Aalto University

Tietoturvan tutkimuksesta

Tuomas Aura, Aalto-yliopisto

Taustaa

- Tuomas Aura, tietotekniikan professori
- Secure Systems Group, Aalto-yliopisto
  - 2+1 professoria, 6 tohtoria, 8+ tohtoriopiskelijaa
  - R&D-kokemus ja tiivis teollisuusyhteistyö
  - Rahoitus: Suomen Akatemia, Tekes, teollisuus
  - Helsinki-Aalto Center for Information Security (HAIC), EU:n rahoittama Master-ohjelma SECCLO
- Oma tutkimus: tietoverkkojen ja protokollien turvallisuus, esineiden Internet

Miksei tietoturvaa vain korjata?

- Tekniikan monimutkaisuus
  - Koodin määrä, kerrokset, hajautus, koodin muuttuvuus
- Avoimet arkkitehtuurit tietokoneen ja Internetin menestyksen takana
- Moderni ohjelmistokehitys
  - Pilvipalvelujen ja ohjelmistojen alihankinta
  - Nopea tuotekehityssykli
- Rikollisuus ei lopu, torjunta jatkuva prosessi
  - Vastapuolella myös valtioita miljardibudjeteilla

Mitä akateeminen tutkimus voi tehdä

- Olla osa jatkuvaa tietoturvaprosessia
  - Hiukan pitkäjännitteisempi kuin yritykset
- Menetelmiä ja ymmärrystä
  - Tietoturva-analyysi
  - Haavoittuvuuksia ja hyökkäyksiä
- Uusia teknisiä ratkaisuja ja periaatteita
- Parhaita toimintatapoja järjestelmiin ja prosesseihin

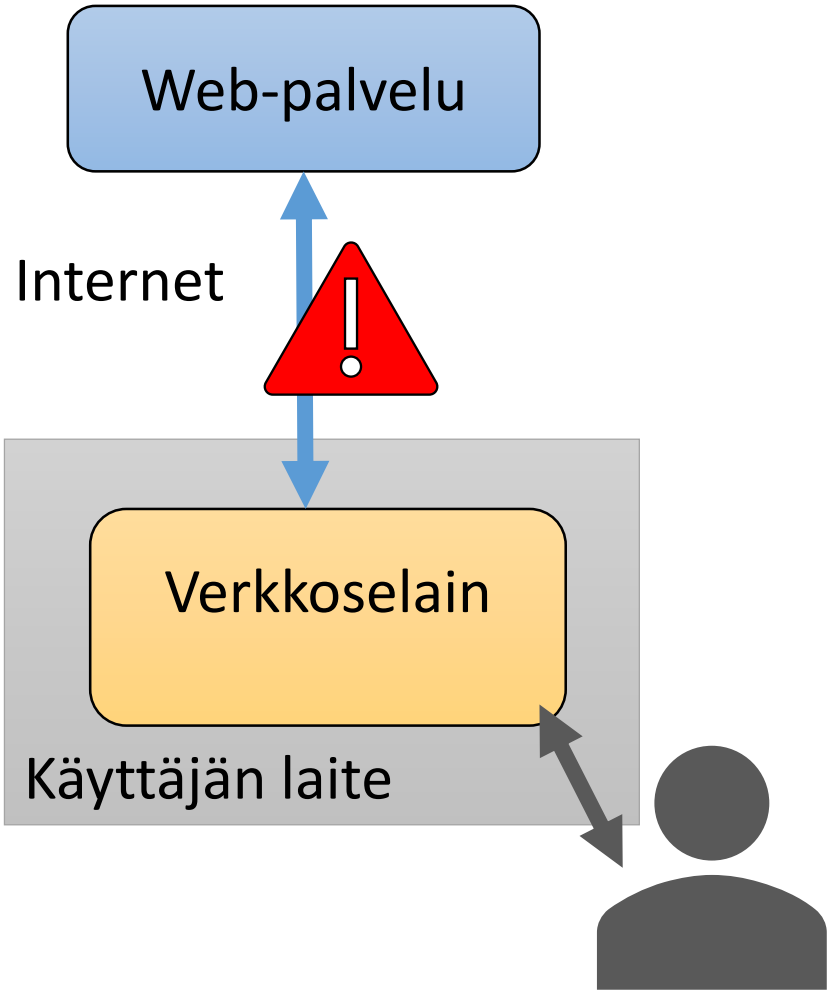
Kyber!

R&D

Kyber!

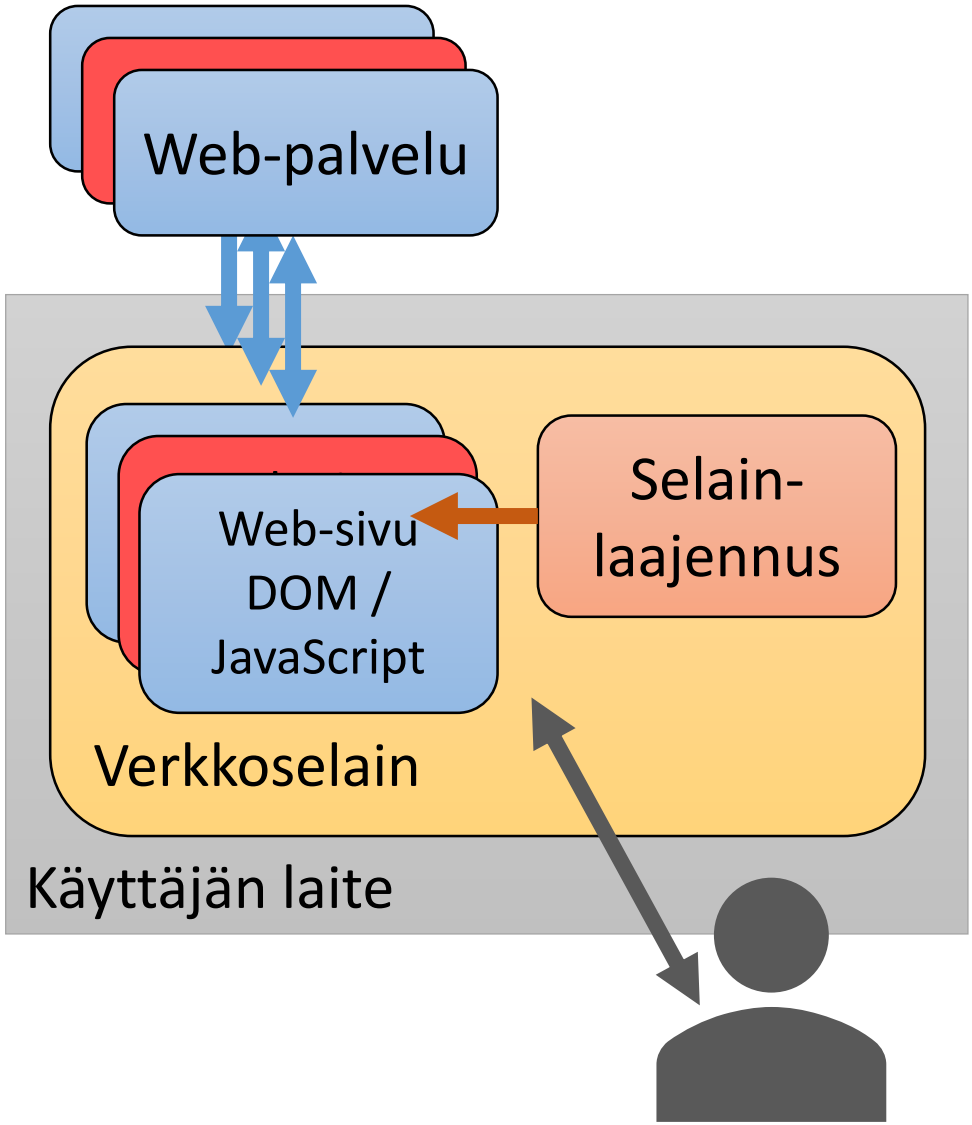
Esimerkki tietoturva-analyysistä:
mies koneessa -hyökkäys

Perinteinen tietoverkon uhkamalli



- Luotettu palvelin ja käyttäjän laite
- Luotetut ohjelmistot
- Epäluotettu tietoverkko:
  ”mies välissä”

Todellisuus

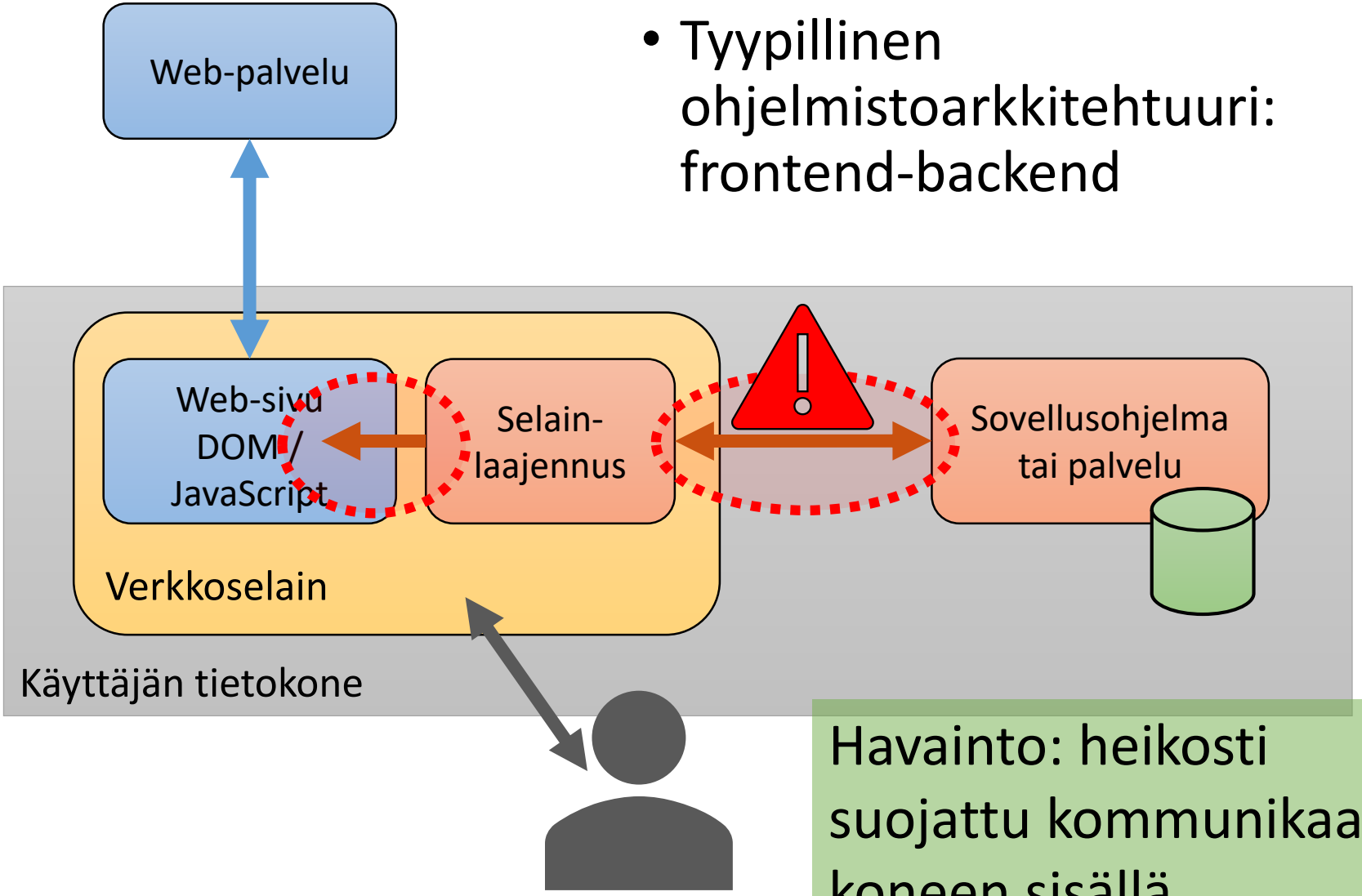


- Useita epäluotettuja palveluita
- Epäluotettu suoritettava sisältö
- Osittain luotettuja ohjelmistoja

➔Monia tunnettuja ongelmia

Tutkimme ohjelmistojen toimintaa tässä ympäristössä
(Aalto, F-Secure, Tekes)

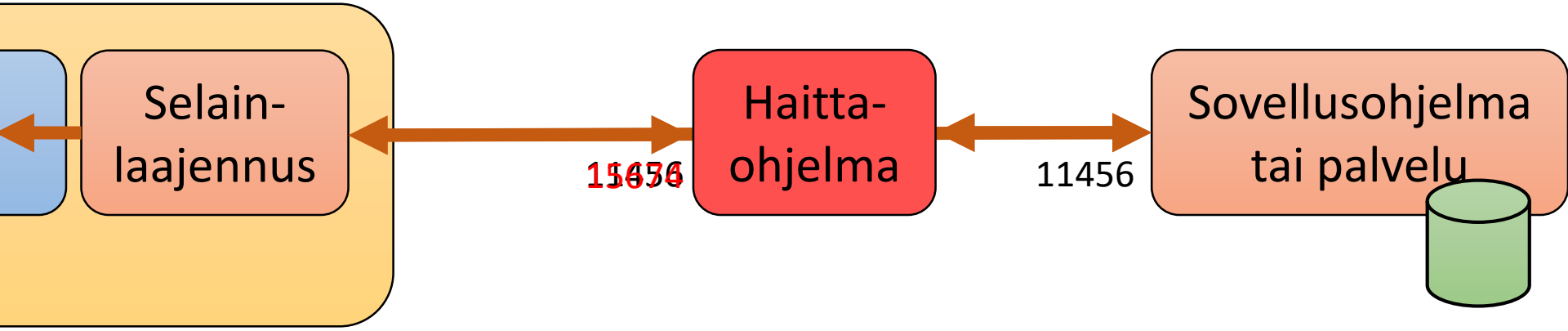
Esimerkkisovellus: salasanamanageri



- Tyypillinen ohjelmistoarkkitehtuuri: frontend-backend

Havainto: heikosti suojattu kommunikaatio koneen sisällä

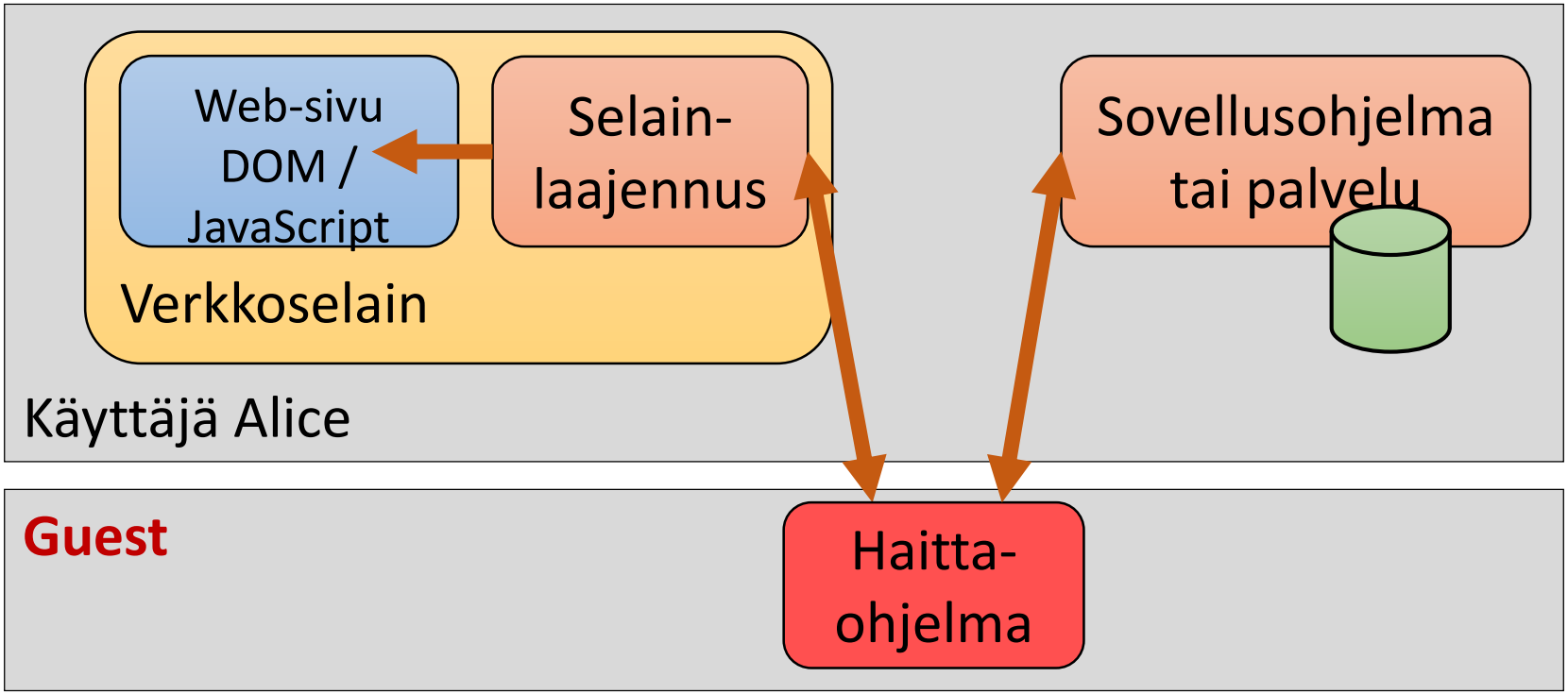
”Mies koneessa”



- Haittaohjelma asettuu ohjelmiston osien väliin käyttäjän koneen sisällä
- Perinteinen tietoverkon uhkamalli, mutta kommunikaatio heikommin suojattu!

Miten saada haittaohjelma koneelle?
Ovatko oikeat sovellukset haavoittuvia?

Miten saada haittaohjelma koneelle?



- ”Mies koneessa” voi olla toinen käyttäjä kotona tai samassa yrityksessä tai vierailija

Toimiiko mies koneessa -hyökkäys oikeasti?

- Haavoittuvia sovelluksia:
  - 6 salasanamanageria,
  - 2 todennuslaitetta
  - pelinlataaja, musiikkisoitin, tietokanta, …
- Windows, macOS, Linux
- On myös haavoittumattomia ohjelmistoja

Hyökkäykset tutkimuksen ytimessä

- Järjestelmän heikkouksien ja hyökkäysten pohtiminen on tietoturvatutkijan arkipäivää
- Monimutkaisia shakkitehtäviä
  - Esim. Intelin prosessorien haavoittuvuudet
- Tavoitteena kehittää teknisiä ratkaisuja; usein vaikeinta on ymmärtää uhkat ja vaatimukset

Yhteenveto

- Tutkimus tuottaa turvallisten järjestelmien suunnitteluperiaatteita, uutta tekniikkaa
- Tärkein kontribuutio tietoturvalle on kuitenkin tutkijan ajattelutapa:
  - Hyökkäysten ja suojausten jatkuva parantaminen
  - Oletusten jatkuva kyseenalaistaminen
  - Kriittiset ja analyyttiset asiantuntijat
  - Taito ajatella kuin hyökkääjä