

Sähköisten palveluiden tietoturva

Maksufoorumi, Suomen Pankki

29.5.2008

Jari Pirhonen

Turvallisuusjohtaja, CISSP, CISA

Samlink - www.samlink.fi



Samlinkin visiona on olla finanssialalla asiakaslähtöisin, kasvava ja arvostettu palvelukeskus integraattori- ja lisäarvopalveluissa

Asiakkaamme

- Aktia
- Finnvera
- Henkivakuutusyhtiö Duo
- Handelsbanken
- Paikallisosuuspankit
- Suomen Hypoteekkiyhdistys
- Säästöpankit

Palvelumme

- Peruspankkijärjestelmät
- Verkkopalvelut
- Vakuutusjärjestelmät
- Johdon ja viranomaisjärjestelmät
- Asiakashallintajärjestelmät
- Laskenta- ja taloushallinnon palvelut
- Infrastrukturi...

Verkkomme

- Asiakaspankeissa työskentelee kaikkiaan reilut 3000 henkilöä
- Asiakaspankit palvelevat yhteensä vajaassa 500 konttorissa
- Asiakaspankeilla on tällä hetkellä 1-1,5 miljoonaa asiakasta,
- ...joista yli puolet käyttää internet-pankkipalveluja

Lyhyesti meistä

- Pitkäaikainen finanssisektorin tuntemus muodostaa toiminnan perustan
- Toimitamme järjestelmiä ASP palveluna ja BPO palveluita (esim. kirjanpito)
- N. 300 asiantuntijaa + laaja kumppaniverkosto
- Liikevaihto 60,6 M€ vuonna 2007
- Paras AAA luottoluokitus

29.5.2008

Jari Pirhonen

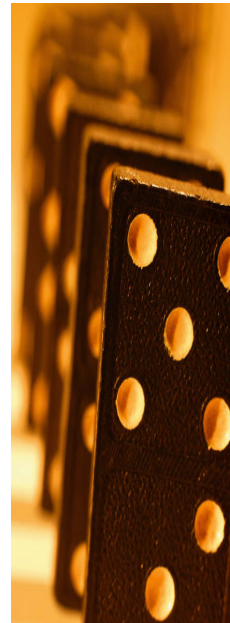


Sisältö

1. Käyttäjän luotettava tunnistaminen on vain jäävuoren huippu verkkoasioinnin tietoturvassa
2. Tietoturvallisuus on mietittävä kokonaisuutena
3. Verkkopankista tee-se-itse palveluun

"Falling coconuts kill 150 people worldwide each year, 15 times the number of fatalities attributable to sharks"

-- George Burgess, Director of the University of Florida's International Shark Attack File



29.5.2008 Jari Pirhonen



Reality check?

SP uskoo: Mobiilimaksaminen tulee lopultakin

Kännykkä mullistaa maksutavat

HELENA RAUNIO
helen.raunio@kat.fi

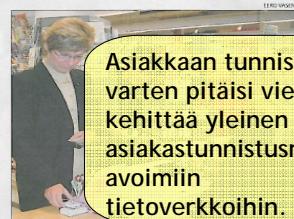
Näppäille ja maksa
Mobiilimaksaminen on jo nyt käytössä Suomessa, mutta se ei ole vielä yleistynyt. Pelkästään e-laskutuksen leveyden lasketaan olevan vähintään 100 miljoonaa euroa vuodessa Suomessa.

Maksutapojen muutokset ovat hitaata prosessia. Koska ne koskettavat niin monia osapuolia: pankkia, maksuyrityksiä, kauppoja, kuluttajia, viranomaisia ja tele-yrityksiä.

Jatkossa maavoikotit voidaan muuttaa digitaalisiksi maksupalveluiksi.

Mobiilimaksaminen voi tulla sovellettavimmaksi parannetuksi ja oppimisen perusteella. Koptioita niistä voidaan säilyttää turvallisesti verkossa ja ladata tarvittaessa uuteen puhelimeen tai suoraan.

Tiedot maksuista voidaan hoitaa lähytyksellä rihä käyttä-



Väljän silloja. Tähänastiset mobiilimaksamiskokeilut eivät tienneet paljon mitenkään. Netia, nordea ja visa testasivat kassamaksamista jo vuonna 2004. Kaupassa etukäteen lasketaan talletetaan Lahden koulun maksuillenneasiainhoitajan Jaana Ryyppö-Raikkonen.

Leimonen myöntää kuitenkin alieen ongelmia. E-tunnuksista tarvitaan yhä lausumia ja suostuminen.

On myös luotava kansainvälinen maksusormastandardi maailmalla käytössä sekä helppokäyttöinen malli mobiilimaksamiselle.

Asiakkaan tunnistamista ja maksutapojen säilyttämistä varten

Yksinkertaisimmillaan maksaminen voi olla yhtä helppoa ja nopeaa kuin tekstiviestin tai sähköpostin lähettäminen.

Asiakkaan tunnistamista varten pitäisi vielä kehittää yleinen asiakastunnistusratkaisu avoimiin tietoverkkoihin.

29.5.2008 Jari Pirhonen

lähde: Tekniikka & Talous 2.5.08



Vuosisadan suunnitteluhaasteet



Make solar energy economical



Provide energy from fusion



Manage the nitrogen cycle



Provide access to clean water



Advance health informatics



Engineer better medicines



Prevent nuclear terror



Secure cyberspace



Advance personalized learning



Engineer the tools of scientific discovery

- Laitteiden, sovellusten, tiedon ja käyttäjien vahva todentaminen
- Turvallisten sovellusten tuottaminen ja todentaminen
- Tietoliikenteen aitouden ja oikeellisuuden varmistaminen
- Tietoturvatkaisujen helppokäyttöisyys
- Kokonaisuuksien turvaaminen

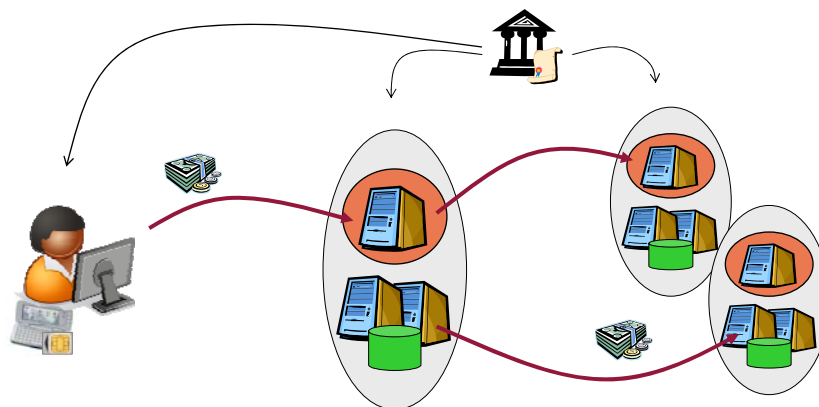
29.5.2008

Jari Pirhonen

lähde: <http://www.engineeringchallenges.org/>



Tietoturvallinen kokonaisuus



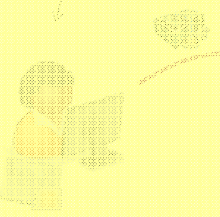
29.5.2008

Jari Pirhonen



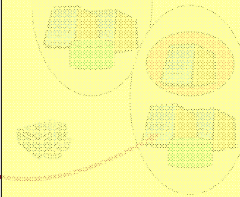
Tietoturvallinen kokonaisuus

- käyttäjän tunnistaminen
- tapahtumien vahvistus
- helppokäyttöisyys - ei tietoturvapäätöksiä



- palvelun tunnistaminen
- käyttövaltuudet
- tietojen oikeellisuuden todentaminen
- tapahtumien kiistämättömyys
- sopimusten sähköinen allekirjoittaminen
- tietojen säilytys luottamuksellisena ja muuttumattomana
- palvelun häiriöttömyyden varmistaminen
- tietoturvatapahtumien seuranta

- osapuolten tunnistaminen
- käyttäjäidentiteetin ja valtuuksien välitys
- tietojen välitys vain käyttöoikeuksien mukaisesti



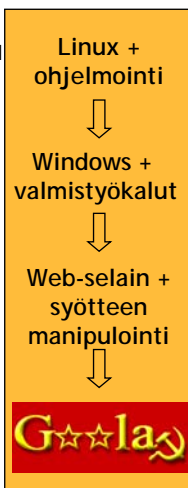
tietojen salaus käyttäjältä tietokantaan, tapahtumien aukoton jäljitettävyyys koko palveluketjussa, yhteiset tietoturvaperiaatteet, tietoturvallisiksi suunnitellut ja testatut palvelut, tietoturvallisuuden toteutumisen osoittaminen

29.5.2008 Jari Pirhonen



Turvallisten palveluiden tekeminen on vaativaa - yksittäisten ongelmien löytäminen helppoa

ENNEN



NYT

Lista XSS-aukoista

Linkitettävät XSS-aukot

- telkku.com 1 screenshot mirror
- www.webstudio.fi
- tarvaanta.lasपालति.fi
- kassio.fi
- www.mattiavoinit.fi
- SLarkki
- Eline
- Sapiin Seudun Pugetitjat ry
- LaatuLavaari 1
- haakket-verkkokirjasto 11 screenshot mirror
- ARVOPAPERI ONLINE screenshot mirror
- Häiriöngin ylläpito
- Sallena
- Enins Videochaku screenshot mirror
- Warner Music Finland screenshot
- Täastokas Webstat - verkkolastot
- Bursrock
- Datawell screenshot
- Eurler screenshot
- Suomenrytilyket screenshot (käytössä)
- Marnemusic screenshot (käytössä julka)
- Mobile Avenue Finland screenshot
- Eikka Juhabotki screenshot
- Oulun Käpät screenshot
- Vaasan S. Vaasan screenshot (käytössä)
- M:Donald's screenshot
- YLE (chat-yhteisö) screenshot
- Talentum screenshot
- Suomen Terveysystävö screenshot
- Silava.fi screenshot
- Afieldaan screenshot
- Hälävittu screenshot
- Huuto.net screenshot
- Radonova screenshot
- muuhet.net
- life.fi screenshot
- OnOff screenshot
- A-kinkkaario screenshot
- Storlines screenshot
- Ruukki Finland screenshot Lisäksi useasta Ruukin maastuvuostosta löytyi aukot.
- Mstomaria screenshot
- arvani.com screenshot
- Somers screenshot Sarana SSL screenshot

xss.dy.fi listasi 25.5.08 yli 100 haavoittuvaa sivustoa

→ ohjelmoijan tärkein tietoturvaohje: syöte on aina tarkistettava

29.5.2008 Jari Pirhonen



Tee-se-itse verkkopankki?

| | | |
|---------|--|--|
| Web | Pankkikohtaiset palvelut ja käyttöliittymät. Fokus verkkopankissa. | Käyttäjän tunnistaminen, tapahtumien vahvistaminen, verkkopankkisovelluksen turvaaminen. |
| Web+ | Kommunikoinnin tehostaminen: VoIP, videoneuvottelu ja pikaviestintä. Fokus verkkopankissa. | Uusien teknologioiden tietoturva-aiheet ja osaaminen kypsyvät hitaasti. |
| Web 2.0 | Pankkipalvelukomponentit. Mashups. Käyttäjä tekee oman käyttöliittymänsä. Erikoistuneita verkkopankki-liittymiä palveluna. Fokus käyttäjässä. | Pankin kontrolli pienenee, käyttötavat voivat olla arvaamattomia, pankki-palvelut integroituvat sovelluksiin. Tietoturvatiedon ja luottamuksen välittäminen. |
| Web 3.0 | Räätälöidyt, automaattisesti muodostettavat palvelupaketit, jotka sisältävät usean finanssitalon ja palveluntarjoajan palveluja. Fokus käyttäjän palvelutarpeissa. | Tarvitaan mekanismi palveluiden luotettavuuden todentamiseen ja muita kehittyneitä turvapalveluita. |

29.5.2008 Jari Pirhonen

Samlink

Yhteenveto

- Käyttäjän luotettava tunnistaminen on vain jäävuoren huippu verkkoasioinnin tietoturvassa**
 - Monimutkaisuuden lisääntyminen, käyttäjämäärän kasvu, langattomuus, verkottuminen,...
 - Kehitys ei luontaisesti edistä tietoturvaa
- Tietoturvallisuus on mietittävä kokonaisuutena**
 - Koko palveluketjun on oltava kunnossa
 - Tietoturvaa ei jatkossakaan ratkaista tuotteilla vaan osaamisella
 - Sovellusprojekteihin osallistujille tarvitaan tietoturvakoulutusta - ei "hakkerikurseja"
- Verkkopankista tee-se-itse palveluun**
 - Uudet teknologiat tuovat paitsi uusia mahdollisuuksia myös haasteita
 - Liiketoimintaa on kehitettävä käsi kädessä tietoturvan kanssa



29.5.2008 Jari Pirhonen

Samlink