Behind the scenes of 5G security

Ravishankar Borgaonkar, Research Scientist, SINTEF Digital, Norway
Altaf Shaik, SecT, TU Berlin, Germany

Bsides Zurich , Switzerland (14 Sept 2019)

5G Deployment Types

2019

2020

4G Core Network

Non-Standalone Mode

Ultra Gbps speed
Ultra low latency

5G Core Network

Standalone Mode

5G towers

SINTEF

5G Networks – Future in 2030?

Vehicle to drive digitalization phase & realize a gigabit networked-society!

100 Mbps

5 Gbps

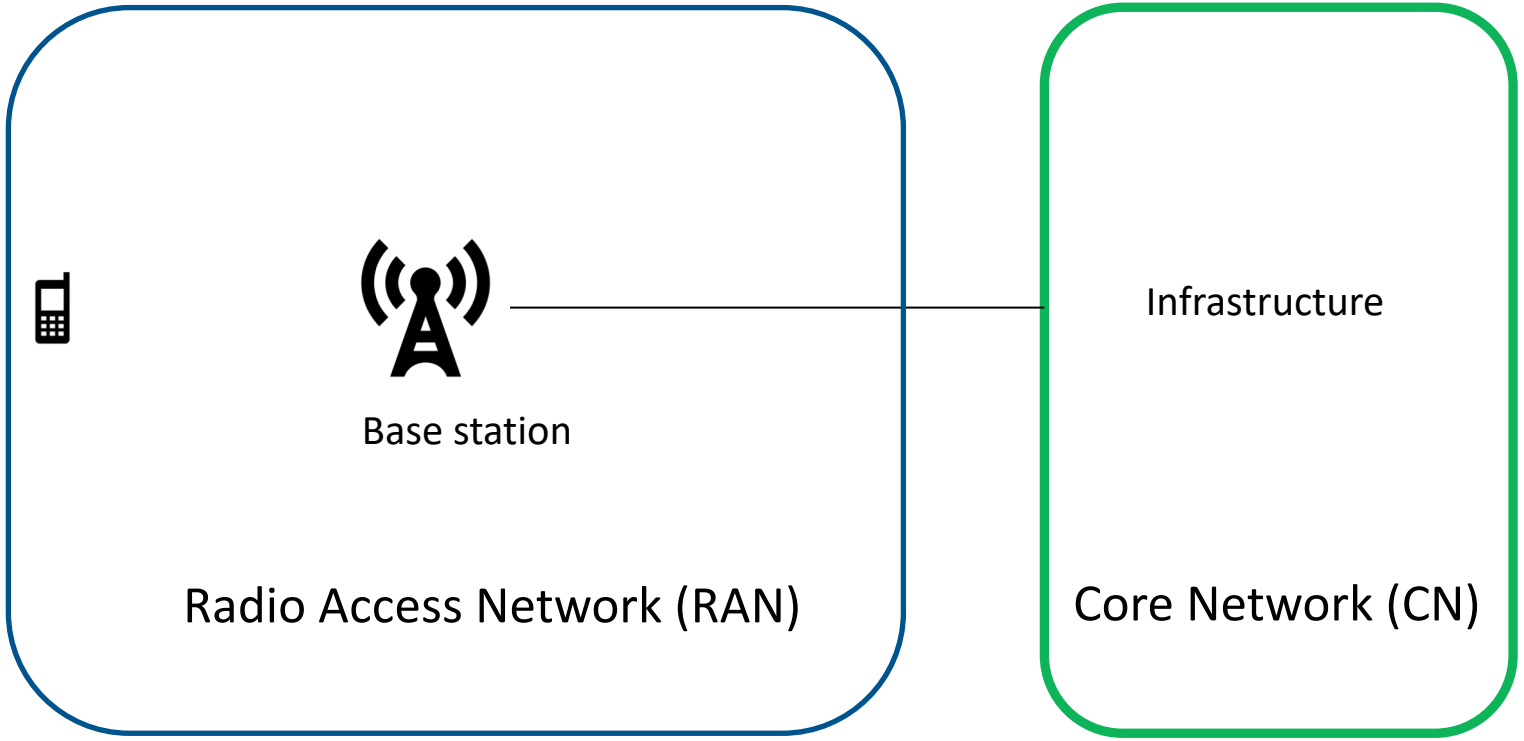
National Critical Infrastructure!

SINTEF

Image Sources: Internet

Let’s look into 5G Architecture & Security

Architecture in General



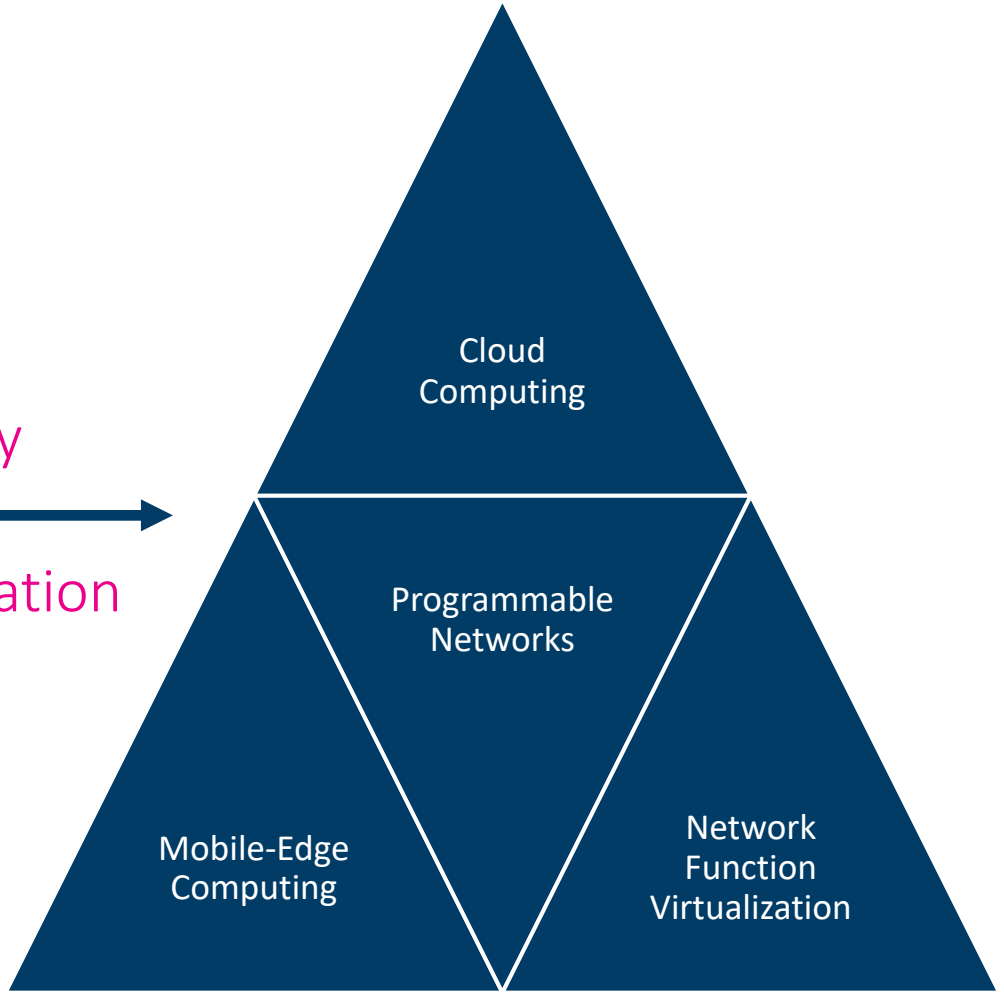
Note: picture provides an abstract view only

Evolution in 5G Architecture

5G Core Network Infrastructure

Technology

Transformation

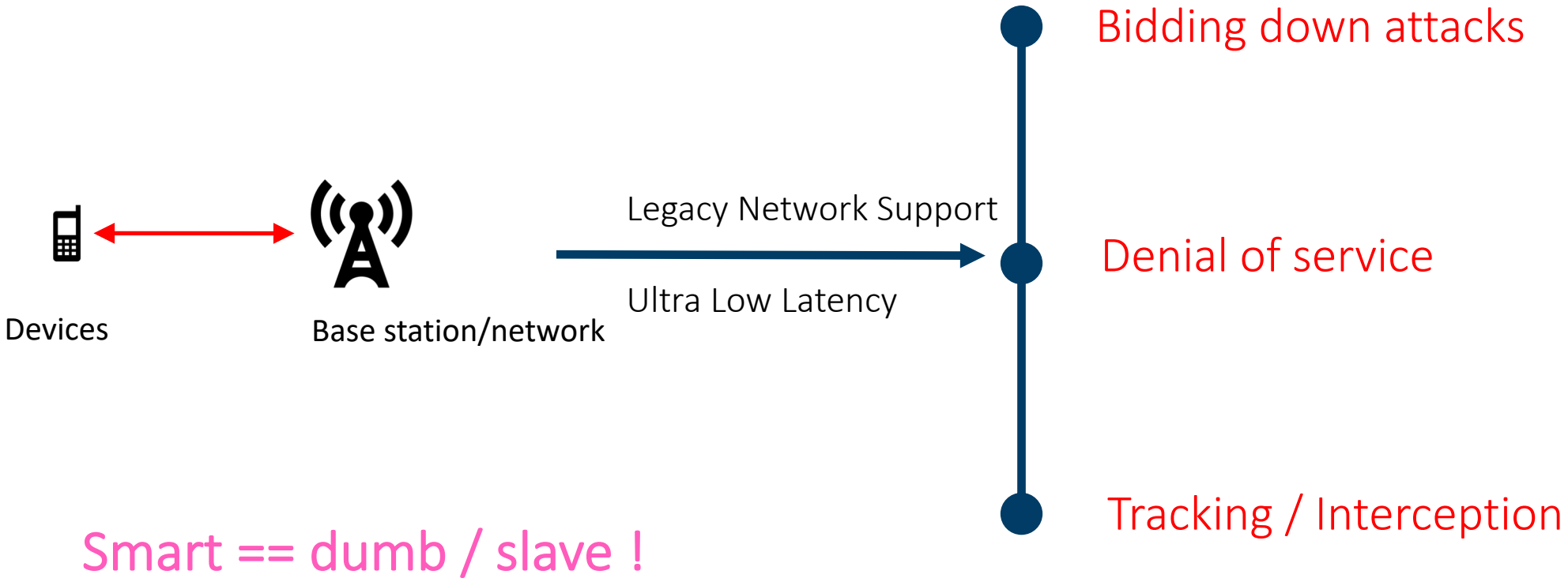


SINTEF

5G Security Issues

SINTEF

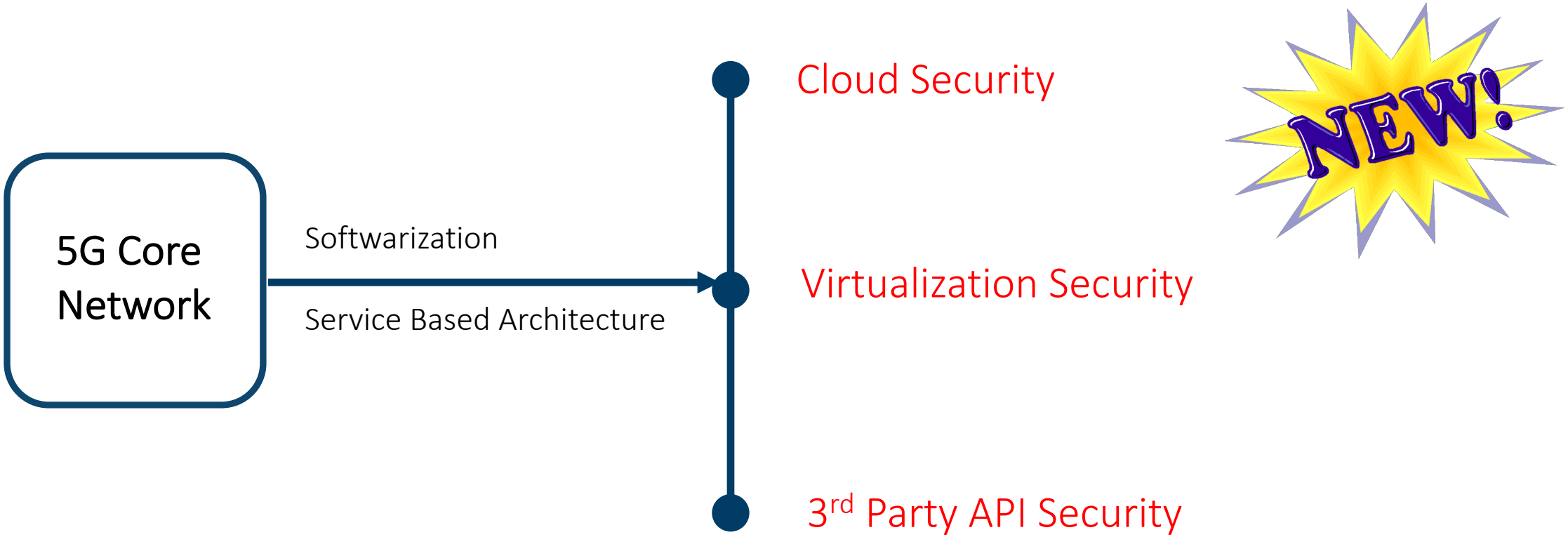
Increased Attack Surface



Smart == dumb / slave !

SINTEF

Increased Attack Surface



Source: Logolynx

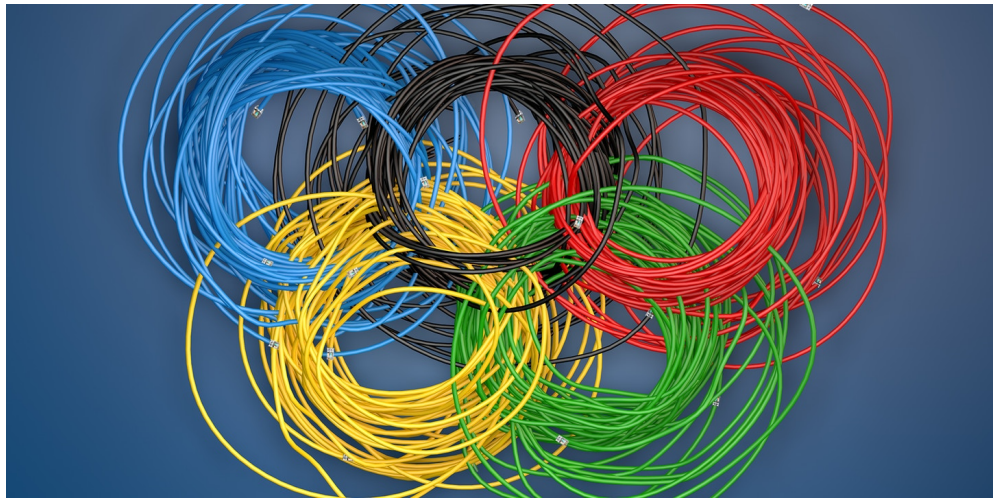
History of incidents – Greek Wiretapping Scandal

29 Jun 2007 | 14:07 GMT

The Athens Affair

How some extremely smart hackers pulled off the most audacious cell-network break-in ever

By **Vassilis Prevelakis and Diomidis Spinellis**



Source: The Intercept

SINTEF

History of incidents – Configurational/Operational mistakes

SS7 SIGNALERING

– Et ondsinnet angrep mot [redacted] ville hatt samme konsekvens

Havariet fredag skjedde via en sårbar protokoll fra 1970-tallet.

AV: MARIUS JØRGENRUD | TELE-KOMMUNIKASJON | PUBLISERT: 22. FEB. 2016 - 13:57

Source: nntb.no

SINTEF

History of incidents – SNOWDEN NSA Briefcase

OTA, master key Ki, …

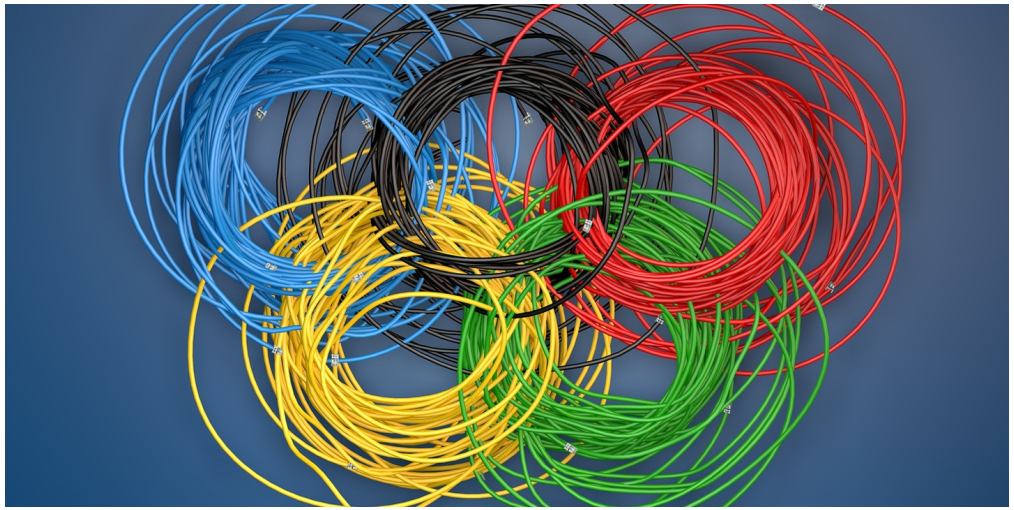
Now eSIM !!

Source: The HackerNews

SINTEF

Security challenges..

✓ 5G as an emerging signal intelligence platform for collecting and processing telemetry data → surveillance from cyber enemies

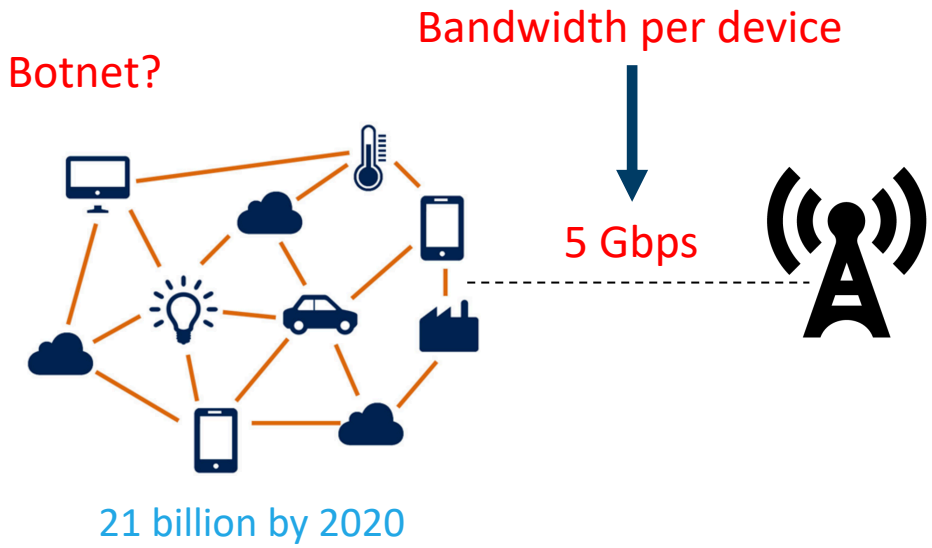


CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

SINTEF

Security challenges..

✓ Denial of Service / Distributed Denial of Service attack protection



Average wired broadband speed

Rank	Country	Average Download Speed (Mbps)	Total Tests	Time To Download HD Movie (5GB)
1	Singapore	**60.39**	524,018	11 Mins, 18 Secs
2	Sweden	**46.00**	367,241	14 Mins, 50 Secs
3	Denmark	**43.99**	150,529	15 Mins, 31 Secs
4	Norway	**40.12**	86,920	17 Mins, 01 Secs
5	Romania	**38.60**	175,948	17 Mins, 41 Secs

Source: Fastmetrics

SINTEF

5G Security challenges & discoveries..

✓ Data privacy issues (vulnerabilities in the 5G access network)

New vulnerabilities in 4G and 5G cellular access network protocols : exposing device capabilities

Altaf Shaik (Technische Universität Berlin, Germany); Ravishankar Borgaonkar (SINTEF Digital, Norway); Shinjo Park and Jean-Pierre Seifert

New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols

Ravishankar Borgaonkar and Lucca Hirschi and Shinjo Park and Altaf Shaik

A Formal Analysis of 5G Authentication

Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion

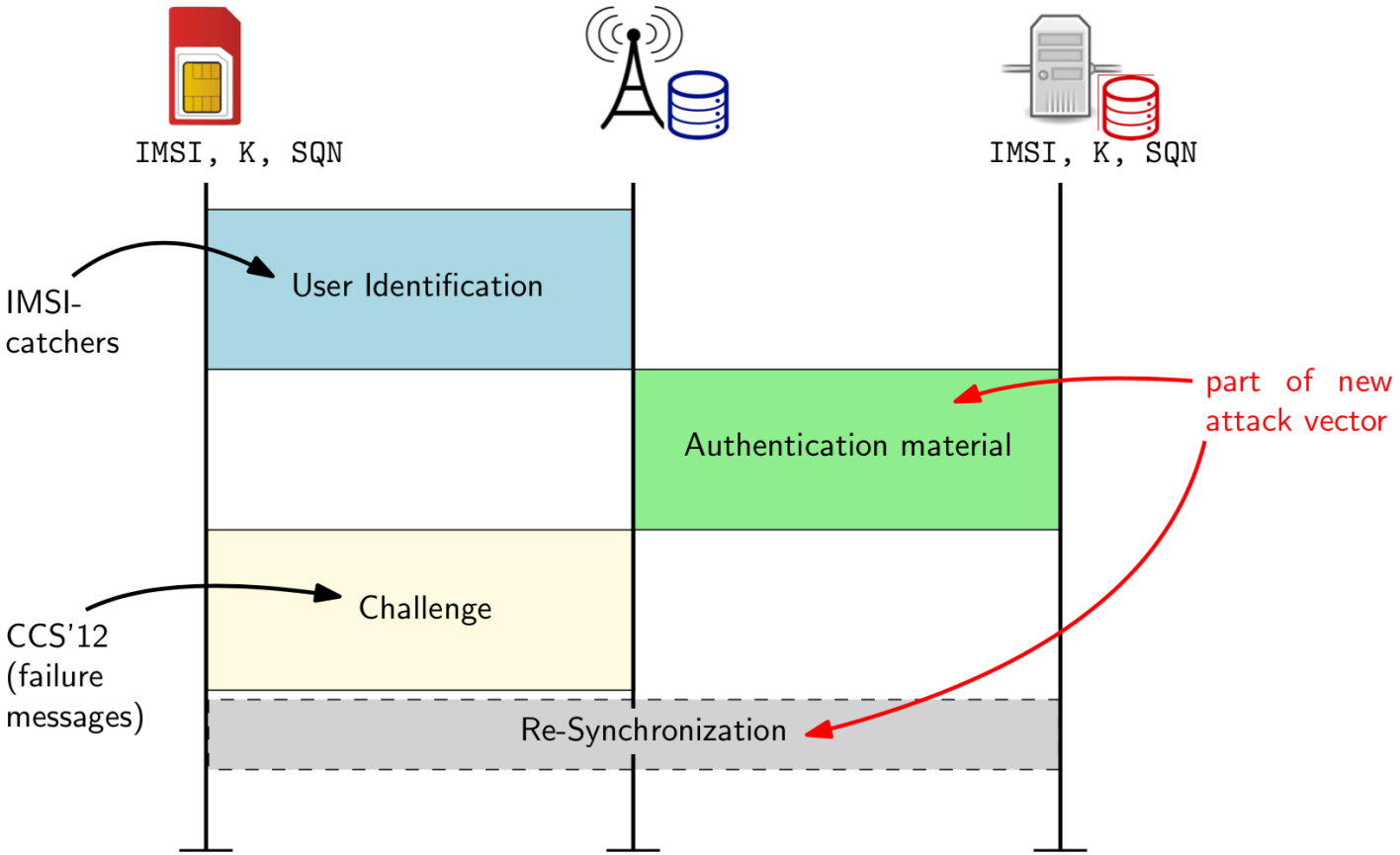
IMSI catcher in 5G?

Locating & Tracking only!

- Existing IMSI catchers will no longer be effective as encrypted IMSI
- Can we identify devices and relates to the end-users?
- Can we exploit AKA protocol vulnerabilities to track users?

Locating, Tracking & Monitoring by AKA protocol issues

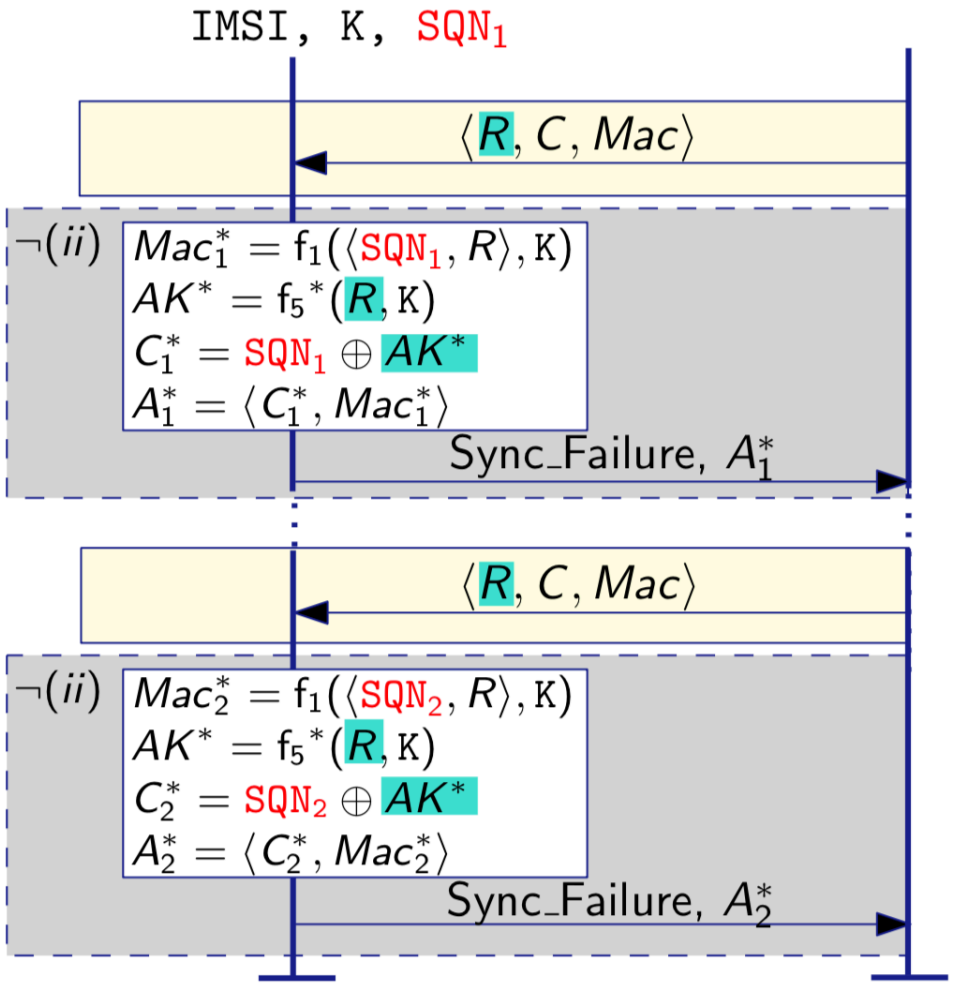
AKA Protocol



5G AKA Attack

Attack vector = combination of:

- Two injections of the same (unfresh) challenge $\rightsquigarrow$ same conceal factor AK^*
- requests of challenges are not authenticated



AUTN = C, MAC

$C_1^* \oplus C_2^* = SQN_1 \oplus SQN_2$

SINTEF

Demo (IMSI catcher in 5G)

Summary and Looking forward

- 5G path towards digital & gigabit society
- Stronger security than 4G but

  new features ==increase in attack surface

  support to the legacy systems == attack inheritance?
- Need of risk assessment and management tools
- **Best security practices while using 5G**
- New security solutions tailored towards protecting the infrastructure telemetry data

SINTEF

Teknologi for et bedre samfunn

Contact at - ravishankar.borgaonkar@sinetf.no