Authentisierte Positionsbestimmung

Thomas Mundt
Lehrstuhl IuK
Institut für Informatik
Objectives

- Limit access to classified or copyrighted material to a dedicated area
- Providing an authenticated position information for several applications
Scenarios

- A company wants to make sure that secret material remains within the company’s ground
- An Oscar nominated movie shall be only viewable at the referee’s home only
- TV shows or DVD movies are licensed to a single country only
- An amoured car for money transport can be opened next to the bank only
- A harddisk can only be read when the harddisk is on the premises of the lab
Research priorities

- Location provider
  1. Satellite based (GPS / Galileo)
  2. Fingerprinting / probabilistic with return channel or combination with tracking (WLAN, BT, GSM)
  3. Fingerprinting / probabilistic w/o return channel

- Topics
  1. Confidence in position information (How precise?)
  2. Confidence in trust (How much can we trust?)
  3. Static region (shape, polygone) and Neighborhood / complex relations
Basic principle

Authenticated signal

Signed shape data
Basic principle

Authenticated signal

Signed shape data

WLAN Signal

Shape

Encrypted Data

Positioning Engine

Authentication Unit

Trusted Computing Platform Architecture

DRM Module

Decrypted Data (Plaintext)
Attacks

- Attacks against cryptographic subsystem
  - Out of scope
- DoS
  - Causes false rejects
  - Obvious for all wireless technology
  - Solved in regulatory domain
Attacks

- Rerouting
  - Forwarding the signal from the point of reception to a spoofing client
  - On different network layers
- Replay
  - Recording and playback of signals
Building blocks

- Trusted hardware
  - Authentication module (enables / denies access)
  - Trusted clock (for detection of rerouting)
Defending against rerouting

- Determination of rerouting attacks
  - Latency is the only suitable means
- Latency caused by forwarding the signal
  - Speed of light
  - Transistor switching time
  - Store and forward of frames / packets in network components
  - We have chosen 5ms reasonable minimal latency in WANs
Latency detection

Authenticated signal

Dial-up connection
Mutual authenticated clock adjustment
Was wir gut können

- Location Provider
  - WLAN
  - Ubisense
  - Nahbereichssensoren / RFID
  - GPS / Galileo

- Algorithmen
  - Konfidenzabschätzungen
  - Positionsbestimmung
  - Security
Was wir brauchen

- Hardware Entwicklung
  - Prototyp
  - Security / DRM Modul
Veröffentlichungen

