Web Services – mitä vaaditaan tietoturvalta?

Mikko Tiihonen, Valuecode Oy
www.valuecode.com

VALUECODE

Esityksen runko

Mikä on Web Services?

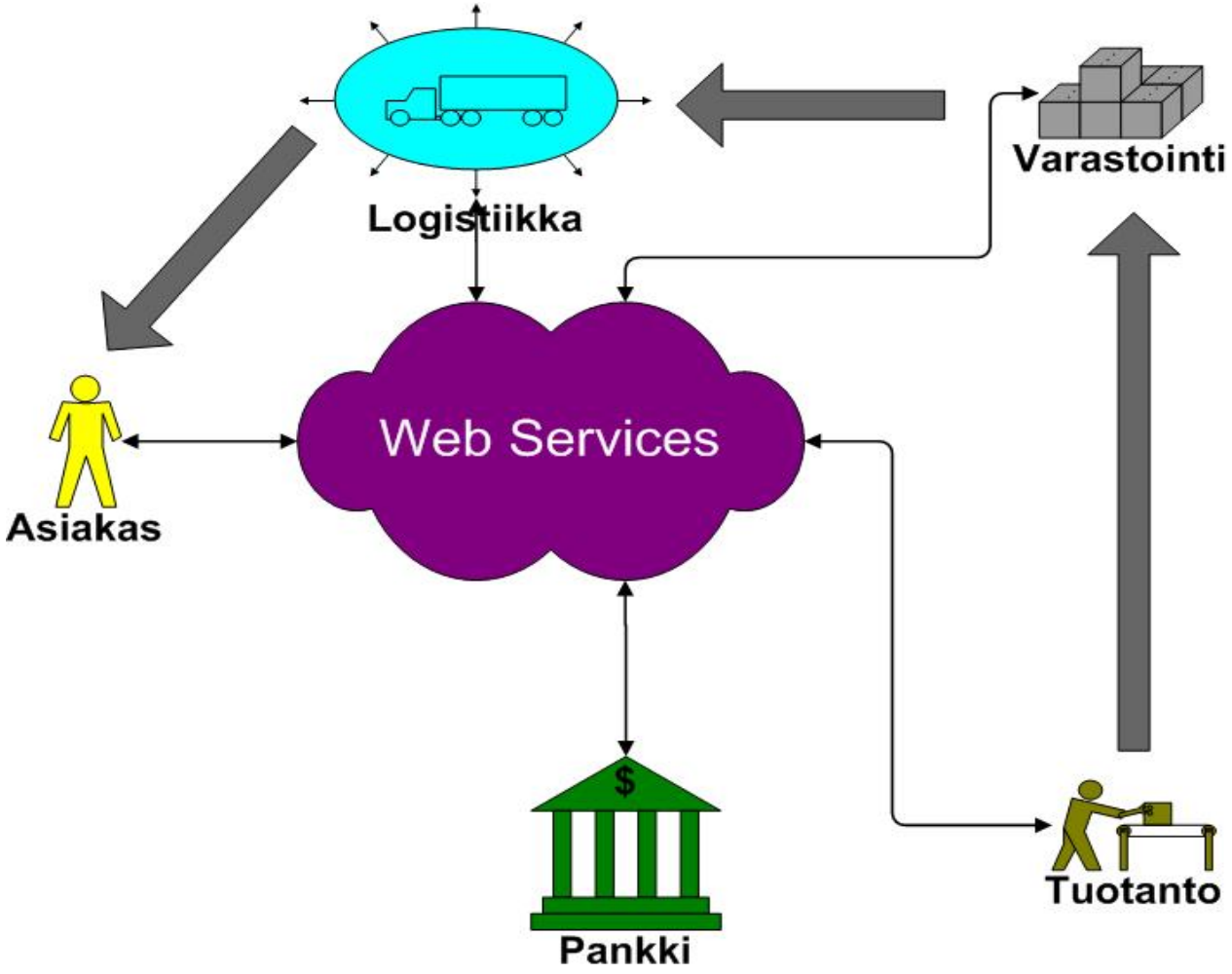
Tietoturvavaatimukset

Tietoturvatoteutus Web Services-ympäristössä

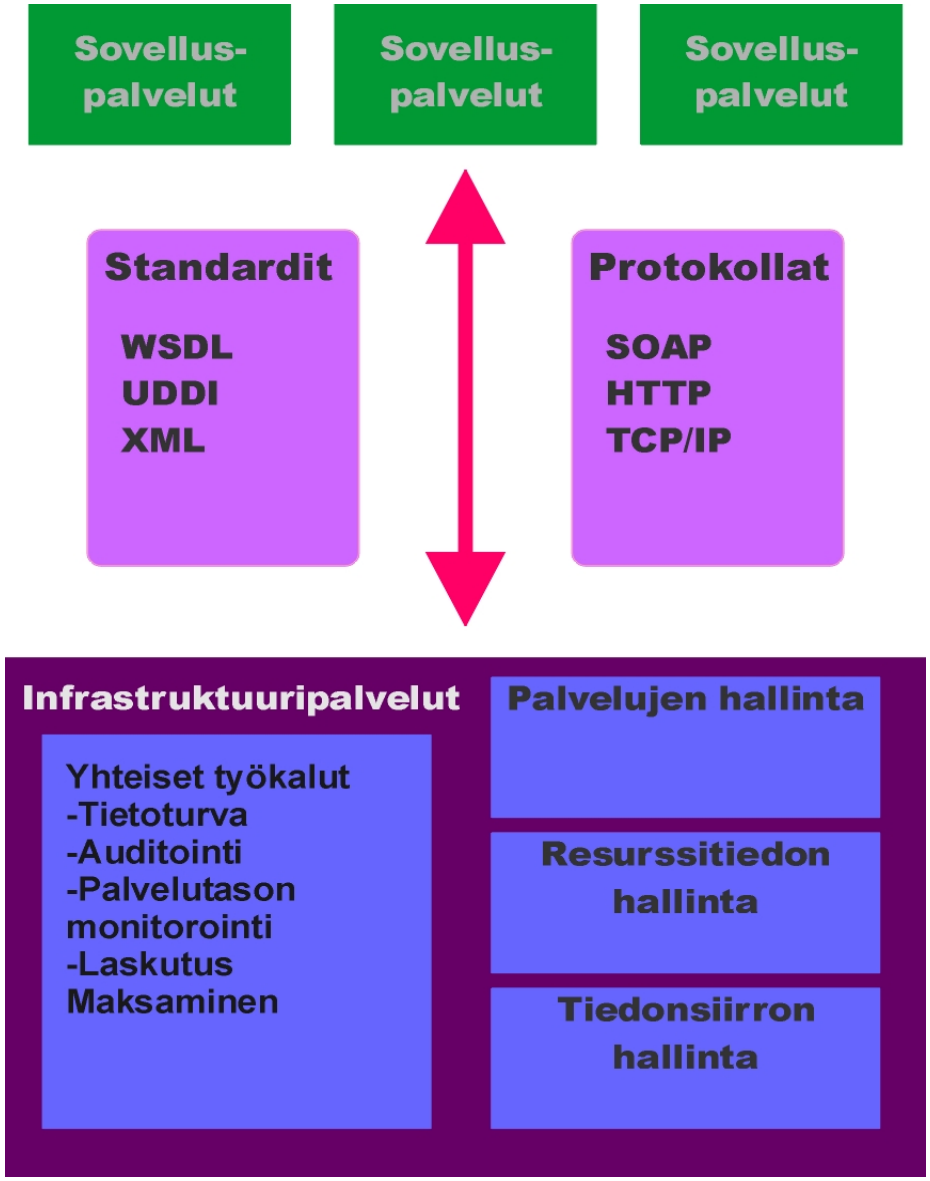
Web Services

- ”.Net” (Microsoft), ”Network Services” (Oracle), ”Open Network Environment” (Sun), ”Web Services” (IBM)
- XML-kielellä kuvatut verkkopalvelut
- XML-viestit järjestelmien välillä
- Edut
  - Yhteensopivuus
  - Prosessien yhdistäminen ilman systeemi-integraation perinteisiä vaikeuksia
  - Kustannustehokkuus

Web Services-esimerkki



Web Services-arkkitehtuuri

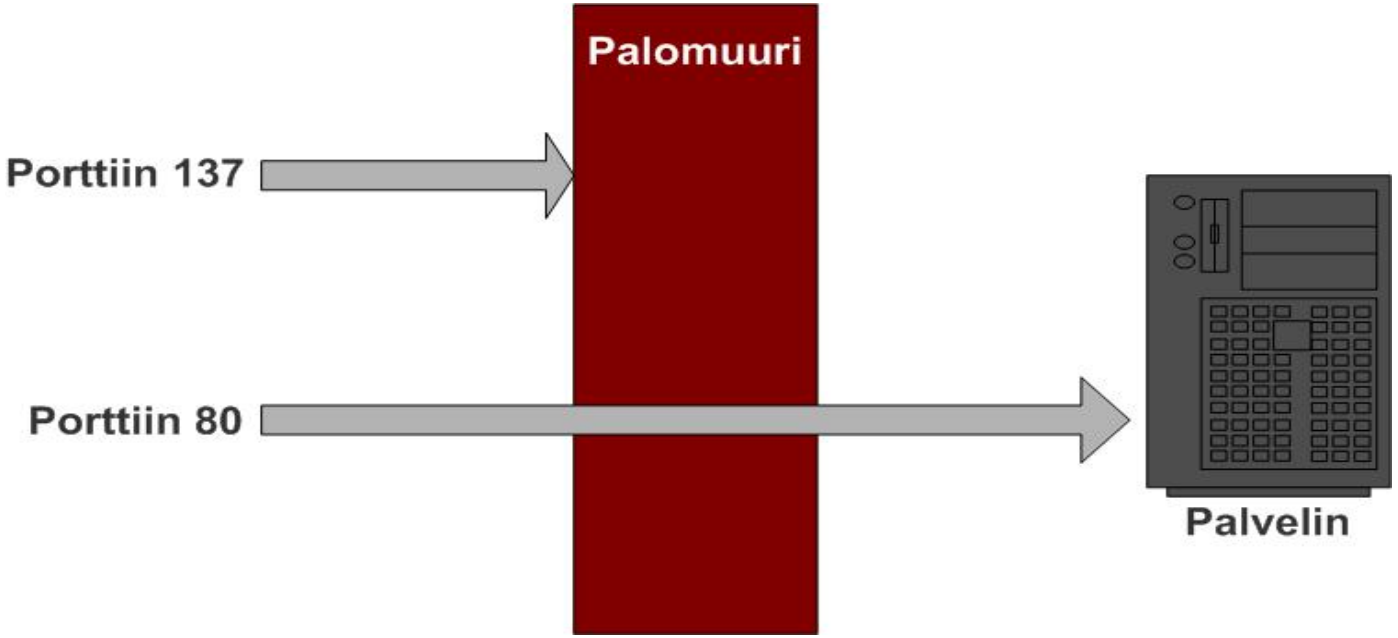


Perinteinen tietoturvamalli ei riitä

Yhteysorientoitunut, OSI-mallin verkko-/kuljetustaso

Perustuu vyöhykkeisiin ja eristämiseen

Sovellustaso on suojaton!



Miltä suojataan?

- Yhteyden salakuuntelu
- Yhteyden kaappaus
- Salausalgoritmien murtaminen
- Spoofing
- Syötteen modifiointi

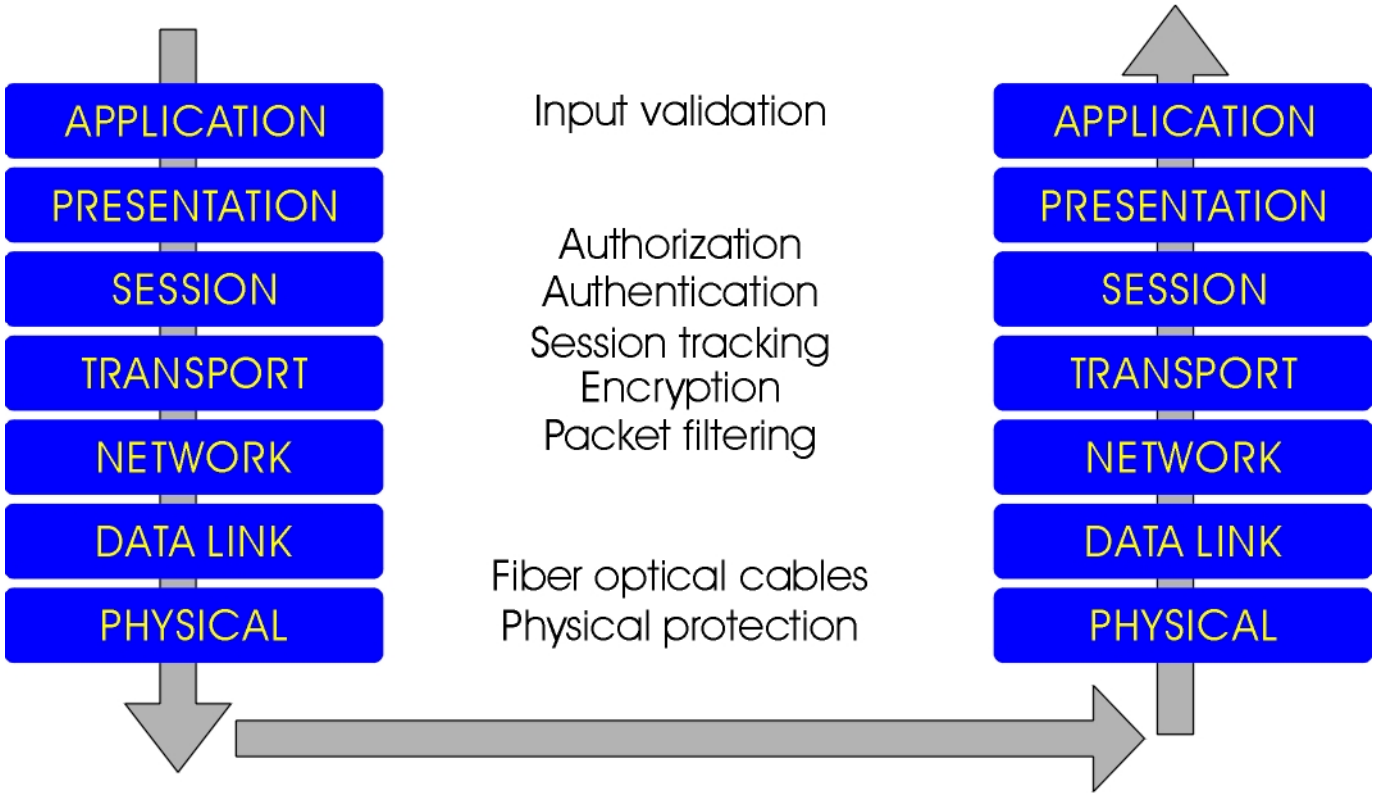
VALUECODE

Miten suojaukset murretaan?

- Luotetun koneen murtaminen
  - Social engineering!
  - Korjaamattomien heikkouksien hyödyntäminen
- Salausalgoritmin murtaminen
  - Man-in-the-middle attack
  - Known plaintext attack
  - Brute force attack

Miten Web Services suojataan?

Kaikki OSI-mallin kerrokset on huomioitava



Turvallinen ohjelmointi

- Pääkäyttäjäoikeuksin ajettavan koodin minimointi ja eristäminen
- Autentikointitiedon tallennus sessiomuuttujaan
- Autentikoinnin epäonnistumisen käsittely
- Syötteen validointi
- Tiedon tallennus serverille, ei clientille
- Virhetilanteiden turvallinen käsittely
- Virheilmoitukset eivät saa paljastaa yksityiskohtia

Laadunvarmennusprosessi

- Järjestelmällinen dokumentointi
- Järjestelmällinen, määrittelyihin perustuva testausprosessi
- CERT:in varoitusten ja muiden tietoturvajakelulistojen seuranta

Web Services-tietoturvamalli

Security Authority / Security Intermediary

- Identiteetin ja luottamussuhteiden hallinta
- Luotettava autentikointi ja auktorisointi
- SAML, XKMS, XACML

Digitaaliset allekirjoitukset

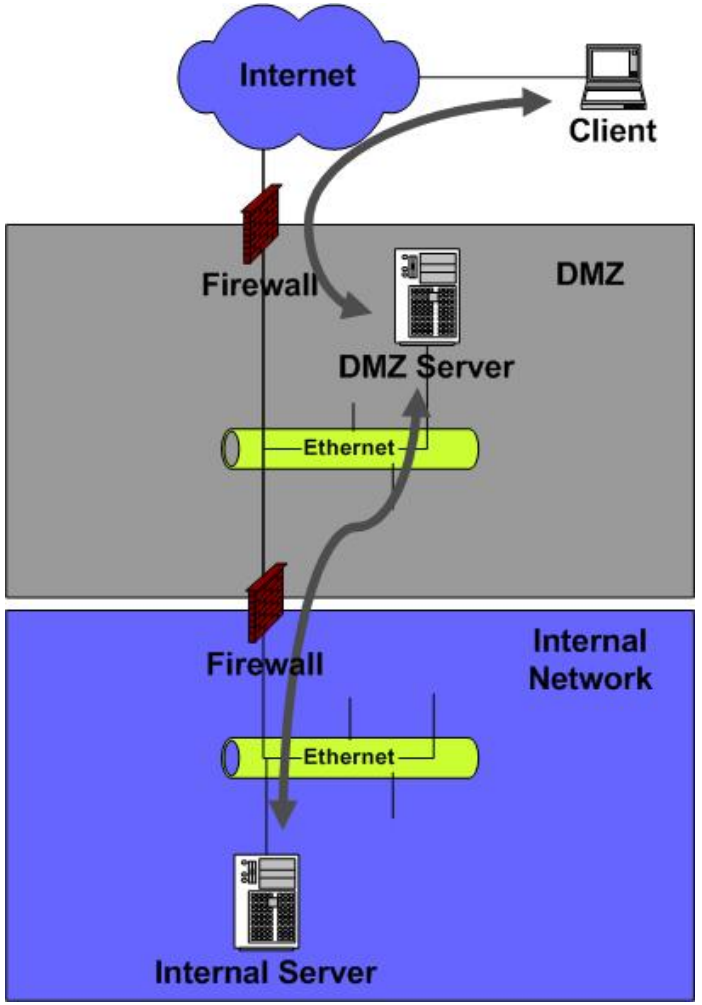
- Transaktioiden eheyden ja kiistämättömyyden turvaaminen
- XML Signature

Salaus

- Transaktioiden luottamuksellisuuden turvaaminen
- SSL / TLS / IPSec, XML Encryption

Web Services-palvelimen suojaus

- Käytetään syötteen validoivaa edustapalvelinta (proxy)
  - ”Default deny”
- Sijoitetaan demilitarisoidulle vyöhykkeelle palomuurien väliin



Turvallisen Web Services -implementaation toteutus

- Tietoturva otettava yhdeksi suunnittelutavoitteeksi ja huomioitava jo määrittelyvaihetta aloitettaessa
- Määriteltävä tietoturvakriteerit mukaan hyväksyttäville järjestelmille ja noudatettava niitä
- Järjestelmien säännöllinen tietoturva-auditointi

Valuecode Oy
Tekniikantie 14 (Innopoli2)
02150 Espoo

http://www.valuecode.com