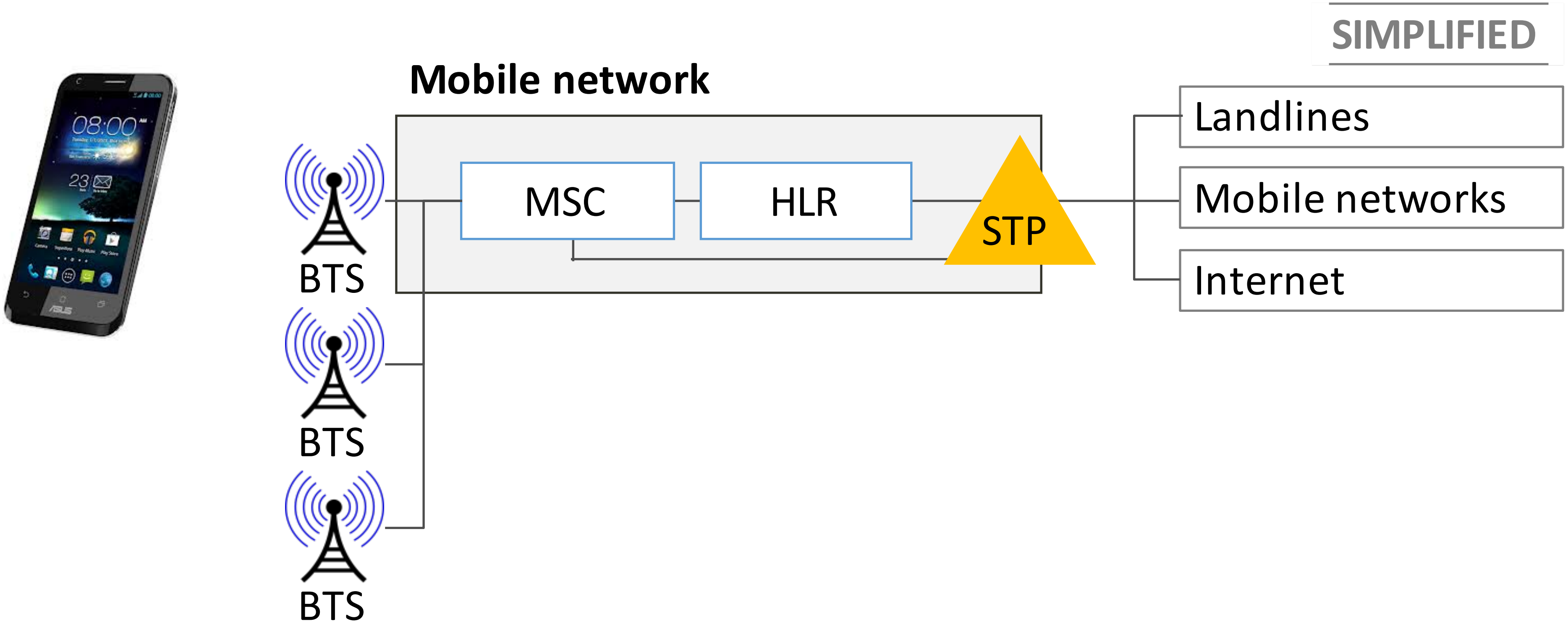
Mobile network insecurities

and what we can learn from them

Introduction: Mobile networks are complex



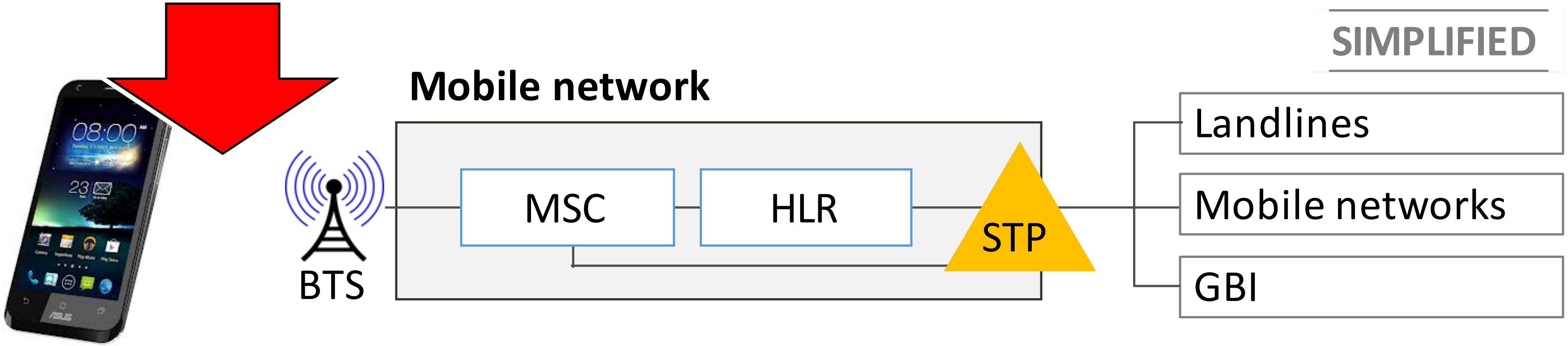
Mobile network users are exposed to three attack categories

Attack type	User risk
Tracking	▪ User's location is disclosed to the adversary
Intercept	▪ Contents of calls and short messages are accessible to third parties
Impersonation	▪ Attacker performs actions on user's behalf, e.g. use premium services, drop calls

Agenda

- **Radio Interface**
- SIM card
- Interconnect

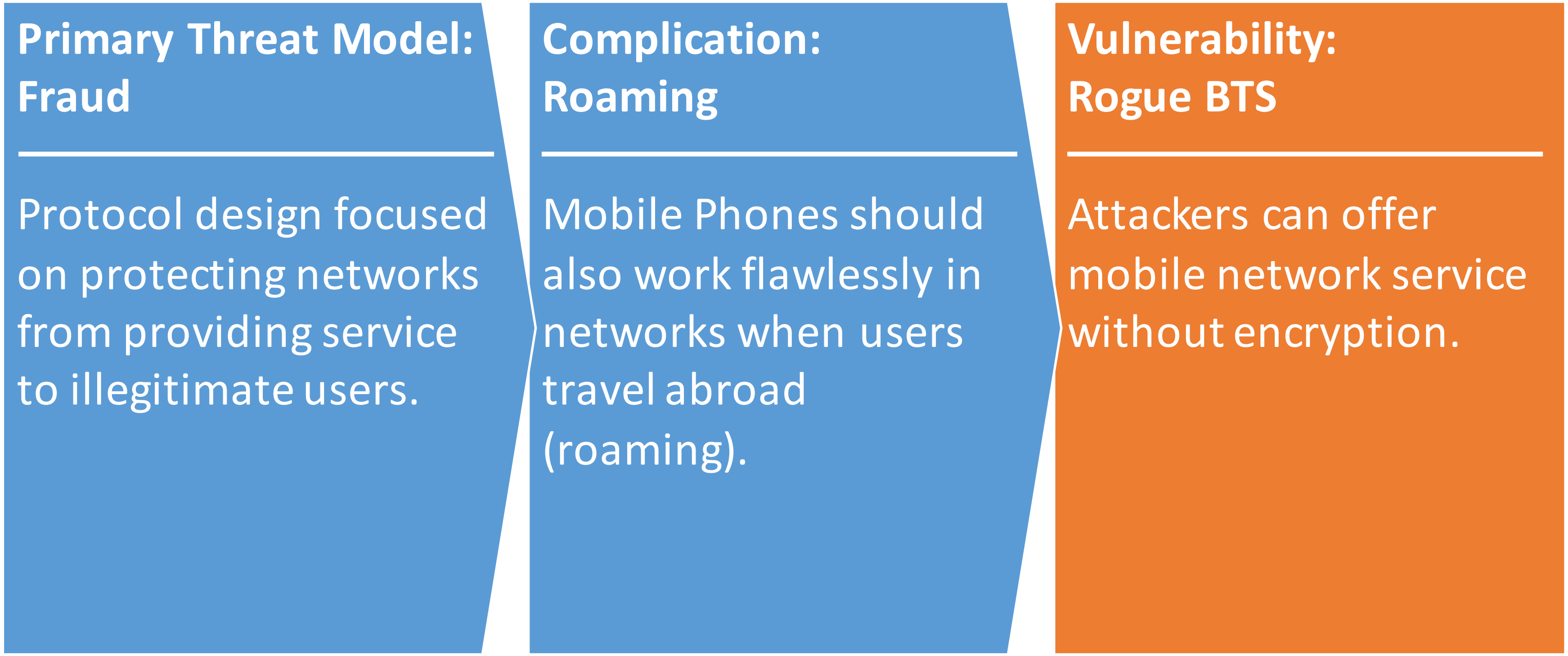
Attacks on the radio interface



Agenda

- **Radio Interface**
  - **Active Intercept**
  - Passive Intercept
- SIM card
- Interconnect

GSM problem I: subscribers authenticate to the network, but the network is not authenticated



Primary Threat Model: Fraud

Protocol design focused on protecting networks from providing service to illegitimate users.

Complication: Roaming

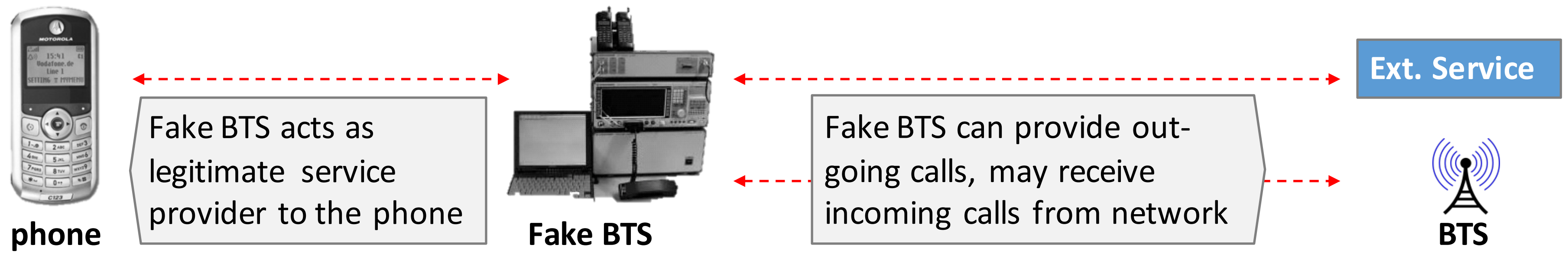
Mobile Phones should also work flawlessly in networks when users travel abroad (roaming).

Vulnerability: Rogue BTS

Attackers can offer mobile network service without encryption.

Fake base stations can offer rogue service

Attack setup



Fake BTS acts as legitimate service provider to the phone

Fake BTS can provide out-going calls, may receive incoming calls from network

Attack type	Fake BTS capabilities
Tracking	▪ Log IMSIs, TIMSIs and IMEIs of users in vicinity.
Intercept	▪ Drop encryption and intercept outgoing transactions ▪ Intercept of incoming transactions feasible when acting as man-in-the middle, connecting to legitimate network.

Agenda

- **Radio Interface**
  - Active Intercept
  - **Passive Intercept**
- SIM card
- Interconnect

GSM problem II: Cryptographic attack surface

Some GSM frame contents are fully **know or partially predictable.**
This enables **know-plaintext attacks** on the key material

Vulnerable GSM frames

- NULL-padding in empty or partially empty frames
- SI5 and SI6-messages
- Empty ACK messages after
  - Assignment complete
  - Alerting
  - Cipher mode complete
- Etc …

Attack:

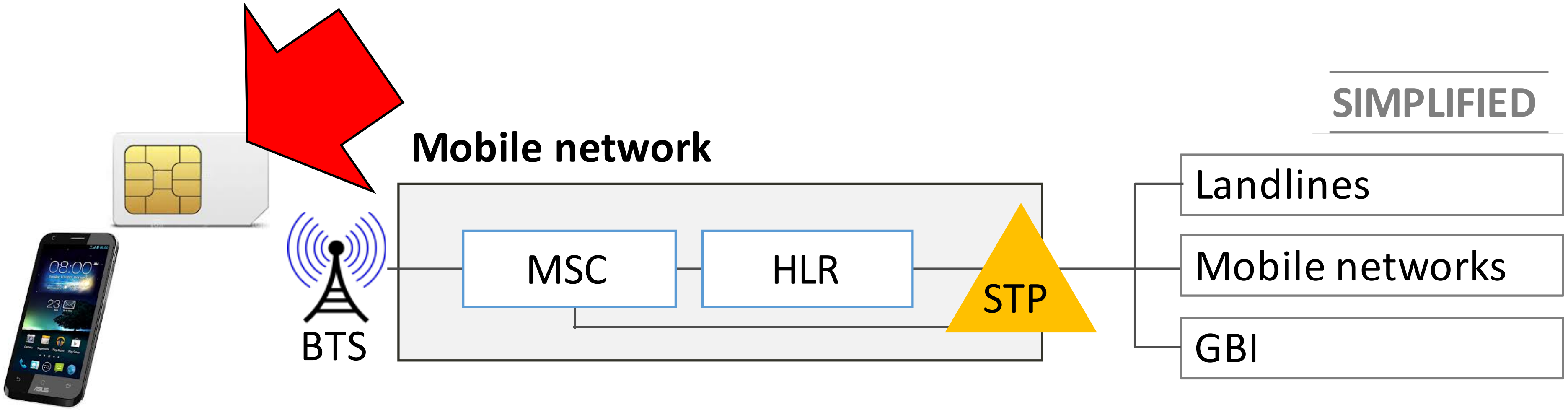
- Stream cipher
- Key length: 64bit (effectively 54bit in Comp128)
- Time-memory-trade-off

Karsten Nohl, Chris Paget (2009): *GSM– SRSLY?* – 26th Chaos Communication Congress
https://media.ccc.de/v/26c3-3654-en-gsm_srsly

Agenda

- Radio Interface
- **SIM card**
- Interconnect

Mobile networks combine many technologies and attack surfaces



Operators can send
short message commands to the SIM cards

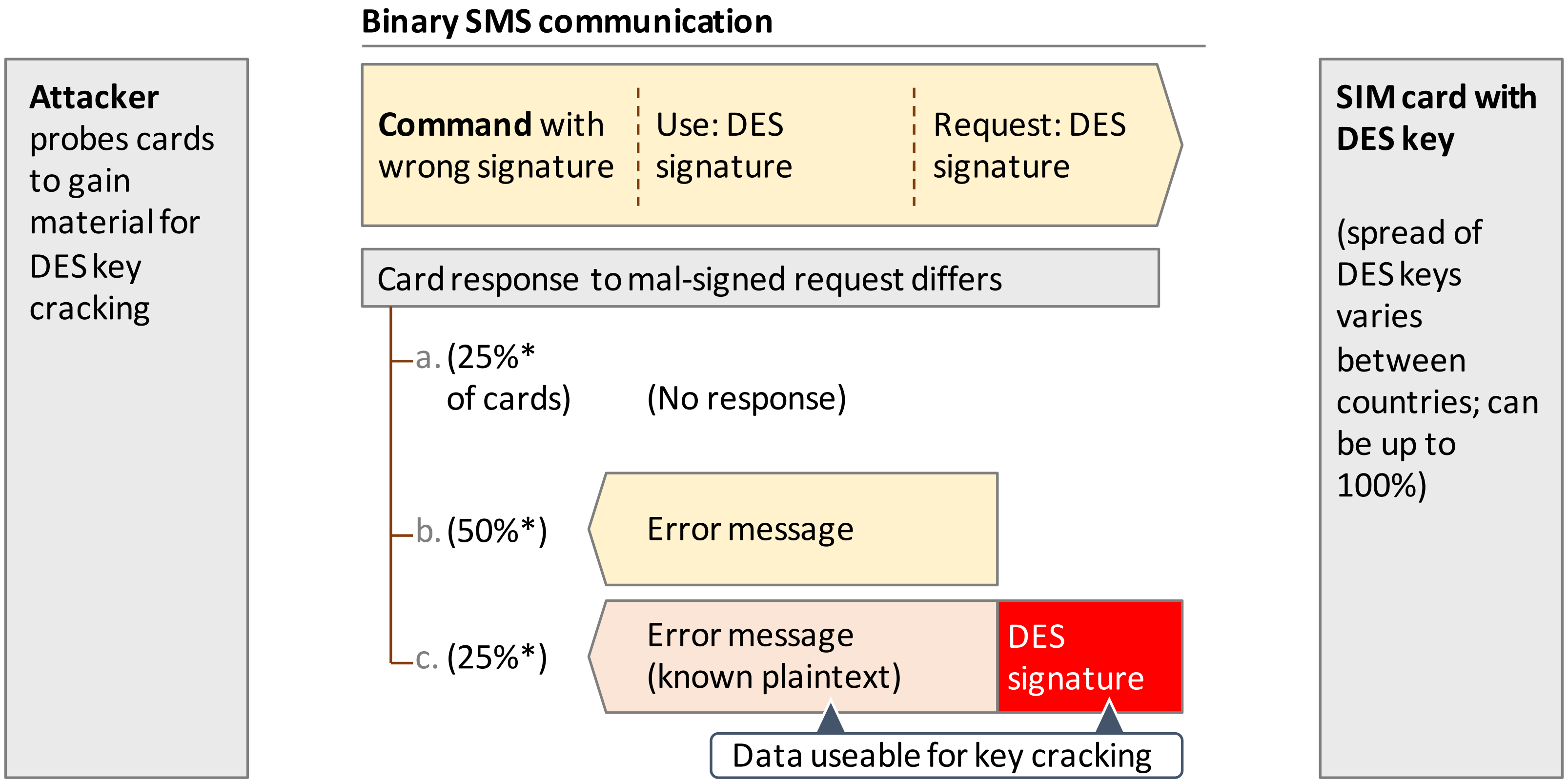
Configuration updates
e.g. preferred roaming networks

Java applications & commands
e.g. NFC & payment

File management
e.g. App installation

- ✓ Messages processed directly by SIM card
- ✓ Card can respond via SMS
- ✓ No user notification

SIM problem I: OTA error handling underspecified



Attacker probes cards to gain material for DES key cracking

Binary SMS communication

Command with wrong signature | Use: DES signature | Request: DES signature

Card response to mal-signed request differs

a. (25%* of cards) (No response)

b. (50%*) Error message

c. (25%*) Error message (known plaintext) DES signature

Data useable for key cracking

SIM card with DES key

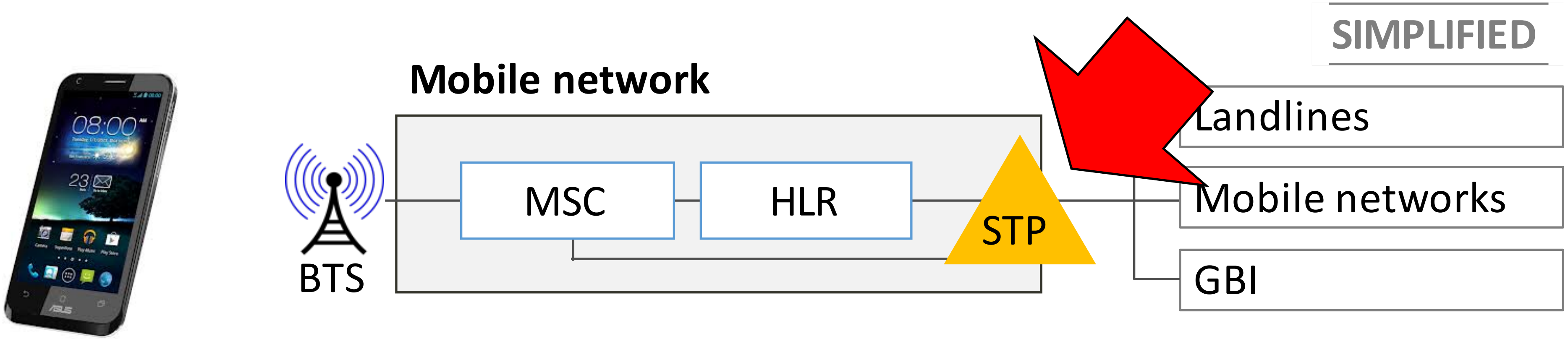
(spread of DES keys varies between countries; can be up to 100%)

Karsten Nohl (2013): *Rooting SIM cards* – Blackhat USA / OHM 2013
https://srlabs.de/rooting-sim-cards/

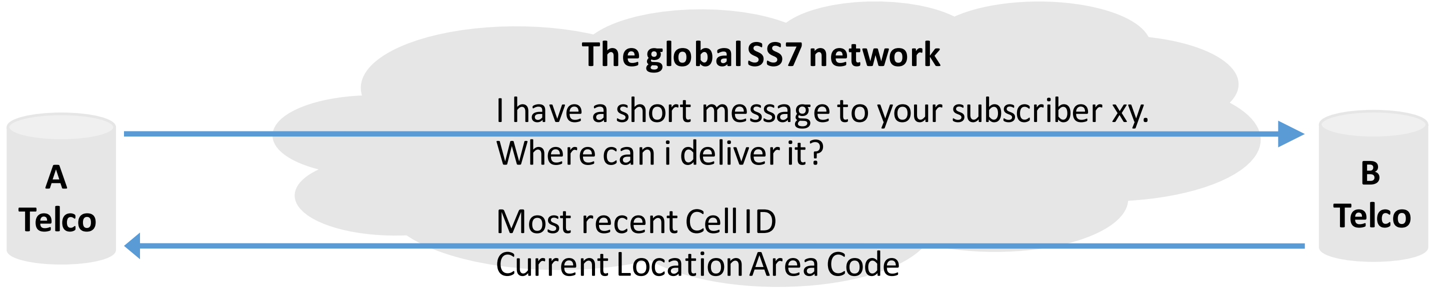
Agenda

- Radio Interface
- SIM card
- **Interconnect**

Mobile networks combine many technologies and attack surfaces



Interconnect problem: Telcos do not authenticate each other but leak private user data



The global SS7 network

I have a short message to your subscriber xy.
Where can i deliver it?

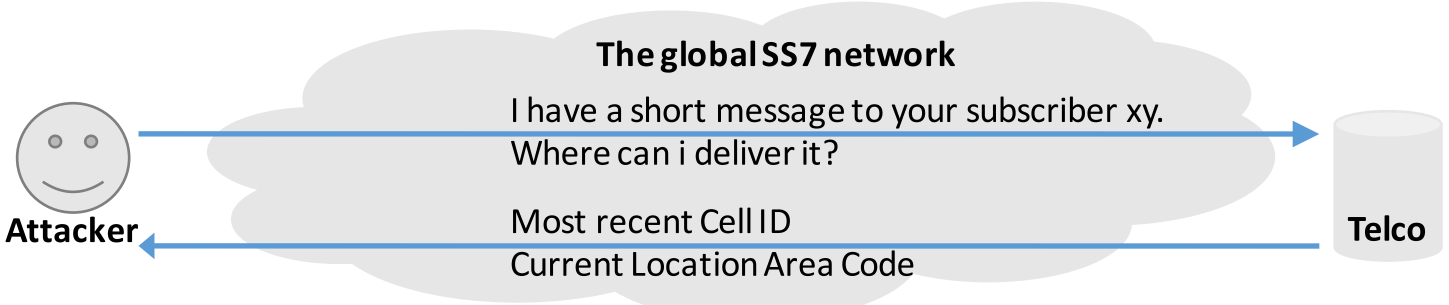
Most recent Cell ID
Current Location Area Code

Query	Accessible to	Location granularity
SEND ROUTING INFO FOR SHORT MESSAGE	▪ Anybody on the Internet	▪ General region (rural) to city district (urban)
ANYTIME INTERROGATION REQ.	▪ Network operators	▪ Cell ID: precise location

Tobias Engel (2008): *Locating Mobile Phones using SS7* – 25. Chaos Communication Congress
https://media.ccc.de/v/25c3-2997-en-locating_mobile_phones_using_ss7

Interconnect problem: Telcos do not authenticate each other but leak private user data

Anybody with access to the SS7-network can issue these queries and will receive a response, unless filtered.



The global SS7 network
I have a short message to your subscriber xy. Where can i deliver it?
Attacker
Most recent Cell ID
Current Location Area Code
Telco

Query	Accessible to	Location granularity
SEND ROUTING INFO FOR SHORT MESSAGE	▪ Anybody on the Internet	▪ General region (rural) to city district (urban)
ANYTIME INTERROGATION REQ.	▪ Network operators	▪ Cell ID: precise location

Tobias Engel (2008): *Locating Mobile Phones using SS7* – 25. Chaos Communication Congress
https://media.ccc.de/v/25c3-2997-en-locating_mobile_phones_using_ss7

Philippe Langlois (2010): *Getting in the SS7 Kingdom* – Hackito ergo sum
http://www.hackitoergosum.org/2010/HES2010-planglois-Attacking-SS7.pdf

Further Interconnect research

Interconnect attacks allow for more than just location **tracking**.
Encryption key leakage and call forwarding can be exploited to facilitate **Intercept** attacks. **Fraudulent** subscriber data manipulation can be exploited in numerous ways.

Kasten Nohl & team (2014):
Mobile self-defense.
31st Chaos Communication Congress

https://media.ccc.de/v/31c3_-_6122_-_en_-_saal_1_-_201412271830_-_mobile_self-defense_-_karsten_nohl

Tobias Engel (2014):
Locate. Track. Manipulate.
31st Chaos Communication Congress

https://media.ccc.de/v/31c3_-_6249_-_en_-_saal_1_-_201412271715_-_ss7_locate_track_manipulate_-_tobias_engel

Lessons learned:

Attack surface	Advice
Authen-tication	- Implement a bilateral end-to-end authentication scheme. - Do not rely on ”walled gardens” or Firewall zones.
Specification	- Specify protocols and behaviors thoroughly, especially for corner cases and error conditions.
Obscurity	- Rely on well-hung cryptographic algorithms and abolish attack surface, even it if is only theoretical.