Turvaline infovoog

Sisendid

- salajased
- mittesalajased

$\longrightarrow$ Programm $\longrightarrow$

Väljundid

- avalikud
- mitteavalikud

- Programmil on turvaline infovoog, kui avalikud väljundid ei aita salajaste sisendite kohta midagi leida.
- Turvalise infovoo tagamiseks:
  - Programmianalüüsid.
  - Sertifitseerivad kompilaatorid.
    - tüübid „avalik", „salajane". . .
    - ei luba avalikule muutujale salajast väärtust omistada.
- Neid kompilaatoreid võiks uurida.

Krüptoprotokollide turvalisus

- Krüptoprotokolle kasutavad osapooled mingite objektide salajasuse ja terviklikkuse säilitamiseks mingites tegevustes.
- Salajasus — ründaja vaade protokollijooksule ei aita salajase asja kohta midagi leida.
- Terviklus — ründaja ei suuda mõnele osapoolele jätta muljet, et objekt on teistsugune kui ta tegelikult on.
- Erinevad definitsioonid on võimalikud.
  - Neid on kahte põhimõtteliselt erinevat laadi.
- Definitsioonid peaksid ka arutlemise jaoks sobima.
- Definitsioone ja automaatseid arutlemisviise võiks uurida.

Simuleeritavus

- Simuleeritavus on üks neid „sobivaid definitsioone" krüptoprimitiivide turvalisuse jaoks.
- Ta ütleb, et primitiiv peab igas olukorras käituma samamoodi nagu mingi „ideaalne primitiiv".
- Ideaalsed primitiivid on detailirohked. Simuleeritavuse enda definitsioon on ka detailirohke.
- Simuleeritavus võib sobida mainitud kahe erilaadi abstraktsiooni lähendamiseks.
- Võiks uurida.

teema Jan Villemsonilt

Õpiprogrammide kaitsmine õpilasepoolsete rünnete eest.

- Õpilaseprogrammiga kaasas olevate lahenduste salajasuse tagamine.
- Vastusefailide tervikluse tagamine.
- Infrastruktuur võtmevahetuseks.

veel üks Janilt

Gaim-i või mõne muu vabavaralise sõnumivahetustarkvarale videokonverentsivõimaluse lisamine.