Veebipõhine andmesisestus kõrgete privaatsusnõuetega rakendustes

Riivo Talviste

Bakalaureusetöö (4 AP)

Juhendaja: Dan Bogdanov, MSc

Motivatsioon

- Delikaatsete isikuandmete käitlemist reguleerivad nii Eesti Vabariigi seadused kui ka Euroopa Liidu direktiivid
- Mõningatel juhtudel pole algseid andmeid vajagi, huvitatud ollakse ainult andmeanalüüsi tulemustest
- Internet on odav ja mugav vahend andmete kogumiseks

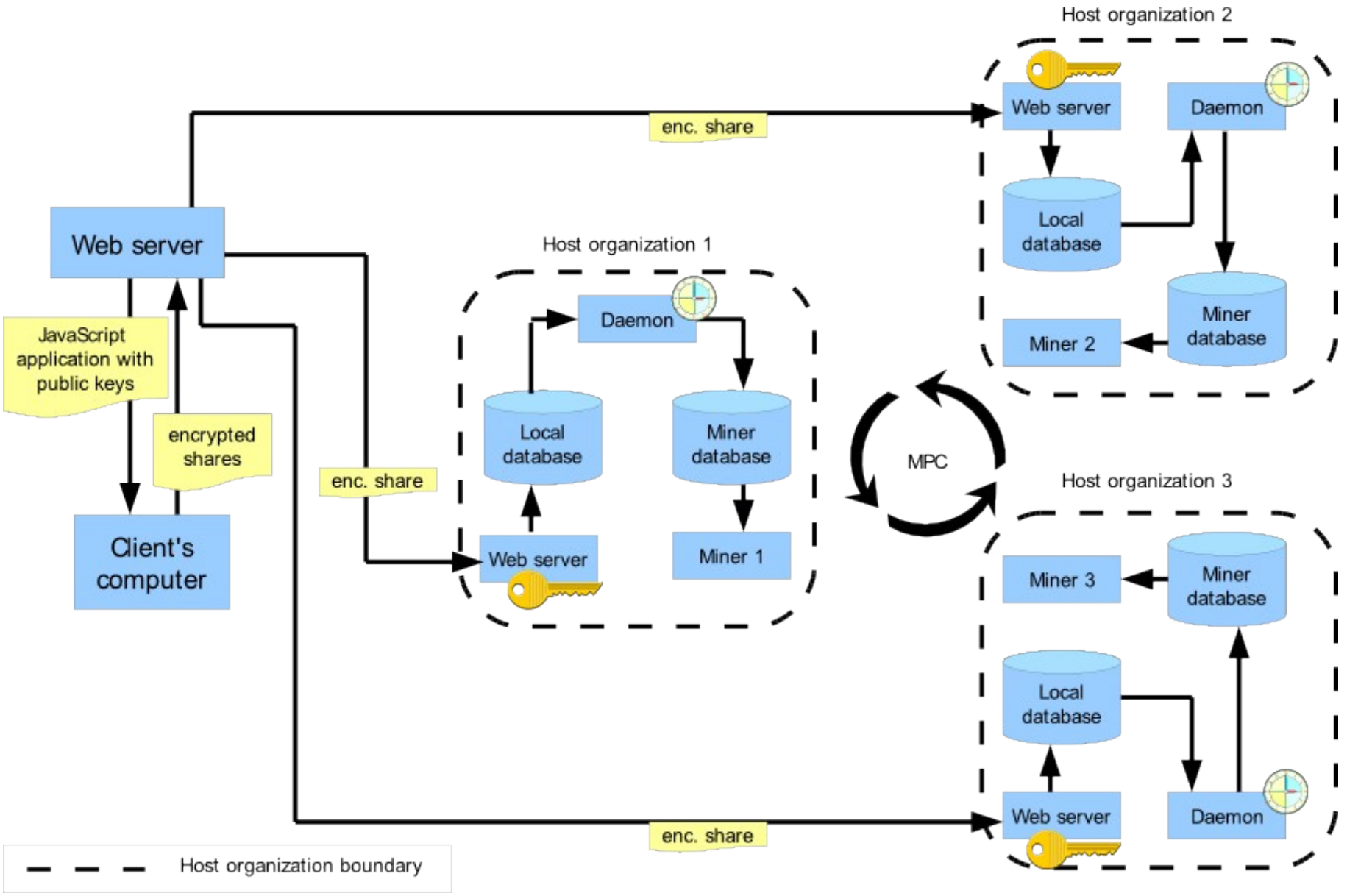
Töö ülevaade

- Eesmärk: veebipõhine andmekogumine, mis säilitab kasutaja andmete privaatsust
- Olemasolevate lahenduste tutvustus
  - Danisco oksjon Taanis 2008. aastal
  - Kasutati ühissalastust ja turvalist ühisarvutamist
- Käesolevas töös kaks täiustatud lahendust:
  - JavaScript
  - Flex

Sharemindi raamistik

- Hajus virtuaalmasin
- Võimaldab turvalist ühisarvutust ühissalastatud andmete peal
- Kolm sõltumatut andmekaevurit (*miner*)
  - Salvestavad osakud oma andmebaasi
- Programmeerimisliides (API)

JavaScript: arhitektuur



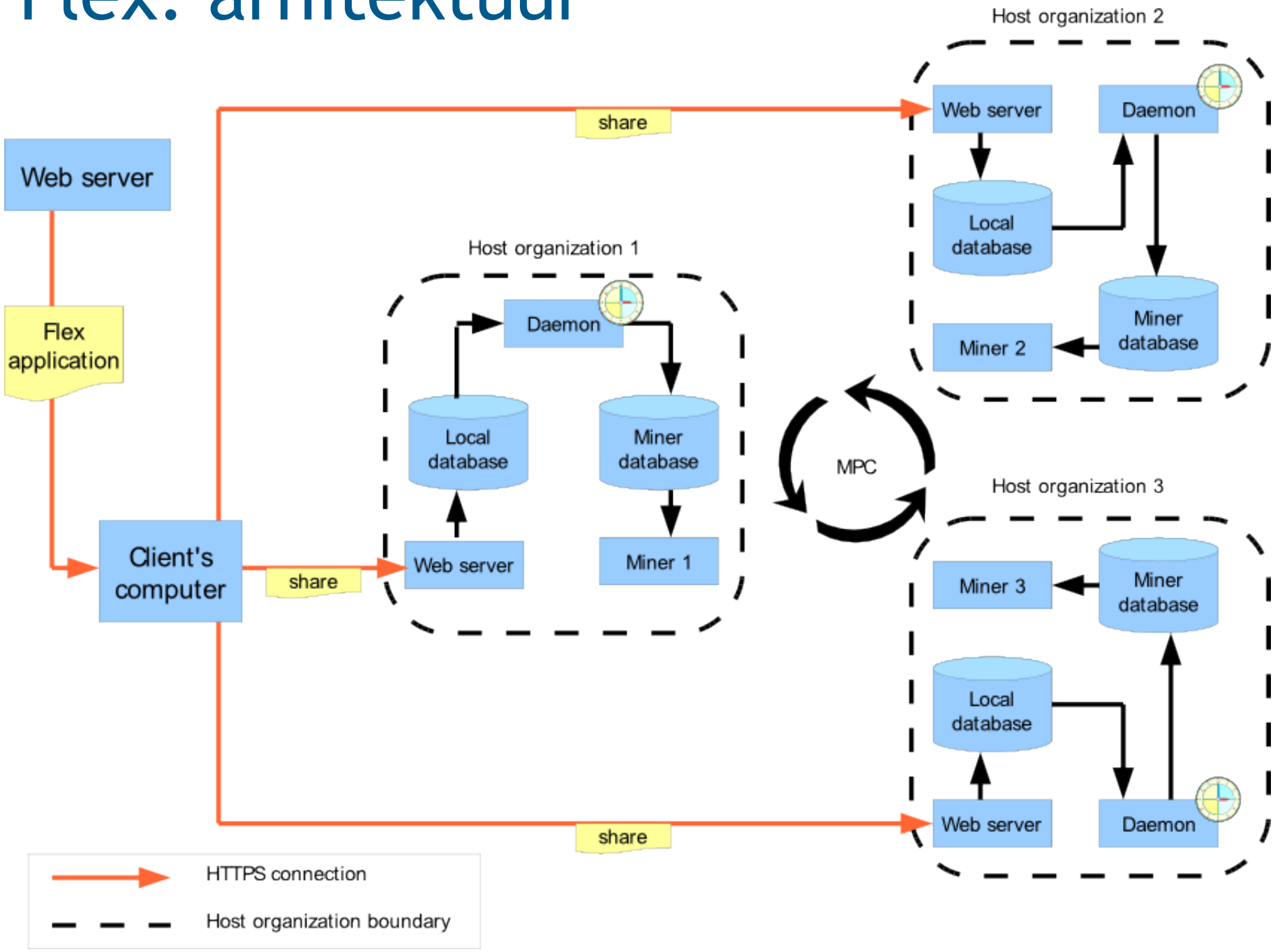
JavaScript: lahendus

- Ei saa luua HTTPS ühendusi
  - Kasutame osakute krüpteerimist
- Puudub korralik pseudojuhuslike arvude generaator

- Turvarisk: kasutaja peab veebiserverit täielikult usaldama

- Danisco lahenduses kasutati Java rakendit
  - JavaScript parandab kasutatavust

Flex: arhitektuur



Flex: lahendus

- Adobe Flex
  - Eeldab kasutajalt Adobe Flash Player olemasolu
- Võimaldab luua HTTPS ühendusi
  - Kolm turvalist otseühendust andmekaevuritega
- Puudub korralik pseudojuhuslike arvude generaator
- Turvarisk: Pahatahtlike andmekaevurite sertifikaadid on kasutaja poolt eelnevalt usaldatud

Kokkuvõte

- Uurisin, kuidas koguda veebilehitseja kaudu andmeid nii, et nende privaatsus säiliks
- Näitena vaatlesin Danisco oksjoni lahendust
- Kaks uut lahendust:
  - Kasutatavuse parendamine (JavaScript)
  - Turvalisuse parendamine (Flex)
- Kasutatavad koos
  - Sharemindi raamistikuga
  - Teiste turvaliste ühisarvutuse süsteemidega