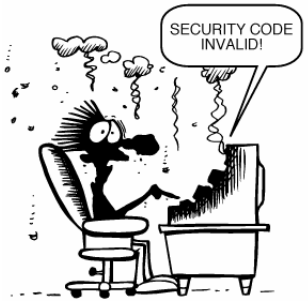
Tietoturvan toteuttaminen web-palvelussa

Tieturi: Internet-ohjelmoijan ajankohtaispäivät



26.5.1999
Jari Pirhonen
Projektipäällikkö, CISSP
AtBusiness Communications Oy
http://www.atbusiness.com/staff/japi/

AtBusiness Communications Oy / Jari Pirhonen © 1999

Tietoturvan toteuttaminen web-palvelussa

Tietoturvallisuus?
Haasteet Internetissä
Ratkaisuja
Toteutusesimerkkejä
Ohjelmoijan haasteet

Amnesty International

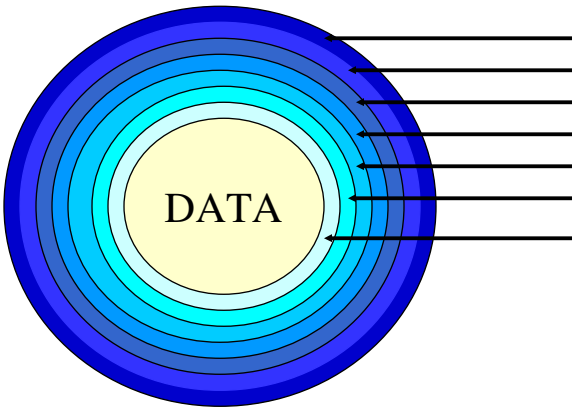
AtBusiness Communications Oy / Jari Pirhonen © 1999

Tietoturvaratkaisusi?

Java SSL IDS Palomuuri Radius
Toimikortti SET PKI RSA
VPN PGP S/MIME
X509.3 ActiveX IPSEC
Unix
3DES NT
Kerberos
LDAP

Tietoturva on liiketoimintaongelma

- Tietoturva EI OLE teknologiaongelma



Tietoturvakerrokset
Organisaatio + hallinto
Henkilökunta
Fyysinen
Laitteistot
Tietoliikenne
Ohjelmistot
Hallinta

AtBusiness Communications Oy / Jari Pirhonen © 1999

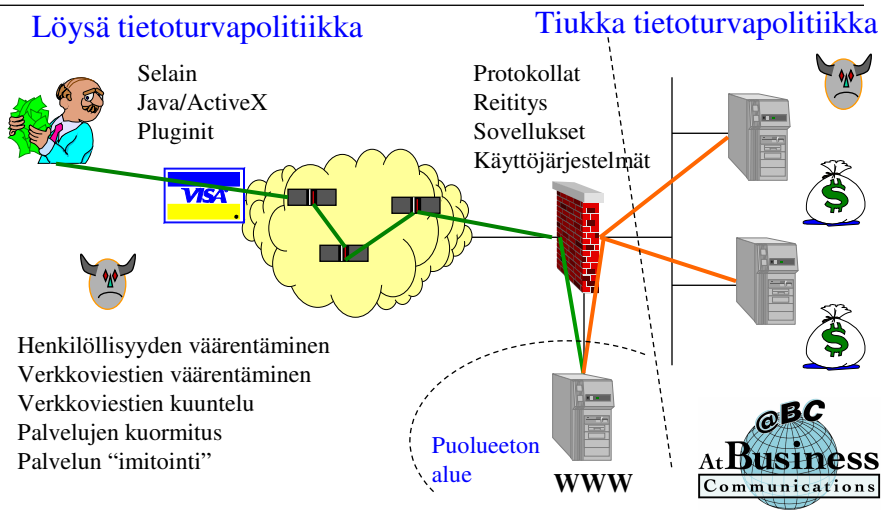
Tavoite

- Tunnista tarpeesi ja velvollisuutesi!
- Luottamuksellisuus - eheys - käytettävyys
- Tunnistus - valtuutus - kiistämättömyys
- Auditointi - monitorointi

“Tietoturvakaava”

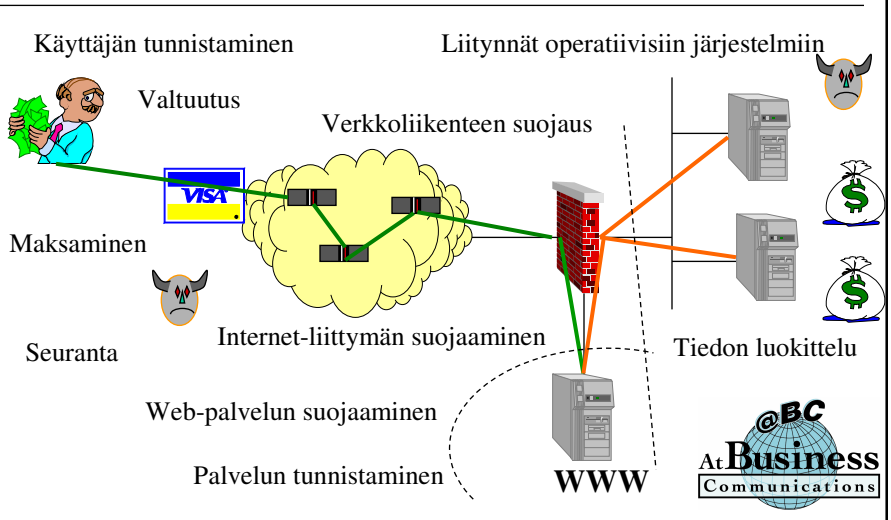
Tietoturvallisuus = uhkakartoitus +
tietoturvapolitiikka +
tekninen implementointi +
monitorointi ja auditointi +
reagointi rikkomuksiin

Uhat Internetissä

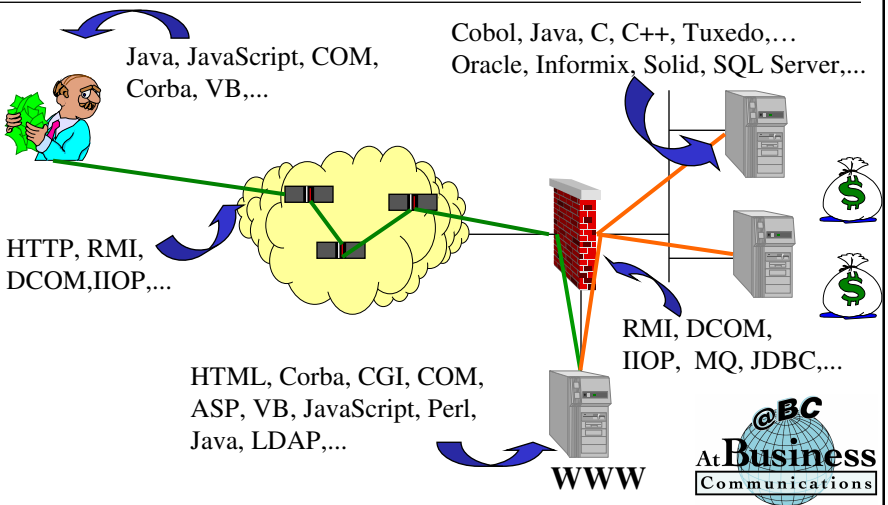


AtBusiness Communications Oy / Jari Pirhonen © 1999

Ratkaistavaa



Sovellusnäkökulma



AtBusiness Communications Oy / Jari Pirhonen © 1999

Mihin luotat?

- Ongelmia on käyttöjärjestelmissä:
  NT, Linux, Solaris, AIX, HP-UX, SCO,...
- Ongelmia on web-palvelinohjelmissa:
  MS IIS, Netscape, Apache, Lotus Domino, Novell IntranetWare, CERN httpd, Purveyor, WebSite,…
- Ongelmia on työkaluissa:
  Java, JavaScript, Perl, ASP, ActiveX,…
- Ongelmia on valmisohjelmistoissa ja -komponenteissa
  tietokannat, sovelluskehittimet,…
- Ongelmia on omissa sovelluksissa?

1999 CSI Computer Security Survey

http://www.gocsi.com/prelea990301.htm

- 521 USA:n yritystä, virastoa, finanssilaitosta ja yliopistoa
- 62% joutunut hyökkäyksen kohteeksi 12 kk:n aikana
- 51% kärsi taloudellisia vahinkoja
- 31% ilmoitti menettäneensä yli $123 miljoonaa
- 96%:lla web-site, 30%:lla e-commerce site
- 20% web-saiteista oli murrettu/käytetty väärin tai luvatta
- 12 kpl laski kustannukset web-murrosta, keskimääräinen kustannus $200.000

AtBusiness Communications Oy / Jari Pirhonen © 1999

1999 CSI Computer Security Survey

- Ulkopuoliset hyökkäykset lisääntyneet
- digitaalisten varmenteiden käyttö lisääntynyt
- IDS-järjestelmien käyttö lisääntynyt

- 98% käyttää virustorjuntaohjelmistoja - 90% raportoi virusongelmista
- 91%:lla palomuurijärjestelmä - ulkopuolisten tunkeutumiset järjestelmiin lisääntyneet

Hyökkäykset “TOP 10”

1. sosiaaliset keinot
2. salasanat
3. luottamusmalli
4. tietoturvatoteutus
5. versiot ja konfigurointi
6. vaarallinen linkki
7. hyökkäysten tunnistaminen
8. laitteisto
9. salausalgoritmien toteutus
10. salausalgoritmit

AtBusiness Communications Oy / Jari Pirhonen © 1999

UNICEF

Ratkaisuja

- **Internet-liittymän suojaus**
  - palomuurijärjestelmä
- **Käyttäjätunnistus**
  - salasana, SecureID, S/KEY, RADIUS, varmenteet, toimikortti
- **Valtuutukset**
  - pääsylistat (ACL), valtuutuspalvelin, roolit, IP-osoitteet
- **Verkkoliikenteen suojaus**
  - salaus, VPN, SSL, SSH
- **Web-palvelun suojaus**
  - HP VirtualVault

AtBusiness Communications Oy / Jari Pirhonen © 1999

Ratkaisuja

- **Sähköpostin suojaaminen**
  - PGP, S/MIME
- **Maksaminen**
  - SET, eCash, Solo, Kultaraha, Leonia, iNet PrePaid
- **Liityntä web-palvelimesta operatiivisiin järjestelmiin**
  - sovelluskohtaisia ratkaisuja, HP VirtualVault
- **Hallinta**
  - tietoturvapolitiikan implementointi, toipumissuunnitelma
- **Seuranta**
  - lokit, hälytykset (IDS), auditointi, patchit

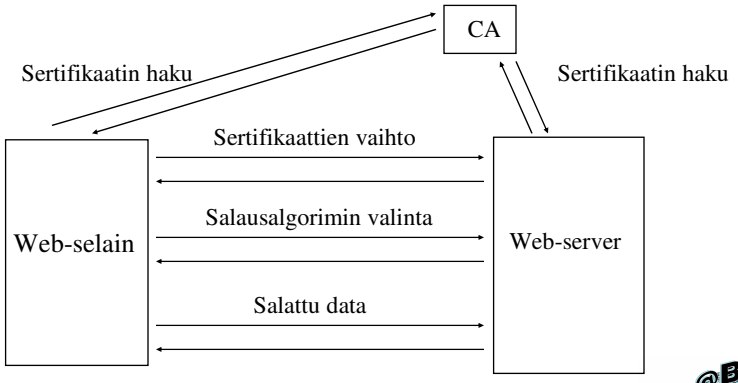
Web-palvelun turvaaminen

Vahva salaus	Vahva käyttäjätunnistus	Valtuutus	Käyttäjähallinta	Liitynnät oper. järjestelmiin	Maksaminen	Operointi	Seuranta	Käytettävyys

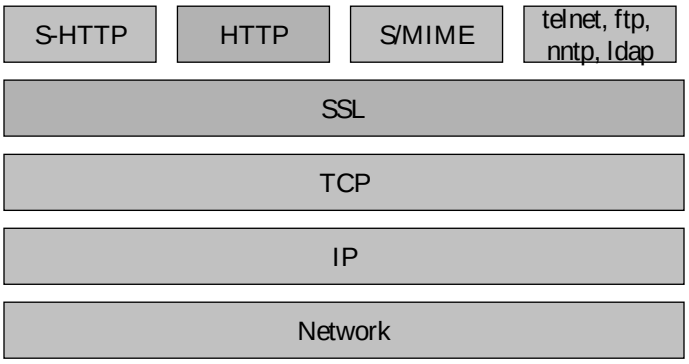
Web-palvelin: oikeaoppinen asennus, SSL, varmenteet, ACL, tunnus/salasana

Perustoimet: minimaalinen kj, patchit, palvelimen sijoitus, palomuuri,...

Secure Socket Layer



Protokollapino



Web-palvelun suojaus / SSL

Web-selain		Web-palvelin
Anonymous	1 →	Anonymous
Tunnus/salasana	2 →	Anonymous
Anonymous	3 →	SSL
Tunnus/salasana	4 →	SSL
Digitaalinen varmenne	5 →	SSL

SSL + vahva salaus

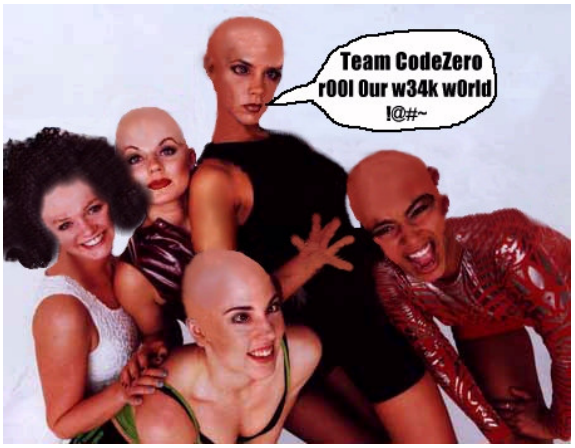
- Netscape “Step Up Encryption”, Microsoft “Server Gated Cryptography”
  - selainten export-versiot pystyvät vahvaan salaukseen, JOS web-palvelin on US versio JA palvelimelle on haettu special-varmenne
  - Web-palvelimen US-version saa Suomeen vain erityisluvalla (pankit)
- Apache
  - saadaan vahva salaus
  - IE ei ymmärrä
  - Netscape Communicator + fortify (www.fortify.net)
  - Opera-selaimeen tulossa vahvan SSL:n tuki

AtBusiness Communications Oy / Jari Pirhonen © 1999

Web-palvelimet Internetissä

- http://www.netcraft.com
- 5/99 5,414,325 web-palvelinta
  - Apache 57 %
  - Microsoft 23 %
  - Netscape 6.5 %
- Apache nopeimmin kasvava SSL-palvelin

Spice Girls



AtBusiness Communications Oy / Jari Pirhonen © 1999

Käyttäjätunnistus

Mitä tiedät?
Mitä sinulla on?
Kuka olet?

heikko

vahva

- Verkko-osoite
- Tunnus ja salasana
- Kertakäyttöiset salasanat: S/Key, SecureID
- Digitaaliset varmenteet: Public Key Infrastructure
- Toimikortit
- Biometriikka

Käyttäjän valtuutus / Web

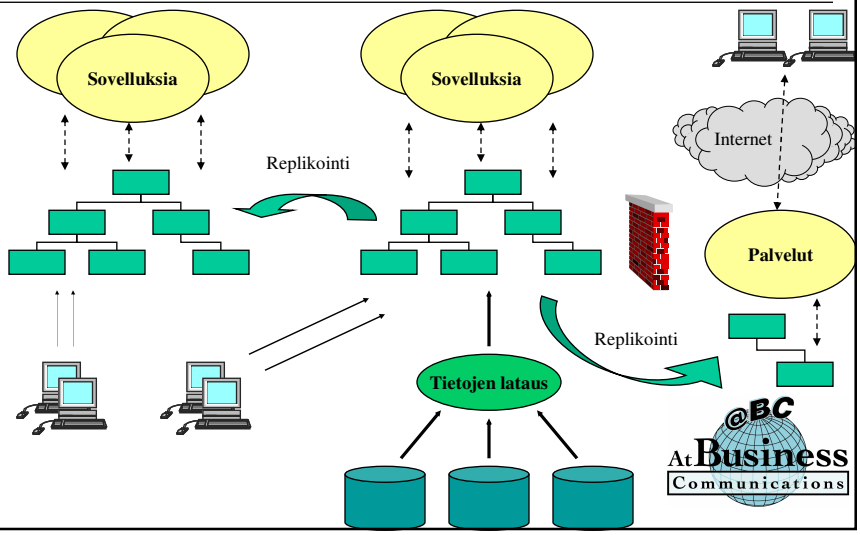
- Mitä käyttäjä saa tehdä?
- Tekniikoita:
  - pääsylistat (ACL, access control list)
  - oikeuslistat (privilege list)
  - turvaleimat (labels, mandatory access control)
  - aikaan/paikkaan perustuva pääsylupa
- Missä tarkistus tehdään?
  - web-palvelin
  - Sovellus
  - Käyttöjärjestelmä
  - Valtuutuspalvelin
    Encommerce getAccess, HP DomainGuard,
    @BC Application Security Manager,….

AtBusiness Communications Oy / Jari Pirhonen © 1999

Sovelluksen tilan säilyttäminen

- Tunnistetun käyttäjän seuraavat yhteydenotot
- Tekniikoita:
  - web-palvelin pitää yllä istuntoa, jos käyttäjä tunnistettu web-palvelimen käyttäjätietokannasta
  - cookies
  - piilotetut kentät HTML-dokumentissa
  - sivut luodaan dynaamisesti, sivun nimeen liitetään käyttäjäkohtainen satunnaisluku
  - Microsoft ASP
  - työkalukohtaiset ratkaisut

LDAP-hakemisto



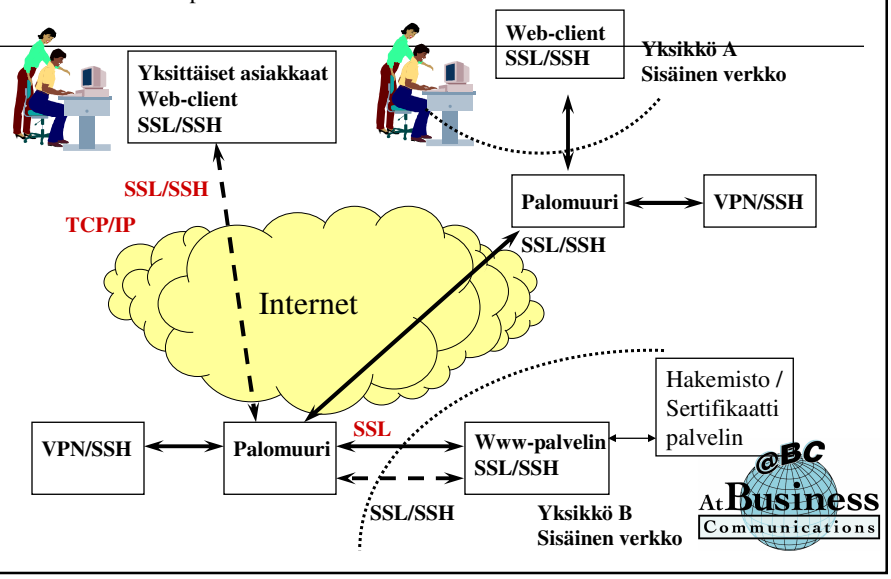
LDAP-käyttömahdollisuudet

- Käyttäjätunnistus (single sign-on)
- valtuutus (käyttäjäroolit)
- digitaalisten varmenteiden talletuspaikka
- IP-puhelut
- verkkokomponenttien hallinta
- selainasetusten hallinta - roaming access
- omat sovellukset
- valmisohjelmistojen LDAP-tuki

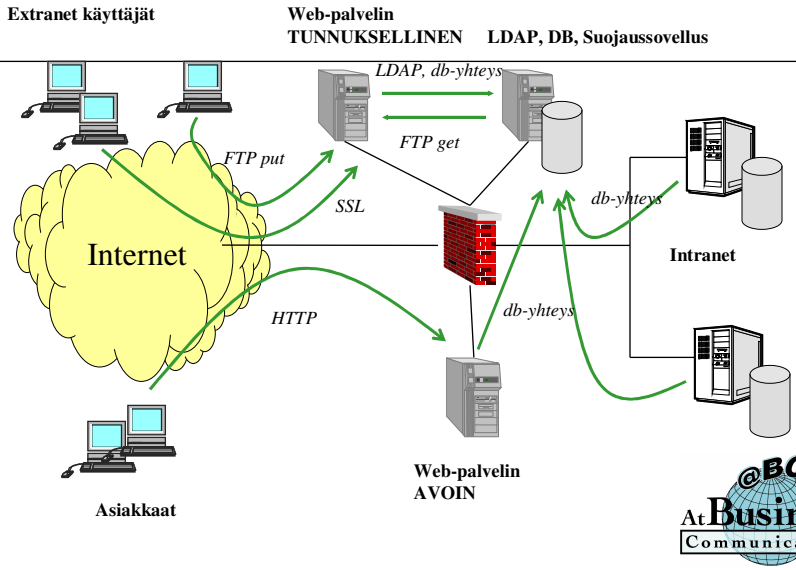
@BC
AtBusiness
Communications

MediciTool

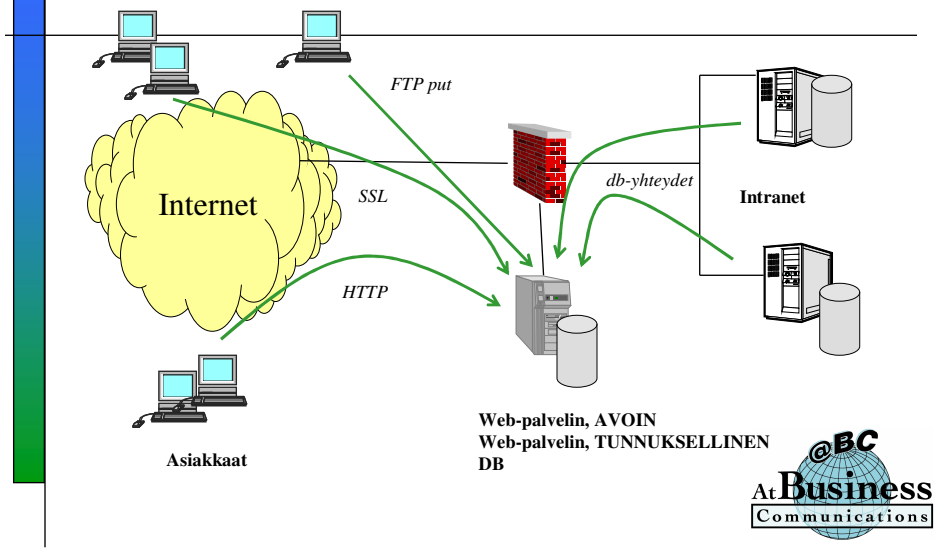
http://telmo.telmo.fi/tiveke/turva/turva-3.htm#Medicitool



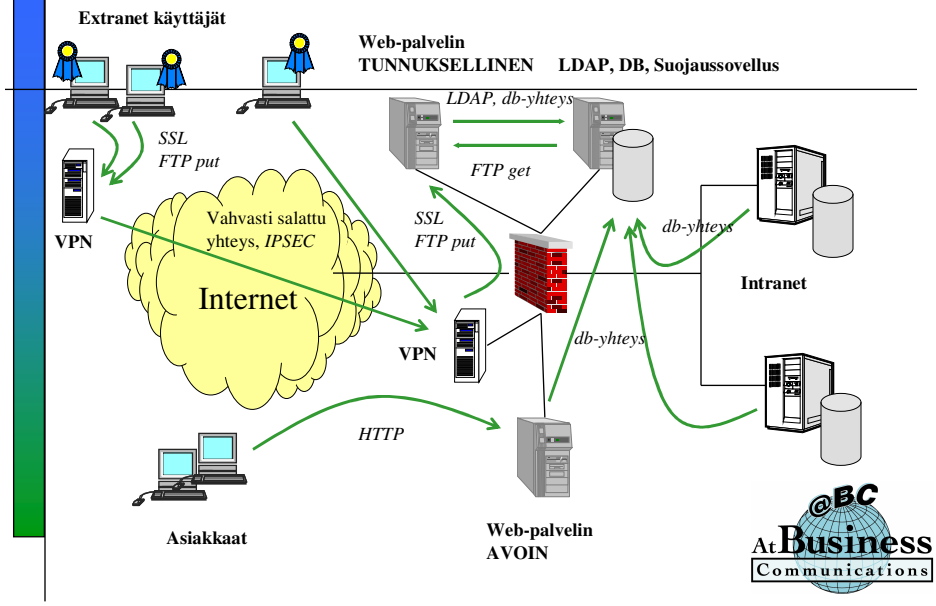
Asiakas / vaihtoehto 1



Asiakas / vaihtoehto 2

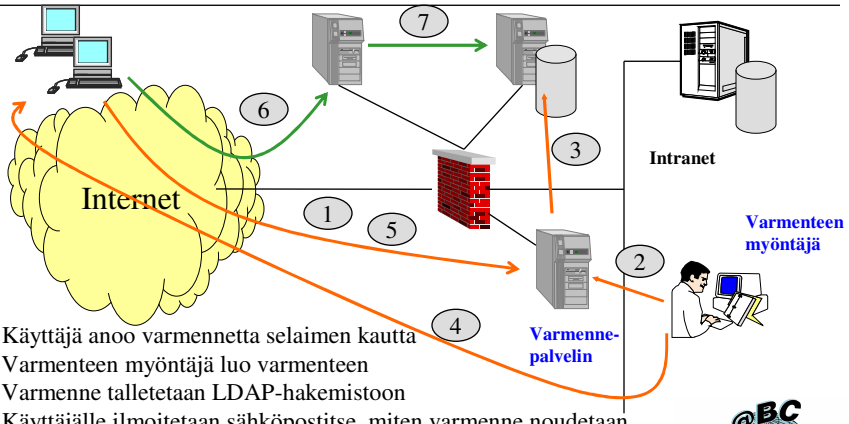


Asiakas / vaihtoehto 3



Asiakas / digitaaliset varmenteet

Extranet käyttäjät | **Web-palvelin** TUNNUKSELLINEN | **DB, Suojaussovellus** LDAP



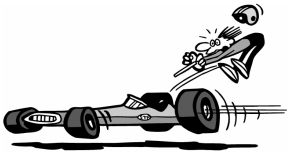
1. Käyttäjä anoo varmennetta selaimen kautta
2. Varmenteen myöntäjä luo varmenteen
3. Varmenne talletetaan LDAP-hakemistoon
4. Käyttäjälle ilmoitetaan sähköpostitse, miten varmenne noudetaan
5. Käyttäjä noutaa varmenteen selaimeensa
6. Sovellukseen pääsee vain esittämällä varmenteen
7. Sulkulistat ja käyttäjien varmenteet saatavilla LDAP-hakemistosta

AtBusiness Communications Oy / Jari Pirhonen © 1999

NY Times

<!-- Obviously we don't really offer training seminars, but -->
<!-- damn well we should. Look at how many clueless admins are -->
<!-- out there. Look at what kind of proprietary data they are -->
<!-- tasked to guard. Think of how easy it is to get past their -->
<!-- pathetic defenses and compromise their security. I knew -->
<!-- working as a Taco Bell manager wouldn't cut it. -->

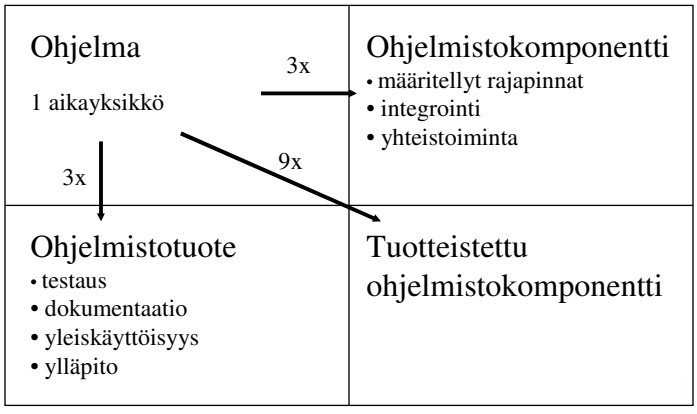
Sovelluskehityksen haasteet



- kiire, kiire, kiire
- beta-kulttuuri
- kilpailevat standardit
- välineiden ja protokollien runsaus, nopea kehitys
- ympäristön vaikeus: hajautettu oliomalli, C++
- valmiskomponentit
- tietoturva koetaan add-on piirteenä
- sovelluksista testataan toiminnallisuutta ei tietoturvaa
  => toimiva sovellus ei välttämättä ole turvallinen
- tietoturva ei ole hauskaa

AtBusiness Communications Oy / Jari Pirhonen © 1999

The Mythical Man-Month



Frederick P. Brooks

Vinkkejä

- Tietoturva mietittävä alusta pitäen sovelluksen osaksi
- Tietoturvaexpertti mukaan projektiin
- Käytetään koeteltuja välineitä ja komponentteja
- Käytä mahdollisimman “riisuttua” ajoalustaa (NT, Unix)
- Tehdään sovelluksista siirrettäviä => alustaa voidaan vaihtaa
- Kaikki on suojattava: sulje paitsi etuovi, myös takaovi ja ikkunat. Varmista savupiippu ja saranat. Pääseekö autotallin kautta sisään?
- KISS

AtBusiness Communications Oy / Jari Pirhonen © 1999

Vinkkejä

- Älä luota käyttäjään
- Älä luota client tai server-sovellukseen
- Älä luota alla olevaan järjestelmään
- Ohjelmalla oltava vain välttämättömät oikeudet
- Tekeehän ohjelma vain sen mitä pitää?
- Tarkista kutsujen paluuarvot
- Älä luota systeemin tilaan
- Älä pidä luottamuksellista tietoa salaamattomana tiedostoissa tai puskureissa
- Ajattele niin kuin hakkeri

Motto?

"History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system. It's always better to assume the worst. Assume your adversaries are better than they are...Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens you'll be glad you did."

Bruce Schneier,
Counterpane Systems