The known unknowns of SS7 and beyond

Siddharth Rao[1] Silke Holtmanns[2] Ian Oliver[2] Tuomas Aura[1]

[1]Aalto University, Finland [2]Bell Labs - Nokia Networks, Finland

Telco Security Day - Troopers

15 March 2016

Aalto University

NOKIA

Overview

1. SS7 based attacks
   - SS7 attacks recap
   - More SS7-MAP attacks
2. LTE/ Diameter based attacks
   - Motivation
   - Interworking Functions (IWF)
   - LTE IMSI disclosure attack
   - Location disclosure
3. Surveillance and signalling systems
   - Co-traveller: How NSA did it?
   - Is there any room for more surveillance-like attacks?

Aalto University

NOKIA

Co-authors - Dr. Silke Holtmanns

Aalto University

Dr. Silke Holtmanns is working for Nokia Security Research, now part of Bell Labs. She has 16 years of cellular security experience. She is rapporteur of many 3GPP security specifications and reports and also contributes actively to other cellular security standardization bodies e.g. GSMA, ETSI. She authored a book and several book chapters in addition to a wide range of cellular security articles.

NOKIA

Co-authors - Dr. Ian Oliver

Dr. Ian Oliver is a security researcher in Bell Labs working on NFV, Trusted Computing and Privacy. Prior to this he worked with Semantic Web technologies at Nokia Research and was the privacy officer for Here. He holds a research fellow position at the University of Brighton and is the author of the book Privacy Engineering: A Dataflow and Ontological Approach. He has published numerous papers and holds over 40 patents.

Aalto University

NOKIA

Co-authors - Dr. Tuomas Aura

Dr. Tuomas Aura was appointed as professor of computer science at Aalto University in 2008. Before that, he worked as a researcher at Microsoft Research in Cambridge, England.

His recent research has focused on Internet and mobility protocols, user privacy protection and distributed security policies. Tuomas took part in developing the security solutions for the Mobile IPv6 and SEND protocol standards in the IETF.

Aalto University

NOKIA

About me: Twitter @sidnext2none

- Currently a research assistant in Secure Systems group in Aalto.
- Master's in information and network security; Master's in cryptography.
- Research Interests:
  - Security and privacy in network protocols.
  - Evolution of inter-networking technologies.

Aalto University

NOKIA

My journey so far with TelcoSec

- Started in January, 2015 as a security intern at Nokia Networks.
- Exploratory analysis survey of SS7 attacks → *Thesis* "**Analysis and mitigation of recent attacks on mobile communication backend networks**".
- Core network SS7 LTE IWF
- Location tracking beyond GSM networks.
- Pedagogical study of evolution of Telco attacks.
- Emerging threats to the network community via Telco backbone.

Aalto University

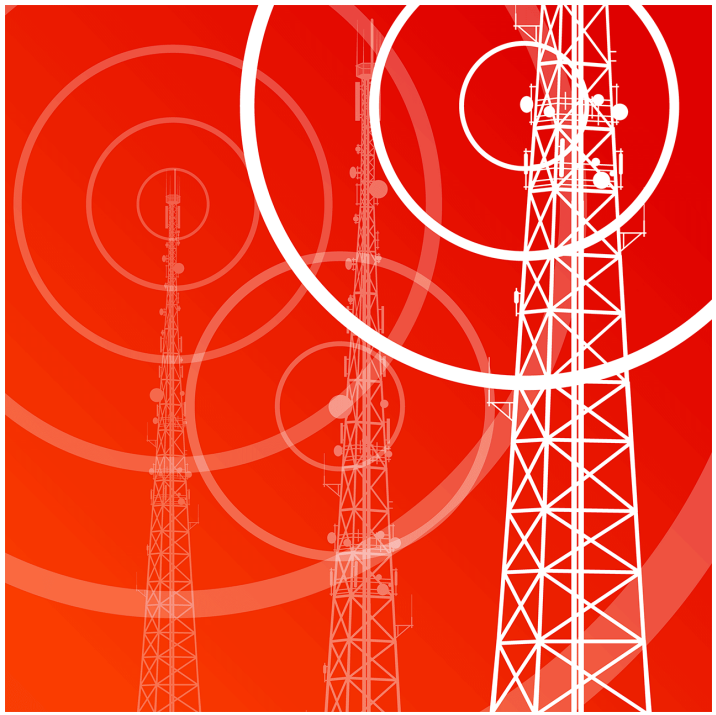
NOKIA

SS7 background
and
new attacks

Aalto University

NOKIA

Background - Signalling System no. 7 (SS7)

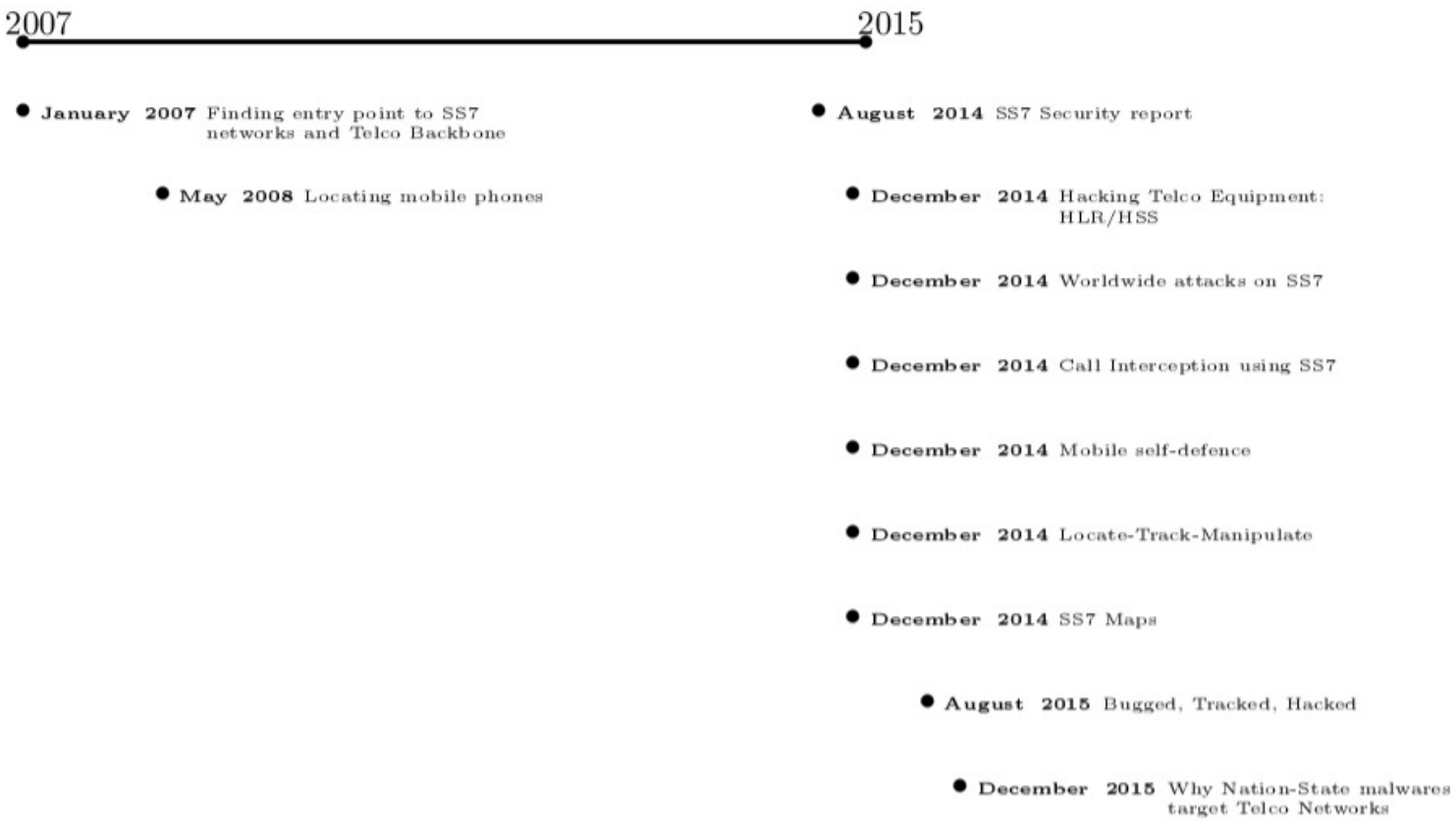


- Protocol foundation to enable roaming.
- Short Message and Supplementary services.
- Toll free numbers and tele-voting.
- Enhanced Message Service (EMS).
- Local Number Portability (LNP).

Aalto University

NOKIA

SS7 Attck timeline



Aalto University

NOKIA

SS7 attack impact(1)

Location disclosure

1. Call setup messages.
2. SMS protocol messages.
3. Emergency services.
4. Billing platform messages.

Call based attacks

1. Billing platform messages.
2. Profile manipulation.
3. TMSI de-anonymization

Aalto University

NOKIA

SS7 attack impact(2)

SMS based attacks

1. SMS interception.
2. Sending fraud SMS messages.

DoS attacks

1. Interconnection handover messages.
2. MSC choking.

Aalto University

NOKIA

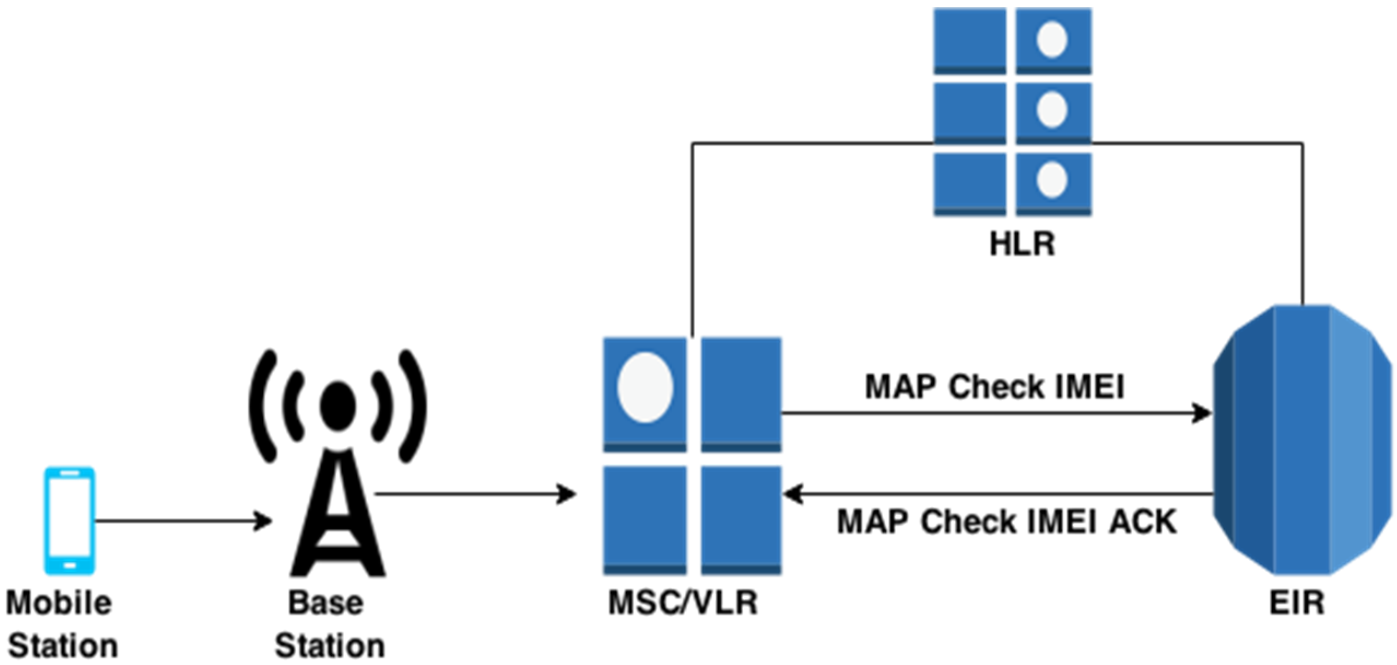
Check_IMEI misusage

- **Check_IMEI** is used to query the EIR to know whether a mobile phone (IMEI) is stolen (blacklisted), legitimate (white-listed) or on alert (grey-listed).
- Exploits a hidden relationship between IMEI and IMSI in some of the EIRs.
- Unnecessary/unknown feature which is not widely used.

Aalto University

NOKIA

Regular IMEI check procedure



International Mobile Equipment Identity (IMEI) = heart of the phone.
(15 – 16 digits long)

Aalto University

NOKIA

CheckIMEI ASN structure

```
CheckIMEI-Arg ::= SEQUENCE {
imei                    IMEI,
requestedEquipmentInfo  RequestedEquipmentInfo,
extensionContainer      ExtensionContainer OPTIONAL,
...}
```

Contains only IMEI

Aalto University

NOKIA

Assumptions

- Attacker has a stolen phone which is blacklisted and he knows the IMSI (Subsriber id) which was associated with it while blocking or last use by the victim.
- The attacker does not need to have the original SIM as it is sufficient to have just the IMSI.
- Attacker has access to SS7 network.
- The Global Title (GT, SS7 name of a node) of the Equipment Identity Register (EIR) is required.
- Mobile Switching Center (MSC) GT might be needed (depending on operator configuration).
- Feature and IMSI check options are enabled.

Aalto University

NOKIA

Feature

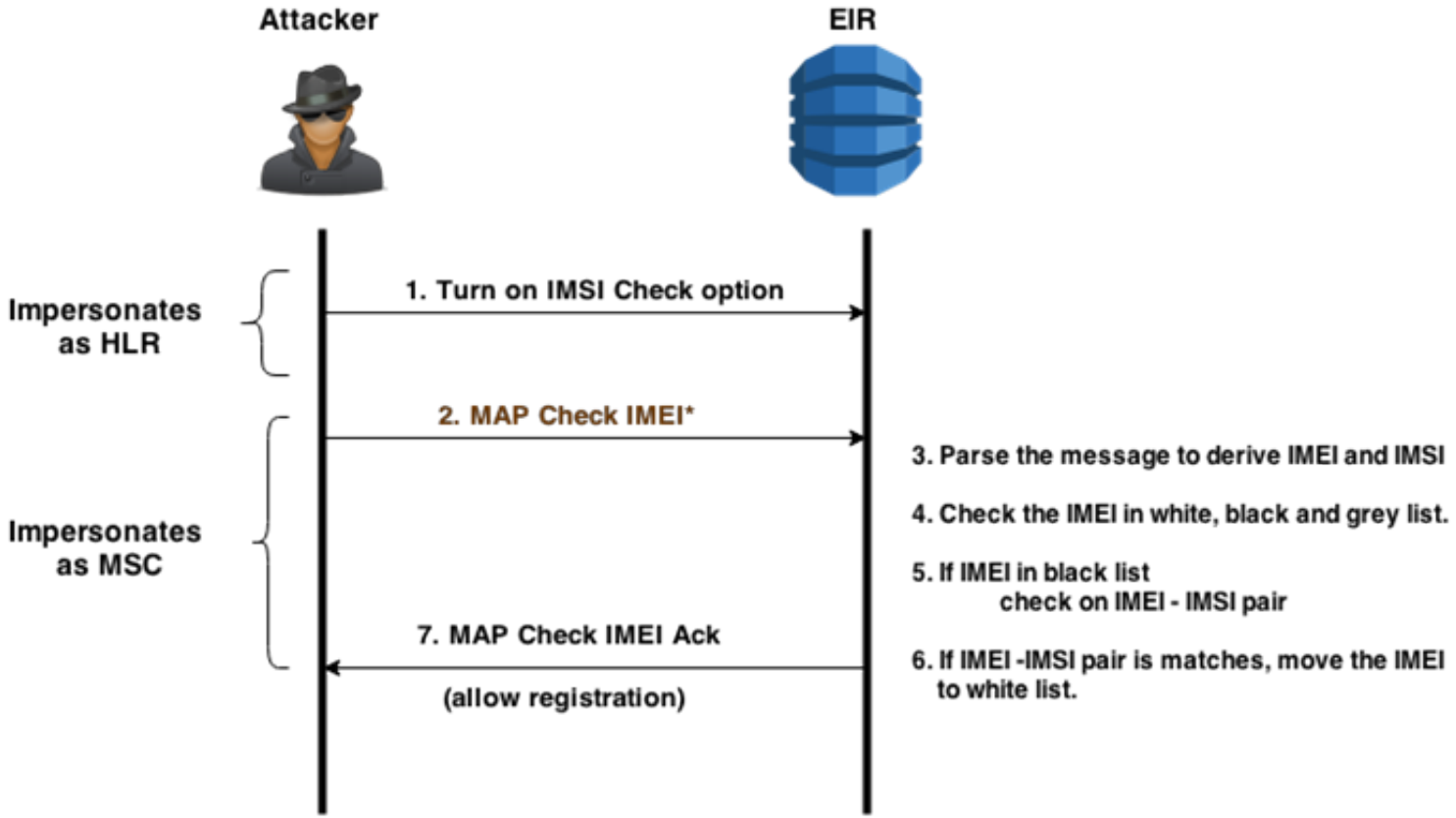
Users loose their phones and find it again → An easy **"recovery"** in EIR wanted:

- MSC sends IMEI (device id) along with IMSI (subscriber id) during MAP_CHECK_IMEI.
- Initially the IMEI is checked to know the list it belongs to. If it is found on the black list, an additional check of IMSI is made.
- If there is a match between IMSI provisioned with IMEI in the EIR database (This is the IMSI-IMEI pair in the EIR before the victim blocks his stolen device) with the IMSI found in MAP_CHECK_IMEI message then this overrides the blacklist condition.
- Phone no longer blacklisted.

Aalto University

NOKIA

Attack scenario



Aalto University

NOKIA

CheckIMEI* ASN structure

```
EnhancedCheckIMEI-Arg ::= SEQUENCE {
 imei                    IMEI,
 requestedEquipmentInfo RequestedEquipmentInfo OPTIONAL,
 imsi                     [PRIVATE 1] IMSI OPTIONAL,
 locationInformat         [PRIVATE 3] OCTET STRING (SIZE (1..7)) OPTIONAL,
 extensionContainer     ExtensionContainer      OPTIONAL,
 ...}
```

Contains IMEI and IMSI !!!

Aalto University

NOKIA

Example

1. A CHECK_IMEI* is received with **IMEI = 12345678901234**, and **IMSI = 495867256894125**.
2. An individual IMEI match is found indicating that the IMEI is on the **Black List**.
3. Normally required response would be Black Listed, however; because an IMSI is present in the message, and the IMEI is on the Black List, the IMSI is compared to the IMSI entry in the database for this IMEI.
4. In this case, the IMSI in the RTDB matches the IMSI in the query, thus the Black Listed condition is cancelled/overridden.
5. EIR formulates a CHECK_IMEI* response with Equipment **Status = 0 whiteListed**.

Aalto University

NOKIA

Why should somebody do this?

Stolen phones would have much higher value, if they are not blacklisted and can be sold via ebay or similar means.

- 1 in 10 smart-phone owners are the victims of phone theft.
- In United States, 113 phones per minute are stolen or lost.
  - $7 million worth of smart phones on a daily basis.

Figure : Source - /Wired/black-market

Aalto University

NOKIA

EIR coverage

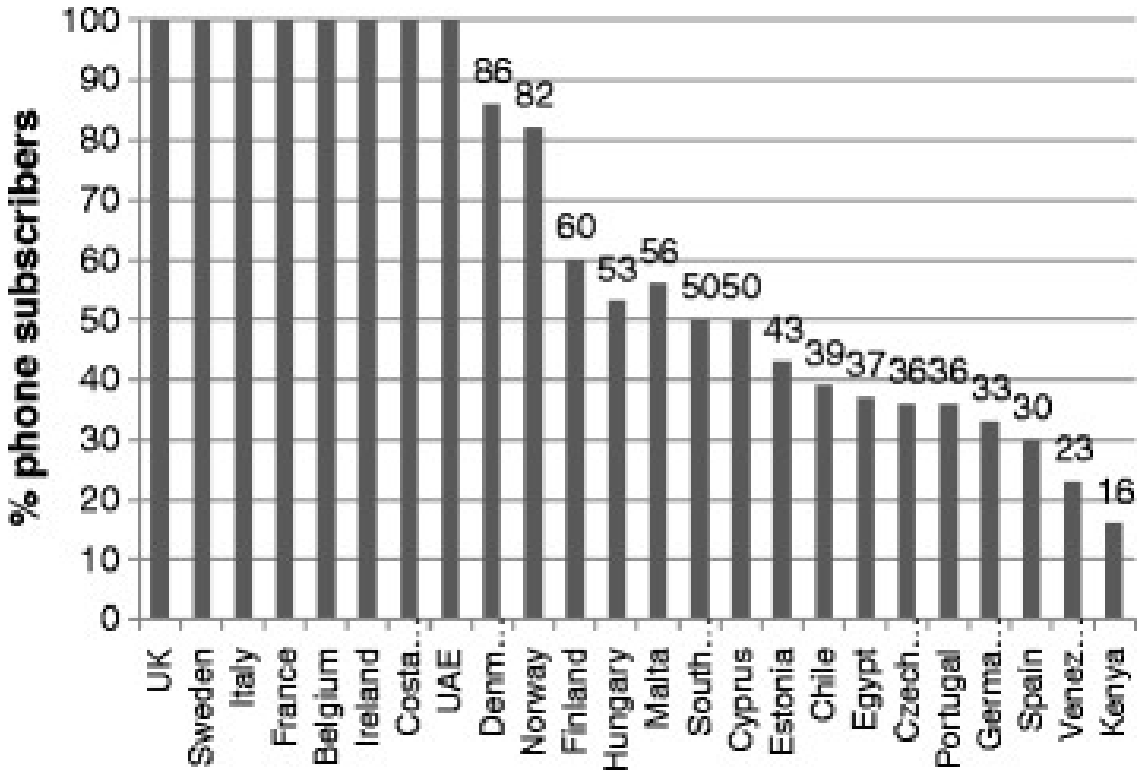


Figure : Source: Farrell, G. (2015). Preventing phone theft and robbery: the need for government action and international coordination. Crime Science, 4(1), 1-11.

Aalto University

NOKIA

Summary

- Attack has not been observed in real networks.
- Research was done on protocol level and publicly available information.
- Not all EIRs affected.
- Business case exist for the attack.
- Check IMEI command can be added to the list of message to be filtered by an SS7 specific firewall in the STP at the border of the network, since this is a network internal message.

Aalto University

NOKIA

LTE
and
Diameter attacks

Aalto University

NOKIA

Motivation

- Most MNO upgrade their network gradually to avoid service interruption and optimize ROI of infrastructure.
  - Inhomogeneous set-up $\Longrightarrow$ interesting attack vectors.
- For interoperability with partners, edge nodes have the ability to **translate** between Diameter $\Longleftrightarrow$ SS7.

Attack translation

We wanted an easy way to port SS7 attacks to Diameter.

Aalto University

NOKIA

Ideal Diameter Network

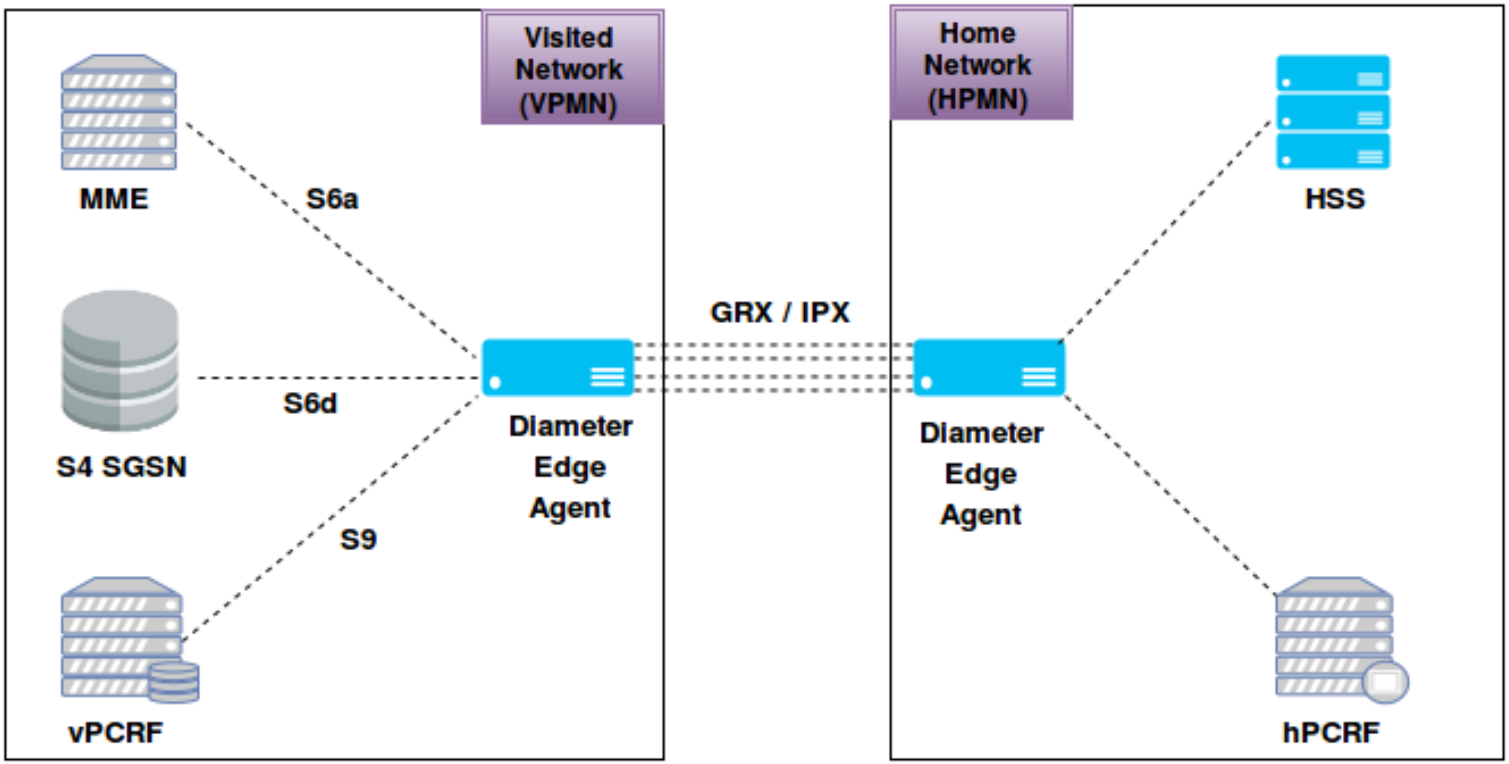


Figure : Diameter roaming architecture between two newer networks.

Aalto University

NOKIA

Inhomogeneous Network

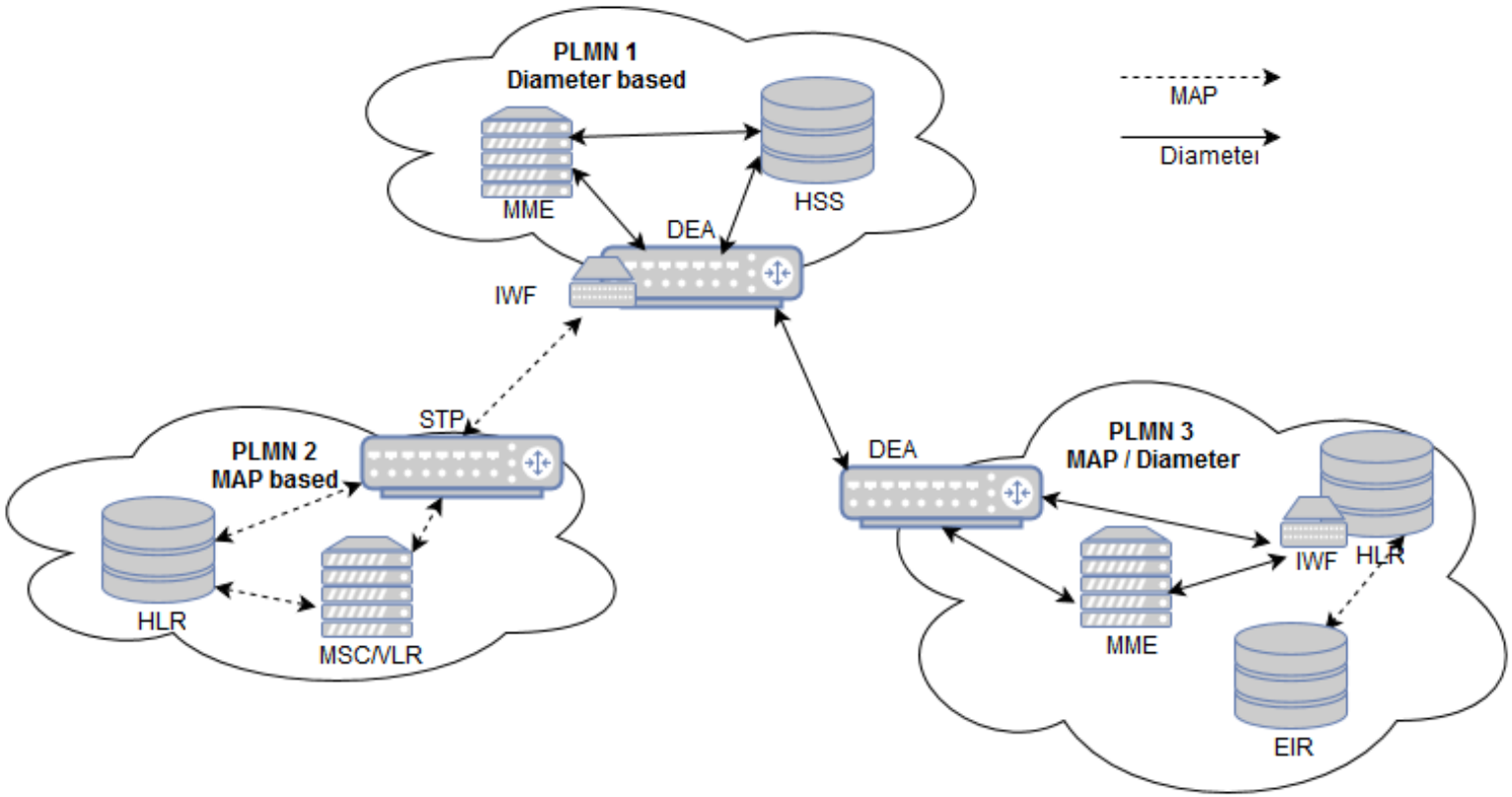


Figure : Different networks with different protocol support.

Aalto University

NOKIA

Interworking functions

- Technical specification **TS 29.305** and non-binding report **TR 29.805**.
  - Describes how Diameter and SS7-MAP messages should be translated to each other *i.e.* **Attribute Value Pairs (AVP)** mapping.

General idea:

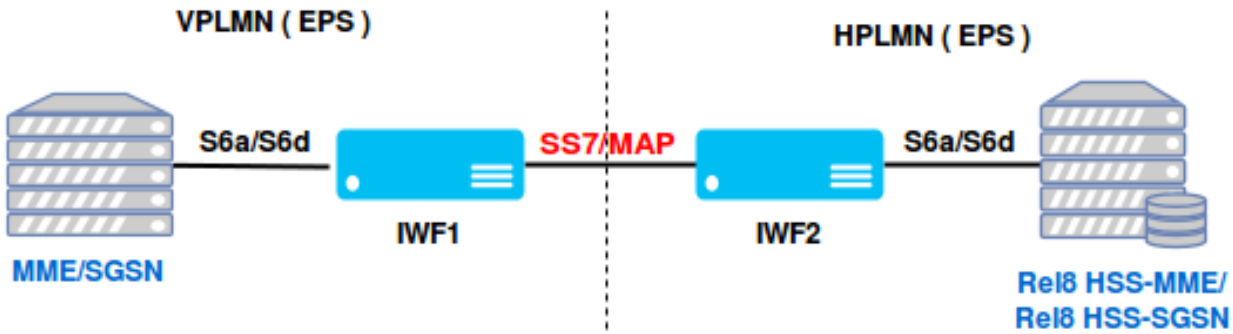
- Attacker pretends to be an old type network or node.
- It forces IPSec secured LTE Diameter network or nodes into using the less secured SS7-MAP.
- Craft SS7-like attack messages and IWF will take care of the rest.

Aalto University

NOKIA

Obtaining IMSI

- Attacker claims to be an IWF node

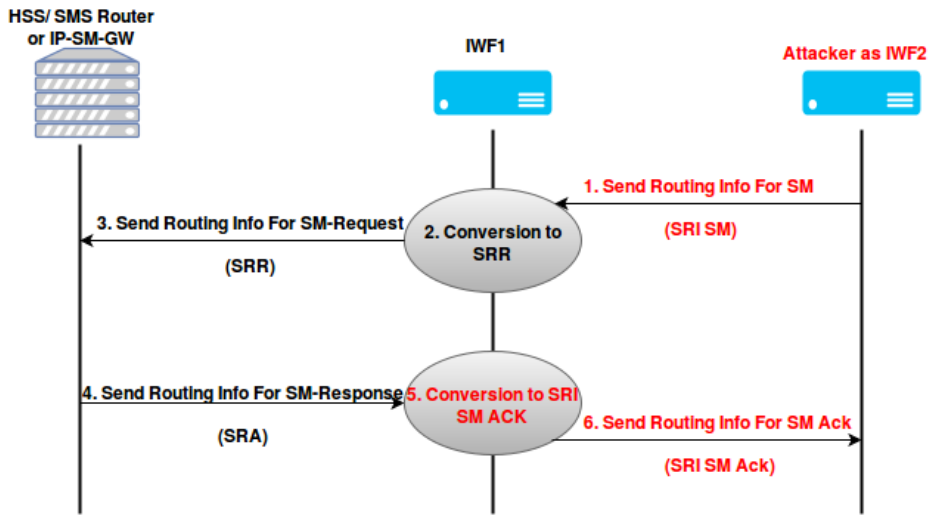


- The attacker sends a Send Routing Info For SM-Request (SRI SM), which contains the MSISDN of the victim.
- Typical multi-domain support scenario for roaming and routing incoming SMS.
  - MAP commands have to be translated to Diameter specific commands by the receiving IWF node.

Aalto University

NOKIA

Obtaining IMSI(2)



- The IWF (in step 5) **copies IMSI** of the victim from username AVP from SRA to SRI SM ACK.
- TS 29.338 section 6.3.2 and TS 29.305 section A2.5.2.3

Aalto University

NOKIA

LTE Location disclosure attacks summary

SS7 attack vector	IWF Attack?	Reason
MAP SRI	No	Very few operators connect HSS directly to DEA or inter-connection.
MAP SRI SM	**Yes**	**Location upto granularity of MME.**
MAP ATI	No	IWF cannot directly map ATI commands.

Aalto University

NOKIA

LTE Location disclosure attacks summary (2)

MAP PSI	**Yes**	**EPS Location Info i.e. cell ID, subscriber state, IMEI, software version and encryption keys.**
Emergency calls (PSL)	No	IWF cannot directly map PSL commands.

More Details at IFIP Networking 2016

Look for our paper - "*User Location Tracking Attacks for LTE Networks Using the Inteworking Functionality*"

Aalto University

NOKIA

Surveillance
and
Signalling systems

Aalto University

NOKIA

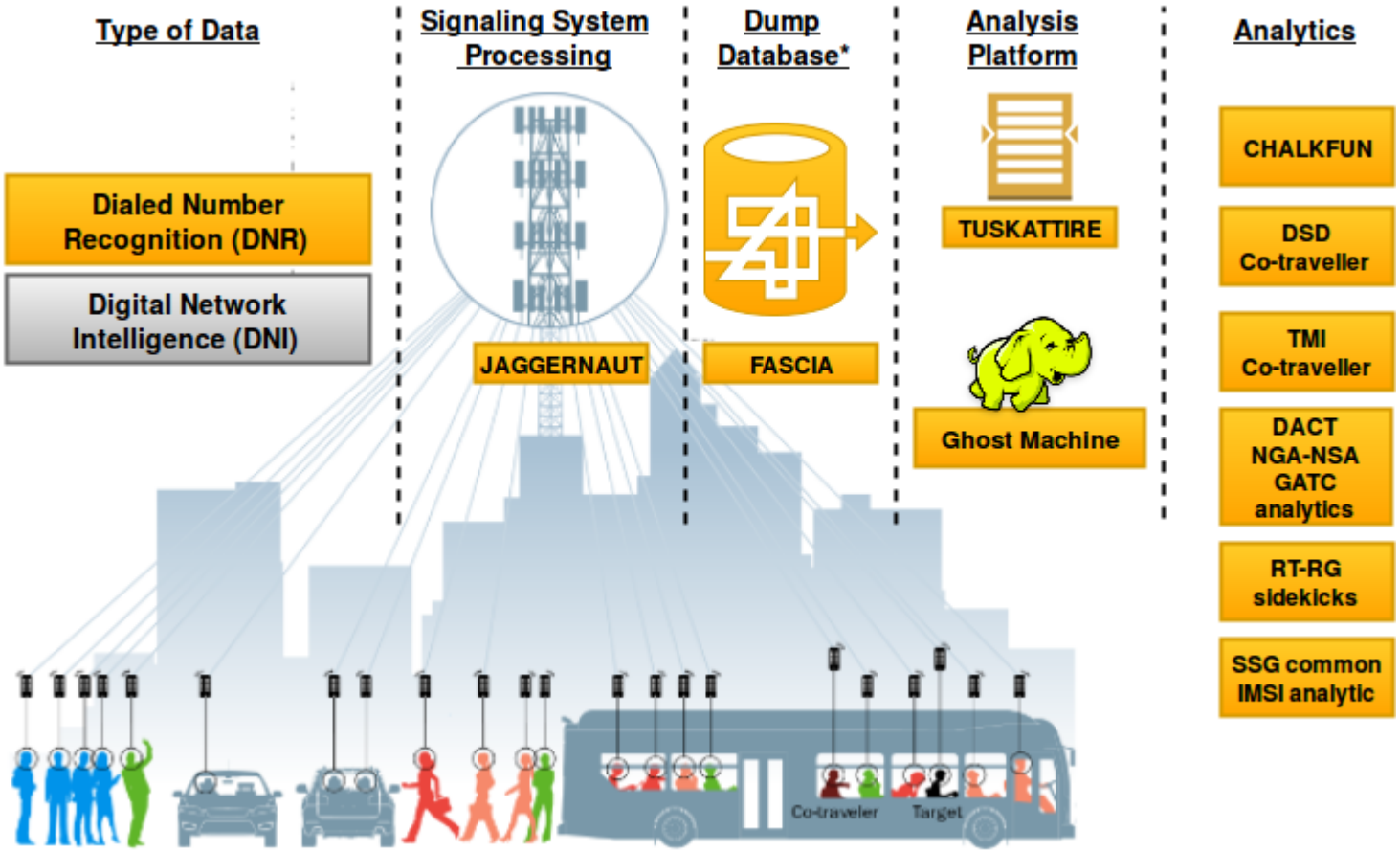
Bigger problems beyond targeted attacks

- Easy remote access to mobile user data $\Longleftrightarrow$ **Mass surveillance**.
- NSA exploited loopholes in Radio Access Network (IMSI catchers) to target specific personnel.
- Exploited core networks and signalling systems worldwide to track cellphone locations of **"Co-travellers"**.
  - Collected **5 billion** records per day.
  - To find and develop more targets.
- "Co-travller" was a sophisticated end-to-end surveillance system to collect and analyze data from signalling systems.
- **Psychology**, the new kind of SIGINT: frequent power-down, handset swapping and SMS styles to analyse the behaviour of mobile users.

Aalto University

NOKIA

Co-traveller surveillance system overview



Aalto University

NOKIA

Types of data collected

Dialed Number Recognition (DNR)

- Information collected from mobile phone network.
- Location data, encryption keys, *etc.*

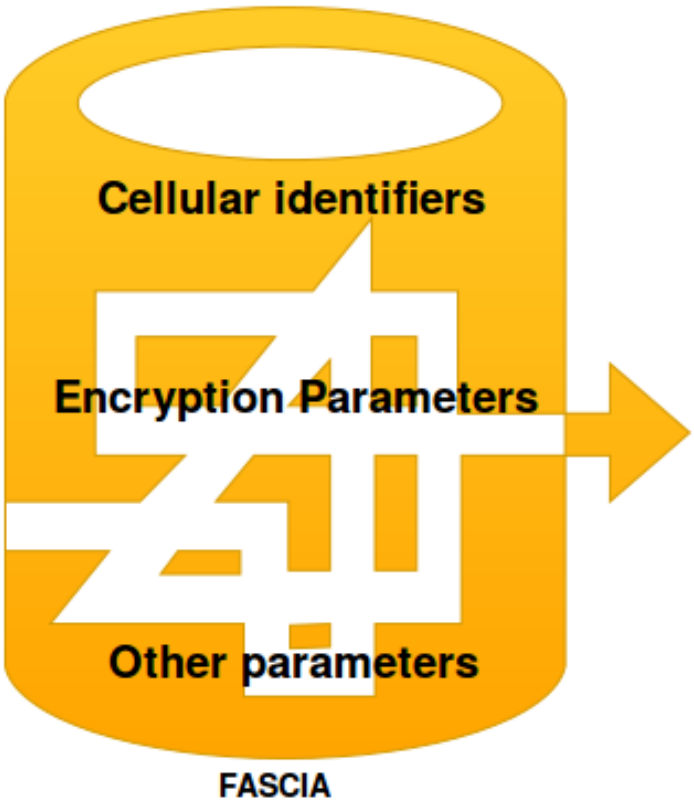
Digital Network Intelligence (DNI)

- Information collected from mobile phone Internet.
- *e.g.* Google location tracking cookie **PREFID**.

Aalto University

NOKIA

FASCIA database



- Big database to dump meta-data from various sources.
- Device-location records $\longrightarrow$ **27 TB** of data (over months).
- **Cellular identifiers**: LAC, CellID, VLR, IMEI, IMSI, TMSI, MSISDN, MSRN, MSC/VLR GT.
- **Encryption parameters**: K_c, Rand, Sres
- Various other parameters from core network and RAN.

Aalto University

NOKIA

Backend processing platforms

Juggernaut

- Digital Receiver Technology, Inc. (DRT) surveillance systems
- Intercepts both SS7 traffic and air interface traffic.

TUSKATTIRE

- Meta-data cleaning, processing and normalizing the collected Call-Related Data (CDR) *i.e.* Dailed Number Recognition.

Ghost machine

- **Hadoop** based cloud analytic platform.
- It can handle multiple analytic features at a time.

Aalto University

NOKIA

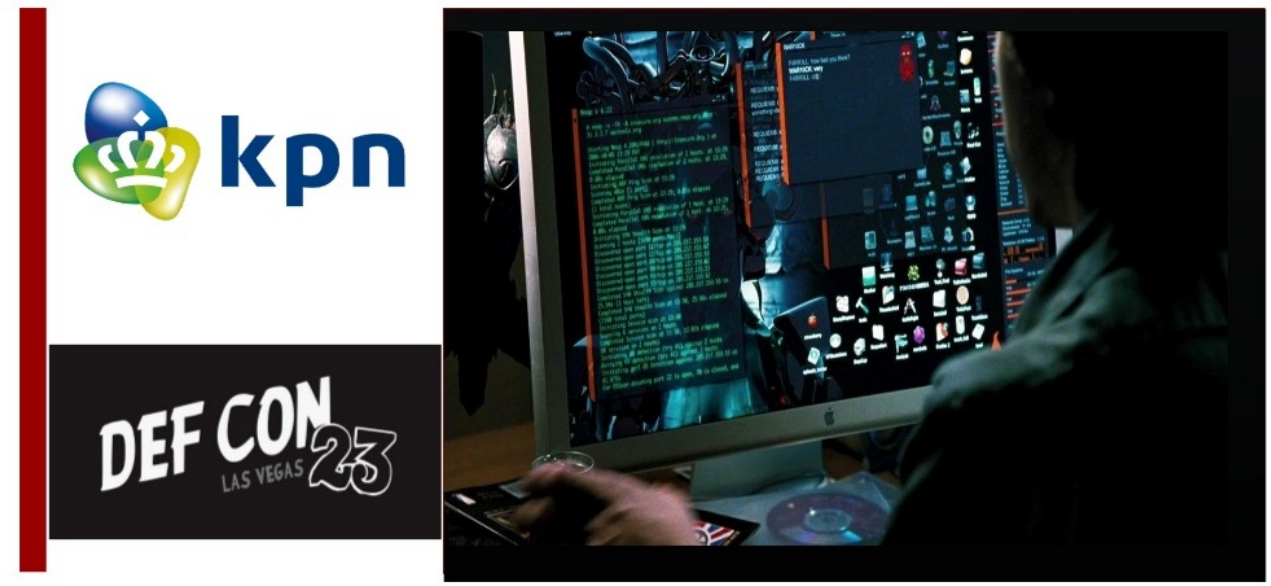
Co-traveller workflow

1. Start with a selector (target) with his IMSI.
2. Query the database for CellID, LAC and MSC/VLR details on specific day and time.
3. Query for the IMSIs of all the mobile users who were in the vicinity of that region (cell or MSC region) at that point of time - They are the potential co-travellers.
4. Query as as in step 1 and rank the potential co-travellers to be the real co-travellers by comparing the pattern of travel, cellular usage and life style with or without the direct connection to the selector.
   - *P.S:* They do some serious datamining and pattern analysis/matching here.
5. Continue tracking everyone :)

Aalto University

NOKIA

Why Nation-State Malwares Target Telco Networks?



Why Nation-State Malwares Target Telco Networks:
Dissecting Technical Capabilities of Regin and Its Counterparts

Author: Ömer Coşkun

The supreme art of war is to subdue the enemy without fighting. *Sun Tzu*

Aalto University

NOKIA

Is there any room for more surveillance-like attacks?

- Snowden revelations have definitely alerted many, especially the security researchers.
- Relatively easy to detect and alert (if not prevent) the attacks from RAN. *e.g:* IMSI Catchers
  - SnoopSnitch, Darshak
- More difficult to know if the attack happens from the core network side - at least for the end users.
  - So they rely on Telcosec experts to protect their privacy.
- More attacks paradigms would help to achieve 'security by design' approach in future mobile generations.
- More room for remote injection or stealing of cellular secrets from mobile users on a mass scale? - Possibly yes.

Aalto University

NOKIA

USSD based attacks

- **Unstructured Supplementary Service Data** (USSD) $\longrightarrow$ cost effective, faster (than SMS) and flexible mechanism.
- Real time (session based) communication channel $\longrightarrow$ suitable for interactive menu based services.
- Supported by majority of the phones - Neither phone based nor SIM based.
- Works on both home and roaming networks without extra charge.
- Earlier talk by Ravi at Troopers on **Dirty use of USSD codes**, attacks using USSD insecurity.

Can we convert dirty USSD to nasty USSD?

Aalto University

NOKIA

Network Initiated USSD operation

- Ongoing work - open research questions/ study of emerging threats.
- **Push-Service mode** or Network-Initiated USSD: The network sends USSD message towards the mobile station.
- HLR, MSC or VLR can initiate it $\longrightarrow$ as a **request** seeking the MS to respond or as a **notification** without the MS intervention.
- Easy to flood/infect a large number of cellphones in a MSC/VLR region.
- Some specifications talk about using USSD for OS updates as well.
  - Trying to steal OTA keys? SIM related secrets?
  - If yes, then it is a big mess!!!

Aalto University

NOKIA

Conclusion

- **The SS7 saga continues** $\Longrightarrow$ It will haunt us for some more years.
- **LTE attacks** $\Longrightarrow$ It is possible to port SS7 attacks to Diameter network using Interworking functions.
  - IMSI disclosure
  - Location tracking upto MME as well as cellID level.
  - IMEI and OS software version disclosure.
- Bigger threats of **surveillance** and **Advanced Persistent Threats** (APTs) via Telco backbones.
- Emphasis in future should be on *'Security by design'*.

Aalto University

NOKIA

References

S.P.Rao (2015)

Unblocking Stolen Mobile Devices Using SS7-MAP Vulnerabilities: Exploiting the Relationship between IMEI and IMSI for EIR Access

Trustcom/BigDataSE/ISPA, 2015 IEEE, Helsinki, 2015, 1171–1176.

TS 29.305

InterWorking Function (IWF) between MAP based and Diameter based interfaces

3rd Generation Partnership Project (3GPP)

A.Soltani (2015)

Snowden files: NSA series

Washington Post

Aalto University

NOKIA

Thank you!

Aalto University

NOKIA