THE PROBLEM OF PRIVATE IDENTIFICATION PROTOCOLS

Ruxandra F. Olimid and Stig F. Mjølsnes

Dept. of Information Security and Communication Technology, NTNU, Norway

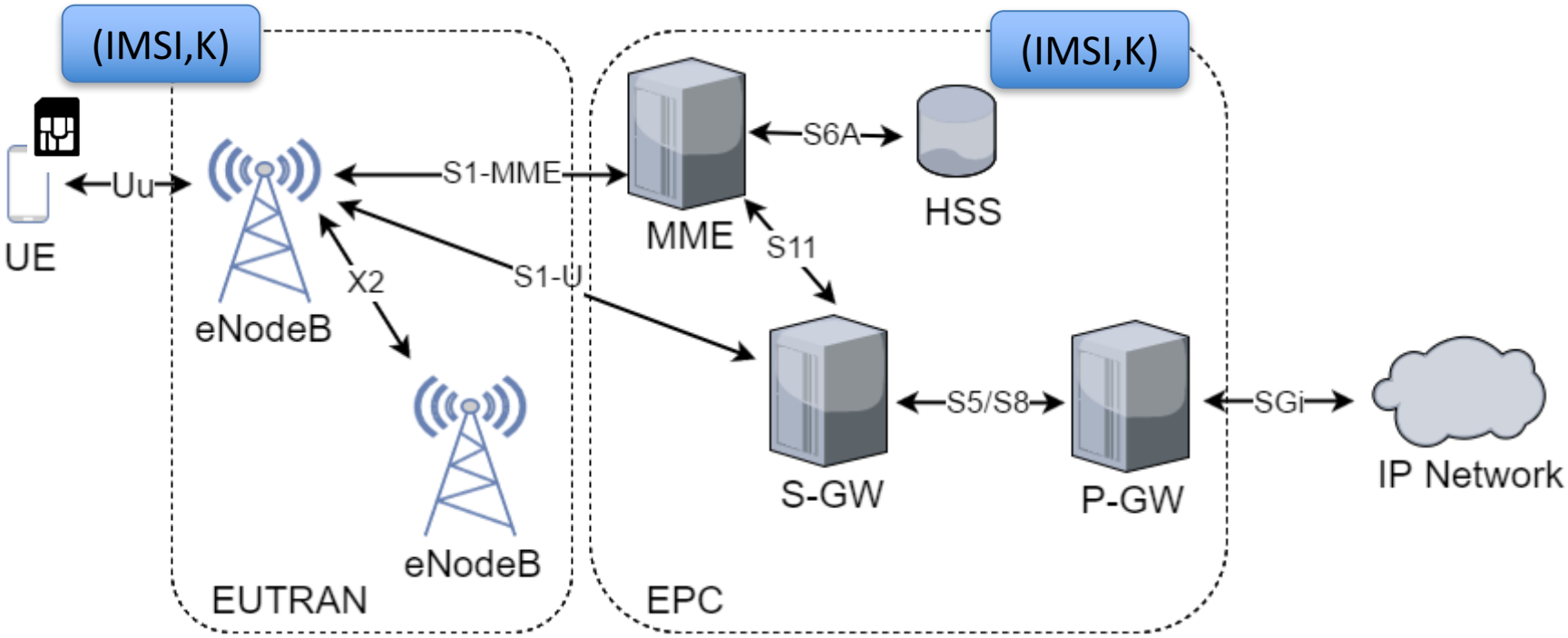
Real World Crypto 2018

Zurich, January 10

Norwegian University of Science and Technology

Motivation - LTE

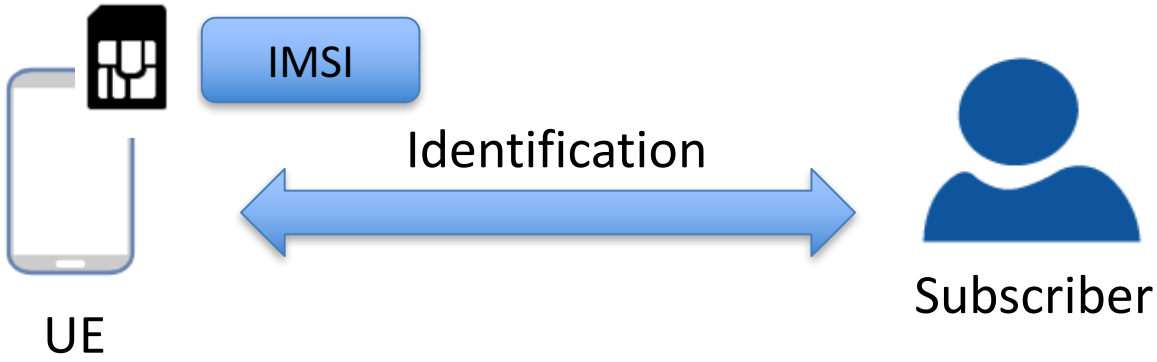
LTE - Subscriber's Identification

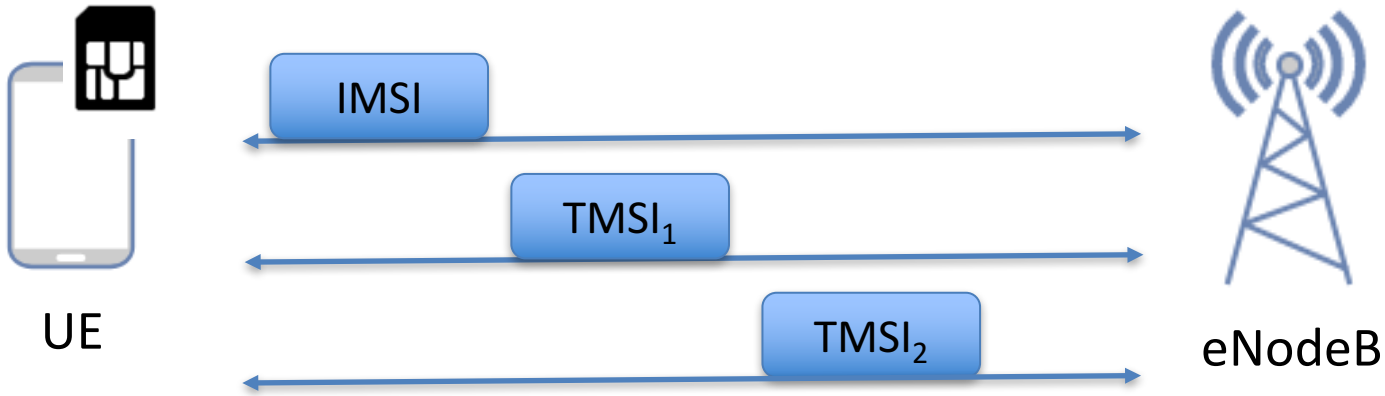


IMSI (International Mobile Subscriber Identity)

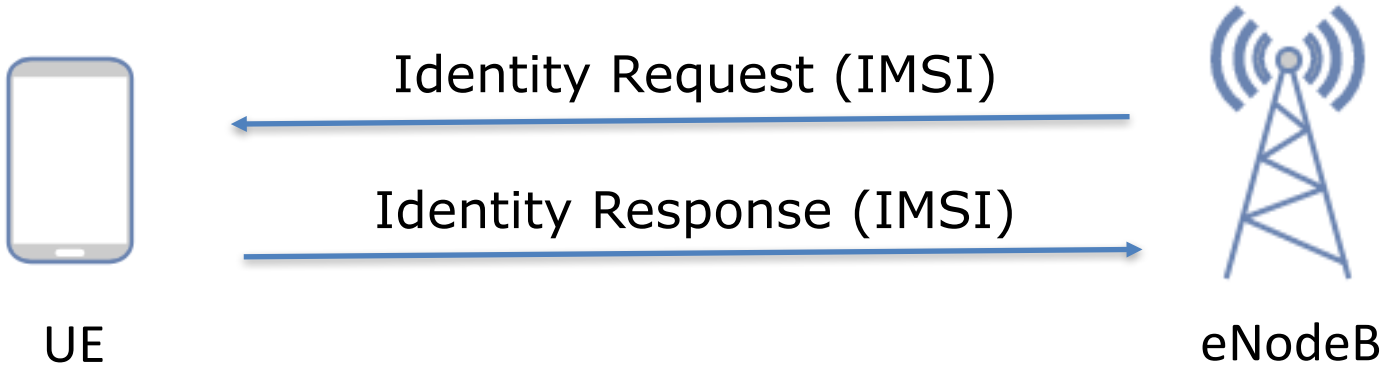
MCC (Mobile Country Code)	**MNC** (Mobile Network Code)	**MSIN** (Mobile Subscriber Identification Number)

LTE - Subscriber's Identification





LTE - Privacy Breach



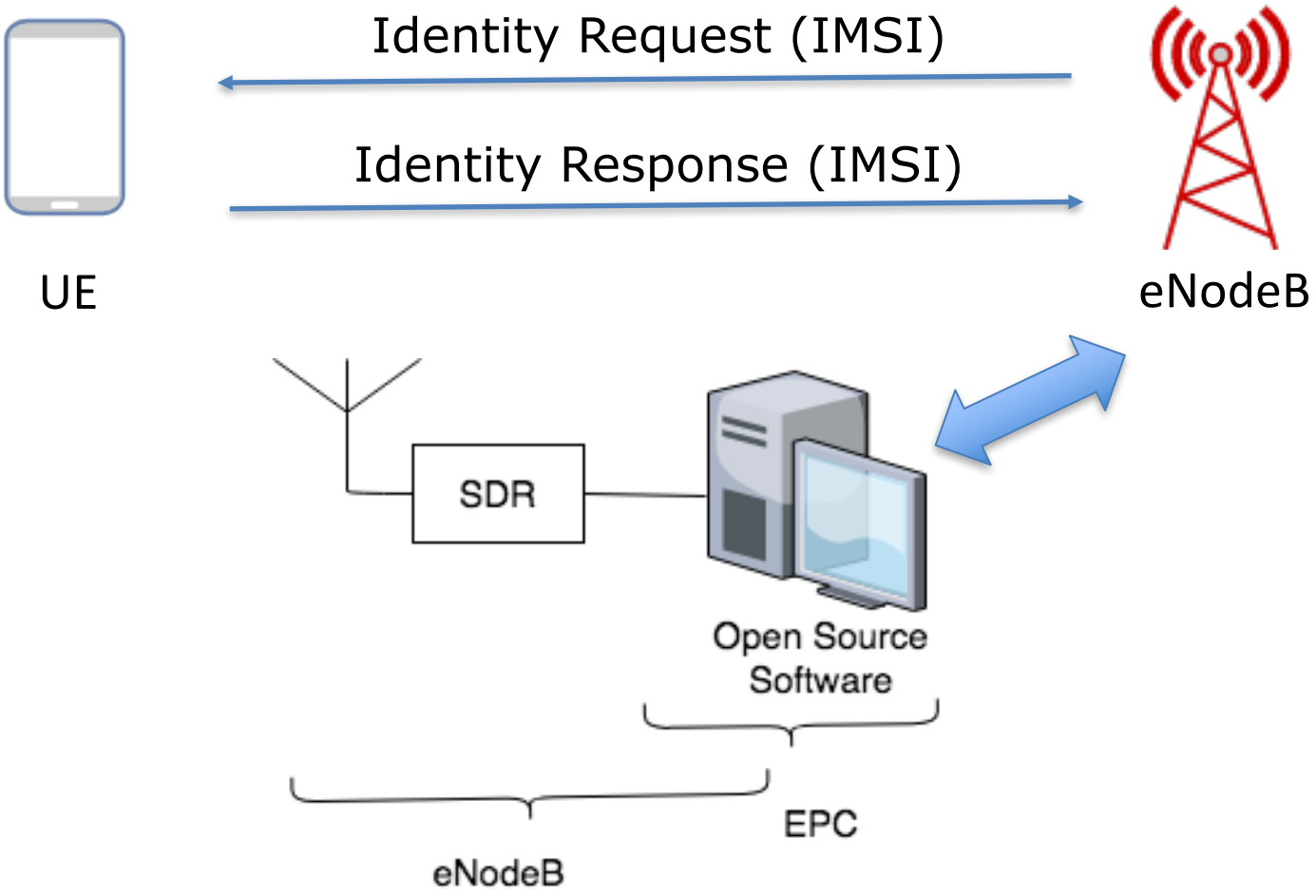
[. . .] requests the user to send its permanent identity. The user's response contains the IMSI in cleartext. This represents ***a breach in the provision of user identity confidentiality****.*

[ETSI TS 133 401 V14.4.0 (2017-10)]

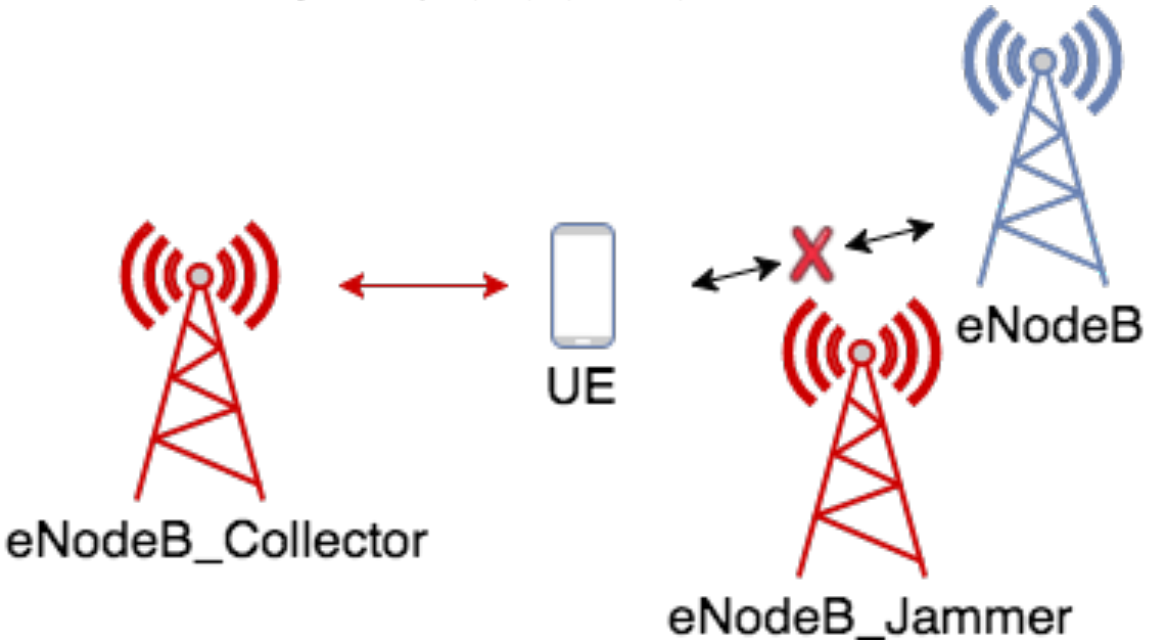
Experimental Work

- S.F.Mjølsnes, R.F.Olimid: *Easy 4G/LTE IMSI Catchers for Non-Programmers,* MMM-ACNS 2017
- S.F.Mjølsnes, R.F.Olimid: *Experimental Assessment of Private Information Disclosure in LTE Mobile Networks,* Secrypt 2017

Experimental Work

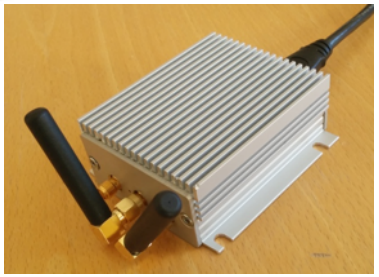


Our LTE IMSI Catcher



- `eNodeB_Jammer:` causes the UE to detach from the serving cell it camps on
- `eNodeB_Collector:` masquerades as an authorized eNodeB running on the (second) highest **priority frequency**, but with higher signal power, causing the UE to try reselection and expose the IMSI

Tools: **Hardware**

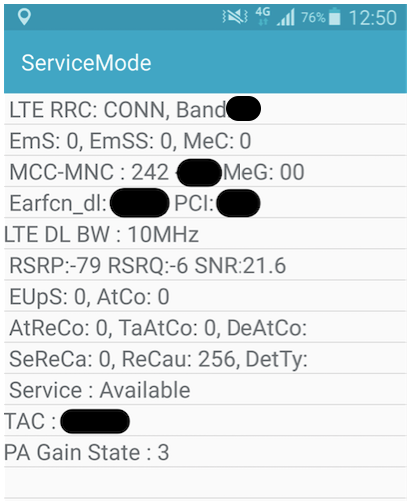


- Software radio peripherals (USRPs)
  - Ettus B200mini + antennas
    [https://www.ettus.com/product/details/USRP-B200mini]
- Computers (access and core network)
  - Standard desktops or laptops: Intel NUC D54250WYK (i5-4250U CPU@1,30GHz), Lenovo ThinkPad T460s (i7-6600U CPU@2,30GHz)

- Mobile terminals:
  - Samsung Galaxy S4 device, used to find the LTE channels and TACs used in the targeted area
  - Two LG Nexus 5X phones running Android v6, used to test our IMSI Catcher
- SIM cards

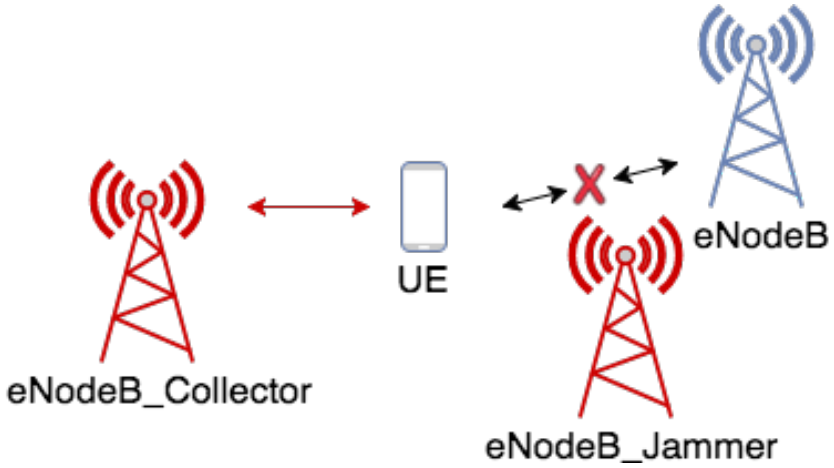
Tools: **Software**

- LTE Emulator:
  - **Open Air Interface (OAI),** an open source software that provides a (partially) standard compliant implementation of LTE



- Service Mode:
  - Dial *#0011# on Samsung Galaxy S4 device
  - Read configuration of the commercial network: EARFCN DL, TAC, MCC, MNC, Cell ID

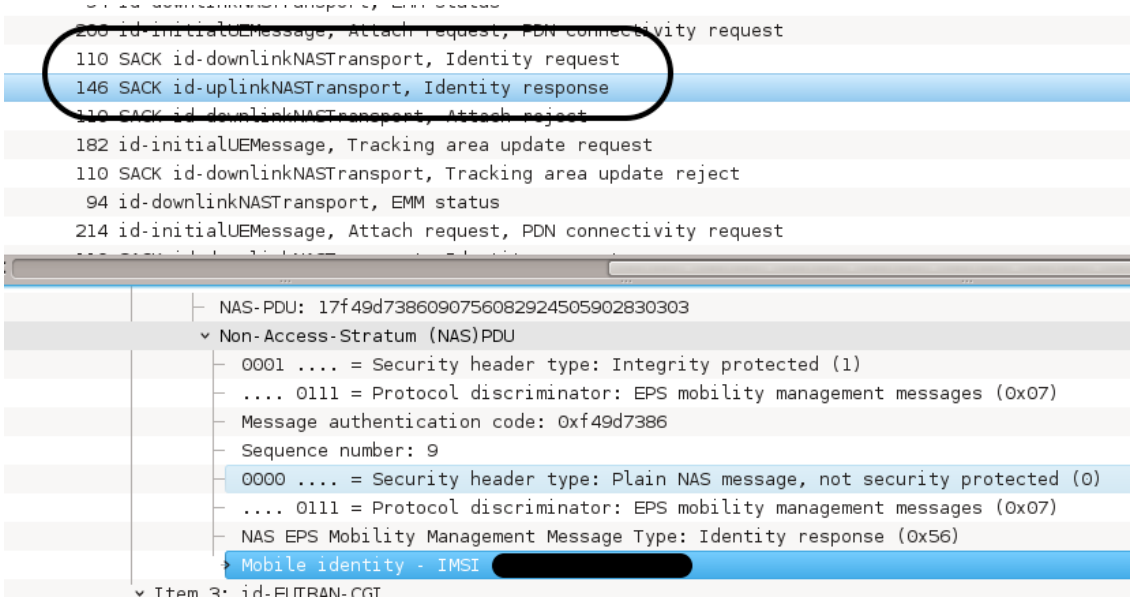
Construction



- **Phase 1. Gather the configuration parameters:**
  - Find the EARFCN DL and TAC (using the Samsung device)
  - Run `eNodeB_Jammer` using MCC, MNC and the EARFCN DL of the commercial cell
  - Read new EARFCN DL after reselection
- **Phase 2. Configure and run the LTE IMSI Catcher:**
  - Run `eNodeB_Collector` using MCC, MNC and the new EARFCN DL after reselection in the commercial network, but a different TAC
  - Run `eNodeB_Jammer` configured as in Phase 1

Results

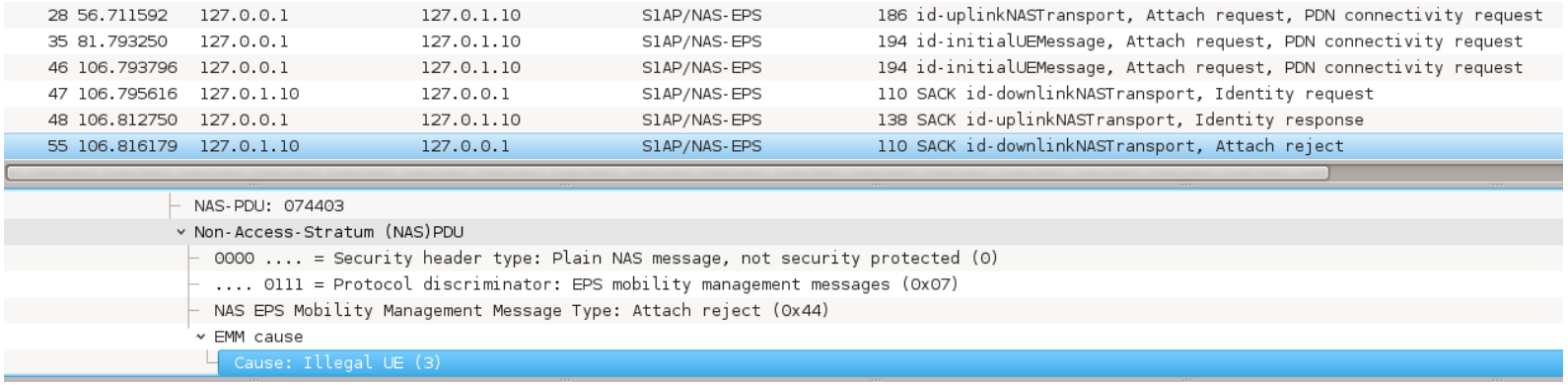
- Low-cost **IMSI Catcher** (< 3000 EUR):
  - COTS hardware and readily available software only
  - No (or very basic) changes in the source code




```
80 [MESSAGE] 9 -> 9 0 0103:990956EMMREG_COMMON_PROC_CNF ue id 0x00000002
81 [EVENT] 9 0103:991075EMM state DEREGISTERED UE 0x00000002
82 [MESSAGE] 8 -> 13 0 0103:9911920 S6A_AUTH_INFO_REQ IMSI 242[redacted] visited_plmn 242.[redacted] re_sync 0
83 [MESSAGE] 13 -> 8 0 0103:9921110 S6A_AUTH_INFO_ANS imsi 242[redacted] DIAMETER_AUTHENTICATION_DATA_UNAVAILABL
84 [EVENT] 7 0103:9921680 S6A_AUTH_INFO_ANS S6A Failure imsi 242[redacted]
85 [MESSAGE] 8 -> 9 0 0103:9921820 EMMCN_AUTHENTICATION_PARAM_FAIL
```

Results

- Behaviour:
  - Denial-of-Service (DoS) until reboot - *cause 3* (`Illegal UE`)
  - Downgrade to non-LTE services - *cause 7* (`EPS services not allowed`)
  - Reconnection to the commercial network - *cause 15* (`No suitable cells in tracking area`)



Similar Work

Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems

Altaf Shaik*, Ravishankar Borgaonkar†, N. Asokan‡, Valtteri Niemi§ and Jean-Pierre Seifert*
*Technische Universität Berlin and Telekom Innovation Laboratories
Email: (altaf329, jpseifert) @sec.t-labs.tu-berlin.de
†Aalto University
Email: ravishankar.borgaonkar@aalto.fi
‡Aalto University and University of Helsinki
Email: asokan@acm.org
§University of Helsinki
Email: valtteri.niemi@helsinki.fi

[NDSS 2016]

LTE security, protocol exploits and location tracking experimentation with low-cost software radio

Roger Piqueras Jover
Bloomberg LP, New York, NY
rpiquerasjov@bloomberg.net

International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security
MMM-ACNS 2017: Computer Network Security pp 235-246

Easy 4G/LTE IMSI Catchers for Non-Programmers

Authors | Authors and affiliations

Stig F. Mjølsnes, Ruxandra F. Olimid

Experimental Assessment of Private Information Disclosure in LTE Mobile Networks

Topics: Security and Privacy in Mobile Systems

In **Proceedings of the 14th International Joint Conference on e-Business and Telecommunications - Volume 6: SECRYPT,** 507-512, 2017, Madrid, Spain

Authors: Stig F. Mjølsnes and Ruxandra F. Olimid

Affiliation: NTNU and Norwegian University of Science and Technology, Norway

NTNU

IMSI Catchers in the Real World

”Real World” IMSI Catchers

[Aftenposten, Dec.16 2014]

”Real World” IMSI Catchers

Piranha - 2G, 3G, and 4G IMSI Catcher

Piranha is a 2G, 3G and 4G (LTE) IMSI Catcher System that enables gathering mobile phone identities in the area of the system.

[http://www.rayzoneg.com/en.piranha.html]

”Real World” IMSI Catchers

[https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/]

The Intercept_

54

Photo: U.S. Patent and Trade Office

LONG-SECRET STINGRAY MANUALS DETAIL HOW POLICE CAN SPY ON PHONES

Sam Biddle

September 12 2016, 9:33 p.m.

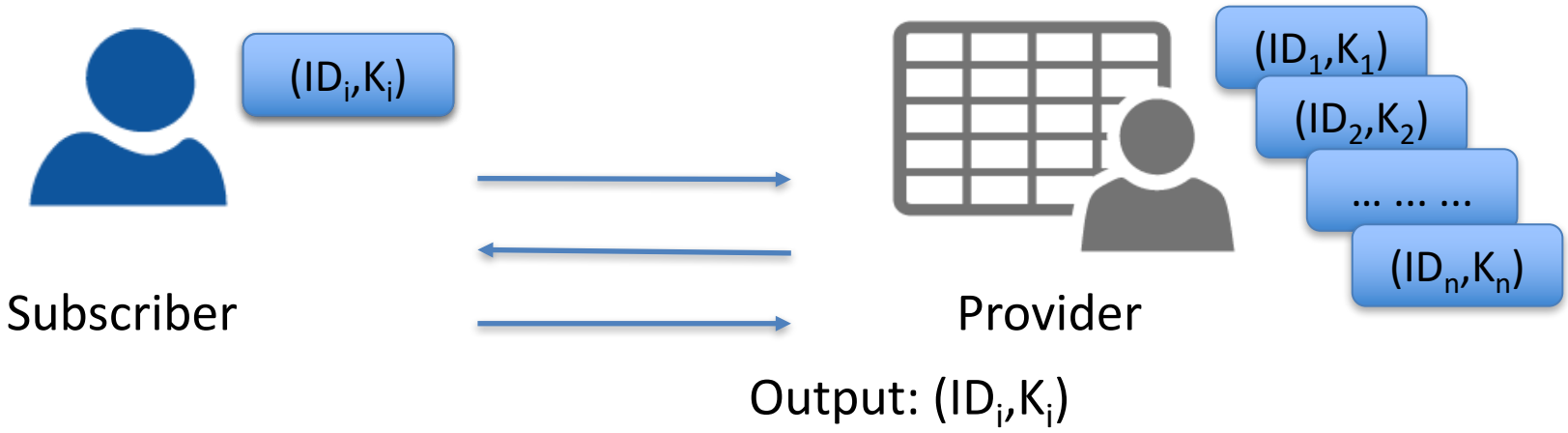
NTNU

The cryptographic problem

- S.F.Mjølsnes, R.F.Olimid: *The challenge of private identification, iNetSec 2017* (to appear)

The Problem

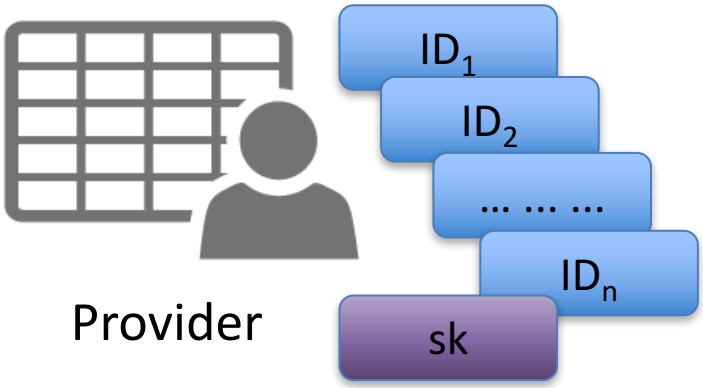
(*How) Can we construct efficient and scalable secure identification mechanisms in (mobile) communication systems?*



We **decouple** the protocol from *registration* and *authentication*, to gain independence in design and analysis - the private identification challenge becomes a *general standalone problem*

Public Key - Trivial Solution

Subscriber



Provider

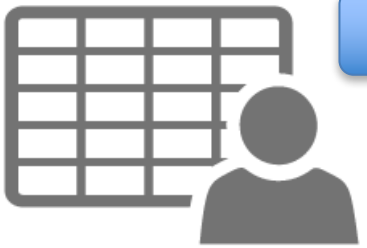
$Enc_{pk}(ID_i)$

No PubKey

$Dec_{sk}(Enc_{pk}(ID_i)) = ID_i$

Key Search - Linear Solution

(ID_i,K_i)



(ID_1,K_1)

(ID_2,K_2)

… … …

(ID_n,K_n)

Subscriber

Provider

$r_j \leftarrow^R \mathcal{R}$

*key-indistinguishable MAC

$r_j, Enc_{Ki}(r_j)$

Linear time

Try all $\{K_i\}$ until successfully decryption of r_j

Output: (ID_i,K_i)

[Weis, Sarma, Rivest, Engels - Security and Pervasive Computing'03]

[Alwen, Hirt, Maurer, Patra, Raykov - Anonymous Authentication with Shared Secrets'14]

Related Work

- Models and definitions:
  - Mobile Networks, include authentication [Alwen et al.'14, Abadi & Fournet'15]
  - RFIDs [Vaudenay'07], [Canard et al.'10], [Hermans et al.'14], [Yang et al.'17]
- Mobile networks (LTE):
  - Several IMSIs for each USIM [Kahn & Mitchel'15]
  - New temporary identifiers: *DMSI* (Dynamic Mobile Subscriber Identities) [Choudhury et al.'12], *PMSI* (Pseudo Mobile Subscriber Identities) [Broek et al.'15], *CMSI* (Changing Mobile Subscriber Identities) [Muthana &Saeed.'17]
  - Public-key solutions [Arapinis et al.'12], [Hermans et al.'14], [Chandrasekaran et al.'17]
- RFID:
  - Linear complexity in the number of subscribers [Weis et al.'03],
  - Surveys [Jules'06], [Langheinrich.'09], [Song et al.'09], [Song et al.'11], [Yang et al.'17]

Summary

- 4G/LTE IMSI-catchers
  - ***is IMSI-catching a bug or a feature?***
  - this problem should be considered for 5G and beyond

- Drawbacks of existing proposals:
  - architectural changes
  - significant modifications to the protocols and/or the exchanged messages
  - high computational costs and difficult management caused by public key cryptography
  - particularity to specific scenarios

- Private Identification Problem:
  - introduced as a **general standalone problem**, being decoupled from authorization (and registration)
  - ***existing efficient and scalable solutions in private key settings ?***

Thank you!