5G SECURITY

Can 5G secure IoT?

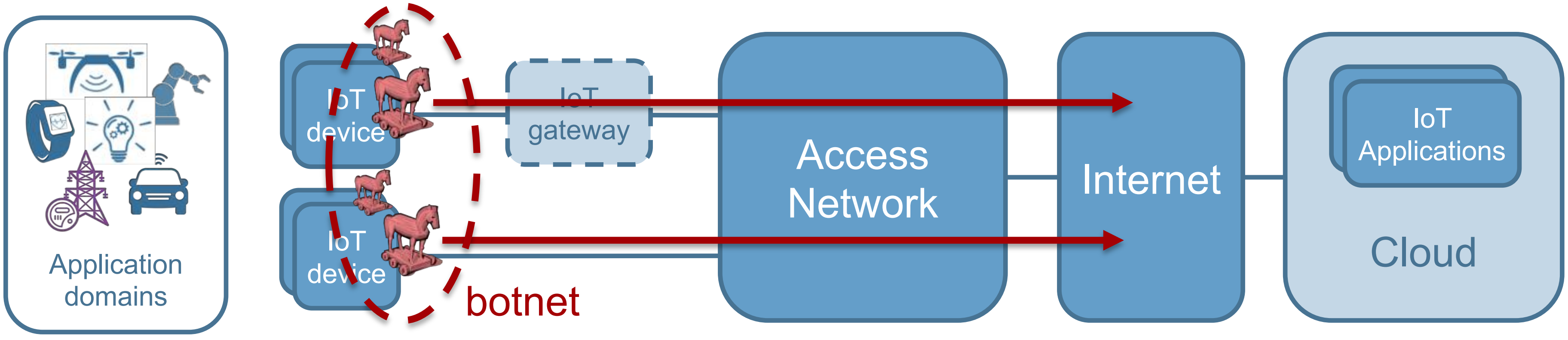
7 March 2019 | Ir. F. Fransen

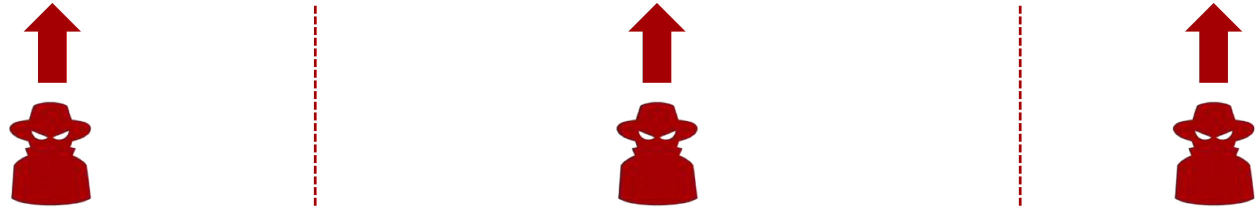
TNO innovation for life

Can 5G secure IoT?

TNO innovation for life

IoT Security threat landscape (non-exhaustive overview of threats)





Impact depends on the application

confidentiality, privacy, reliability, availability, etc.

- Attacks on IoT device (take control)
- Build botnet to attack other systems

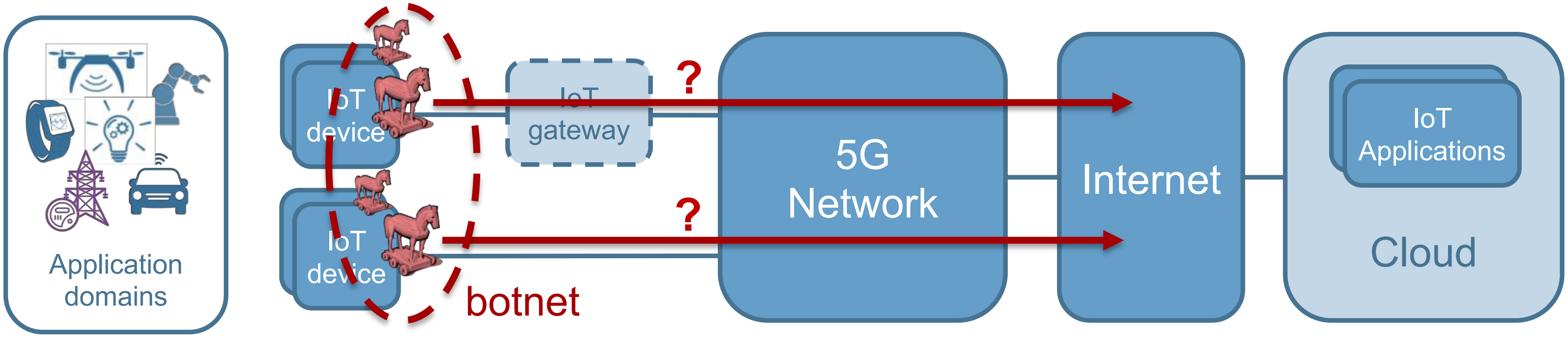
- Attacks on network (eavesdrop communication, inject or manipulate data, etc.)
- Denial of service (e.g. jamming)

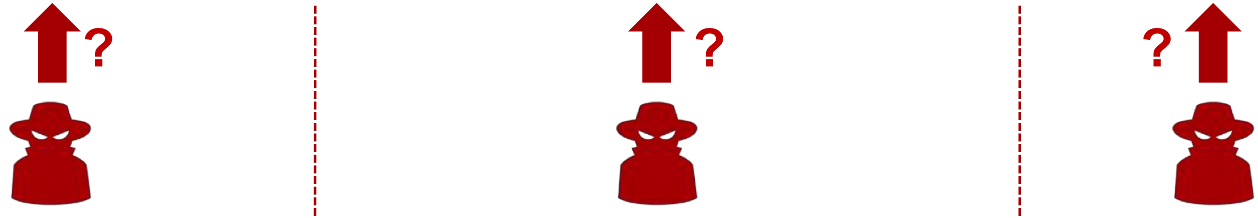
- Attacks on IoT application (take control, steal large amount of IoT data)

Can 5G secure IoT?

TNO innovation for life

IoT Security threat landscape (non-exhaustive overview of threats)





Impact depends on IoT application

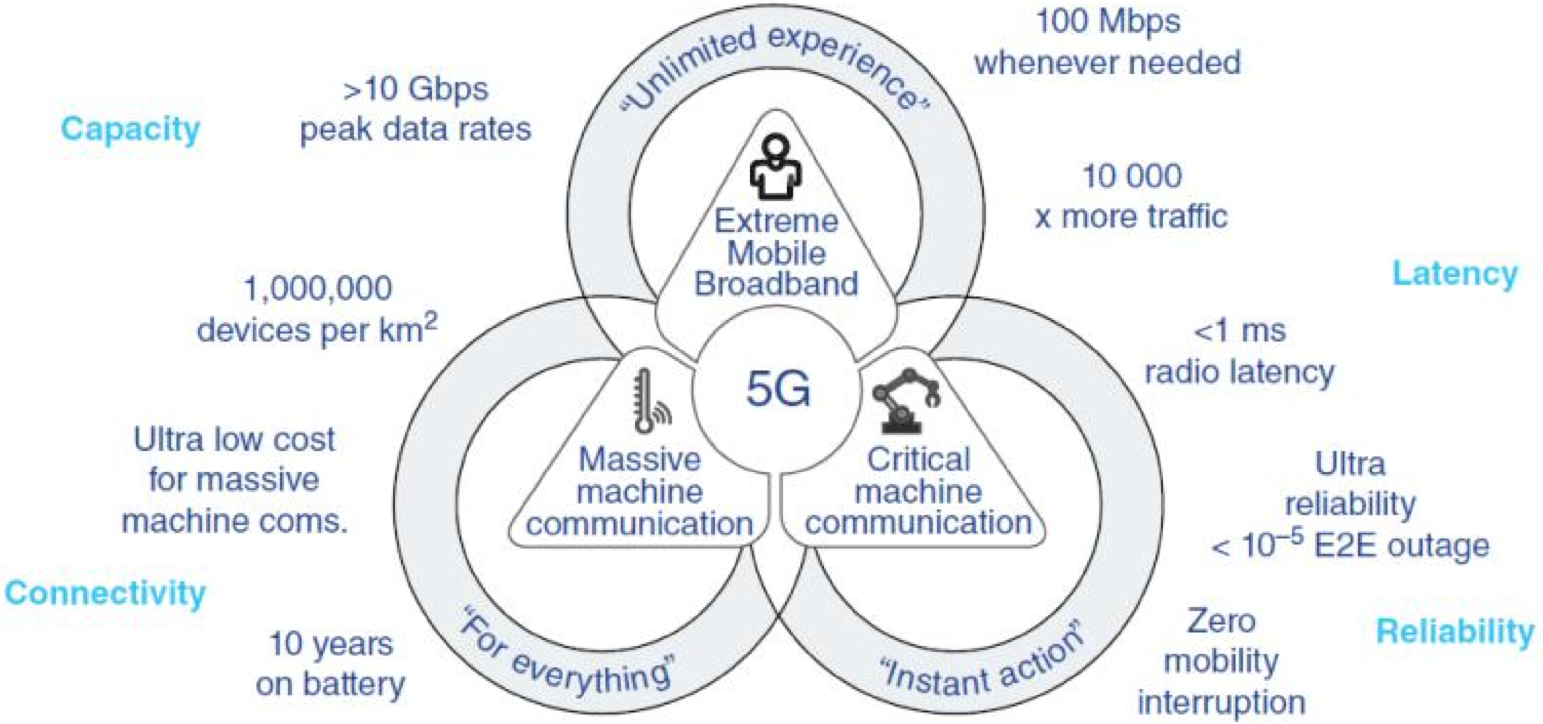
confidentiality, privacy, reliability, availability, etc.

- Attacks on IoT device (take control)
- Build botnet to attack other systems

- Attacks on network (eavesdrop communication, inject or manipulate data, etc.)
- Denial of service (e.g. jamming)

- Attacks on IoT application (take control, steal large amount of IoT data)

THE PROMISE OF 5G

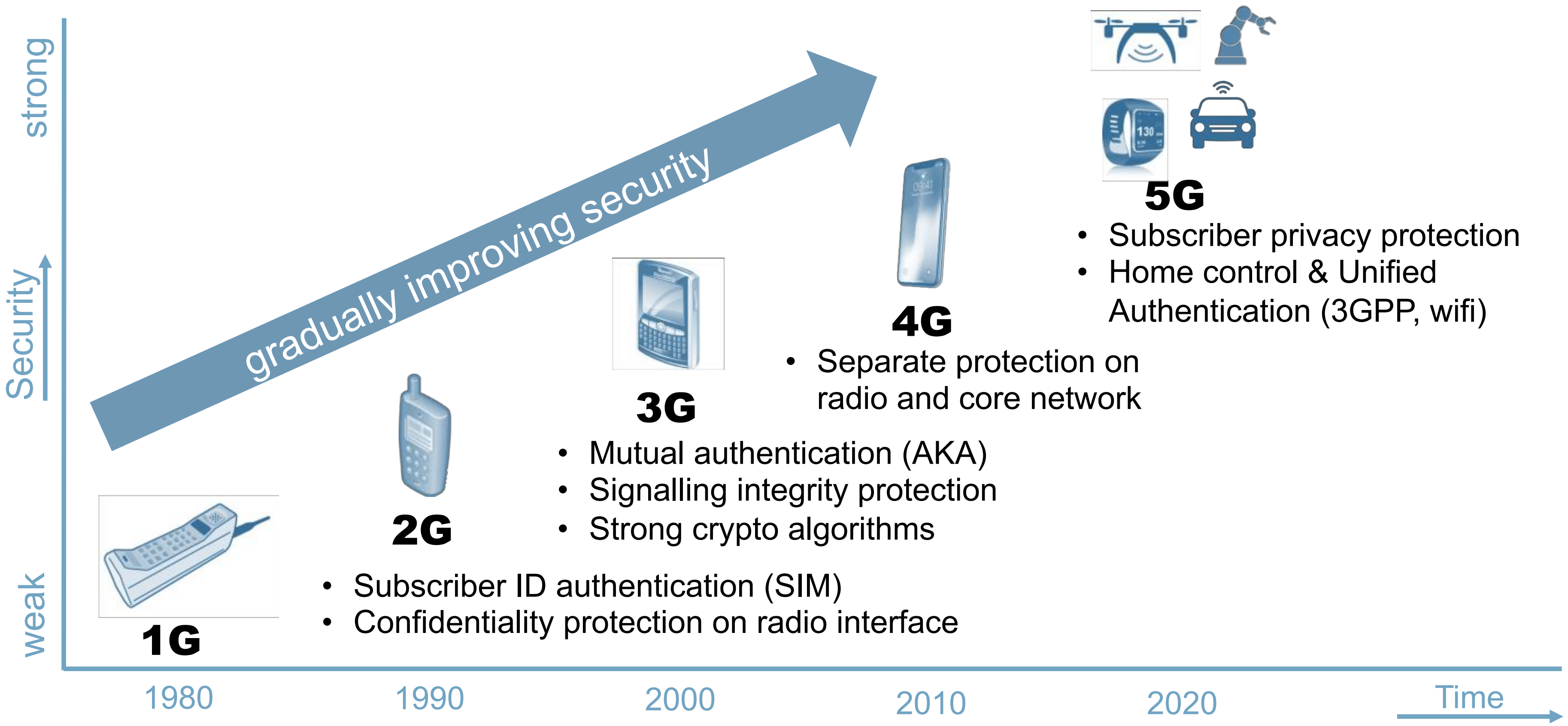


Source: Nokia Networks (2016) 5G masterplan – five keys to create the new communications era. White Paper, C401-011949-WP-201601-1-EN.

5G SECURITY

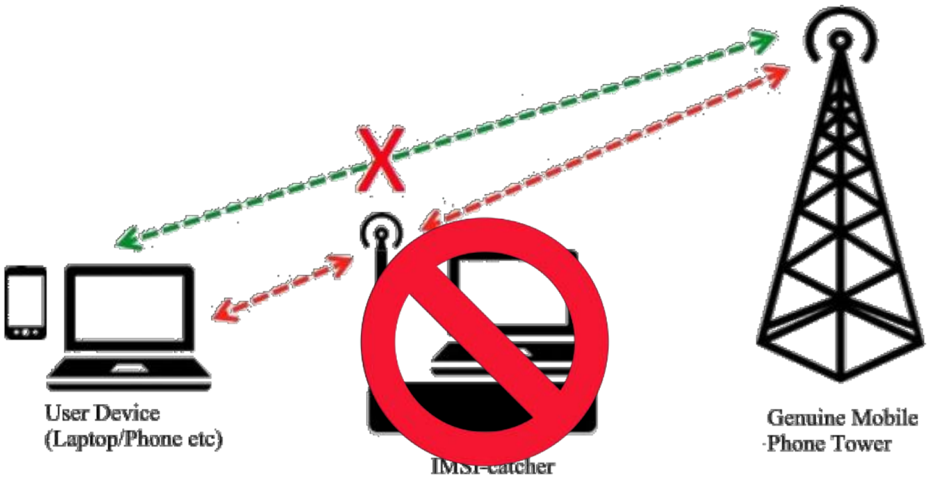
what is new in 5G?

EVOLUTION OF MOBILE SECURITY



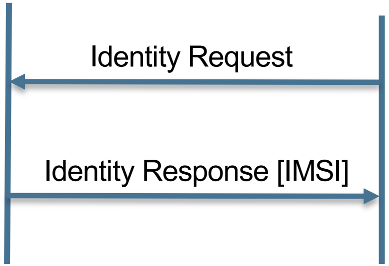
SUBSCRIBER PRIVACY PROTECTION

- False base station (IMSI Catcher) can be used to retrieve the IMSI
- More attention and demand for privacy protection



5G security design goal:

- Defeat IMSI Catcher



SUBSCRIBER PRIVACY PROTECTION

Subscription Permanent Identifier (SUPI)

- <SUPI>:=<MCC>|<MNC>|<MSIN>

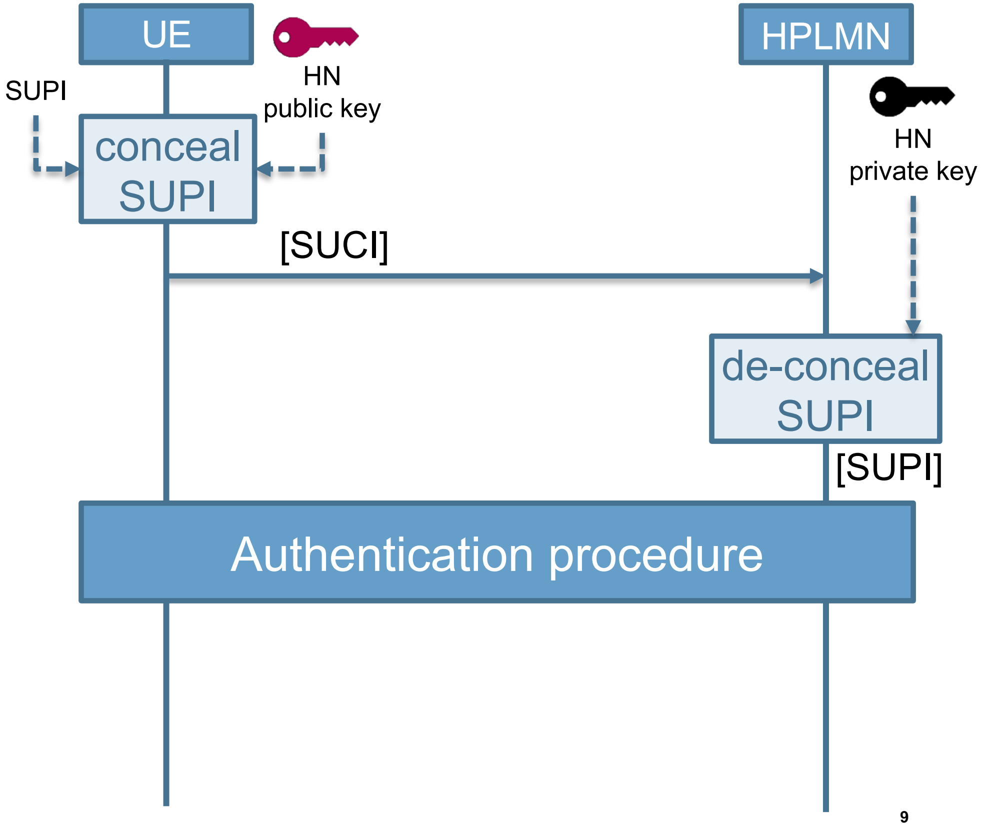
Subscription Concealed Identifier (SUCI)

- <SUCI>:=<MCC>|<MNC>|<encrypted MSIN>

- SUPI should not be transferred in clear text over 5G Radio Access Network

Solution:

- SUPI encrypted with home network *public key* on initial attach (SUCI)
- Complete authentication



SUBSCRIBER PRIVACY PROTECTION

Subscription Permanent Identifier (SUPI)

- <SUPI>:=<MCC>|<MNC>|<MSIN>

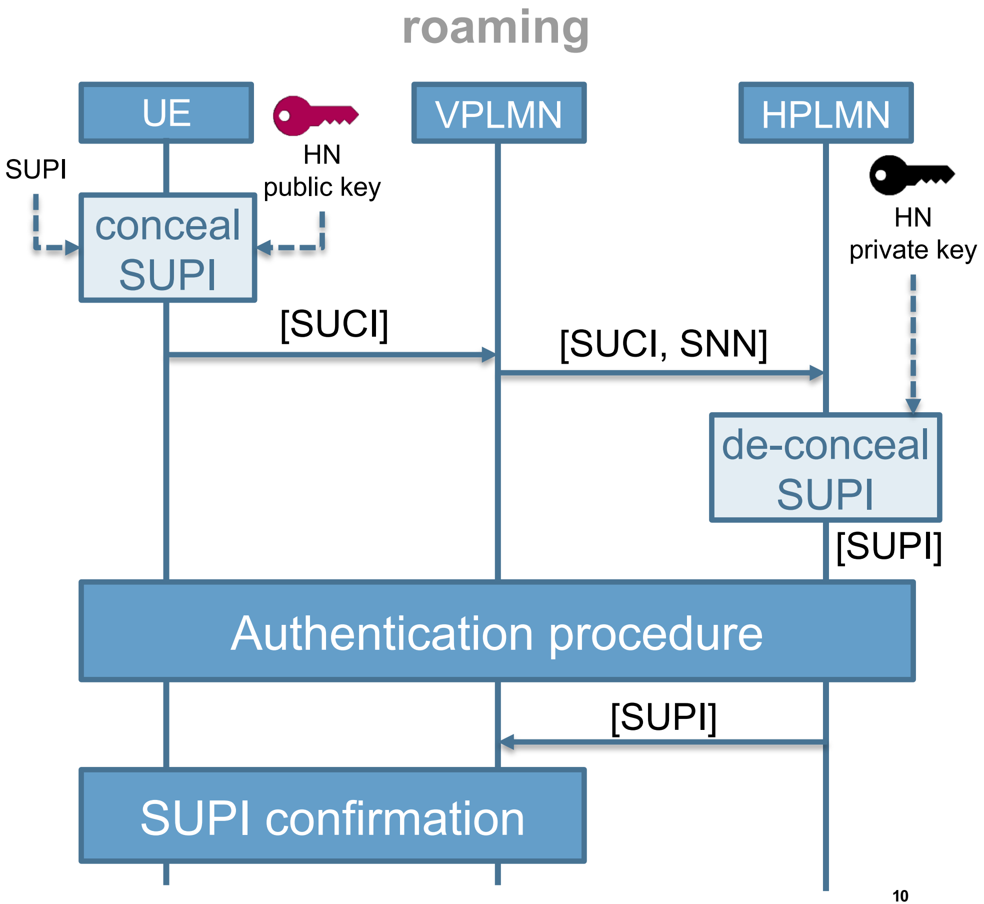
Subscription Concealed Identifier (SUCI)

- <SUCI>:=<MCC>|<MNC>|<encrypted MSIN>

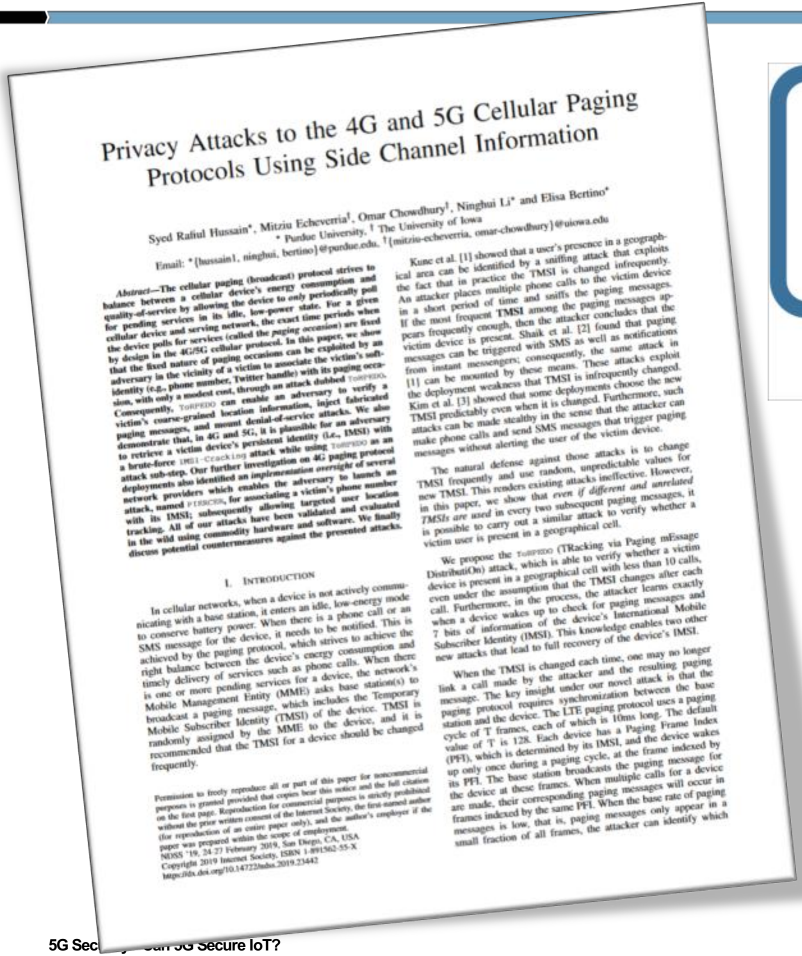
- SUPI should not be transferred in clear text over 5G Radio Access Network

Solution:

- SUPI encrypted with home network *public key* on initial attach (SUCI)
- Complete authentication
- Send SUPI from HPLMN to VPLMN
- Confirm SUPI by binding into a key



SUBSCRIBER PRIVACY PROTECTION



Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information

Syed Rafiul Hussain*, Mitziu Echeverria†, Omar Chowdhury†, Ninghui Li* and Elisa Bertino*
* Purdue University, † The University of Iowa
Email: *{hussain1, ninghui, bertino}@purdue.edu, †{mitziu-echeverria, omar-chowdhury}@uiowa.edu

Abstract—**The cellular paging (broadcast) protocol strives to balance between a cellular device's energy consumption and quality-of-service by allowing the device to *only* periodically poll for pending services in its idle, low-power state. For a given cellular device and serving network, the exact time periods when the device polls for services (called the *paging occasion*) are fixed by design in the 4G/5G cellular protocol. In this paper, we show that the fixed nature of paging occasions can be exploited by an adversary in the vicinity of a victim to associate the victim's soft-identity (e.g., phone number, Twitter handle) with its paging occasion, with only a modest cost, through an attack dubbed ToRPEDO. Consequently, ToRPEDO can enable an adversary to verify a victim's coarse-grained location information, inject fabricated paging messages, and mount denial-of-service attacks. We also demonstrate that, in 4G and 5G, it is plausible for an adversary to retrieve a victim device's persistent identity (i.e., IMSI) with a brute-force IMSI-Cracking attack while using ToRPEDO as an attack sub-step. Our further investigation on 4G paging protocol deployments also identified an *implementation oversight* of several network providers which enables the adversary to launch an attack, named PIERCER, for associating a victim's phone number with its IMSI; subsequently allowing targeted user location tracking. All of our attacks have been validated and evaluated in the wild using commodity hardware and software. We finally discuss potential countermeasures against the presented attacks.**

I. INTRODUCTION

In cellular networks, when a device is not actively communicating with a base station, it enters an idle, low-energy mode to conserve battery power. When there is a phone call or an SMS message for the device, it needs to be notified. This is achieved by the paging protocol, which strives to achieve the right balance between the device's energy consumption and timely delivery of services such as phone calls. When there is one or more pending services for a device, the network's Mobile Management Entity (MME) asks base station(s) to broadcast a paging message, which includes the Temporary Mobile Subscriber Identity (TMSI) of the device. TMSI is randomly assigned by the MME to the device, and it is recommended that the TMSI for a device should be changed frequently.

NDSS '19, 24-27 February 2019, San Diego, CA, USA
ISBN 1-891562-55-X

https://dx.doi.org/10.14722/ndss.2019.23442

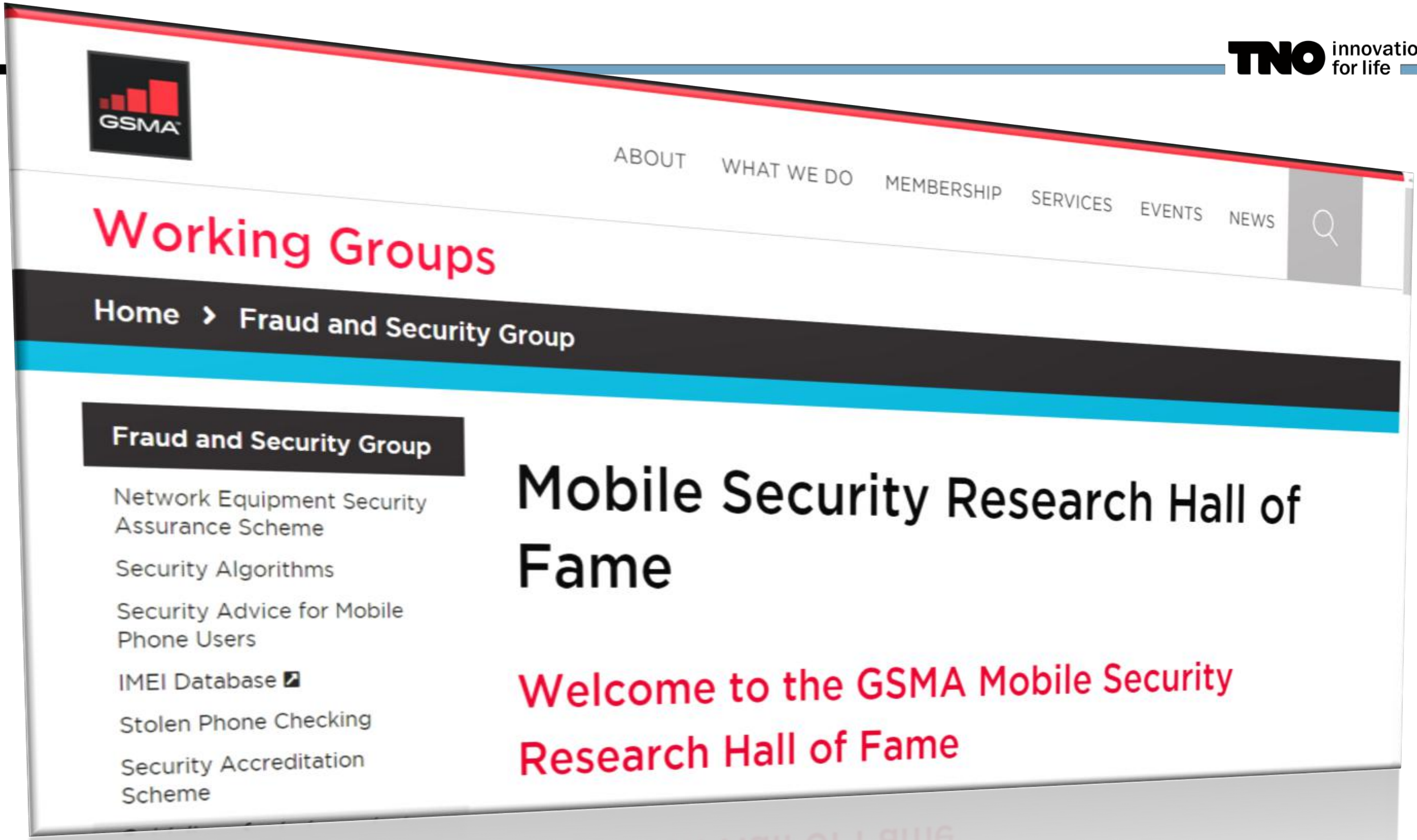
Kune et al. [1] showed that a user's presence in a geographical area can be identified by a sniffing attack that exploits the fact that in practice the TMSI is changed infrequently. An attacker places multiple phone calls to the victim device in a short period of time and sniffs the paging messages. If the most frequent **TMSI** among the paging messages appears frequently enough, then the attacker concludes that the victim device is present. Shaik et al. [2] found that paging messages can be triggered with SMS as well as notifications from instant messengers; consequently, the same attack in [1] can be mounted by these means. These attacks exploit the deployment weakness that TMSI is infrequently changed. Kim et al. [3] showed that some deployments choose the new TMSI predictably even when it is changed. Furthermore, such attacks can be made stealthy in the sense that the attacker can make phone calls and send SMS messages that trigger paging messages without alerting the user of the victim device.

The natural defense against those attacks is to change TMSI frequently and use random, unpredictable values for new TMSI. This renders existing attacks ineffective. However, in this paper, we show that *even if different and unrelated TMSIs are used* in every two subsequent paging messages, it is possible to carry out a similar attack to verify whether a victim user is present in a geographical cell.

We propose the ToRPEDO (TRacking via Paging mEssage DistributiOn) attack, which is able to verify whether a victim device is present in a geographical cell with less than 10 calls, even under the assumption that the TMSI changes after each call. Furthermore, in the process, the attacker learns exactly when a device wakes up to check for paging messages and 7 bits of information of the device's International Mobile Subscriber Identity (IMSI). This knowledge enables two other new attacks that lead to full recovery of the device's IMSI.

When the TMSI is changed each time, one may no longer link a call made by the attacker and the resulting paging message. The key insight under our novel attack is that the paging protocol requires synchronization between the base station and the device. The LTE paging protocol uses a paging cycle of T frames, each of which is 10ms long. The default value of T is 128. Each device has a Paging Frame Index (PFI), which is determined by its IMSI, and the device wakes up only once during a paging cycle, at the frame indexed by its PFI. The base station broadcasts the paging message for the device at these frames. When multiple calls for a device are made, their corresponding paging messages will occur in frames indexed by the same PFI. When the base rate of paging messages is low, that is, paging messages only appear in a small fraction of all frames, the attacker can identify which

- **GSMA Coordinated Vulnerability Disclosure Programme**
  - https://www.gsma.com/aboutus/workinggroups/working-groups/fraud-security-group/gsma-coordinated-vulnerability-disclosure-programme
- **3GPP Coordinated Vulnerability Disclosure (CVD)**
  - http://www.3gpp.org/coordinated-vulnerability-disclosure-cvd

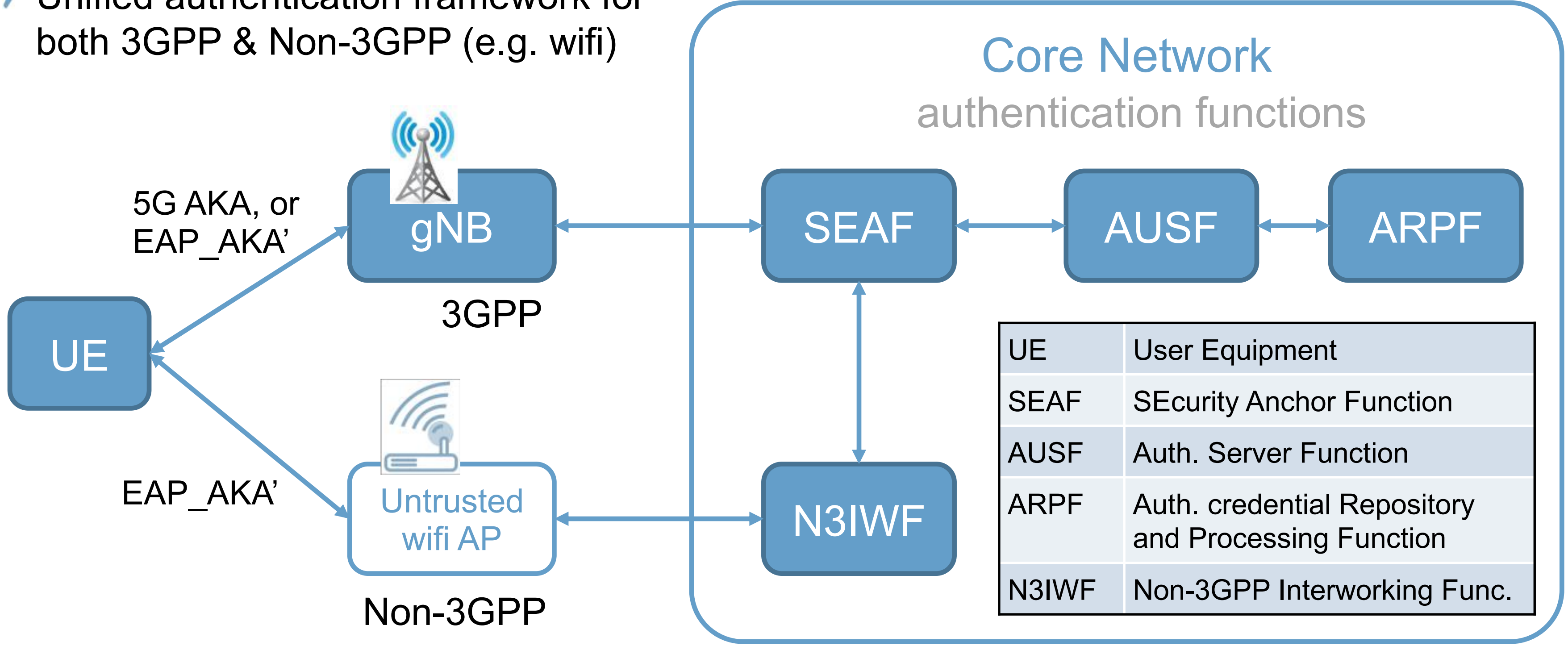

GSMA
ABOUT
WHAT WE DO
MEMBERSHIP
SERVICES
EVENTS
NEWS
Working Groups
Home › Fraud and Security Group
Fraud and Security Group
Network Equipment Security Assurance Scheme
Security Algorithms
Security Advice for Mobile Phone Users
IMEI Database
Stolen Phone Checking
Security Accreditation Scheme
Mobile Security Research Hall of Fame
Welcome to the GSMA Mobile Security Research Hall of Fame

5G AUTHENTICATION – Unified

TNO innovation for life

5G security design goal:

- Unified authentication framework for both 3GPP & Non-3GPP (e.g. wifi)



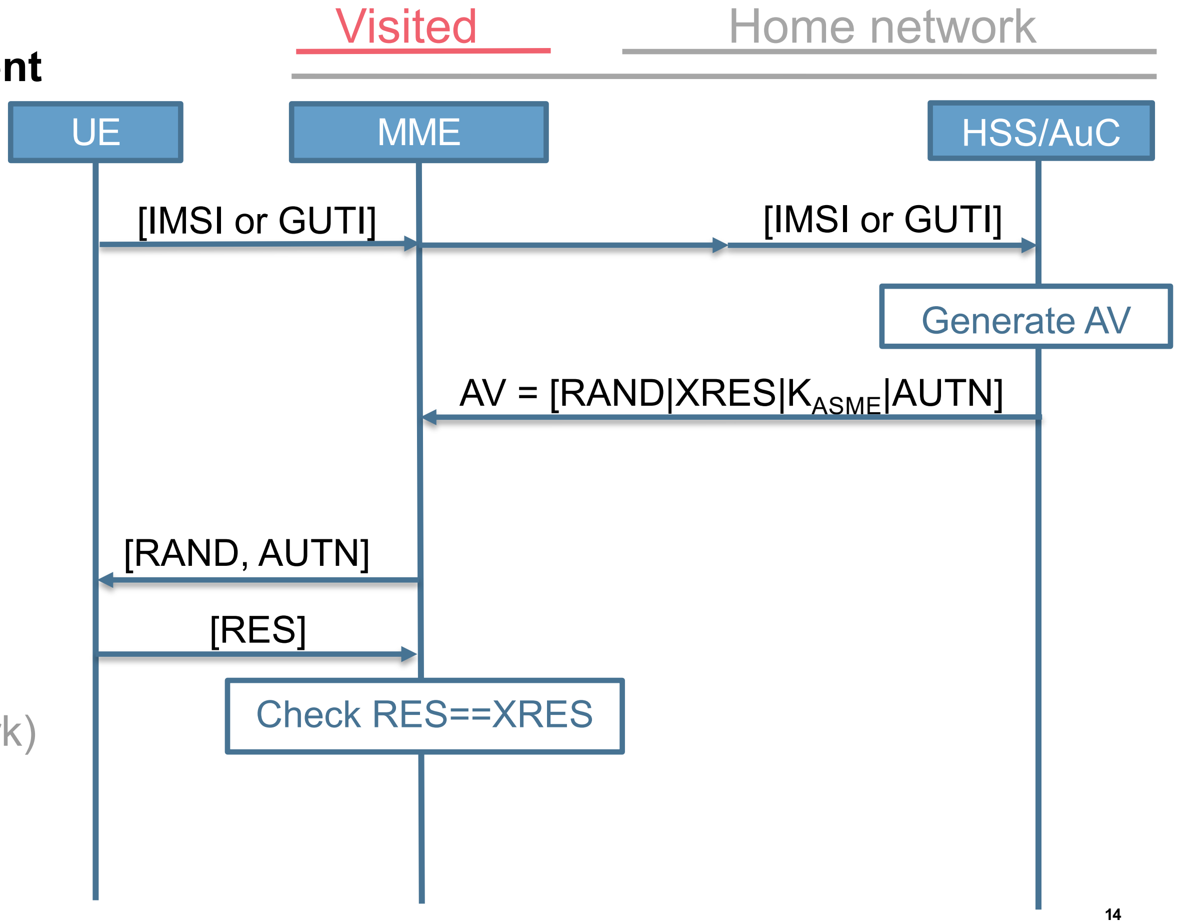
UE	User Equipment
SEAF	SEcurity Anchor Function
AUSF	Auth. Server Function
ARPF	Auth. credential Repository and Processing Function
N3IWF	Non-3GPP Interworking Func.

Extensible Authentication Protocol (EAP)

4G / EPS AKA

Authentication & Key Agreement

- MME verifies RES == XRES
- RAND = Random challenge
- RES = Response
- XRES = eXpected RESponse
- AUTN = AUthentication TokeN
  (used for authenticating network)



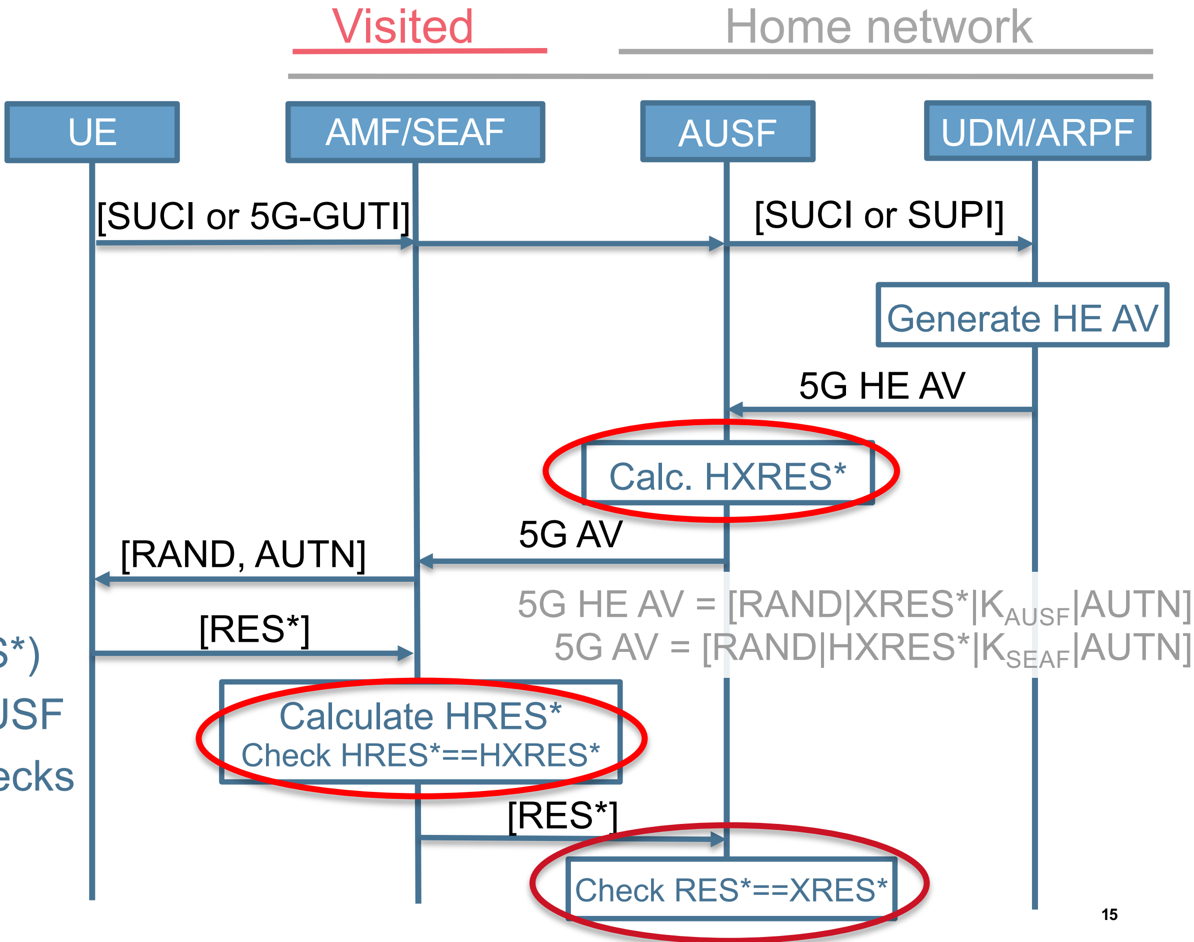
5G AUTHENTICATION - Home Control

5G AKA

- Based on 4G / EPS AKA
- New RES* and H(X)RES*

- Calculation of RES*
  - Home Network (i.e. AUSF) checks if RES* == XRES*

- Calculation of HRES*
  - HRES* = hash(RAND, RES*)
  - Calculated in SEAF and AUSF
  - SEAF / Visited Network checks if HRES*==HXRES*



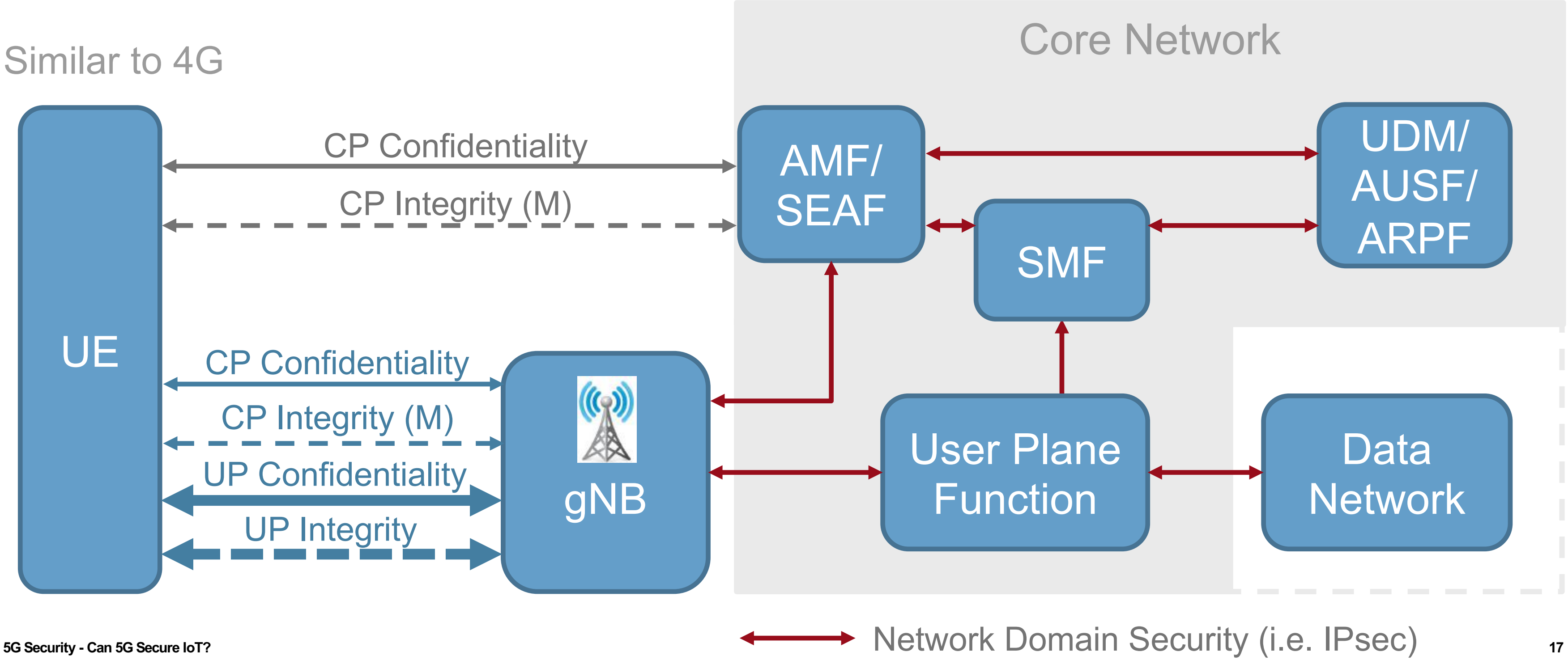
5G SECURITY

how is 5G communication protected?

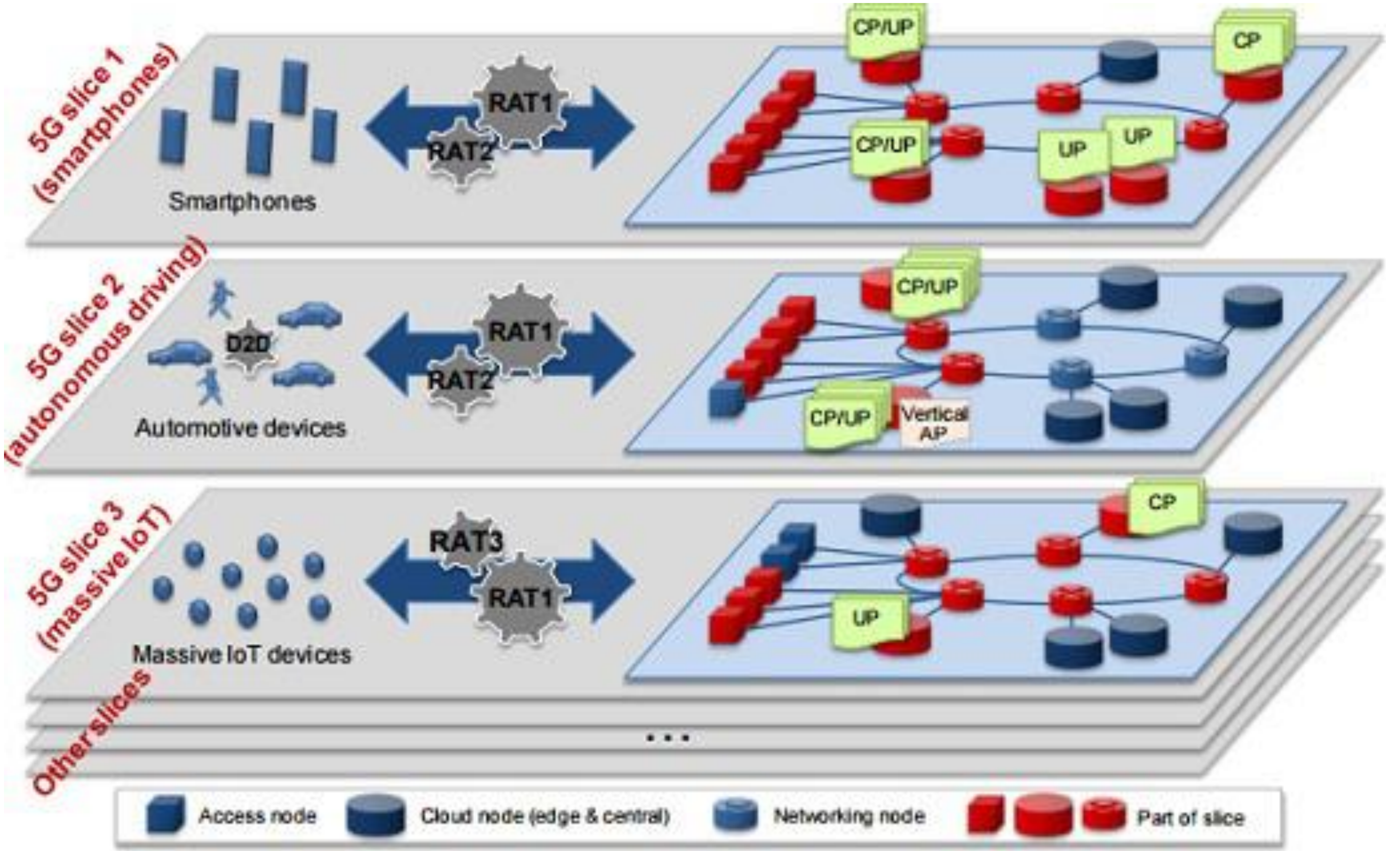
5G SECURITY – UP & CP Protection

- User Plane (UP) traffic integrity & confidentiality protection
- Control Plane (CP) traffic integrity (mandatory) & confidentiality protection

Similar to 4G



NETWORK SLICING



Source: https://www.netmanias.com

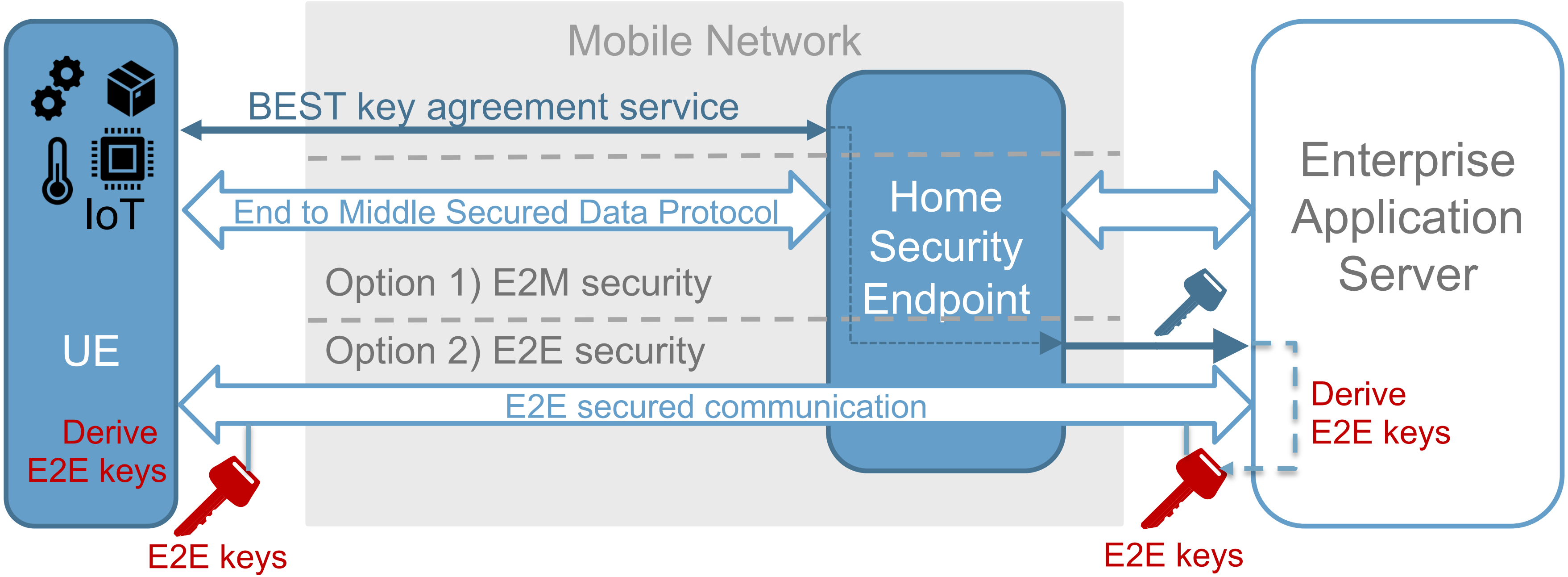
5G SECURITY

additional services for IoT

- 3GPP TR 33.861 - Study on evolution of Cellular IoT security for the 5G System
  includes a.o.
  - *Integrity protection / encryption of small data*
  - *Signalling overload due to Malicious Applications on the UE*

BEST – IoT Security Service

- Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices

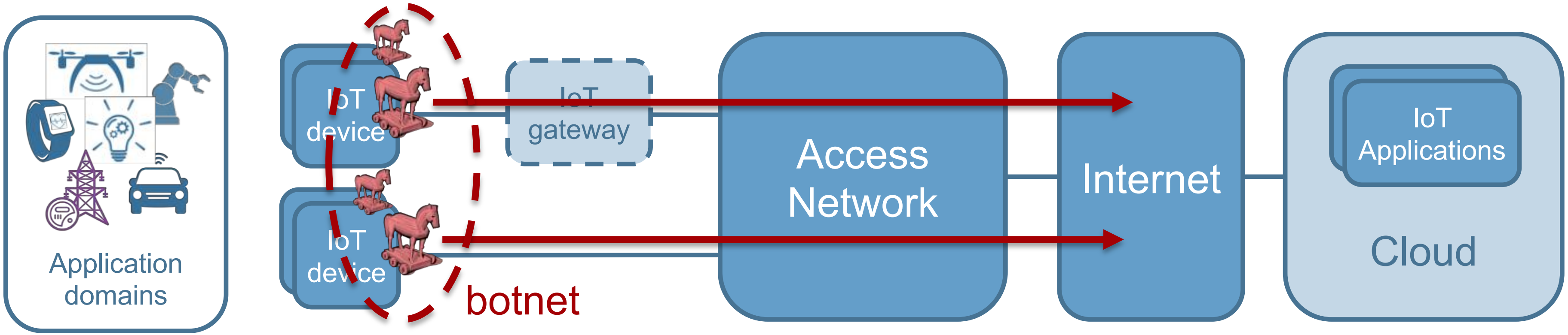


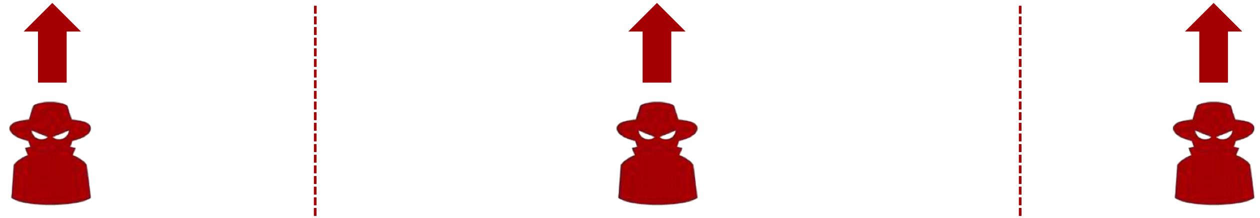
5G SECURITY

Can 5G secure IoT?

Can 5G secure IoT?

IoT Security threat landscape (non-exhaustive overview of threats)





Impact depends on IoT application

confidentiality, privacy, reliability, availability, etc.

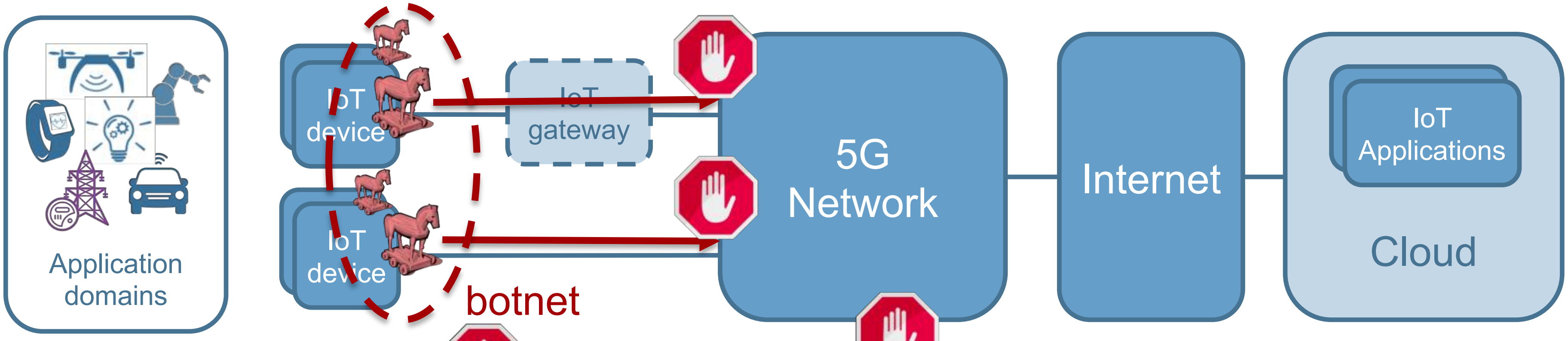
- Attacks on IoT device (take control)
- Build botnet to attack other systems

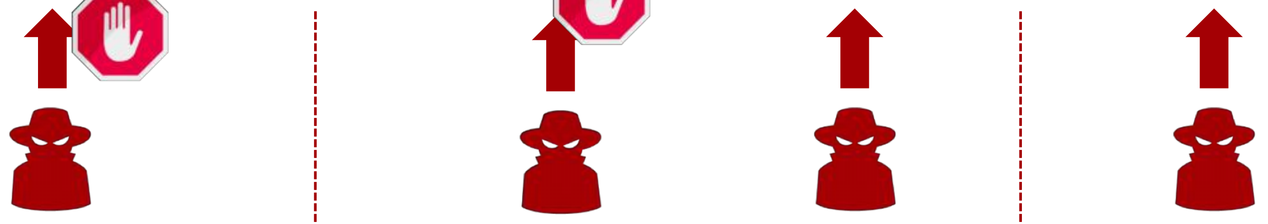
- Attacks on network (eavesdrop communication, inject or manipulate data, etc.)
- Denial of service (e.g. jamming)

- Attacks on IoT application (take control, steal large amount of IoT data)

5G can increase security of IoT, but …

… 5G is not the panacea for IoT security.





Impact depends on IoT application

confidentiality, privacy, reliability, availability, etc.

- Attacks on IoT device (take control)
- Build botnet to attack other systems

- Attacks on network (eavesdrop communication, inject or manipulate data, etc.)
- Denial of service (e.g. jamming)

- Attacks on IoT application (take control, steal large amount of IoT data)

QUESTIONS

Frank Fransen
+31 6 53 72 49 00
frank.fransen@tno.nl

THANK YOU FOR YOUR ATTENTION

Take a look:
TIME.TNO.NL

TNO innovation for life