

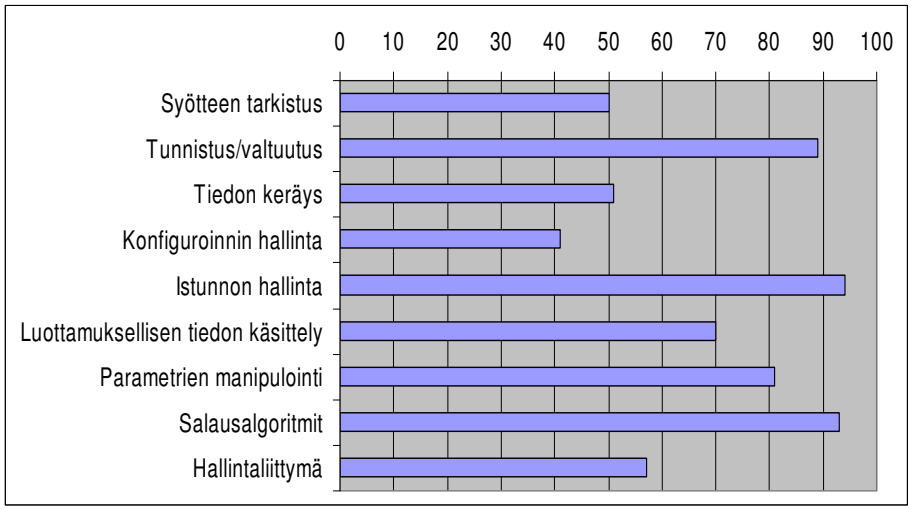
Samlink

Tutkimus: Tietyn tietoturvaongelman sisältävien sovellusten %-osuus



Samlink

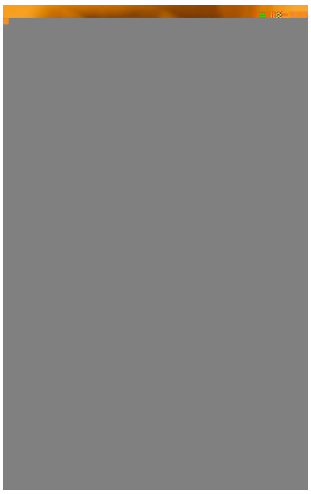
Tutkimus: Suunnitteluvirheiden %-osuus tietystä tietoturvaongelmasta



Samlink

Tietoturvatuotteet

- **Palomuuri – suojaa muita sovelluksia sinun virheiltäsi**
  - **rajoittaa hyökkäyskohteeksi ”vain” sovelluksesi**
- **SSL – salaa myös hyökkäyksen**
  - **suojaa liikenteen verkossa**
- **VPN – rajoittaa potentiaalisten hyökkääjien joukkoa**
  - **rajoittaa yhteydet ”luotettuihin” osapuoliin**
- **IDS/IPS – ei tunne sovellustasi**
  - **suojaa yleisiltä, tunnetuilta tuoteongelmilta**



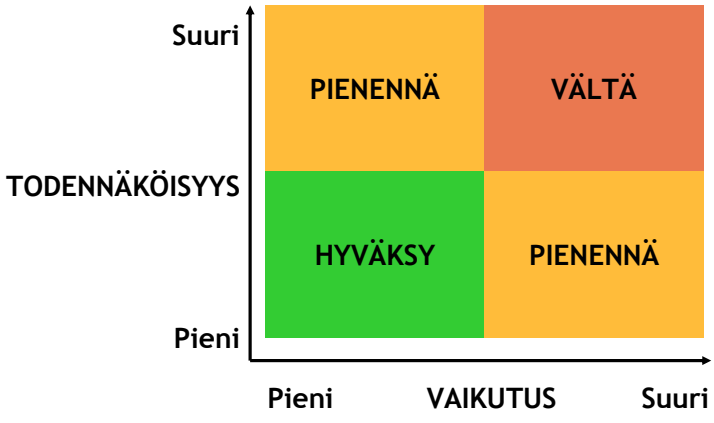
Vastuuta ei pidä sälyttää ohjelmoijille

Gartner: maailmassa arviolta vain 500 sovelluskehittäjää, joilla on tietotaito tieturvavirheiden löytämiseksi sovelluskoodista tehokkaasti

Tietoturvaosaajat?

Lähde: Tietoviikko

Tietoturva on riskien hallintaa

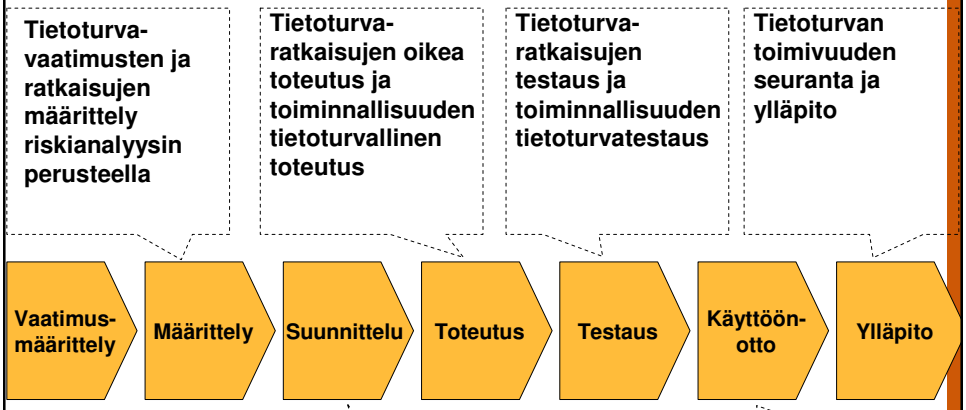


Määritelmä

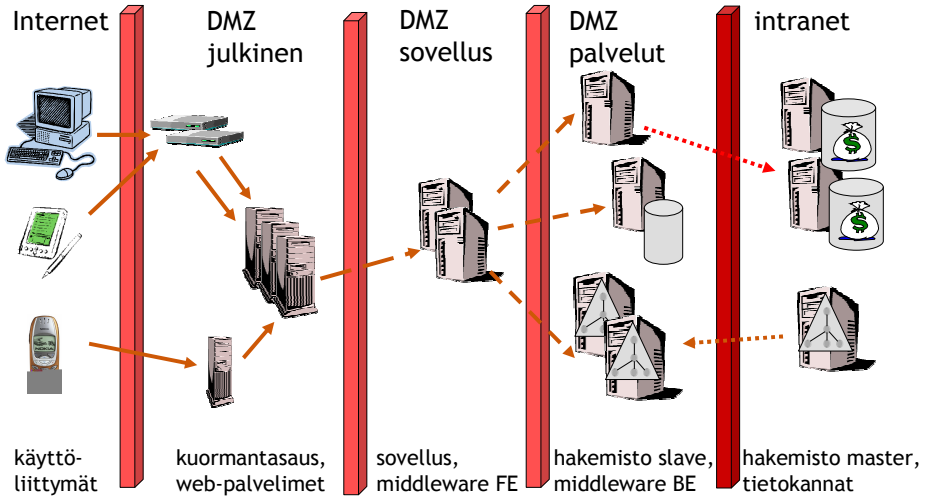
Tietoturvallinen sovellus toteuttaa tietoturvariskianalyysin perusteella määritellyt tietoturvavaatimuksensa siten, että jäännösriski on tiedossa

Muiden vaatimusten osalta sovellus toteuttaa tietoturvallisesti vain ja vain määritellyt toiminnot

Suositeltavat (karkeat) tietoturvatehtävät

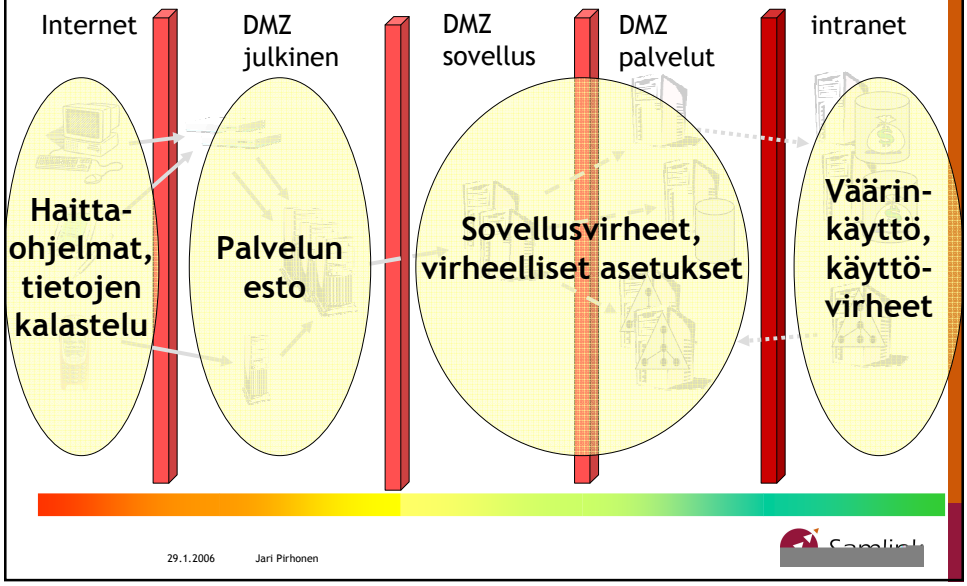


Nykyarkkitehtuuri



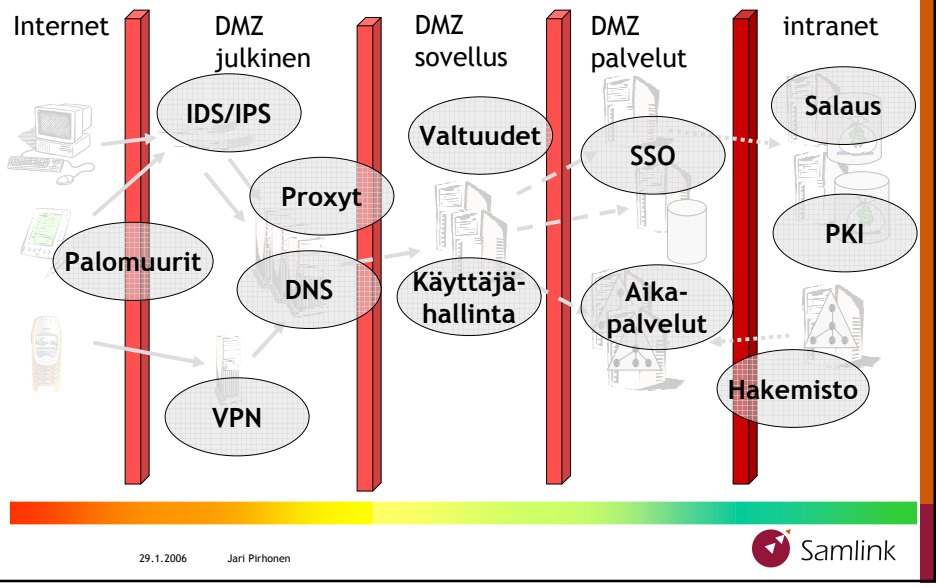
Samlink

Uhkia



Samlink

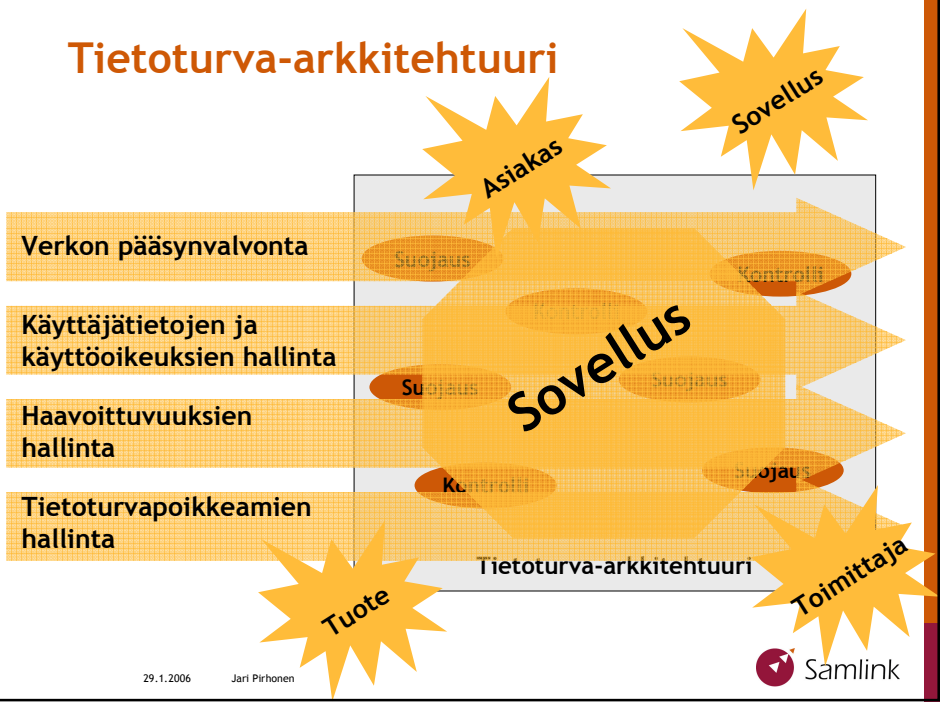
Turvattu nykyarkkitehtuuri



29.1.2006 Jari Pirhonen

Samlink

Tietoturva-arkkitehtuuri



29.1.2006 Jari Pirhonen

Samlink

Parempia sovelluksia

- Sovelluksen tietoturvavaatimukset määritellään riskianalyysin kautta
  - systeemityömallit eivät oletusarvoisesti tue tietoturvallisten sovellusten toteuttamista
  - sovellusturvaa ei voi perustaa yksittäisten ohjelmoijien osaamiseen => ”tasalaatua keskivertokoodareilla”
- Tietoturva-arkkitehtuuri huomioidaan
  - nivoutuminen sovellus- ja verkkoarkkitehtuuriin
- Sovellusten tietoturvallisuus voidaan osoittaa kumppaneille ja asiakkaille
  - sovelluksen tietoturvan suunnitteluperusteet
  - tietoturvatoteutuksen dokumentaatio
  - tietoturvatestauksen ja -tarkastuksen tulokset
  - tietoturvan huomioivat asennus- ja käyttöohjeet

Samlink