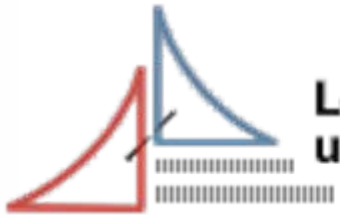


Lehrstuhl für Informations- und Kommunikationsdienste

Location Dependent Digital Rights Management

Thomas Mundt
http://wwwiuk.informatik.uni-rostock.de/
thm@informatik.uni-rostock.de

Objectives

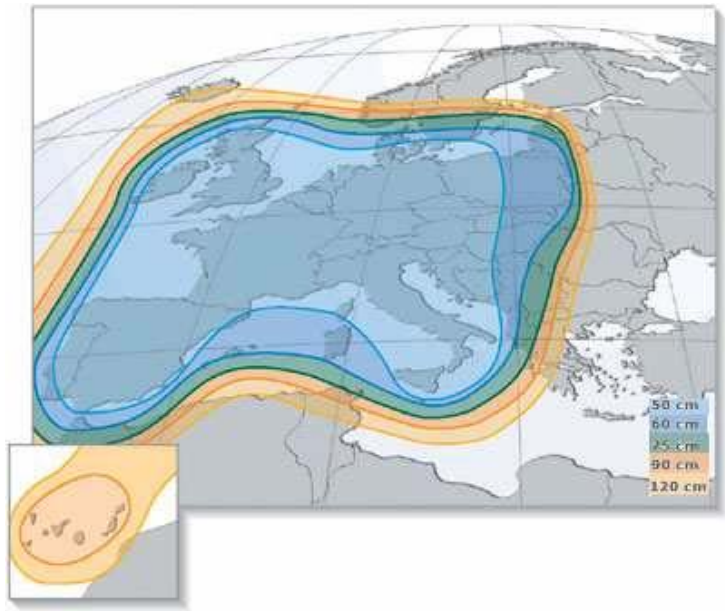
- Limit access to classified or copyrighted material to a dedicated area
- Providing an authenticated position information for several applications

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 harddisc can only be read when the harddisc is on the premises of the lab

Scenarios

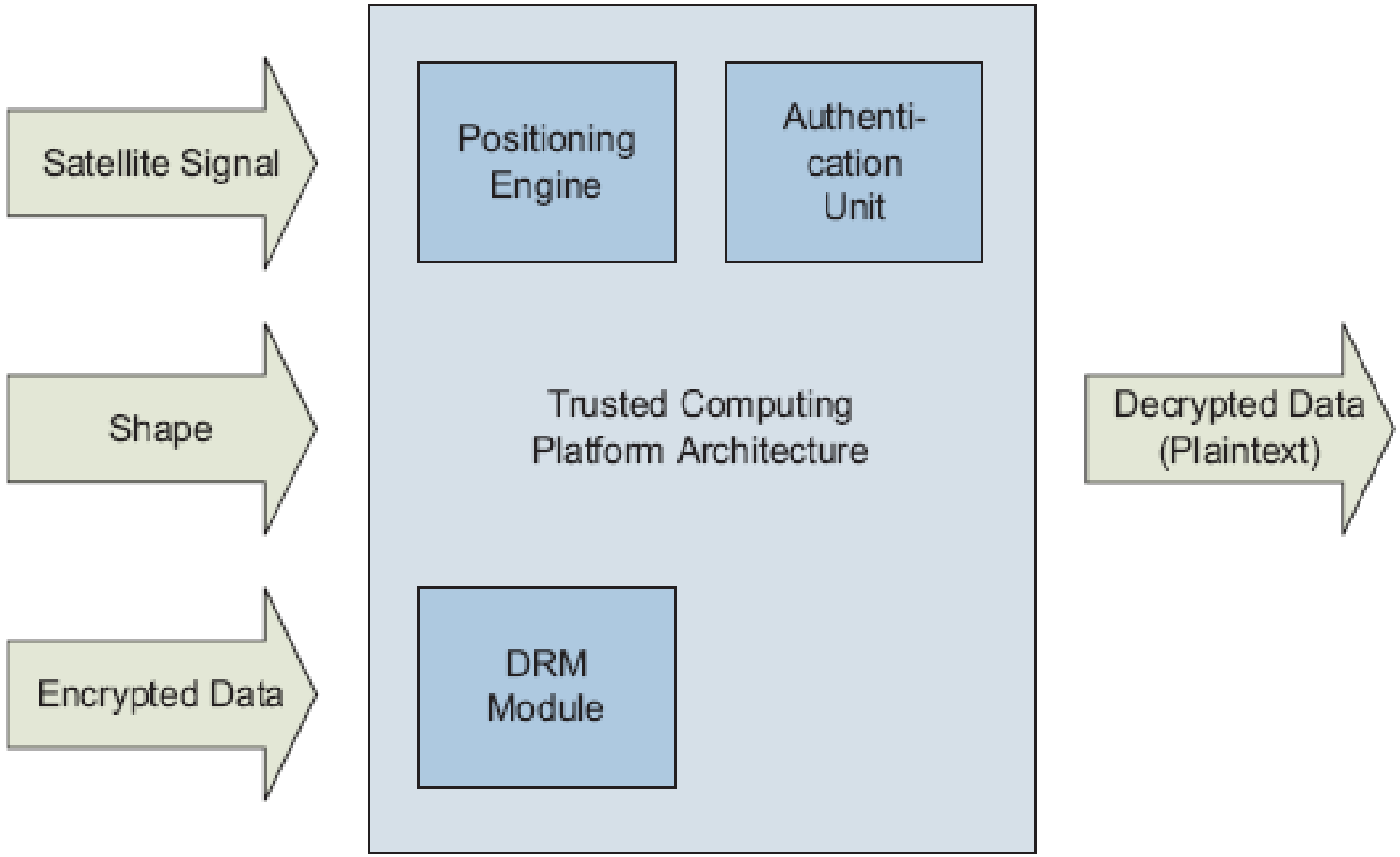
- TV shows or DVD movies are licensed to a single country only
  - Reception area of a German TV station



Research priorities

- Location provider
  1. Satellite based (GPS / Galileo)
  2. Fingerprinting / probabilistic with return channel or combination with tracking (WLAN, BT)
  3. Fingerprinting / probabilistic w/o return channel
- Area definition
  1. Static region (shape, polygone)
  2. Neighborhood / complex relations

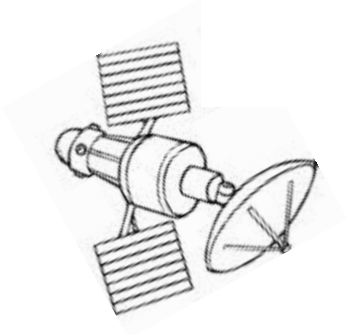
Basic principle



Building blocks

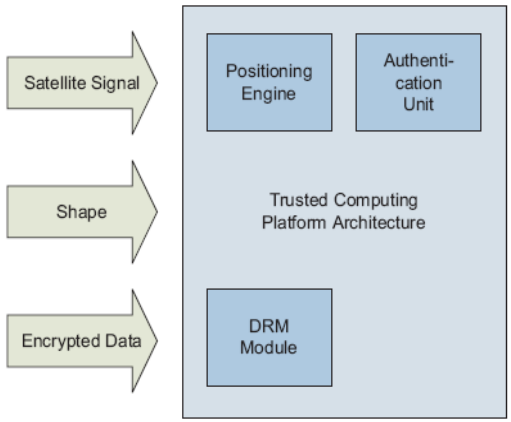
- Satellite based location provider
  - Either Navstar-GPS or Galileo
  - Signed signals
- Trusted hardware
  - Authentication module
  - Precise clock
  - Secure clock adjustment / synchronization

Basic principle



Authenticated signal

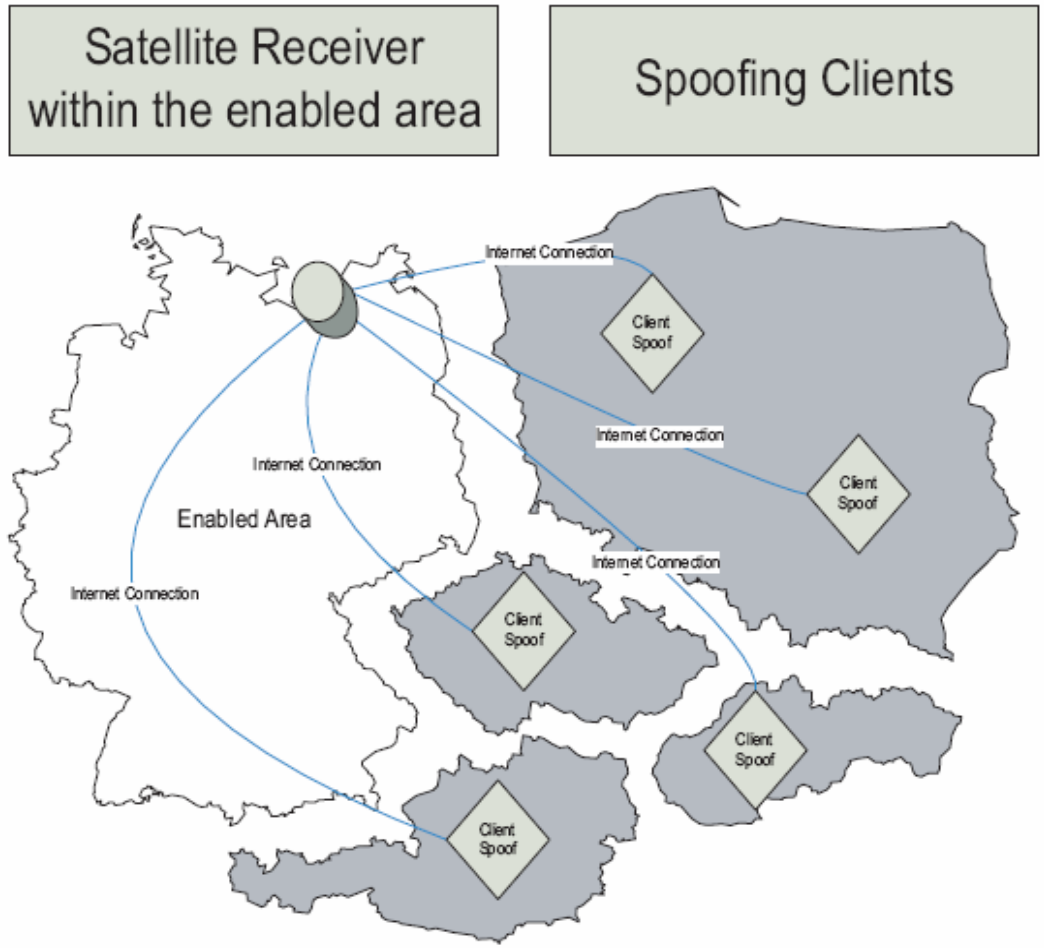
Signed shape data



Attacks

- Attacks against cryptographic subsystem
  - Out of scope
- Pseudolites
  - Solved by definition: satellite signal is digitally signed
- Rerouting
  - Forwarding the signal from the point of reception to a spoofing client
  - On different network layers (bit rate of P-code is 10.23MHz (chipping frequency), L2C 50 bps)
- Replay
  - Recording and playback of signals

Rerouting


Satellite Receiver within the enabled area
Spoofing Clients
Internet Connection
Client Spoof
Internet Connection
Client Spoof
Internet Connection
Enabled Area
Internet Connection
Client Spoof
Internet Connection
Client Spoof
Client Spoof

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

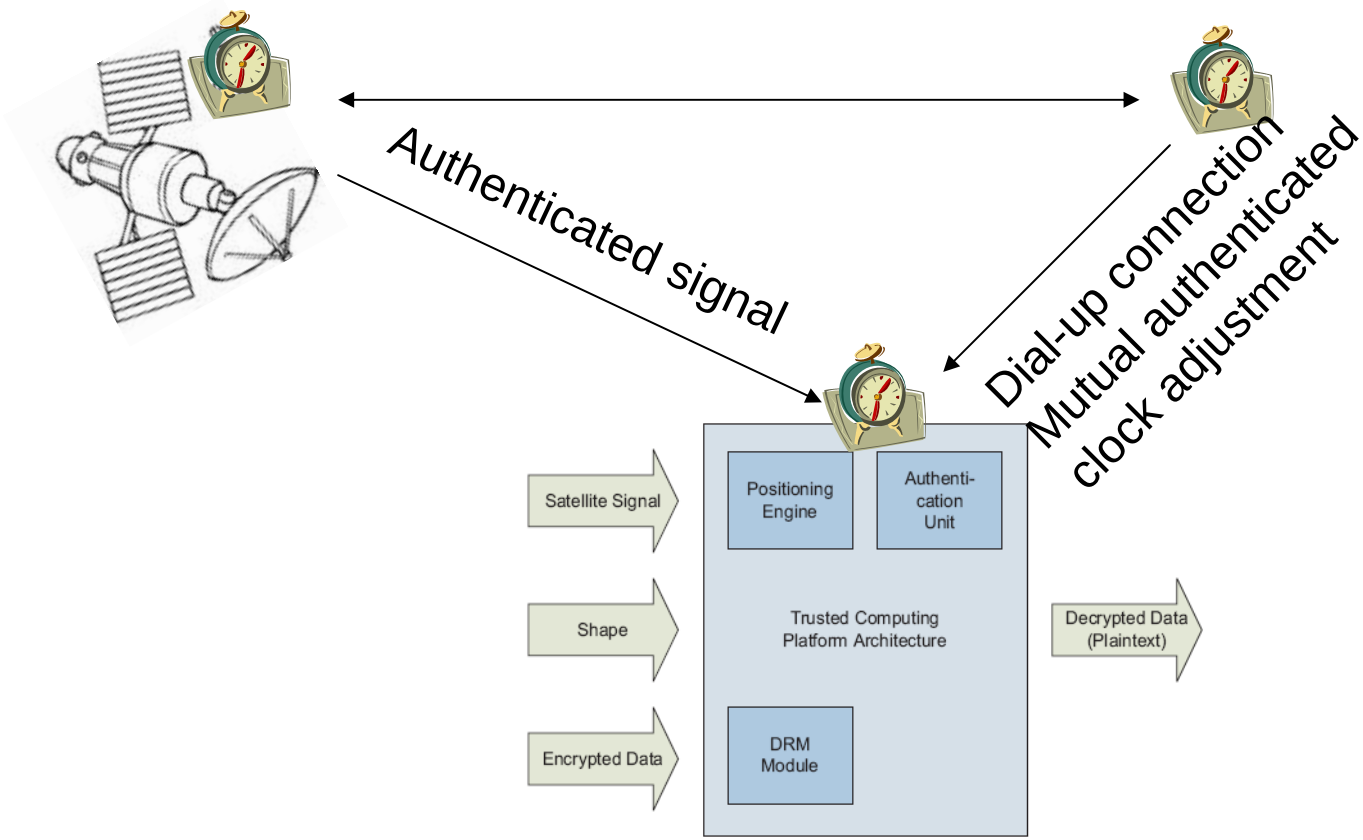
Latencies

```
thm@mammut:/users/iuk00/thm> traceroute 129.143.101.89
traceroute to 129.143.101.89 (129.143.101.89), 30 hops max, 40 byte packets
 1  139.30.3.1 (139.30.3.1)  0.812 ms  0.598 ms  0.660 ms
 2  rrzgate (139.30.5.3)  0.657 ms  0.765 ms  0.604 ms
 3  139.30.2.65 (139.30.2.65)  1.669 ms  0.815 ms  0.819 ms
 4  139.30.0.17 (139.30.0.17)  0.745 ms  0.766 ms  0.712 ms
 5  ar-rostock3.g-win.dfn.de (188.1.32.141)  0.838 ms  0.792 ms  0.874 ms
 6  cr-berlin1-po2-1.g-win.dfn.de (188.1.64.65)  6.806 ms  6.632 ms  6.600 ms
 7  cr-frankfurt1-po13-0.g-win.dfn.de (188.1.18.54)  15.408 ms  15.298 ms  16.280 ms
 8  cr-stuttgart1-po3-0.g-win.dfn.de (188.1.18.70)  18.391 ms  18.399 ms  18.501 ms
 9  ar-stuttgart4-ge3-3.g-win.dfn.de (188.1.76.5)  18.217 ms  18.226 ms  18.232 ms
10  Stuttgart2.BelWue.de (188.1.38.54)  20.104 ms  20.094 ms  20.056 ms
11  Stuttgart1.belwue.de (129.143.1.29)  18.691 ms *  18.781 ms
```

Latency detection

- System works offline most of the time
- DRM module needs to check satellite time for delays caused by rerouting
- DRM module requires a precise clock (error less than 5ms)
- Clock has to be protected against manipulation
- Clock must be adjusted regularly

Latency detection



Adjusting the clock

- Uses a mutual authenticated time synchronization protocol
- NTP‘s accuracy is better than 1ms
- How to deal with connections having asymmetric latencies
  - Switching the roles
  - Makes it much harder for an attacker

Conclusion

- Not able to provide an absolutely secure solution
- But!!!
  - Able to detect rerouting above 5ms
  - Enough security for average requirements
- Authenticated positioning possible with few limitations

Outlook

- Use of different location providers
  - Fingerprinting within Mesh Networks / MANETs with mutual tracking
- Further integration into a chipset
- Prototyping real applications

Thank you!