

Workshop B

Device Security

Discussie

- Welke devices: smartcard, RFID, mobieltje, iPod,..., PC?
- Device security = tamper-resistance + software security.
Moeten we uitgaan van enige tamper-resistance ?
- Moeten we het over security van een device zelf hebben of over device als onderdeel vh geheel, en bbh. design methodology voor hele systeem ?
- smartcard & crypto not the weakest link ?
- metrics voor security ?

Ideeen voor proposals

- security op onveilige devices
- network of low-power sensors
(concreet vb: forest fire detection)
- breedband TV
- low energy crypto

Veilige toepassingen op onveilige devices

Pieter Hartel (UT)

Martijn Oostdijk (RU)

Ronny Wichers Schreur (RU)

Marc Witteman (Riscure)

Probleem

- Hoe kan een veilige applicatie op onveilige (niet tamper-resistant) hardware gerealiseerd worden.
- Context: bestaande embedded devices worden steeds vaker uitgerust met toepassingen die beveiliging vereisen. Het gebrek aan intrinsieke beveiliging moet gecompenseerd worden.
- Devices:
 - mobieltje
 - televisie

Deelproblemen

- Certificatie
- Ontwerp
- Risico analyse
- Flankerend beleid voor de omgeving
- Diefstal device
- Migratie / updates
- Fraude management
- Case studies

- Randvoorwaarden:
 - Embedded consumer electronics
 - Goedkoop
 - Energiezuinig
 - Configureerbaar (beperkt programmeerbaar)
- Toepassingen:
 - Bancair: overal betalen met je device
 - Identificatie
 - Access control
 - Stemmen
- Stakeholders:
 - Telecom
 - Banken
 - Equipment manufacturers
 - Binnenlandse zaken

Netwerk van low-power sensors

Bert Bos (Chess)

H. Braams (VASCO Data Systems)

Bruno Crispo (VU)

Rieks Joosten (TNO Telecom)

Melanie Riebach (VU)

A. Zyck (UT)

- (Wireless) netwerk van goedkope sensoren met beperkte resources
 - Concreet voorbeeld: detectie van bosbranden
 - Kunnen we dit beveiligen, gezien beperkingen
 - weinig rekenkracht
 - weinig power (batterij, zonnecel)
 - mogelijk beperkte levensduur sensoren
- en eisen
- flexible deployment
 - no false alarms
 - ...

Breedband TV

Jerry den Hertog (UT)

Wim Mooij (Irdeto)

Jenno van Zwietering (VZG)

- breedbeeld TV over breedband IP
- afspelen op allerlei hardware (TV,PC,..)
- 1 vd problemen: uniek maken van de ontvanger
 - eigen sleutel, randomness, digitale vingerafdruk hardware,...