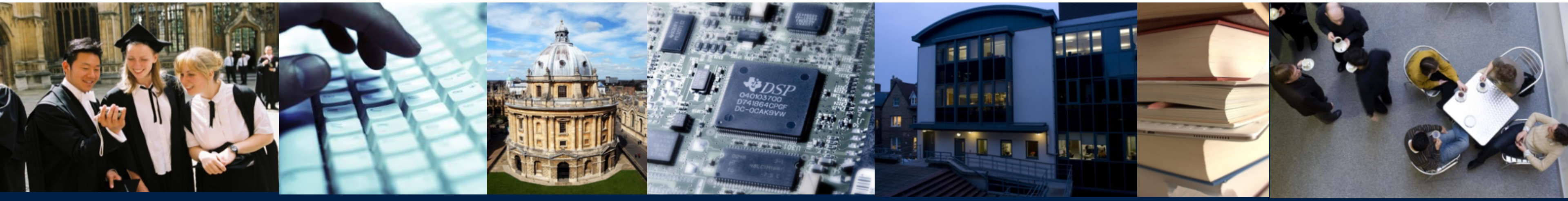
ETH zürich

TU berlin

DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY OF OXFORD



New Adventures in Spying 3G & 4G Users: Locate, Track, Monitor

Ravishankar Borgaonkar, Lucca Hirshi, Shinjo Park, Altaf Shaik, Andrew Martin and Jean-Pierre Seifert

BLACKHAT USA 2017
Las Vegas
26 July 2017

Research Team

- Discovery of attacks:
    - Ravishankar Borgaonkar
    - Lucca Hirschi
- Carried out POC with : Shinjo Park & Altaf Shaik

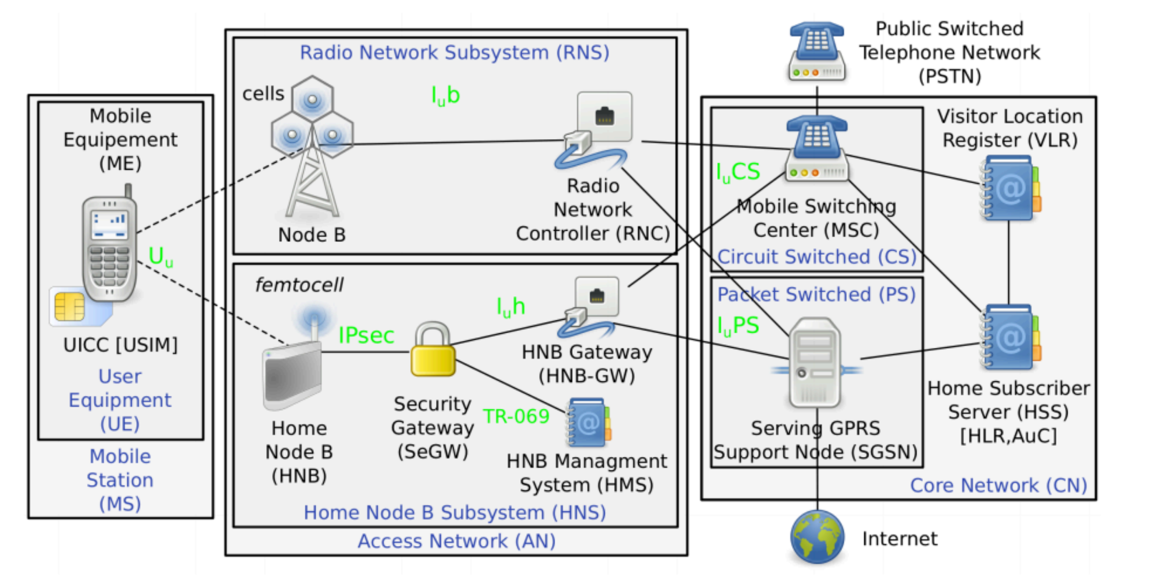
Outline

- Background
- New privacy attacks
- Attacks in practice – exploitation methods and demo
- Impact against mobile users
- Countermeasures
- Conclusions

General cellular architecture

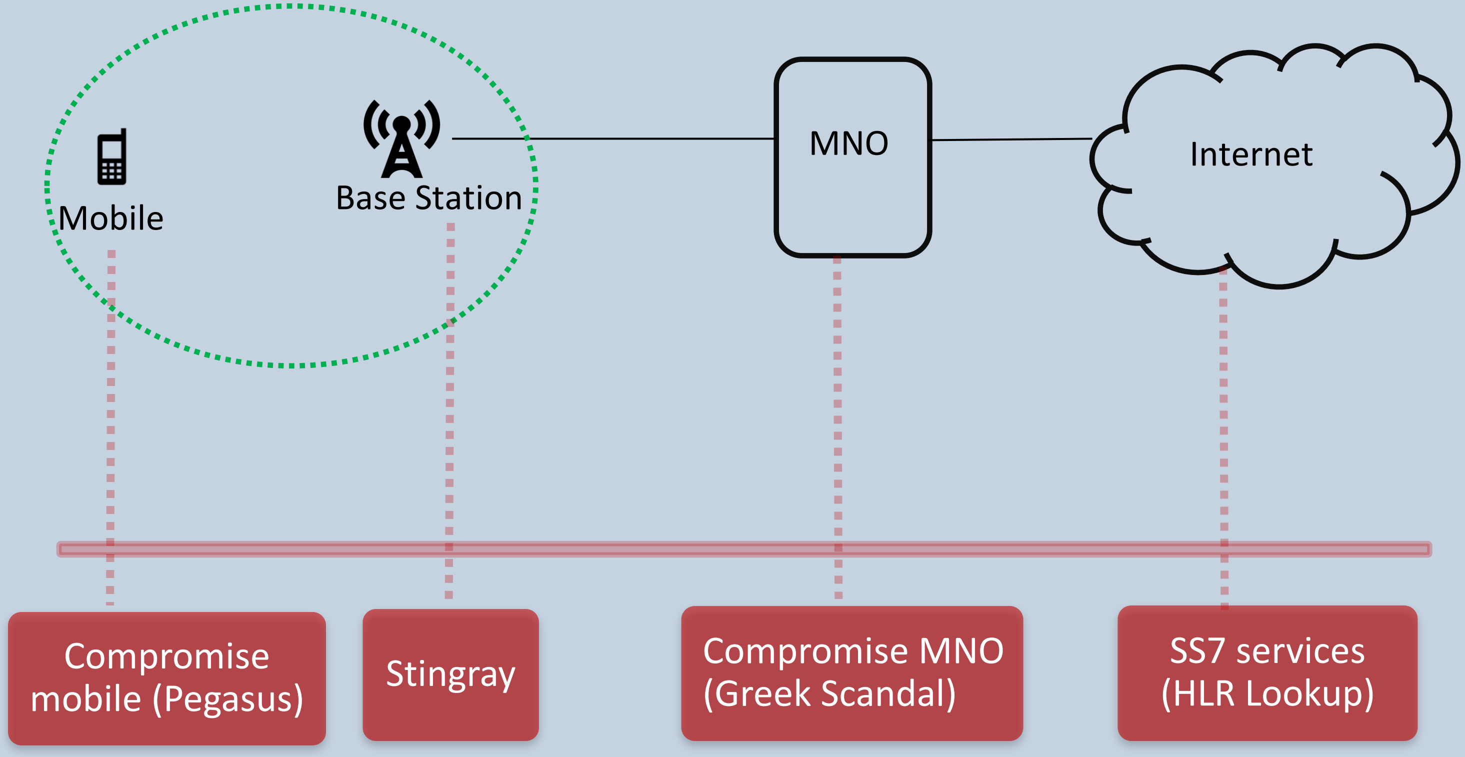
Radio Access Network

Core Network


Radio Network Subsystem (RNS)
cells
$I_u b$
Node B
Radio Network Controller (RNC)
Mobile Equipement (ME)
U_u
UICC [USIM]
User Equipment (UE)
Mobile Station (MS)
femtocell
IPsec
$I_u h$
HNB Gateway (HNB-GW)
Home Node B (HNB)
Security Gateway (SeGW)
TR-069
HNB Managment System (HMS)
Home Node B Subsystem (HNS)
Access Network (AN)
Public Switched Telephone Network (PSTN)
Visitor Location Register (VLR)
$I_u CS$
Mobile Switching Center (MSC)
Circuit Switched (CS)
Packet Switched (PS)
$I_u PS$
Serving GPRS Support Node (SGSN)
Home Subscriber Server (HSS) [HLR,AuC]
Core Network (CN)
Internet

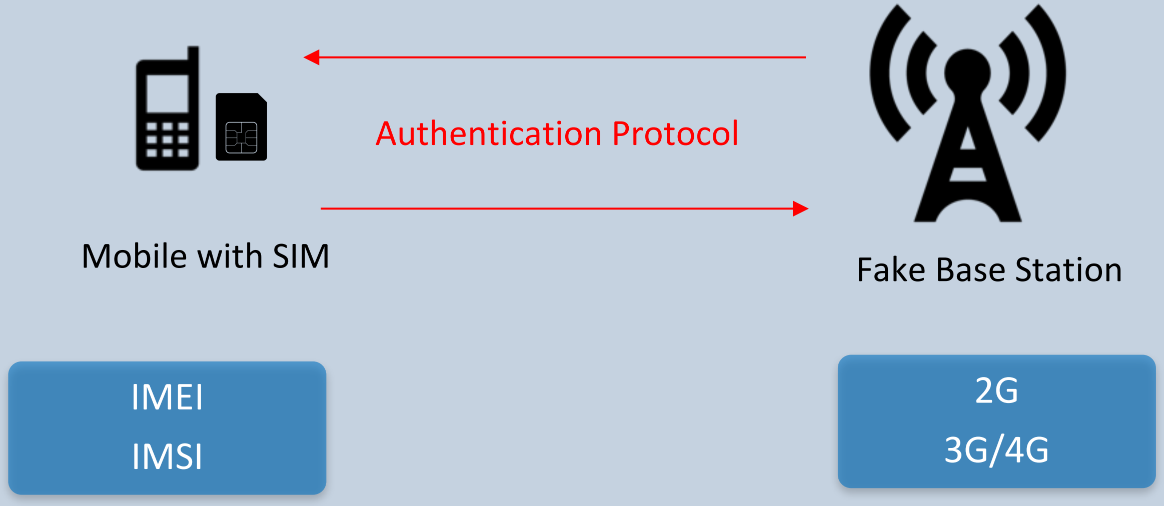
Emerging threats

Tracking mobile users – state of the art


Mobile
Base Station
MNO
Internet
Compromise mobile (Pegasus)
Stingray
Compromise MNO (Greek Scandal)
SS7 services (HLR Lookup)

Note: picture provides an abstract view only

Tracking using Stingray/fake base station



Authentication Protocol

Mobile with SIM

Fake Base Station

IMEI

IMSI

2G

3G/4G

SIM – Subscriber Identity Module

IMEI – International Mobile Equipment Identity

IMSI – International Mobile Subscriber Identity

Authentication and Key Agreement (AKA) Protocol

- Deployed in every 3G/4G terminals since 2002
- Mutual authentication between network and mobile to establish a secure link
- Improved in 4G – key sizes, key separation etc.
- Often termed as one of the most successful widely deployed crypto protocol

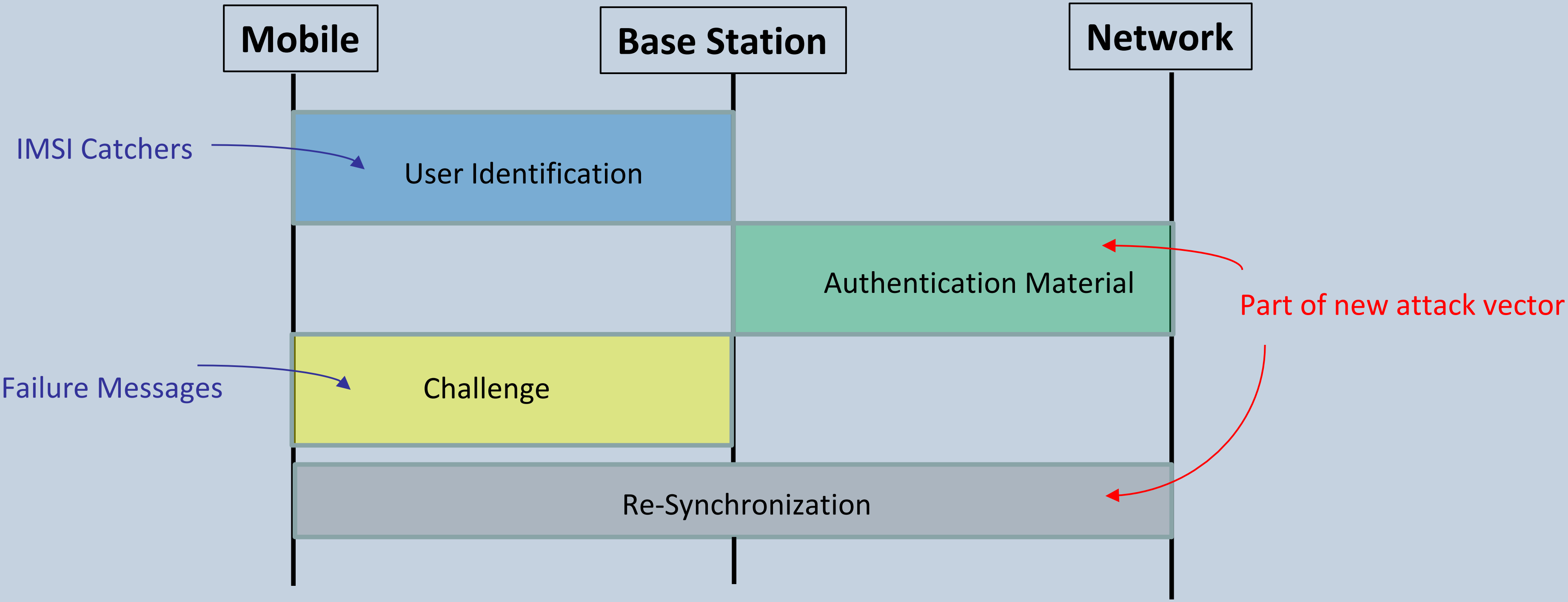
Features

- Symmetric key shared between mobile (USIM) and network (HLR)
- Sequence number for avoiding replay attacks

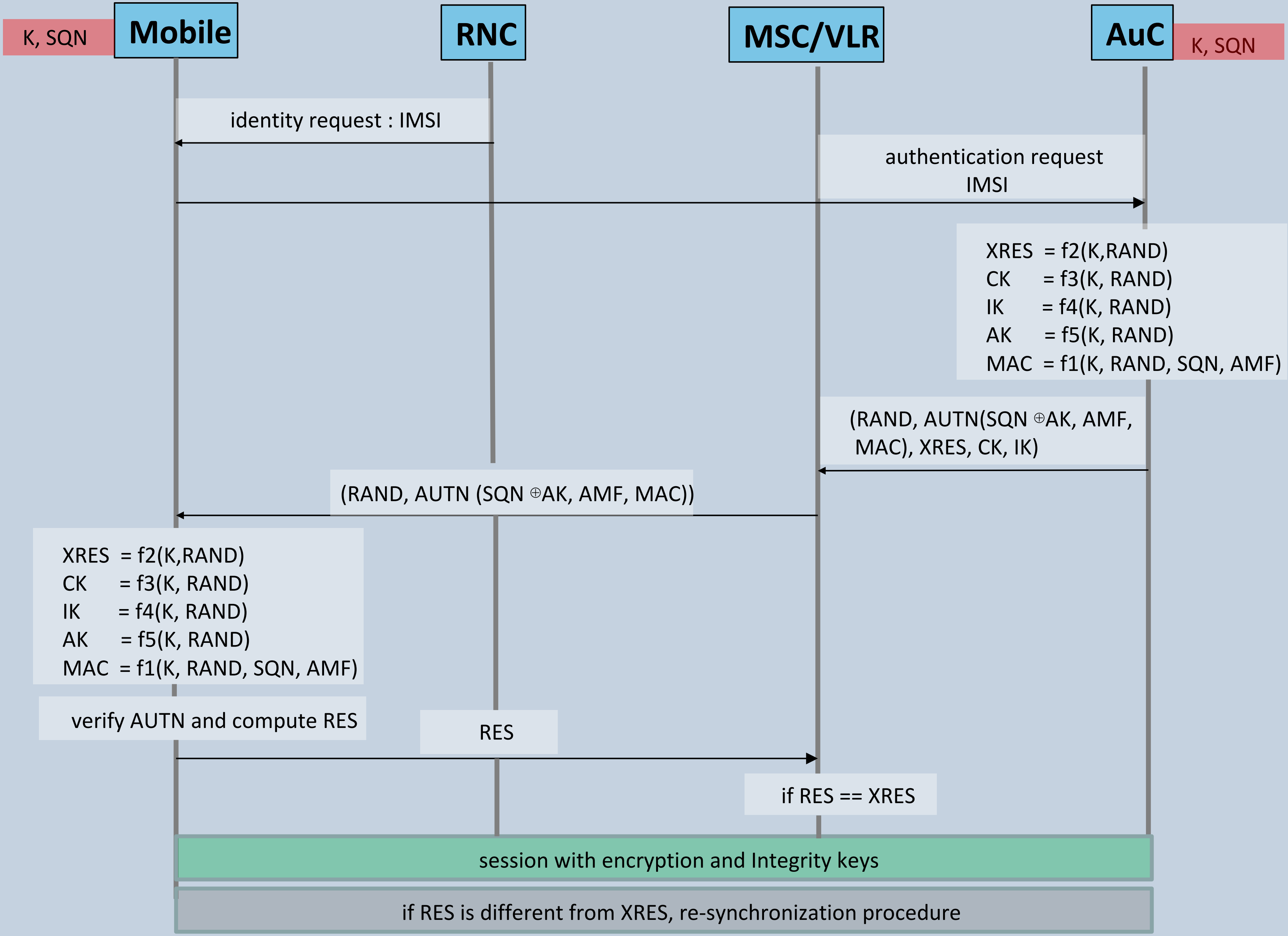
AKA : State of the art

- Known security issues
  - IMSI leakage
  - Linkability attacks
- Availability of low-cost hardware and software tools
- New attacks??

AKA : Big picture



AKA protocol



K, SQN

Mobile

RNC

MSC/VLR

AuC

K, SQN

identity request : IMSI

authentication request
IMSI

XRES = f2(K,RAND)
CK = f3(K, RAND)
IK = f4(K, RAND)
AK = f5(K, RAND)
MAC = f1(K, RAND, SQN, AMF)

(RAND, AUTN(SQN ⊕AK, AMF, MAC), XRES, CK, IK)

(RAND, AUTN (SQN ⊕AK, AMF, MAC))

XRES = f2(K,RAND)
CK = f3(K, RAND)
IK = f4(K, RAND)
AK = f5(K, RAND)
MAC = f1(K, RAND, SQN, AMF)

verify AUTN and compute RES

RES

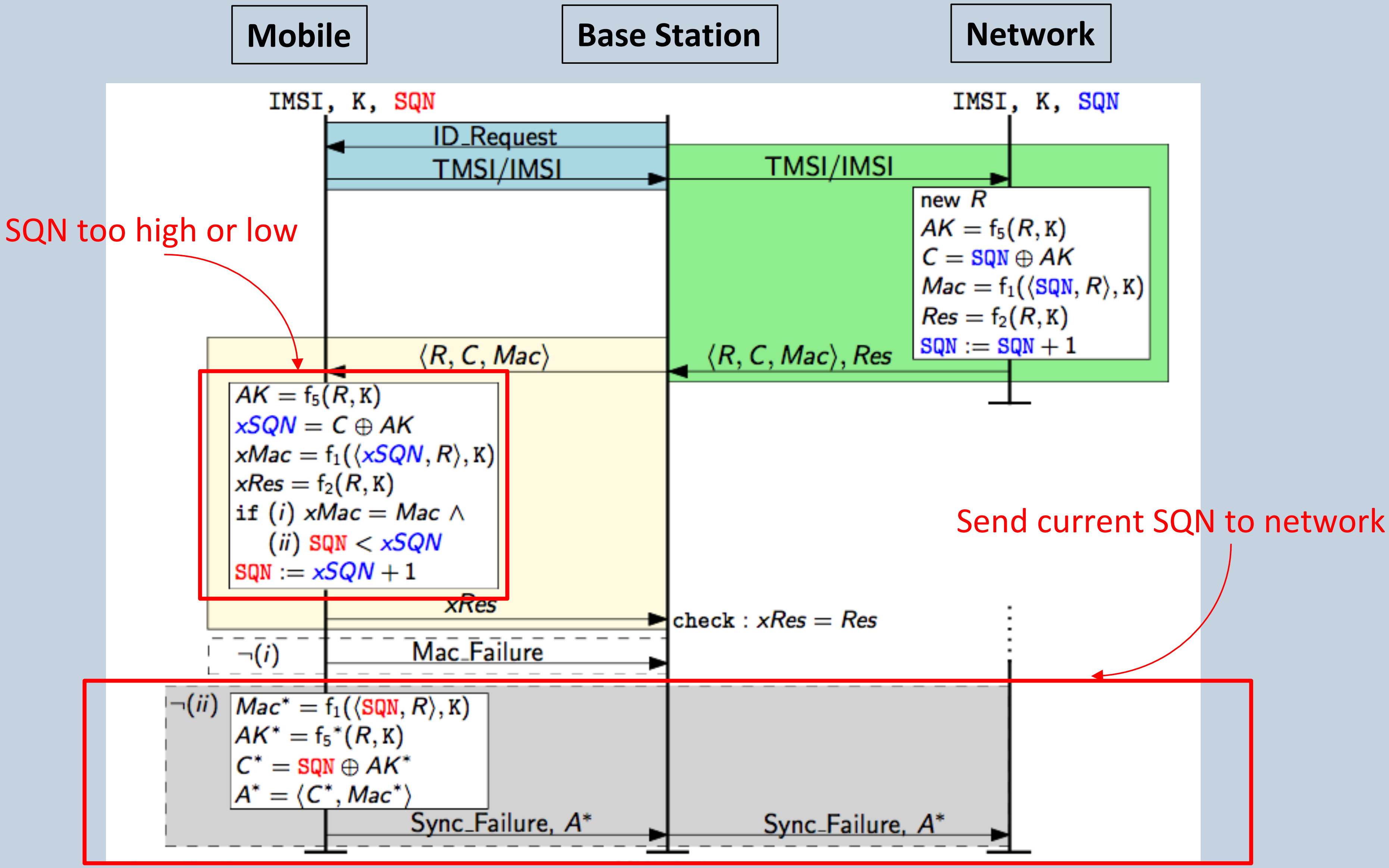
if RES == XRES

session with encryption and Integrity keys

if RES is different from XRES, re-synchronization procedure

Role of Sequence Number (SQN) in AKA

- SQN for providing freshness to mobile (prevent replay attacks)
- Helps in saving one round trip message to AuC
- AuC stores SQN and increment it for each authentication
- Masked with anonymity key AK to protect privacy of mobiles
- USIM stores highest received SQN from the network
- In case of failure, resynchronisation of SQN with AuC
  - USIM must send current SQN to AuC
  - Masked with anonymity key AK*



Mobile

Base Station

Network

IMSI, K, SQN

IMSI, K, SQN

ID_Request

TMSI/IMSI

TMSI/IMSI

new R
$AK = f_5(R, K)$
$C = SQN \oplus AK$
$Mac = f_1(\langle SQN, R \rangle, K)$
$Res = f_2(R, K)$
$SQN := SQN + 1$

$\langle R, C, Mac \rangle, Res$

$\langle R, C, Mac \rangle$

SQN too high or low

$AK = f_5(R, K)$
$xSQN = C \oplus AK$
$xMac = f_1(\langle xSQN, R \rangle, K)$
$xRes = f_2(R, K)$
if (i) $xMac = Mac \wedge$
(ii) $SQN < xSQN$
$SQN := xSQN + 1$

$xRes$

check : $xRes = Res$

$\neg(i)$ Mac_Failure

Send current SQN to network

$\neg(ii)$
$Mac^* = f_1(\langle SQN, R \rangle, K)$
$AK^* = f_5{}^*(R, K)$
$C^* = SQN \oplus AK^*$
$A^* = \langle C^*, Mac^* \rangle$

Sync_Failure, A^*

Sync_Failure, A^*

Sequence Number SQN policies

According to guidelines from 3GPP TS 133.102, different policies for SQN and its update:

- SQN counter may be updated by 1
- SQN may be time-based

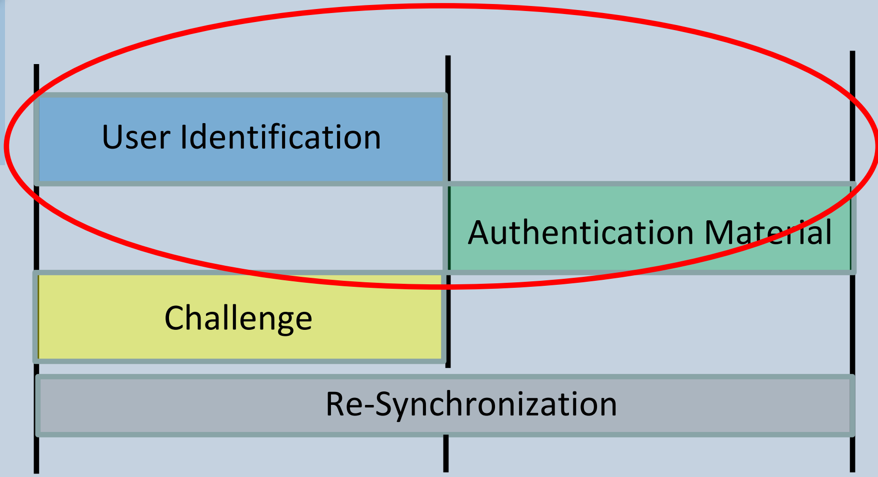
Most of our attacks work for any policies that are not time-based. Other Location attacks work independent of policy.

New vulnerabilities and attacks

First Attack Vector

Request of challenges are not authenticated

- Design choice of symmetric key mechanism
- Seems no check at AuC (HLR) for such queries



Privacy impact

- Build a fake USIM by reprogramming IMSI
- Collect RAND, AUTN pairs
- Re-use them to locate a particular mobile users

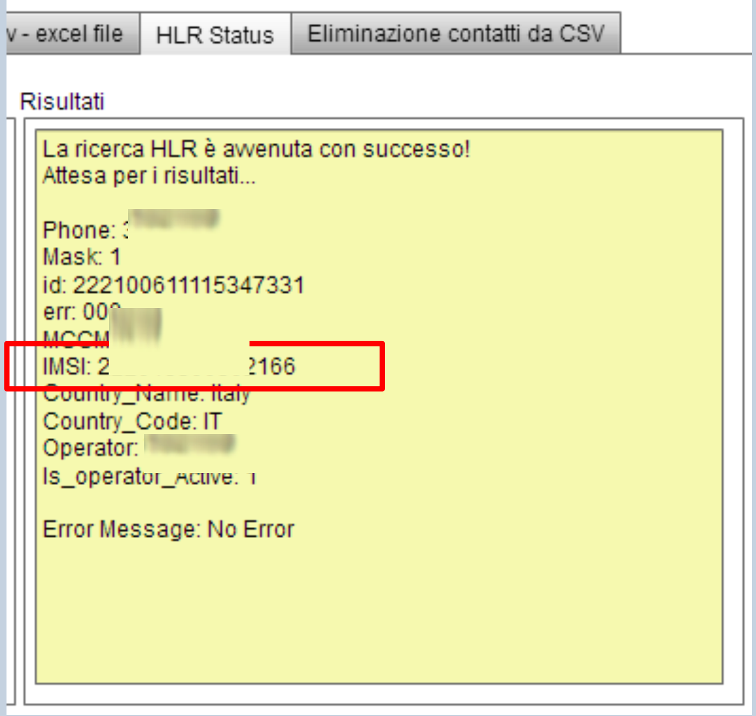
Exploiting first attack vector

How to find IMSI of a target

- HLR Lookup services
- phone number → IMSI

Build a fake USIM card

- Reprogram IMSI
- No other keys required
- Collect RAND, AUTN pairs

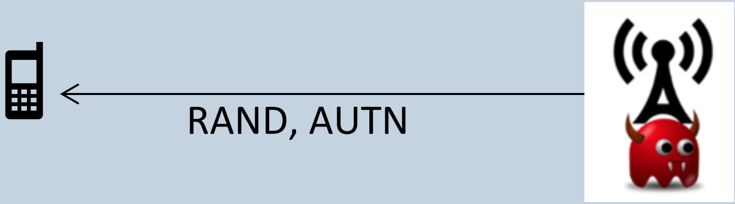


```
La ricerca HLR è awenuta con successo!
Attesa per i risultati...

Phone: 3[redacted]
Mask: 1
id: 221006111115347331
err: 00[redacted]
MCCM[redacted]
IMSI: 2[redacted]2166
Country_Name: Italy
Country_Code: IT
Operator: [redacted]
Is_operator_Active: 1

Error Message: No Error
```

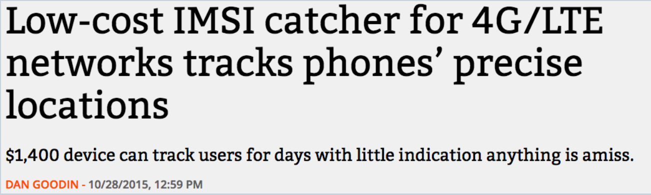
Location attacks against 3G/4G devices



RAND, AUTN

Location attacks

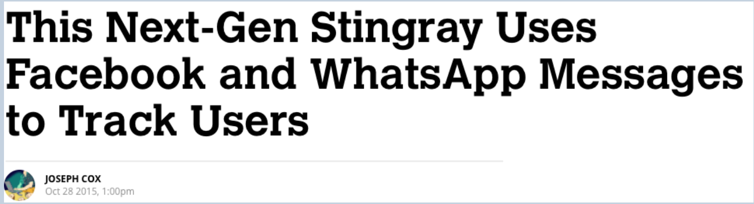
- Locate a targeted phone (range of 2 km)
- Track further using GPS or triangulation method



Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations

$1,400 device can track users for days with little indication anything is amiss.

DAN GOODIN - 10/28/2015, 12:59 PM



This Next-Gen Stingray Uses Facebook and WhatsApp Messages to Track Users

JOSEPH COX
Oct 28 2015, 1:00pm

Our Attacks

Activity monitoring attacks

- Learn n least significant bits of SQN (and IND)
- Learn whether mobile attached to certain network in a certain time window

Service usage (calls/SMS) → number of authentications → increase SQN

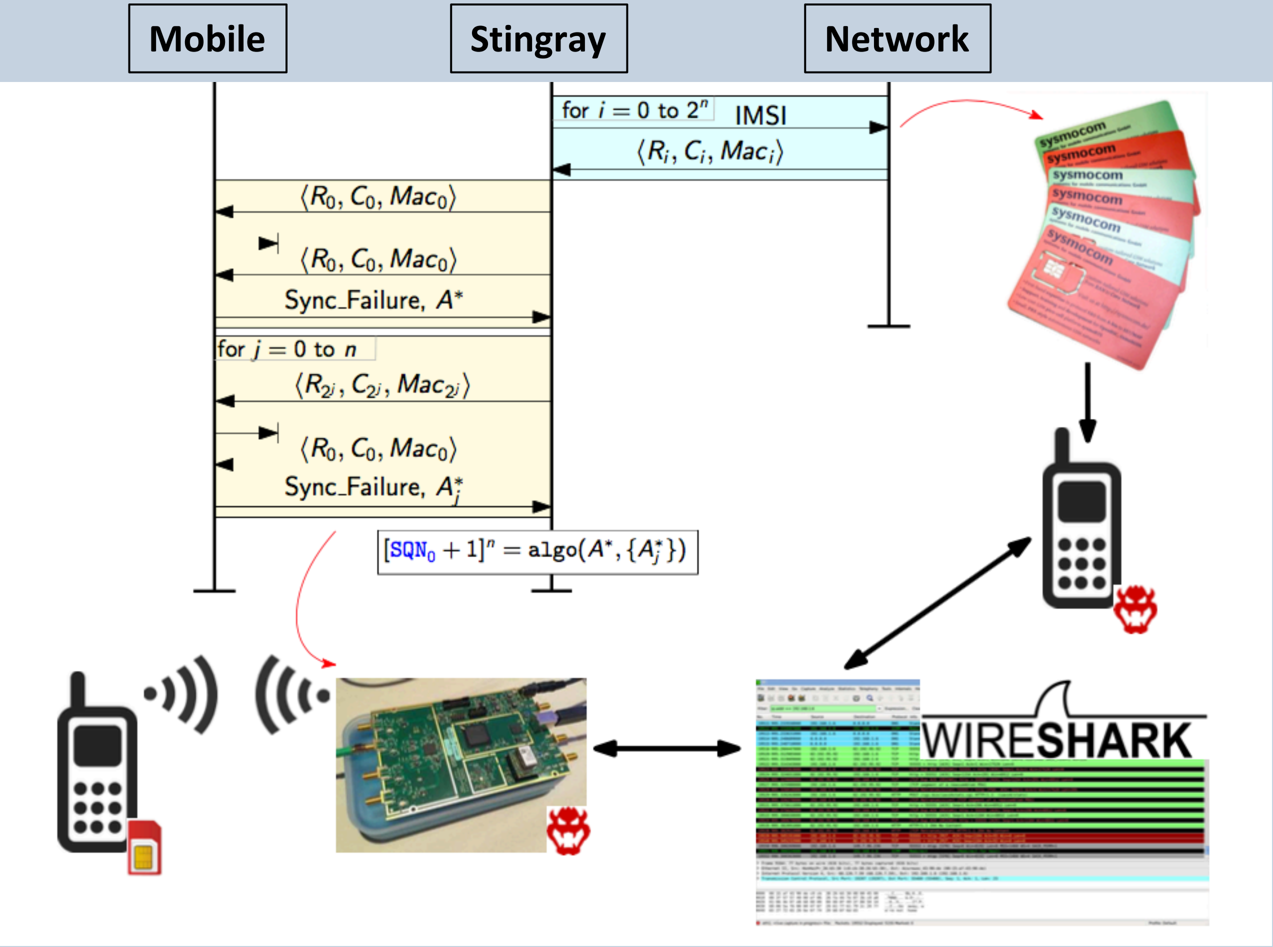
↓

Mobile's activity – new type of threat

Location attacks

- **Track/trace** a mobile in the radius of fake base station

Proof of concept



Mobile

Stingray

Network

for $i = 0$ to 2^n IMSI

$\langle R_i, C_i, Mac_i \rangle$

$\langle R_0, C_0, Mac_0 \rangle$

$\langle R_0, C_0, Mac_0 \rangle$

Sync_Failure, A^*

for $j = 0$ to n

$\langle R_{2^j}, C_{2^j}, Mac_{2^j} \rangle$

$\langle R_0, C_0, Mac_0 \rangle$

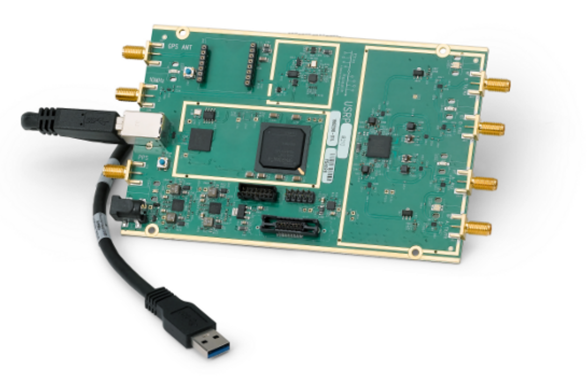
Sync_Failure, A_j^*

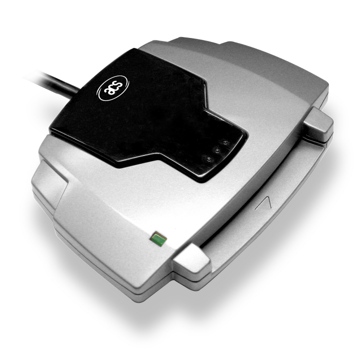
$[\texttt{SQN}_0 + 1]^n = \texttt{algo}(A^*, \{A_j^*\})$

Attacks & Demo

Experimental setup

- Hardware
  - USRP B210
  - Any smartcard reader
  - Programmable USIM
- Software
  - pySIM
  - OpenLTE
- Hardware setup costs about 1400$





Putting attacks into practice

- Practical confirmation of all attacks in real networks
- (Available) hardware setup cost : 1400 $ (100 $ for POC only)
- Monitoring attack : 10 bits of SQN quickly (12 injections + 64 eavesdrops)
- Monitoring attack can be improved with more efficient signalling setup

Observations in deployed 3G/4G networks…1

Issue with a window of acceptable sequence number values to recover from loss or reordering

- No clear requirements in TS 33.102 (only guidelines)
- Different policies about accepting unused AUTN, RAND pair
- Risk to mutual authentication property of AKA

Observations in deployed 3G/4G networks..2

No rate limit **at which AKA tokens can be requested from HLR**

- Tested in few European mobile operators
- Assist in revealing SQN, bypass mutual authentication, and locate a mobile phone
- Protection needed?

Impacts against users & operators

End Users:

- New threat on privacy (activity monitoring attack)
- New location attack, harder to detect, harder to fix
- Affect all 3G and 4G devices
- Likely to affect in 5G??

Cellular Operators:

- New attack interface to inject packets to HLR (heart of the network)
- Poor SQN policies may introduce denial of service attacks
- Problems in detecting modern IMSI catchers

Countermeasures

Mobile Operators :

- Evaluate SQN acceptance policy
- Rate limit authentication request at AuC/HLR?

End Users:

- Unfortunately, nothing much beside use WiFi services without USIM

Vendors:

- Hopefully fake base stations will no longer work in 5G
- Support for legacy network (2G/3G/4G) challenging
- More efforts in mobile OS to tackle fake base station problem

Conclusions..1

Lessons :

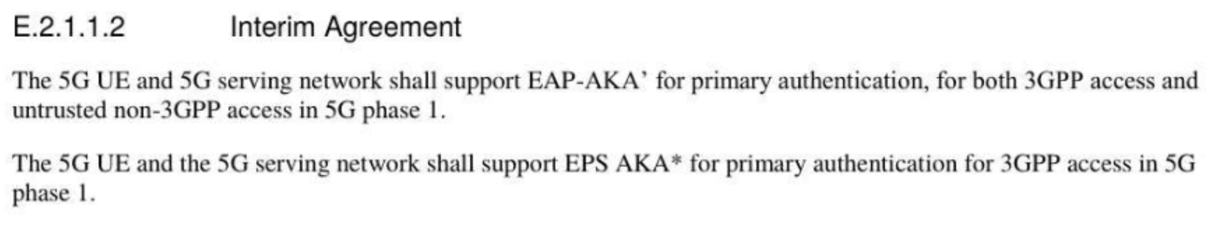
- Trade-offs are still valid - almost 25 years
- Mobile devices are still dumb terminals in the architecture
- There are almost infinite ways to build smart 4G IMSI catchers

Our Findings:

- New attack vector leading to various privacy breaches
- Activity monitoring attack leaking new type of information to attacker
- Affect different variants of AKA : {EAP, EPS} AKA, HTTP digest AKA
- Countermeasures require non-trivial dedicated modifications (for 5G)
- Improved policies on SQN may assist in minimizing impact

Conclusions..2

From 3GPP TR 33.899 V1.1.0 (2017-03) :



E.2.1.1.2 Interim Agreement

The 5G UE and 5G serving network shall support EAP-AKA' for primary authentication, for both 3GPP access and untrusted non-3GPP access in 5G phase 1.

The 5G UE and the 5G serving network shall support EPS AKA* for primary authentication for 3GPP access in 5G phase 1.

Study on the security aspects of the next generation system (5G)

Thank You.

Questions?

This work was partly supported by 5G-Ensure (grant agreement No. 671562 www.5Gensure.eu).