LUND UNIVERSITY

Trust in Cyberspace - mobile networks, concerns

LUND, SWEDEN, OCTOBER 22, 2012

Trust in Cyberspace

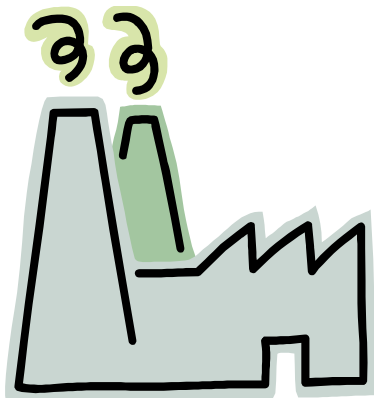
- Growing concerns
- The mobile network case
- Current views on addressing Cybercrime/Cyberwarfare in the EU and US
- Legal interception in the Cloud

We depend on Cyberspace

Social and Health functions

We

Infrastructures
ICT
Power
Buildings
Roads



Business

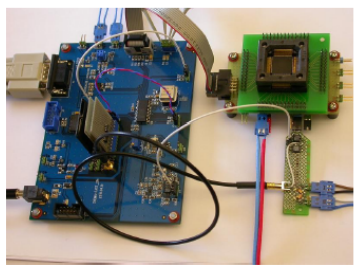
Example of Infrastructure Threats

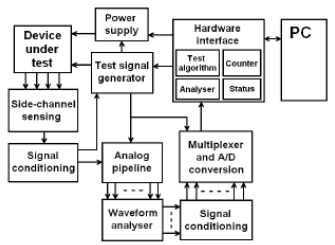
- Infecting software we all know – too well, e.g. Stuxnet
- infected hardware
  - possible too: Hardware Trojan, Y Desmedt 1986
  - Recent example: backdoor in military grade chip

    Cambridge Univ: *http://www.cl.cam.ac.uk/~sps32*

Experimental setup

- Same ProASIC3 A3P250 chip on the test board
- Dedicated hardware for waveform analysis using patented PEA technique
  - same measurement resistor in V_{CC} core supply line
  - analog waveform conditioning and pre-processing before the ADC
  - cost of components below $100 USD

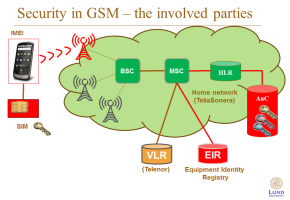




LUND UNIVERSITY

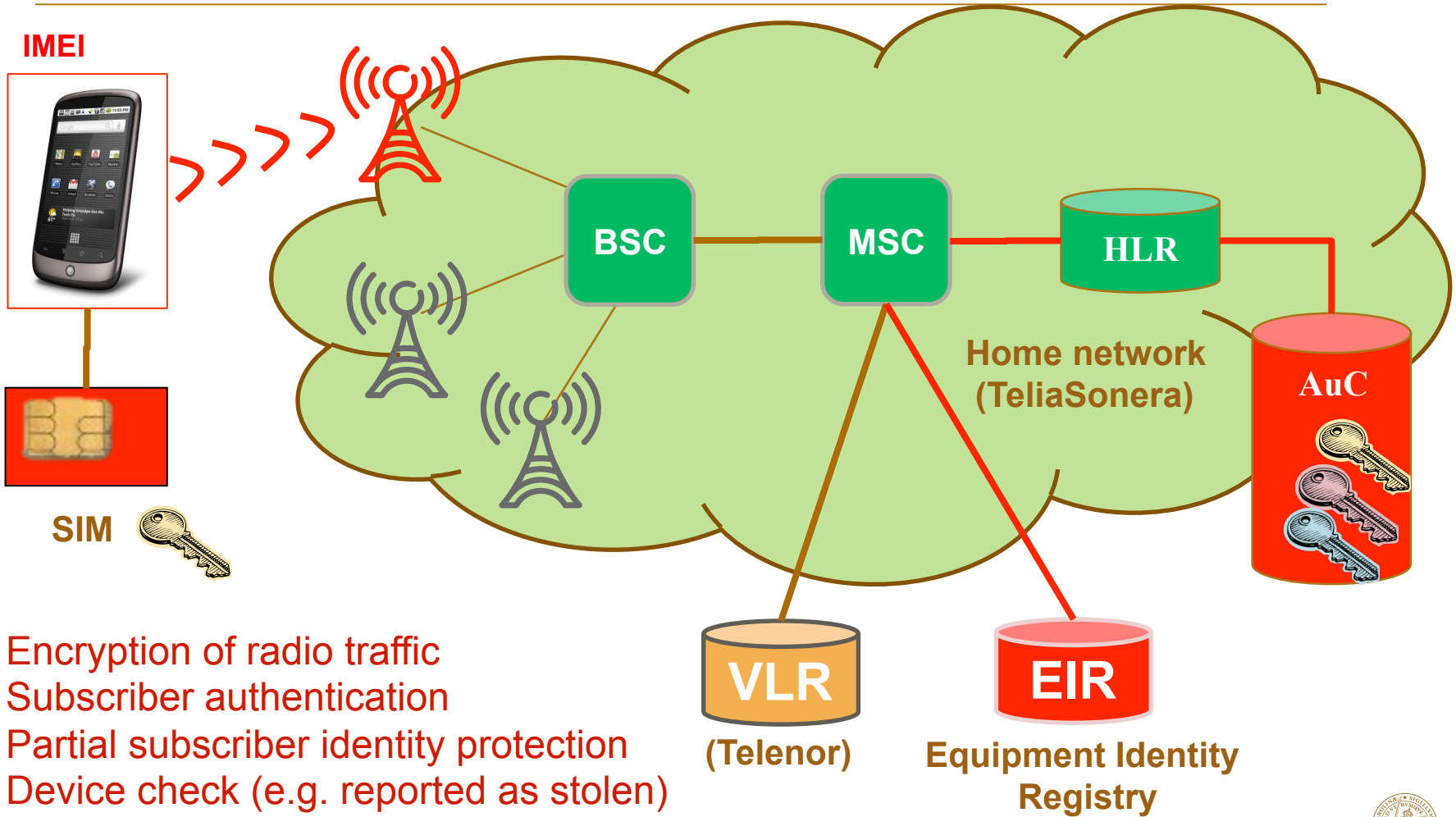
TRUST IN -
MOBILE NETWORKS

- SECURITY IN GSM



- TRUST – TO WHAT EXTEND?

Security in GSM – the most important



1. Encryption of radio traffic
2. Subscriber authentication
3. Partial subscriber identity protection
4. Device check (e.g. reported as stolen)

TRUST – TO WHAT EXTEND?

- GSM has some real problems
  - Mobile can be tricked to connect to false base station (solved in 3G/4G)
  - Old encryption algorithms still in use but are too weak – their use not indicated to user: he/she is unaware
  - Encryption keys are used too long (time wise, across algorithm switchover)
- Protection of user data in the mobile network is limited
  - Voice, data, sms only encrypted over a limited part of the transport channel
  - For data the above is less a problem as in most cases one runs an additional protection layer on top.
- Privacy
  - Tracking of user possible.

TRUST IN -
CYBERSPACE

- CYBERSECURITY CONCERNS IN THE POLITICIANS WORLD OF EU AND US
- LEGAL INTERCEPTION IN THE CLOUD

Cybersecurity – Politicians in EU and US

- EU: Politicians, ENISA
  - Establishing National Cyber Security Strategies
  - There are concerns about the use of the Internet for terrorist purposes and the abuse of legal / neutral websites.

- US: 2009 White House:
  - President Obama has declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity.”

Cybersecurity in the US

Key Documents

- Draft National Strategy for Trusted Identities in Cyberspace
- The Comprehensive National Cybersecurity Initiative
- The Cyberspace Policy Review (pdf)
- The Cyberspace Policy Review supporting documents
- The National Initiative for Cybersecurity Education (pdf)
- Cybersecurtiy R&D

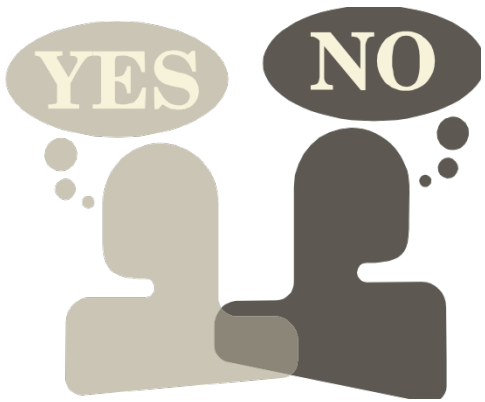
Cybersecurity – in the EU, ENISA

- *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*
- ENISA has launched a Study on National Cyber Security Strategies in the form of a **Good Practice Guide** which will highlight good practices and recommendations on how to develop, implement and maintain a Cyber Security Strategy.
- Links to National Cyber Security Strategies
  - Czech Republic
  - Estonia
  - Finland
  - France
  - Germany
  - Lithuania
  - Netherlands
  - United Kingdom
  - Luxembourg (*in French*)
  - Slovakia: *English version not available online*

Cybersecurity –EU, CleanIT

- There are concerns about the use of the Internet for terrorist purposes and the abuse of legal / neutral websites. The question is if we can reduce the impact of the use of internet for terrorist purposes, without affecting our online freedom. A question this project tackles in a public-private dialogue.

- (Controversial) Proposals:
  - Protection vs Privacy?
  - Technical realistic ?
  - …



http://www.cleanitproject.eu/wp-content/uploads/2010/12/CLEAN-IT-DRAFT-DOCUMENT-066Pub.doc

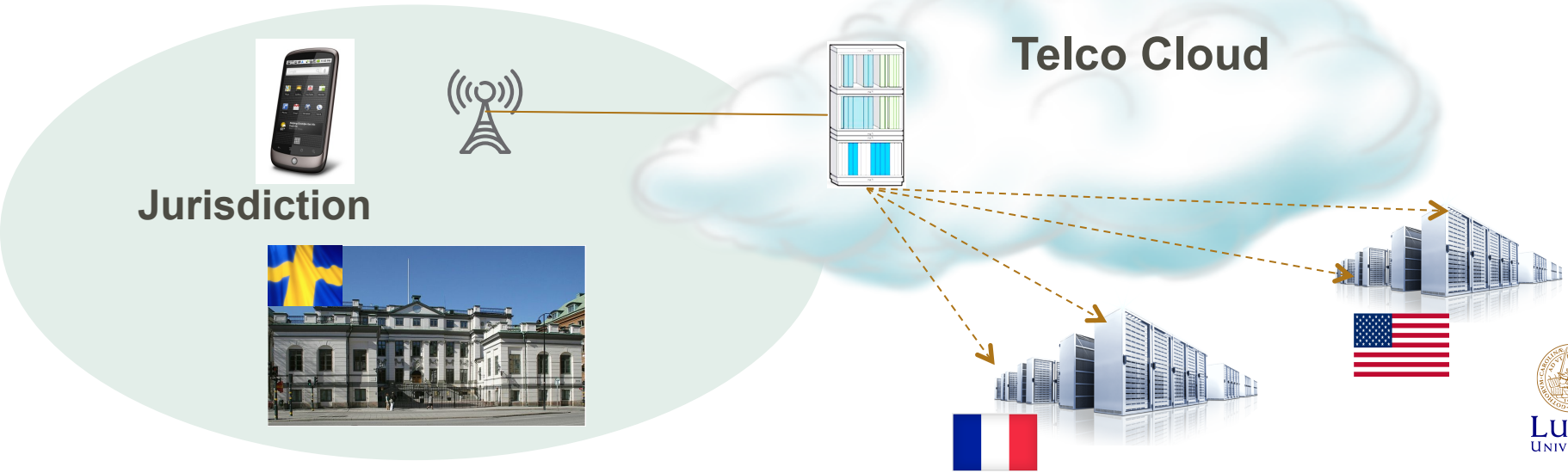
Legal Interception – in the Cloud

The basis: telecom is under control by the state

Example Sv

Lag (2003:389) om elektronisk kommunikation

2 kap. Anmälan
1 § Allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster får endast tillhandahållas efter anmälan till den myndighet som regeringen bestämmer (tillsynsmyndigheten).



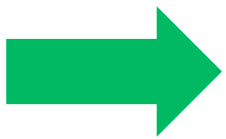
SO ?

more

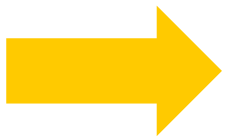
We likely see in the coming years efforts directed towards

- Control and securing of internet and ICT infrastructures
- Privacy and (digital) Identity protection

– Regulators
– Technical/Industry
– Individuals



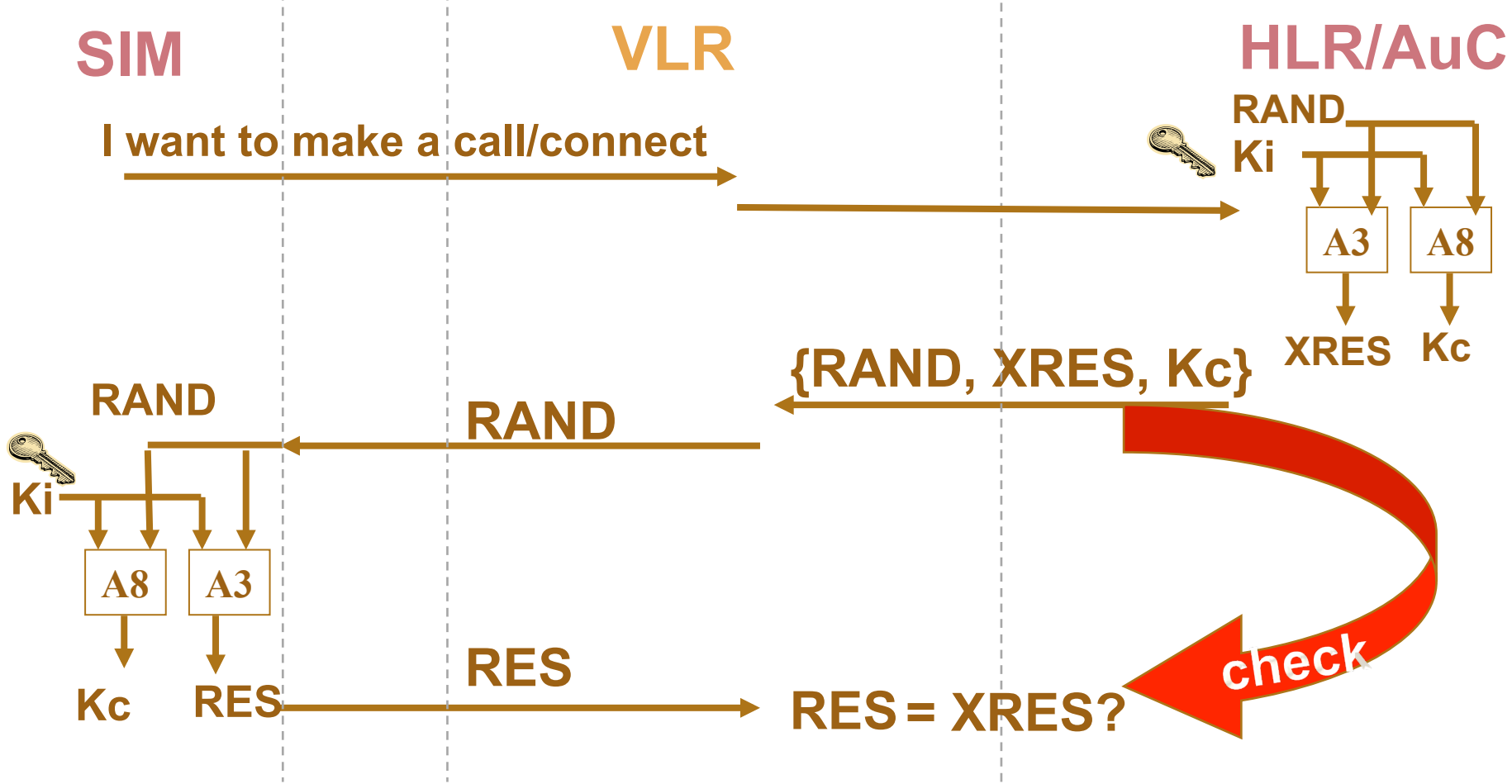
BENEFITS
- dependable infrastructure



RISKs
- of a segmentation of the Internet
- more usage restrictions

Spare slides

GSM Authentication and crypto key setup



LUND UNIVERSITY

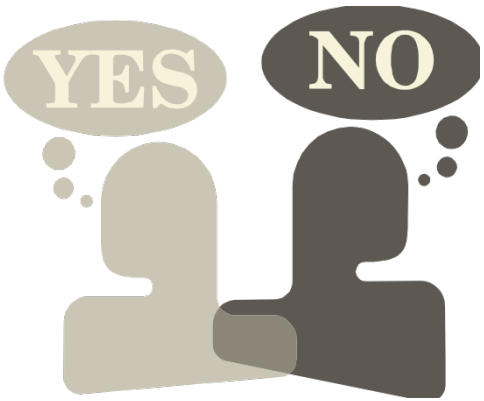
Cybersecurity –EU, CleanIT

CleanIT Project (leaked document aug 2012, now public)

http://www.cleanitproject.eu/wp-content/uploads/2010/12/CLEAN-IT-DRAFT-DOCUMENT-066Pub.doc

It is open for comments:

editorialboard@cleanITproject.eu



Preventive best practices

22. Real identity policies
Problem: Terrorists (and other criminals) profit from the anonymity that large parts of the Internet offer. Even though anonymity to other users is logical and desirable for some Internet services, for many it is not a necessity. Terrorists are less likely to use services in which they are easily recognizable to other users.
PM

23. Police patrol on social media
Problem: Less than in the physical world, Internet users realize their behaviour must be within laws and social norms. On the Internet, users are hardly ever confronted with or reminded of the presence of LEAs, signalling that abusive behaviour will have consequences. On social media platforms, where there is a lot of social interaction, terrorists currently feel secure enough to spread their propaganda on a vast scale and recruit others.
Goal: LEAs will be visible and active on most relevant social media platforms to deter, detect and react to terrorist use of social media.
Benefits: Police patrolling on social media will reduce terrorist incitement, recruitment and learning.

Detection best practices

24. Automated detection systems.
Problem: While users, LEAs, NGOs and Internet companies do report a number of (potential)