THE PROBLEM OF PRIVATE IDENTIFICATION

Ruxandra F. Olimid*,** and Stig F. Mjølsnes*
*Dept. of Information Security and Communication Technology, NTNU, Norway
** Dept. of Computer Science, Univerisity of Bucharest, Romania

Crypto Action Symposium 2018
Sutomore, April 5
Motivation - LTE
LTE - Subscriber’s Identification

**IMSI** (International Mobile Subscriber Identity)

<table>
<thead>
<tr>
<th>MCC (Mobile Country Code)</th>
<th>MNC (Mobile Network Code)</th>
<th>MSIN (Mobile Subscriber Identification Number)</th>
</tr>
</thead>
</table>

**LTE - Subscriber’s Identification**

**IMSI** (International Mobile Subscriber Identity)
LTE - Subscriber’s Identification

UE

IMSI

Identification

Subscriber

UE

IMSI

TMSI_1

eNodeB

UE

TMSI_2
[. . . ] 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

Identity Request (IMSI) → eNodeB

Identity Response (IMSI) ← eNodeB
Our LTE IMSI Catcher

- **eNodeB_Jammer**: causes the UE to detach from the serving cell it camps on
- **eNodeB_Collectors**: 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
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

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

Easy 4G/LTE IMSI Catchers for Non-Programmers

Experimental Assessment of Private Information Disclosure in LTE Mobile Networks

[NDSS 2016]
IMSI Catchers in the Real World
"Real World" IMSI Catchers

[Aftenposten, Dec. 16, 2014]

[ArsTechnica, Apr. 3, 2018]
”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.

“Real World” IMSI Catchers

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

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

ID_i
pk

Enc_{pk}(ID_i)

Provider

ID_1
ID_2
...
ID_n
sk

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

No PubKey
Key Search - Linear Solution

Subscriber

(IDᵢ, Kᵢ)

Provider

(ID₁, K₁)

(ID₂, K₂)

(......)

(IDₙ, Kₙ)

rᵢ ← R R

Linear time

rᵢ, Enc_{Kᵢ}(rᵢ)

*key-indistinguishable MAC

Try all \{Kᵢ\} until successfully decryption of rᵢ

Output: (IDᵢ, Kᵢ)

[Weis, Sarma, Rivest, Engels - Security and Pervasive Computing’03]
[Alwen, Hirt, Maurer, Patra, Raykov - Anonymous Authentication with Shared Secrets’14]
Solutions?

Asymmetric Crypto
Certificate
Certificateless

Symmetric Crypto
Stateless
Stateful

Paradox: private identification requires encryption (under the secret key), but how to know which secret key to use?

[Alomair, Poovendran – Privacy vs. Scalability in RFID Systems’10]
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]
3GPP

- **History:**
  - 3GPP (3rd Generation Partnership Project): 2G/3G/4G
  - TS 33.501 *Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system*

- **Solution:**
  - Elliptic Curve Integrated Encryption Scheme (ECIES)
  - Hybrid encryption: Diffie Hellman (EC) + symmetric encryption

---

*Subscription Identifier Privacy in 5G Systems*

Enrique Cobó Jiménez
School of Electrical Engineering
Royal Institute of Technology (KTH)
Stockholm, Sweden
ecj@kth.se

Prajwol Kumar Nakarmi, Mats Näslund, Karl Norrman
Security Research
Ericsson AB
Stockholm, Sweden
{prajwol.kumar.nakarmi, mats.naslund, karl.norrman}@ericsson.com

Abstract—Privacy is a main concern for mobile network users, and there are many proposed enhancements for the protection of the long-term subscription identifier. Some enhancements require asymmetric key operations, which increase both processing requirements and protocol message sizes. To the best of our knowledge, there has been no practical implementation details about their implementation options.

As we are now moving into the era of fifth-generation (5G) but active attacks on privacy (such as the ones mentioned in [1]) were still left completely unaddressed. With increased off-the-shelf availability of technology such as Software Defined Radio, those active attacks have become a major concern, with a number of attack vectors recently exploited [2].

[MoWNeT’17]
3GPP - ECIES

Subscriber

\[ ID_i \]

pk

pk

sk

enc-k

Provider

\[ ID_1 \]

\[ ID_2 \]

\[ \ldots \] \[ \ldots \] \[ \ldots \]

\[ ID_n \]

sk

\[ \text{Enc}_{\text{enc-k}}(ID_i), \text{pk} \]

\[ \text{Dec}_{\text{enc-k}}(\text{Enc}_{\text{enc-k}}(ID_i)) = ID_i \]
3GPP

Figure C.3.2-1: Encryption based on ECIES at UE

Final output = Eph. public key || Ciphertext || MAC tag || any other parameter

[3GPP TS 33.501]
Summary

• 4G/LTE IMSI-catchers
  – is IMSI-catching a bug or a feature?
  – this problem is now considered for 5G

• Private Identification Problem – symmetric settings:
  – existing efficient and scalable solutions in private key settings?
  – no impossibility result, no lower bounds for computational power on the network side

• 3GPP-ECIES:
  – 5G IMSI-catchers? (null-scheme, recommendations)
  – public key refresh (in USIM)
  – hiding MCC, MNC?
  – post-quantum resistance?
  – …
Thank you!

Q?

A!