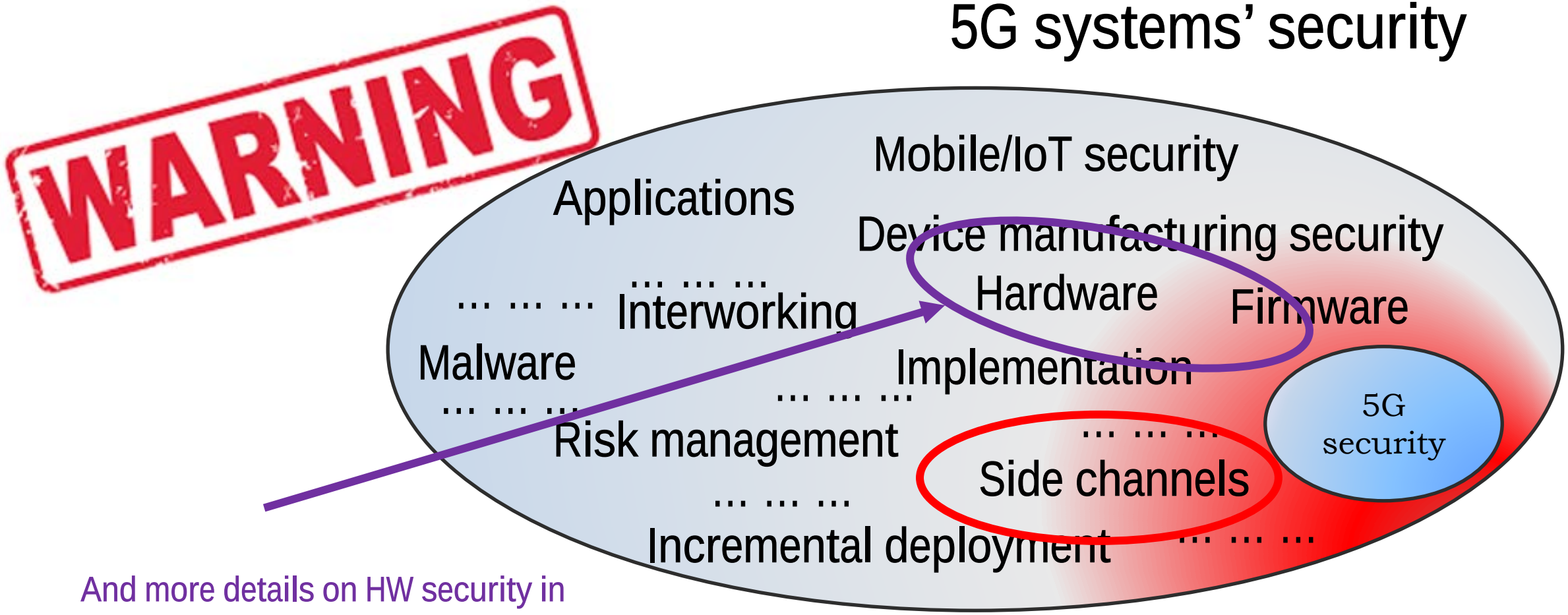
5G Security and Privacy

Giuseppe Bianchi

ISCOM, 28 ottobre 2020

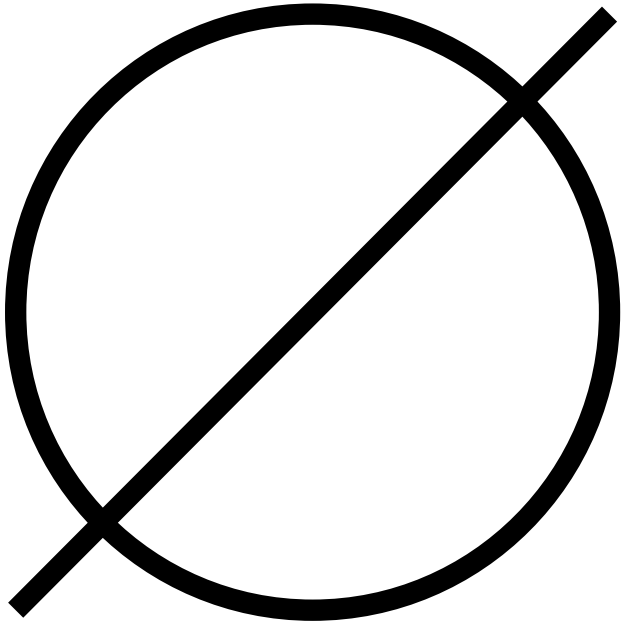
My presentation's main focus: 5G systems' security



And more details on HW security in a dedicated presentation later on

With some hints on modern side channels…

Security in 1G



Security in 2G

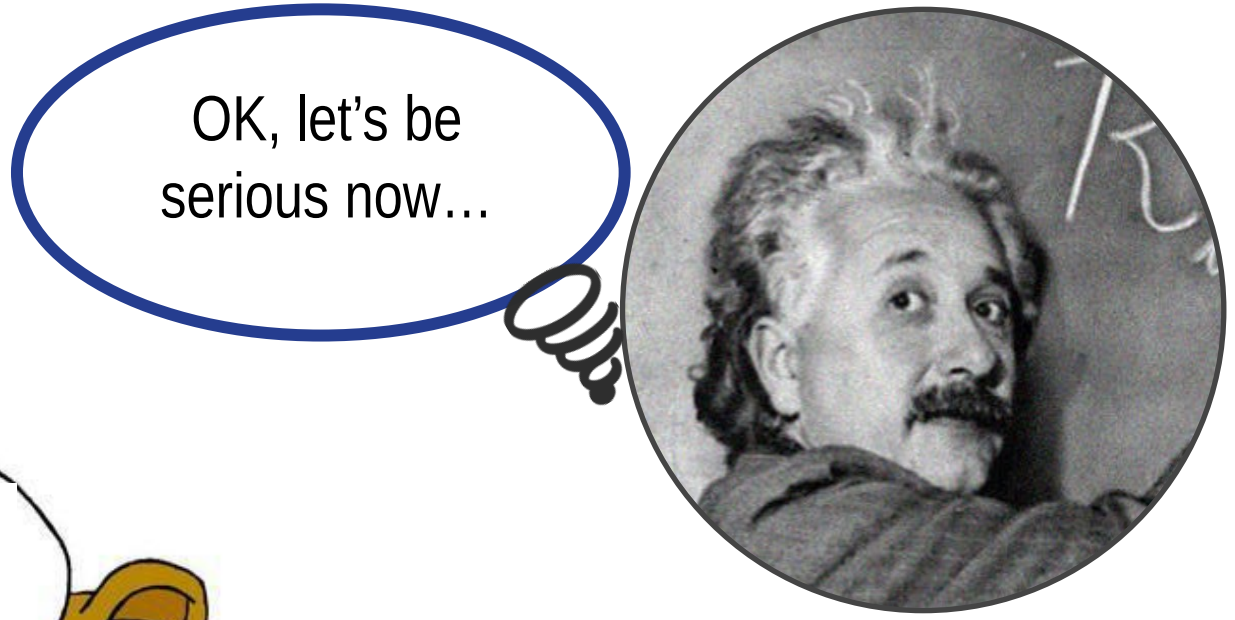
Security? No problem!
Let me do it!!

COMP-128 Security by obscurity

No mutual auth (Rogue BS)

No core network security

Security in 3G



(fairly) good ciphers - public scrutiny!

Encryption AND (in part) Integrity

Multual authentication

Core network security

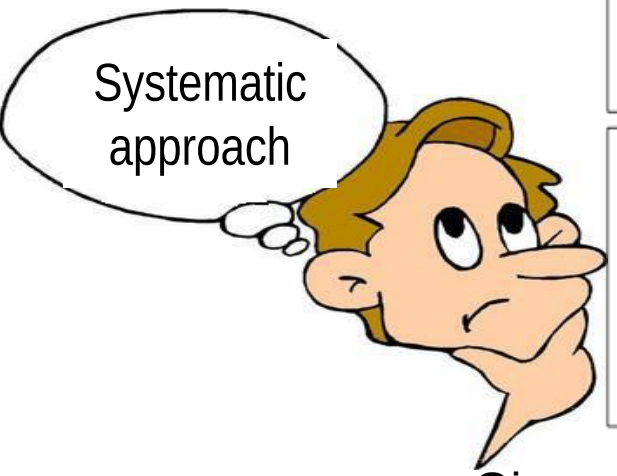
Multiple keys

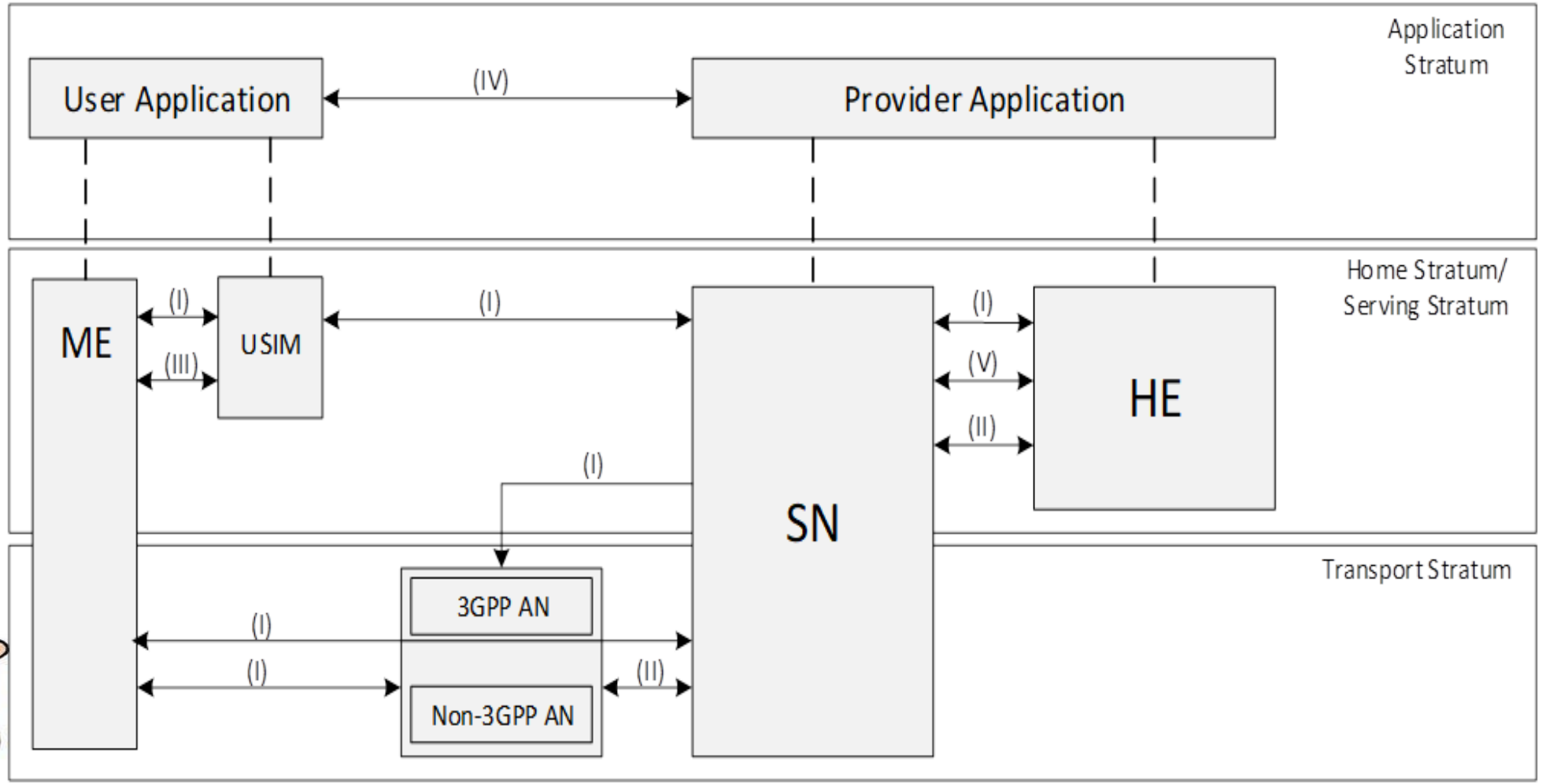
. . . . . .

Security in 4G

Time for a Security architecture!

Systematic approach



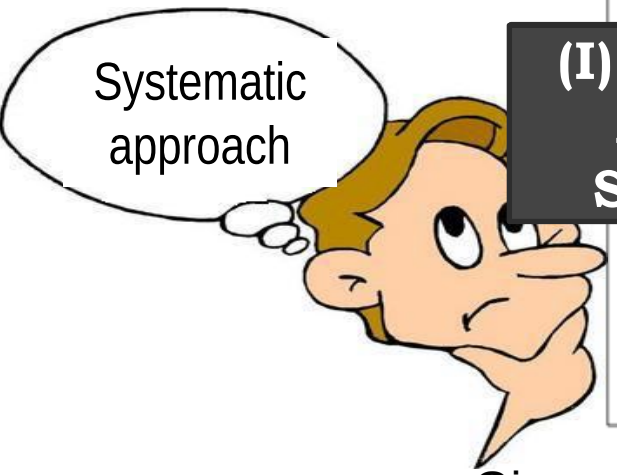


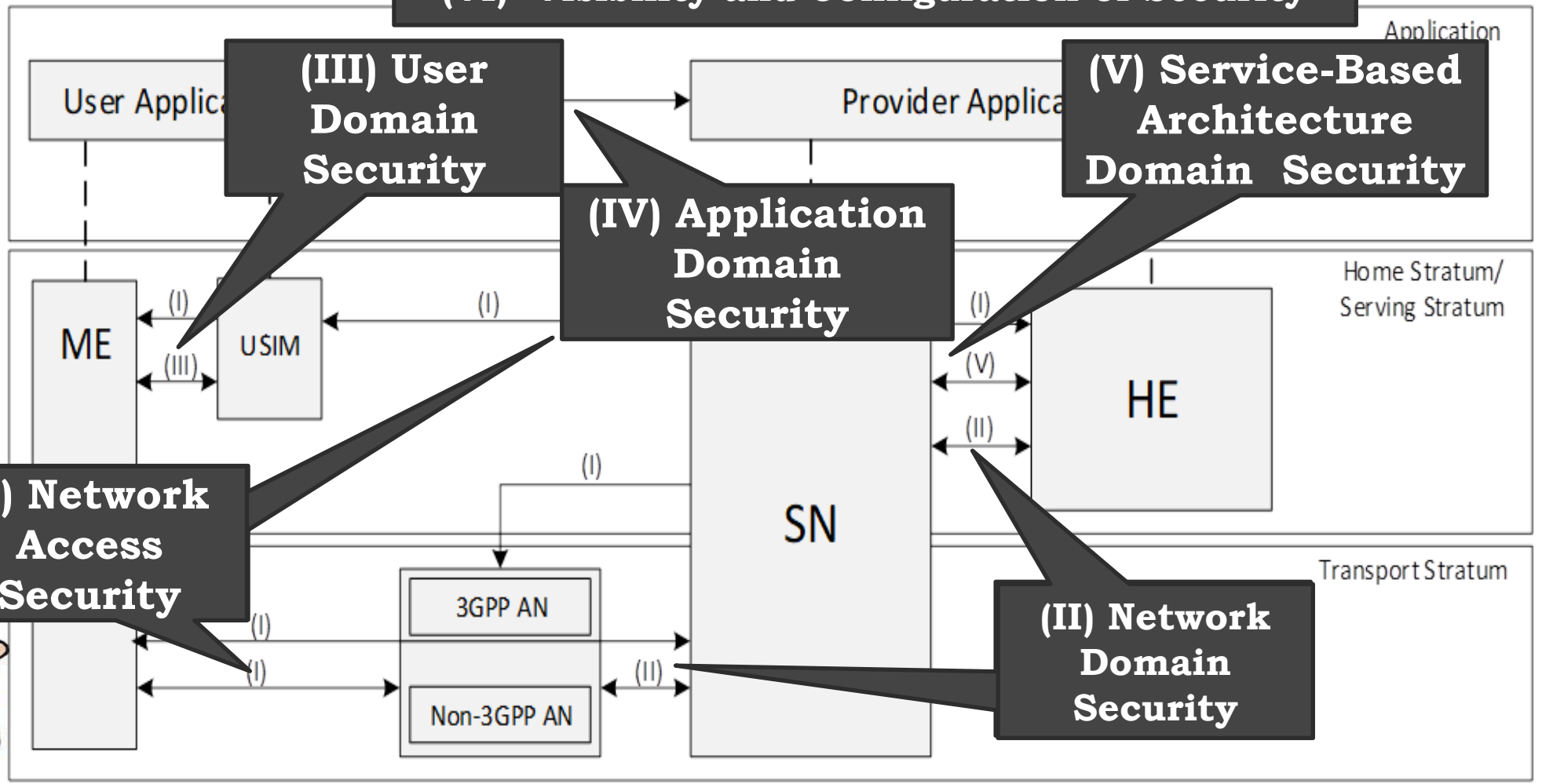
Security in 4G and 5G

Actually… this is already the 5G security architecture… to save one slide (couple of differences over 4G)!

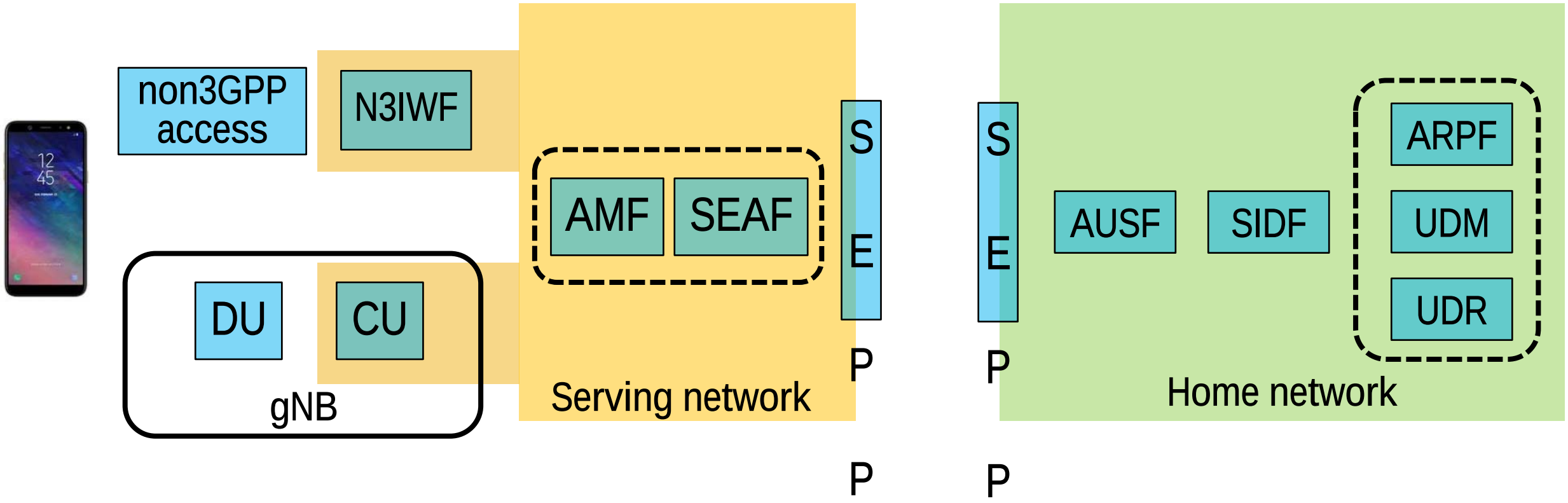
Time for a Security architecture!

Systematic approach





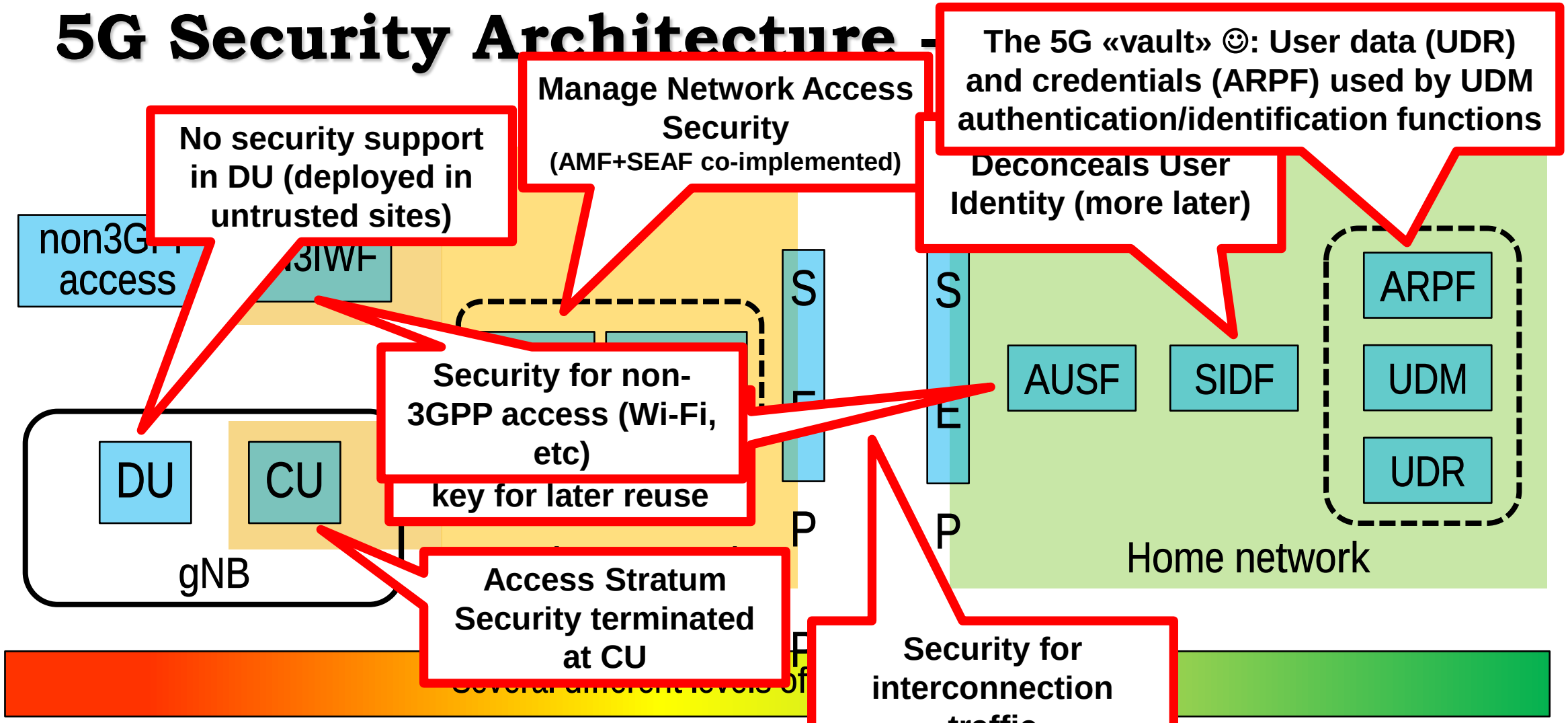
5G Security Architecture - Components



DU	Distributed Unit	AMF	Access Management Function
CU	Central Unit	SEAF	SEcurity Anchor Function
N3IWF	Non 3GPP Inter Working Function	SEPP	Security Edge Protection Proxy

AUSF	AUthentication Server Function
SIDF	Subscription Identifier Deconcealment Fct
ARPF	Auth credential Repository & Processing Fct
UDM	Unified Data Management
UDR	Unified Data Repository

5G Security Architecture -

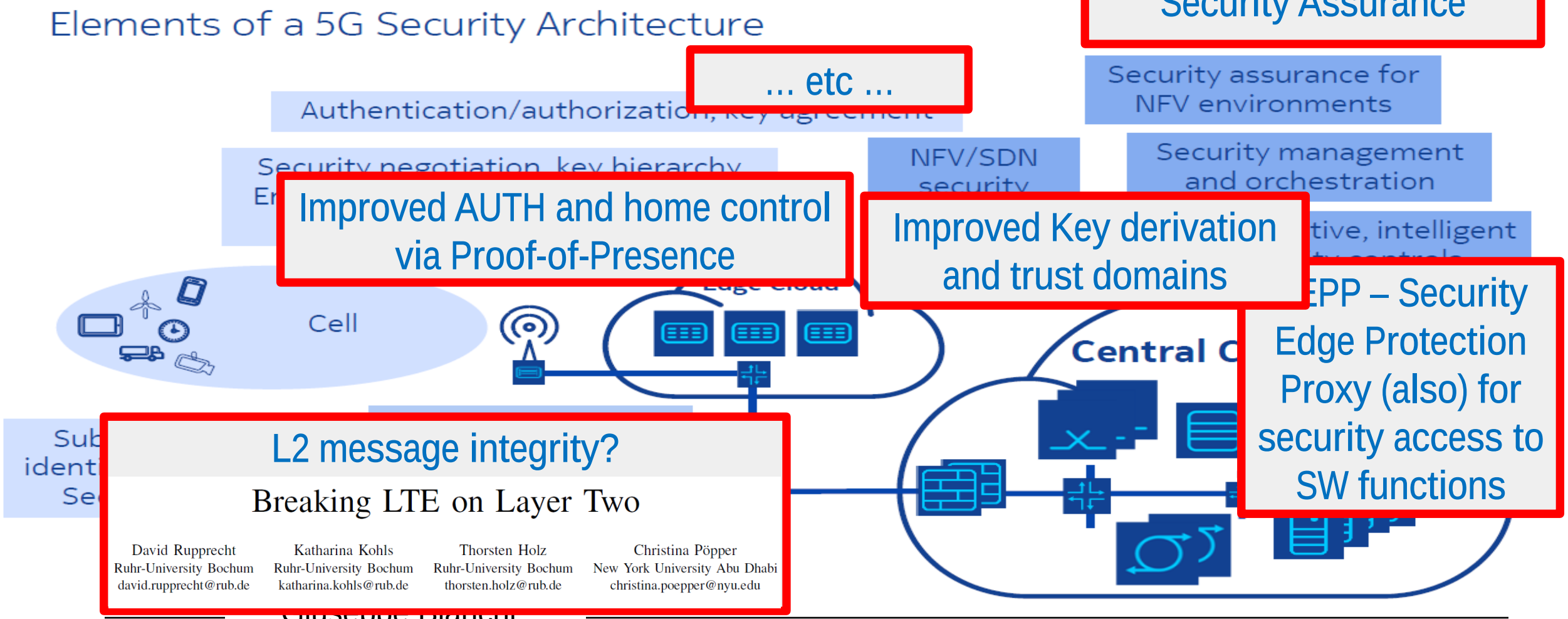


DU	Distributed Unit	AMF	Access Management Function	AUSF	Authentication Server Function
CU	Central Unit	SEAF	SEcurity Anchor Function	SIDF	Subscription Identifier Deconcealment Fct
				ARPF	Auth credential Repository & Processing Fct
N3IWF	Non 3GPP Inter Working Function	SEPP	Security Edge Protection Proxy	UDM	Unified Data Management
				UDR	Unified Data Repository

Security in 5G: evolution?

Many (small and not-so small) tailored/chirurgic

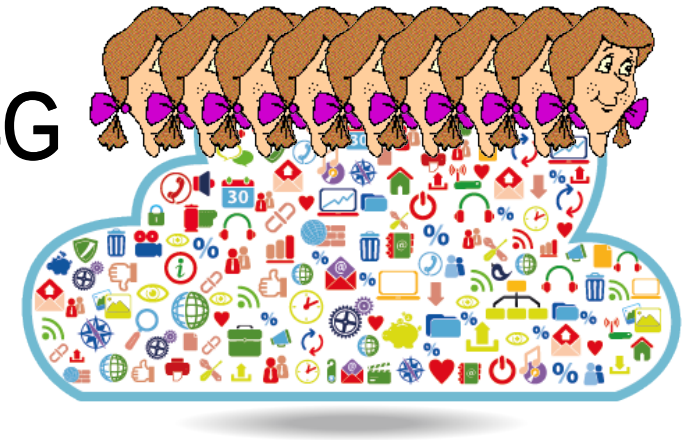
Test Framework SCAS for Security Assurance



Source: Nokia Bell labs, P. Schneider, 2018

Security in 5G: evolution?

Unified Flexible Authentication



Heterogeneous devices
different verticals

⇨ FLEX SEC

4G	5G
EPS-AKA	5G-AKA
	EAP-AKA'
	EAP-TLS?
	Unauthenticated (PARLOS)?

And a couple of (relatively) new pillars!

Ultimate solution to Subscribers' Privacy

IMSI CATCHERS?

5G: NO MORE IMSI (SUPI)
Transmission in clear!
Not even at 1st ever registration!

⇩

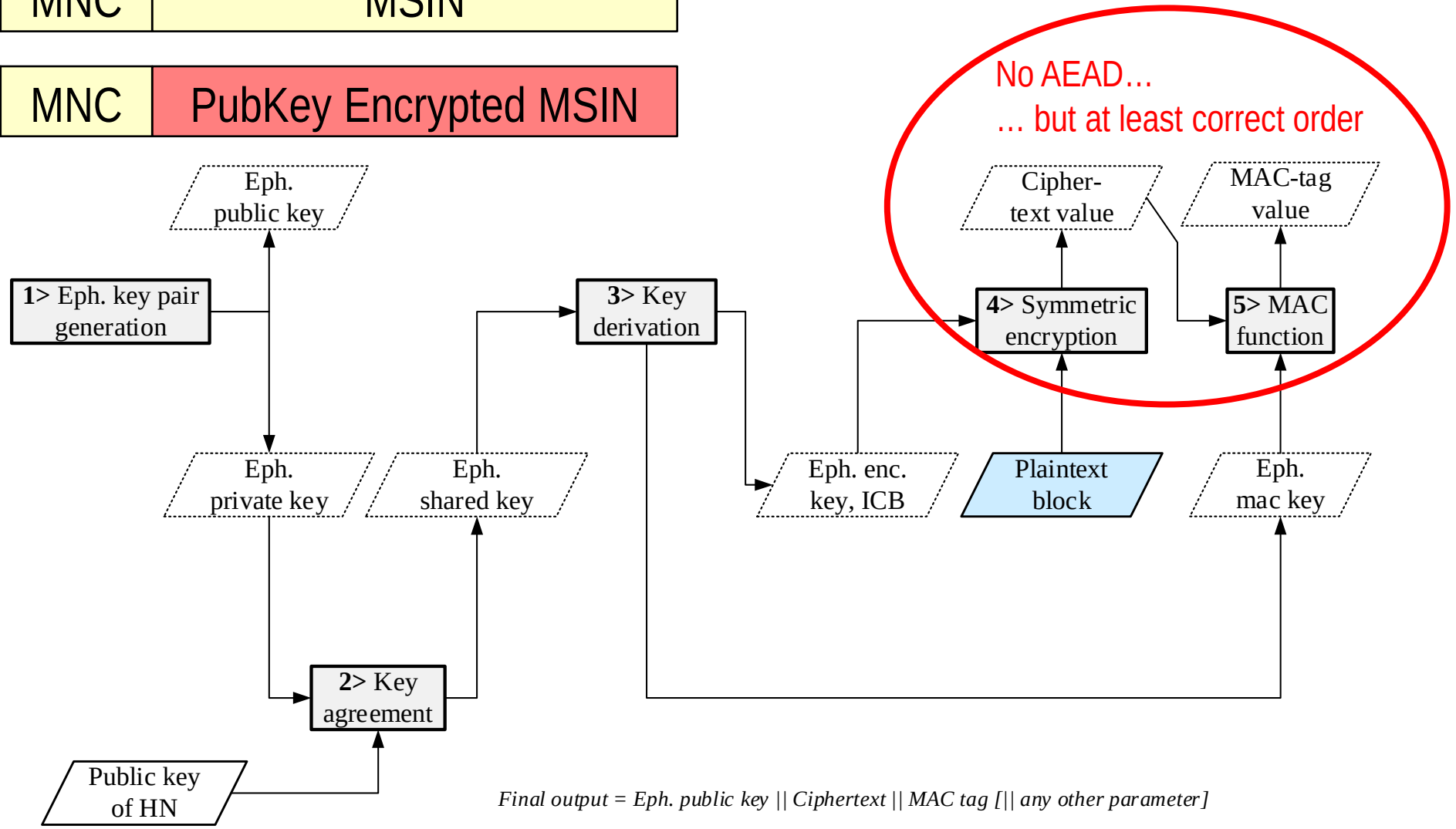
SUCI = Public key (ECIES) encryption of SUPI

SUCI: Public Key's first ever in cellular!

SUPI/IMSI: | MCC | MNC | MSIN |

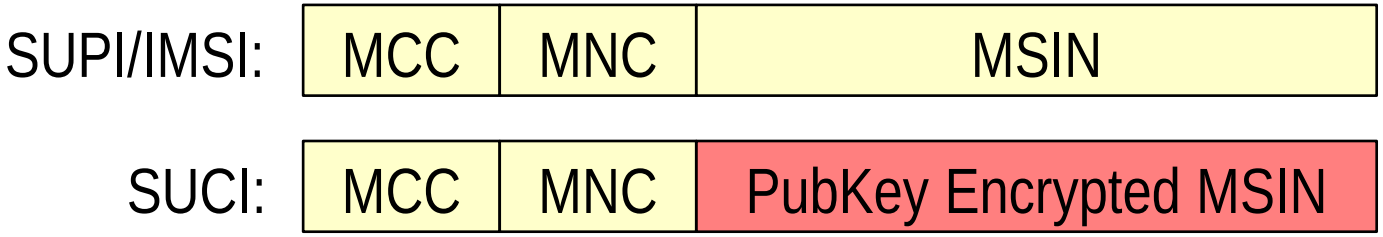
SUCI: | MCC | MNC | PubKey Encrypted MSIN |

ECIES: Elliptic Curve Integrated Encryption Scheme

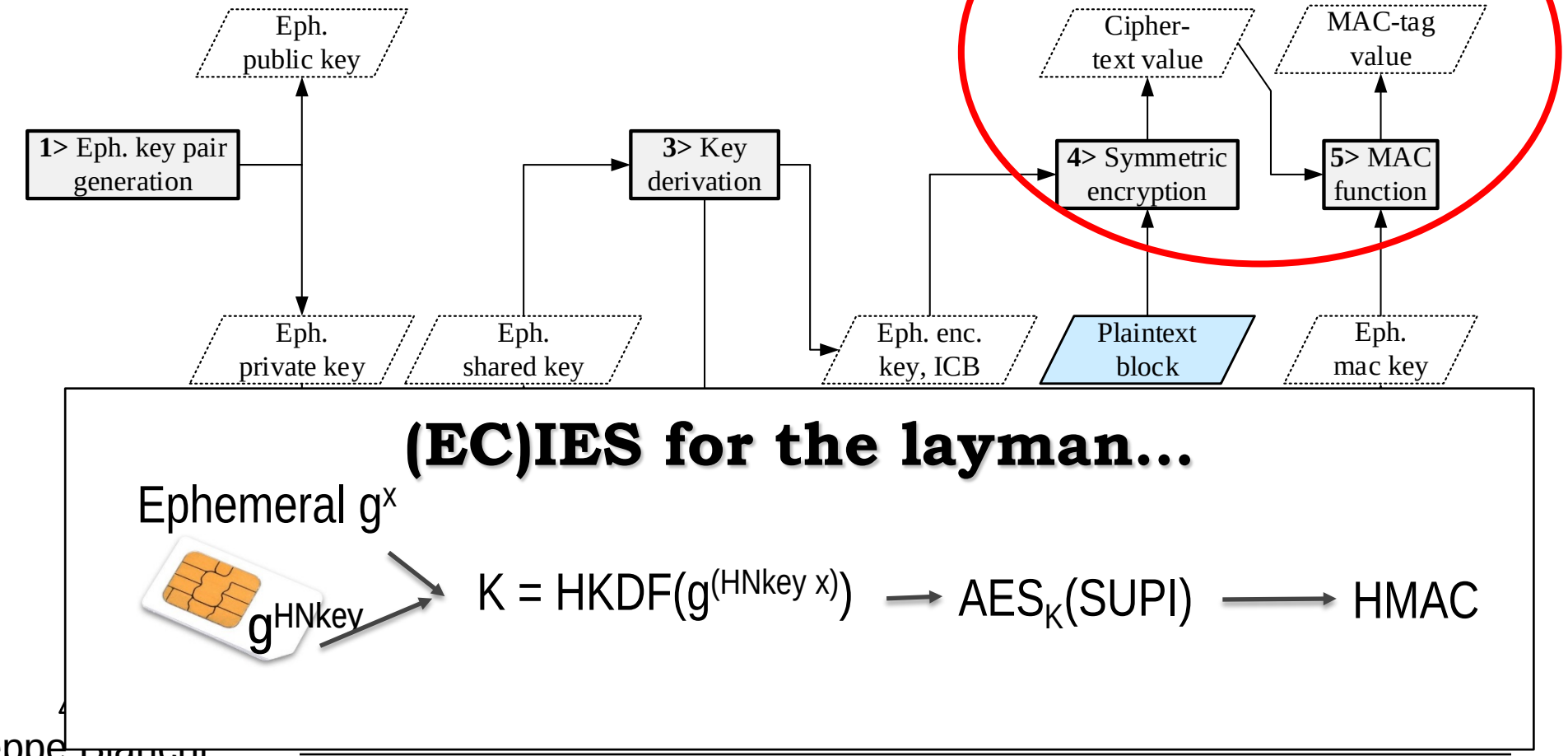


Final output = Eph. public key || Ciphertext || MAC tag [|| any other parameter]

SUCI: Public Key's first ever in cellular!



ECIES:
Elliptic Curve
Integrated
Encryption
Scheme



So, did 5G solve location privacy for good?

⇨5G identity concealment (SUCI):

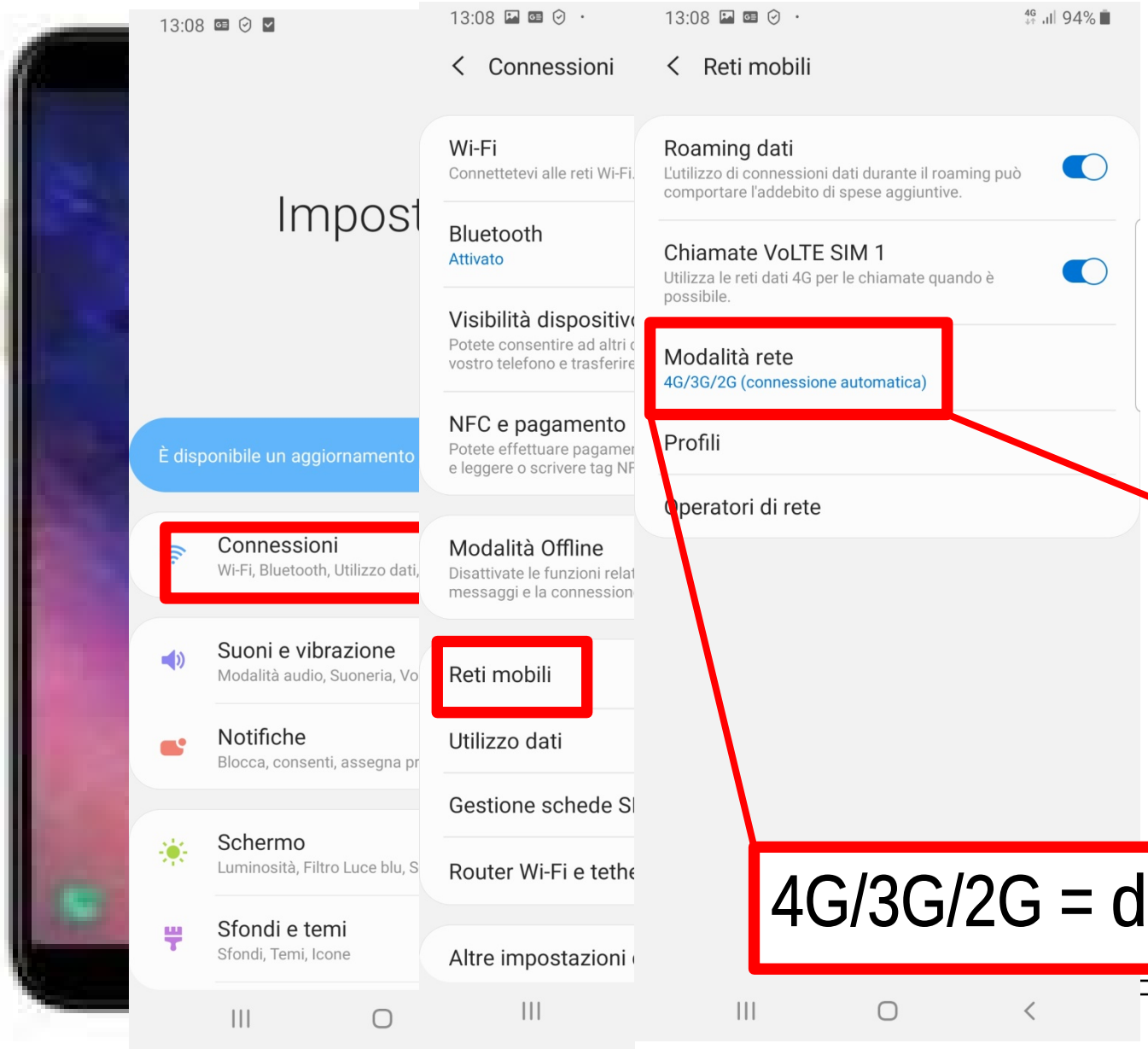
⇨ Optional

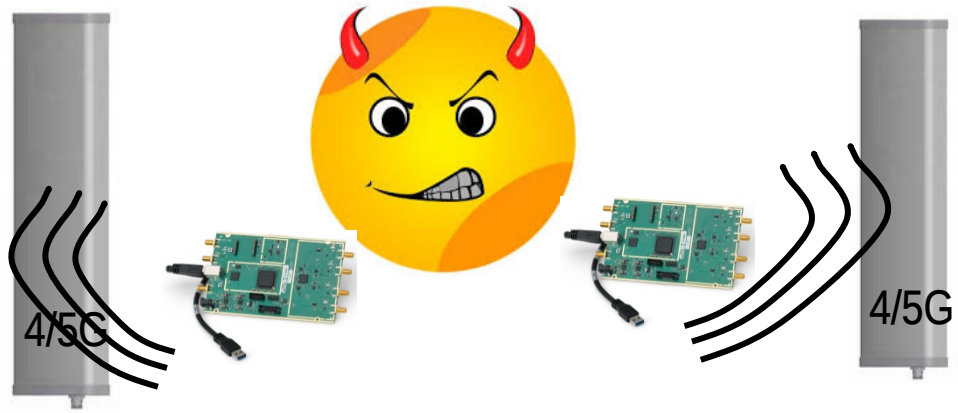
» Catchers can use 4G techniques

– Easy & cheap!!
we'll see this in a few minutes!

⇨What if attacker performs downgrade attack?

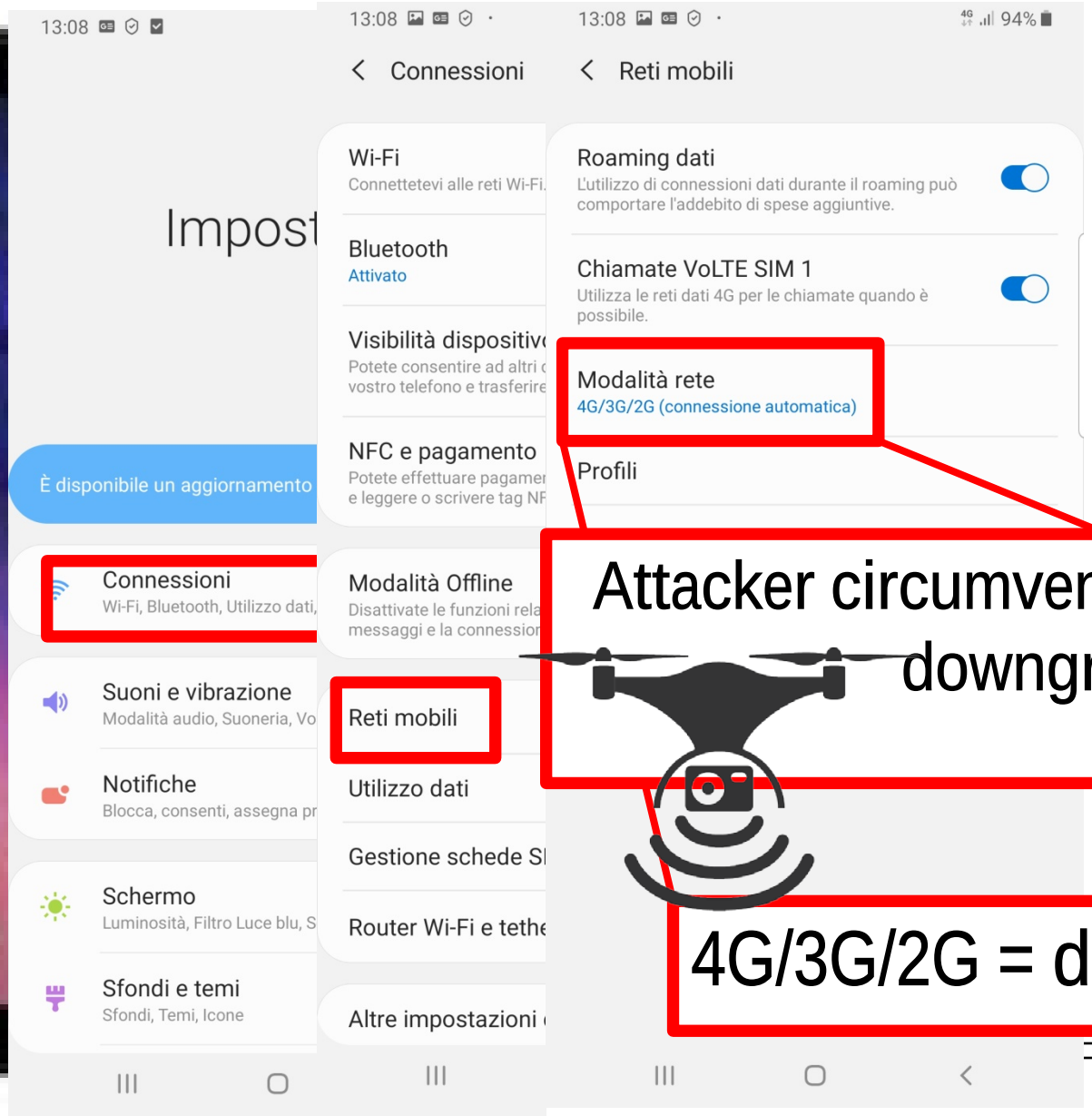
Downgrade?





4G/3G/2G = downgrade *if no better signal*

Downgrade?



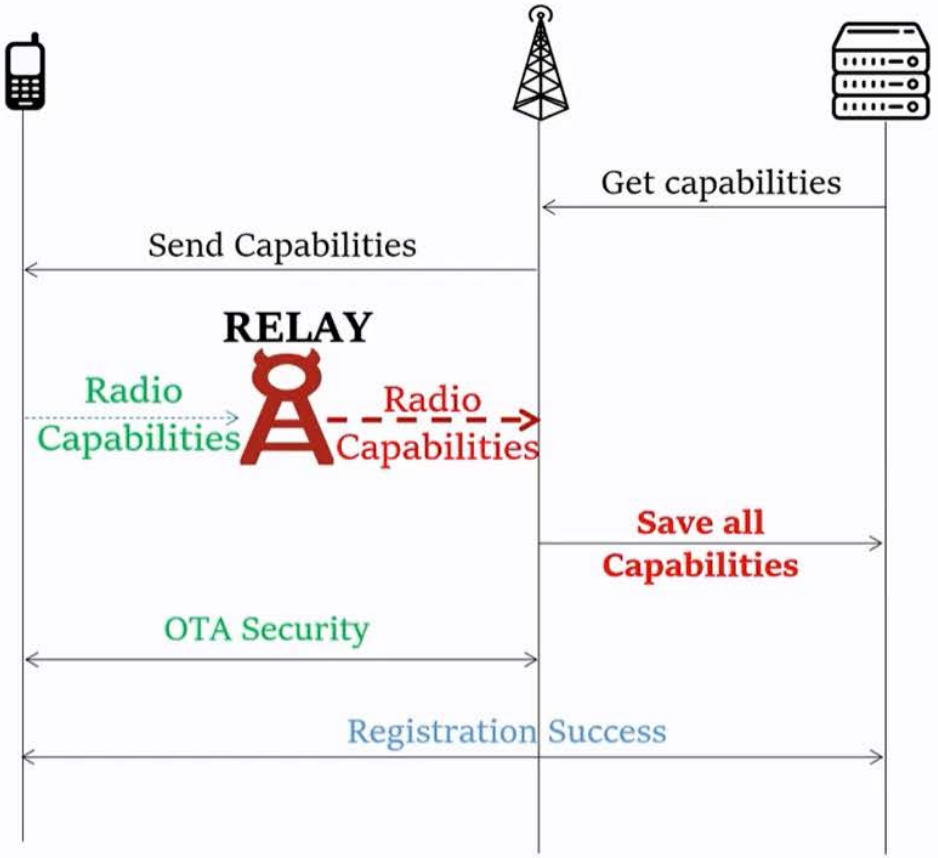
Attacker circumvents 4/5G protections by downgrading you!

4G/3G/2G = downgrade *if no better signal*

… and what about in-protocol downgrades (bid down attacks)?

2. Bidding down

- Hijacking
  - Radio Capabilities
  - MitM relay before OTA Security
  - Network/Phone cannot detect



New Vulnerabilities in 5G Networks

Altaf Shaik
(Technische Universität Berlin, Germany)
Ravishankar Borgaonkar
(SINTEF Digital, Norway)

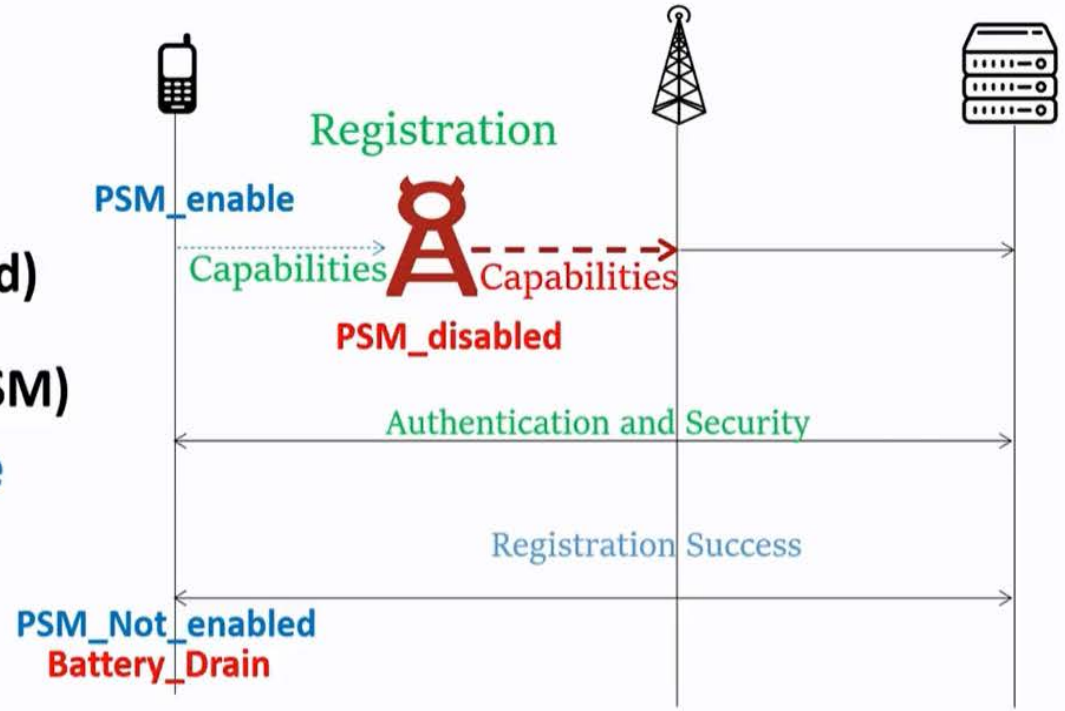
Blackhat 2019. USA

Source:
Altaf Shaik
HITB GSEC 2019

… and what about in-protocol downgrades (bid down attacks)?

3. Battery Drain

- **NB-IoT** (Narrow Band)
- Power Saving Mode (PSM)
  - OFF when not in use



New Vulnerabilities in 5G Networks

Altaf Shaik
(Technische Universität Berlin, Germany)
Ravishankar Borgaonkar
(SINTEF Digital, Norway)

Blackhat 2019. USA

Source:
Altaf Shaik
HITB GSEC 2019

Actually, corrected in Rel15 thanks to Shaik's paper, so 5G is not vulnerable anymore to this specific attack

Four questions

➔**To what extent such vulnerabilities are exploitable using off-the-shelf low-cost SDRs?**

➔**How «easy/hard/practical» are such attacks?**

➔**How different devices behave when attackers try to disclose your persistent identity?**

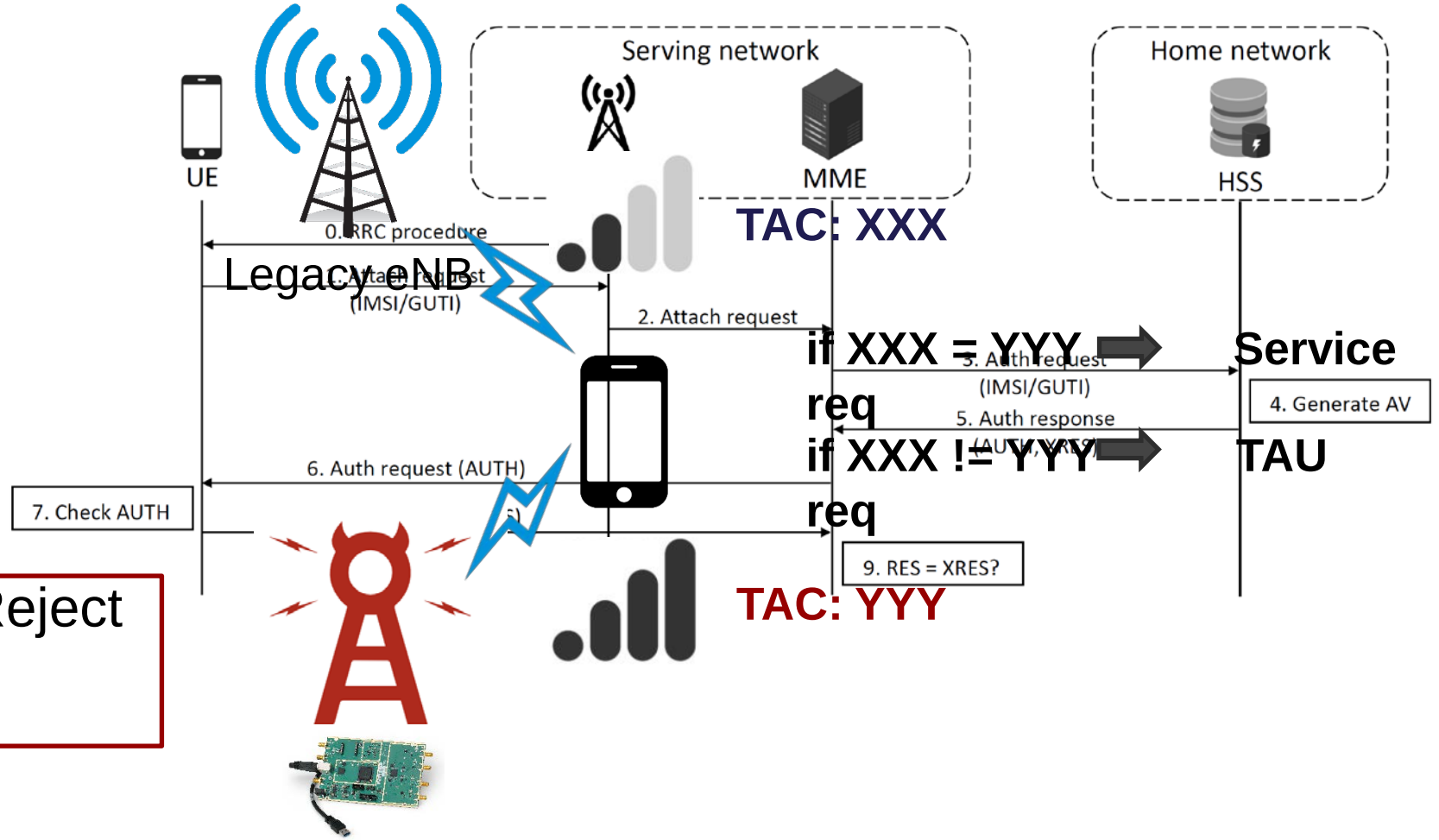
➔**Are current 5G-NSA real world deployments more robust than 4G?**

Our answer: let's see whether we can develop an IMSI catcher with no specialized equipments!

Vulnerability of 4G+ AUTH (chosen trade-off)

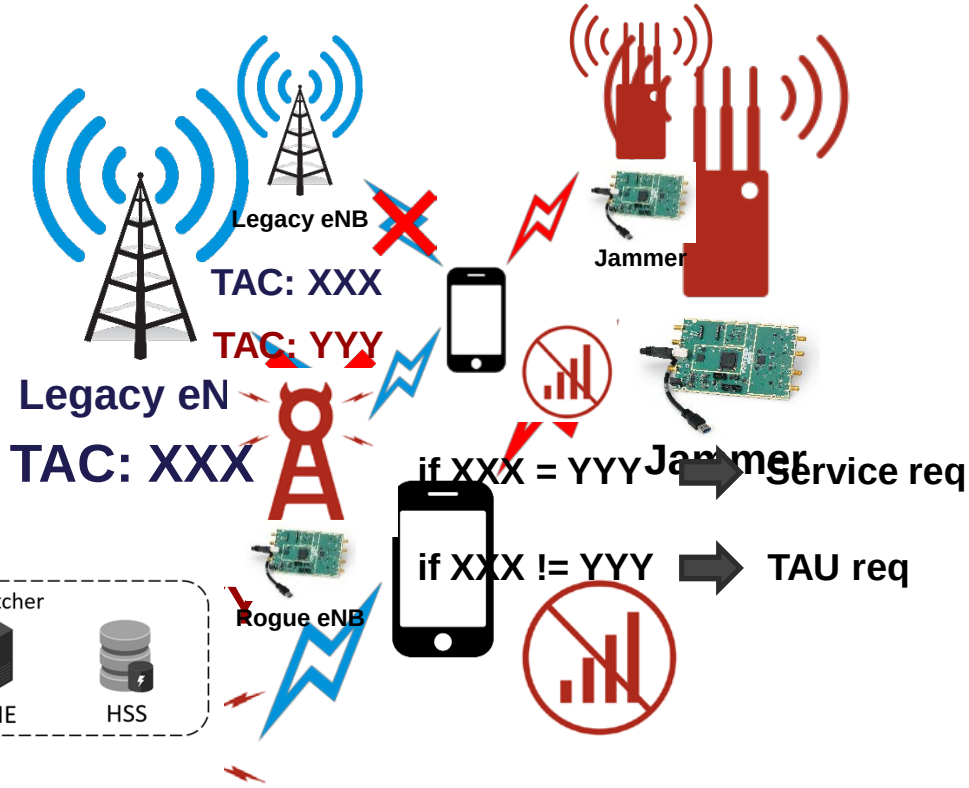
NO signalling msg protection before security mode command

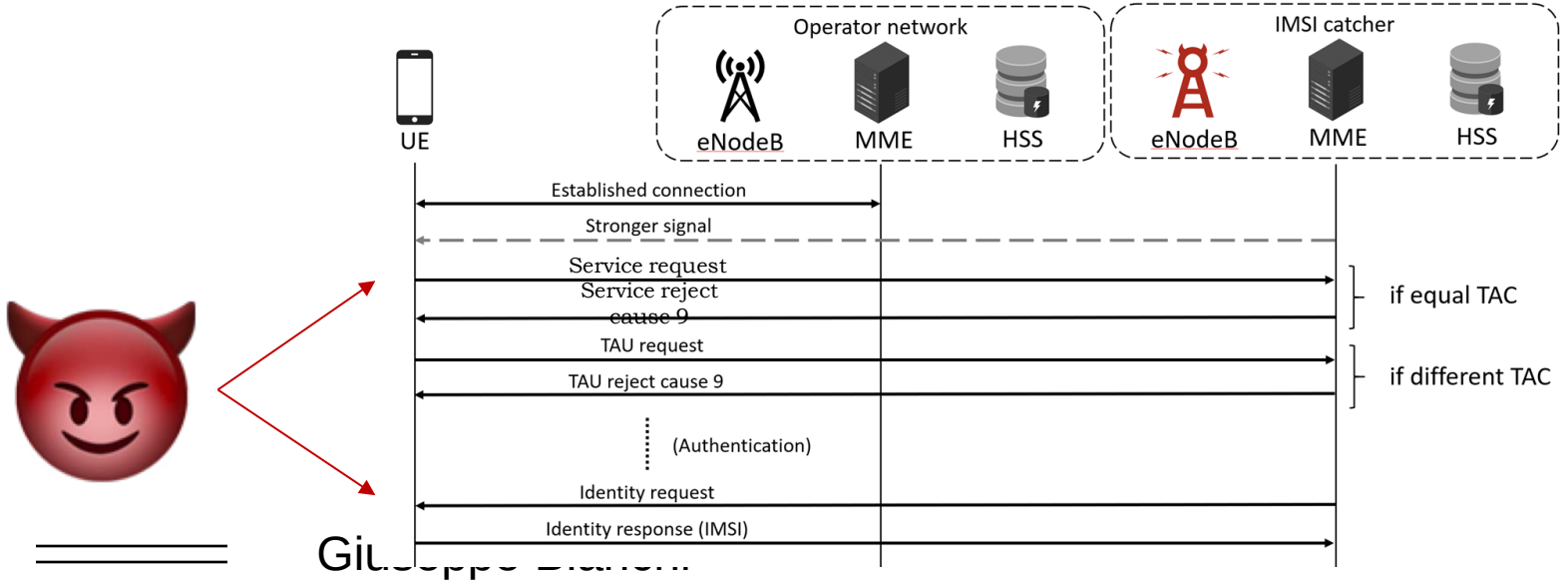
- Identity Request
- Authentication Request
- Authentication Reject
- Attach Reject
- Detach Accept
- Tracking Area Update Reject
- Service Reject



Technical approach at a glance: two logical steps

- Jammer forces UE to perform a cell reselection, so as to select… our rogue BS (the IMSI catcher!)
- UE performs a **Service/TAU request** to the IMSI catcher that exploits an **Identity request** to steal **IMSI**





From theory to practice: a few non trivial details to take care of…

Rogue LTE eNB (network)

- MCC (Mobile Country Code) and the MNC (Mobile Network Code)
- Cell ID
- Tracking Area Code (TAC)
- Inter-frequency cell reselection priorities

SIB5

```
<BCCH-DL-SCH-Message>
 <message>
  <systemInformationBlockType1>
   ...
    <PLMN-IdentityList>
     <plmn-Identity>
      <mcc>
       <MCC-MNCDigit>2</MCC-MNCDigit>
       <MCC-MNCDigit>2</MCC-MNCDigit>
       <MCC-MNCDigit>2</MCC-MNCDigit>
      </mcc>
      <mnc>
       <MCC-MNCDigit>8</MCC-MNCDigit>
       <MCC-MNCDigit>1</MCC-MNCDigit>
      </mnc>
      ...
     <trackingAreaCode>0111011100111000</trackingAreaCode>
     <cellIdentity>01001101001101111100000000001</cellIdentity>
      ...
     <si-Periodicity>
      <rf16/>
     </si-Periodicity>
     <sib-MappingInfo>
      <sibType3/>
      <sibType5/>
     </sib-MappingInfo>
     <sibType3/>
     <sibType5/>
     ...
    <si-WindowLength>
     <ms20/>
    </si-WindowLength>
  </message>
</BCCH-DL-SCH-Message>
```

SIB1

```
<interFreqCarrierFreqList>
 <dl-CarrierFreq>3350</dl-CarrierFreq>
 <cellReselectionPriority>7</cellReselectionPriority>
 <dl-CarrierFreq>6200</dl-CarrierFreq>
 <cellReselectionPriority>5</cellReselectionPriority>
 <dl-CarrierFreq>150</dl-CarrierFreq>
 <cellReselectionPriority>5</cellReselectionPriority>
 <dl-CarrierFreq>1675</dl-CarrierFreq>
 <cellReselectionPriority>6</cellReselectionPriority>
 <dl-CarrierFreq>1500</dl-CarrierFreq>
 <cellReselectionPriority>1</cellReselectionPriority>
 <dl-CarrierFreq>2900</dl-CarrierFreq>
 <cellReselectionPriority>1</cellReselectionPriority>
</interFreqCarrierFreqList>
<SchedulingInfo>
 <si-Periodicity>
  <rf16/>
 </si-Periodicity>
 <sib-MappingInfo>
  <sibType3/>
  <sibType5/>
 </sib-MappingInfo>
</SchedulingInfo>
<si-WindowLength>
 <ms20/>
</si-WindowLength>
```

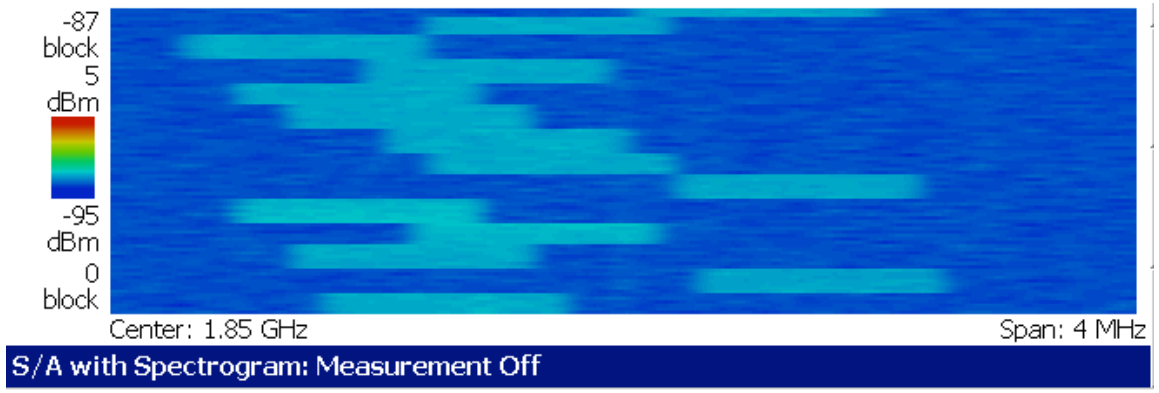
Network monitoring tool
SDR LTE sniffer (SRSLTE)

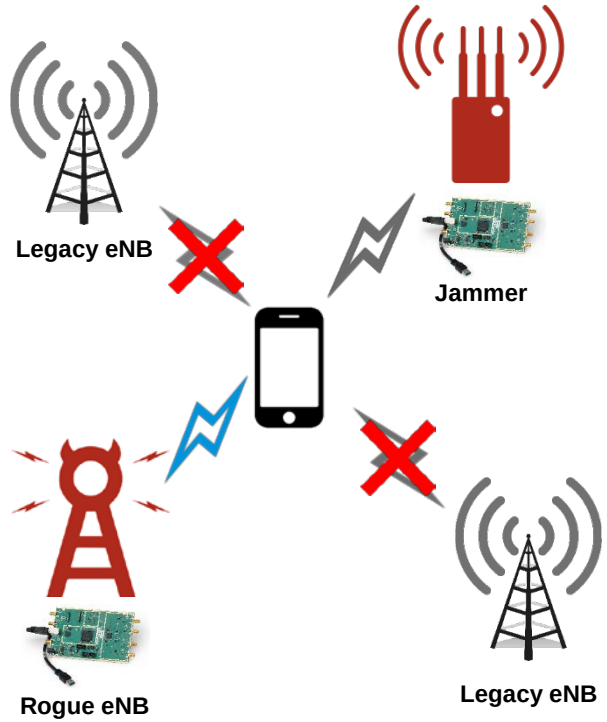
From theory to practice: a few non trivial details to take care of...

How to low-cost Jam with a single SDR

Custom-made Frequency-hopping Jammer!

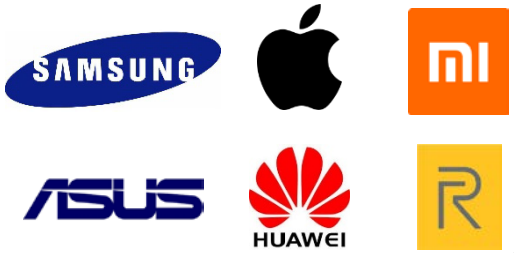
- Exploitation of both tx chain to maximize effectiveness
- inter-channel and intra-channel hopping
  (over Carrier Frequency list gathered from SIB5)
- Exploitation of LTE structure for jamming signal





Once done: extensive assessment campaigns

UE manufacturers



modem manufacturers

network operators

OS and versions

SDR LTE solutions

Attack models

LTE messages

Service Request

TAU Request

Experimental setup

- Off-the-shelf SDRs
  - 2x **USRP B210**
- Open Source Software
  - **OpenAirInterface**
  - **srsLTE**

Cheap instrumentation, free software → affordable to any tech-savvy!

Results & take-home findings

- varying the UE brand
- varying the UE OS
- varying the UE modem
- varying the SDR-based LTE solutions
- varying the attack model
- varying the LTE msg
- varying the network operator

100% of tested brands vulnerable
(though different "breaking" effort)

Model	OS	Modem	LTE C.	Service Request	TAU Request	Service Request	TAU Request	Service Request	TAU Request	Service Request	TAU Request
Samsung Galaxy S9	Android 9	Exynos 9810	18	✓	✓	✓	✓	✓	✓	✓	✓
Samsung Galaxy A7 2018	Android 10	Exynos 7885	12	✓	✓	✓	✓	✓	✓	✓	✓
Samsung Galaxy Note Pro	Android 5	Snapdragon 800	4	✓	✓	✓	✓	✓	✓	✓	✓
Realme X2 Pro	Android 10	Snapdragon X24	20	✓	✓	✓	✓	✓	✓	✓	✓
Realme 6	Android 10	Helio G90T	13	✓	✓	✓	✓	✓	✓	✓	✓
Xiaomi Redr											✓
Xiaomi M											✓
Huawei Ma											✓
Huawei P											✓
Huawei I											✓
Asus Zen											✓
iPhone 11	iOS 13	Intel XMM 7660	18	✗	✗	✓	✓	✗	✗	✓	✓
iPhone XS	iOS 13	Intel XMM 7560	16	✗	✗	✓	✓	✗	✗	✓	✓
iPhone 8	iOS 13	Intel XMM 7480	16	✗	✗	✓	✓	✗	✗	✓	✓
iPhone 7	iOS 13	Intel XMM 7360	9	✗	✓	✓	✓	✗	✓	✓	✓
iPhone SE	iOS 12	Qualcomm MDM9625M	4	✓	✓	✓	✓	✓	✓	✓	✓
iPhone 5S	iOS 12	Qualcomm MDM9615M	3	✓	✓	✓	✓	✓	✓	✓	✓
Huawei E3272 USB Stick	-	HiSilicon Balong						✓	✓	✓	✓
Huawei E392 USB Stick	-	Qualcomm MDM9						✓	✓	✓	✓

✓ : IMSI catched
✗ : IMSI not catched

5G-NSA vulnerable as well
(based on preliminary tests on subset of devices)

iOS vs Android
(iPhone harder to attack)

Tim / Wind3 / Vodafone / Iliad	× OAI / srsLTE	× Service Request / Tracking Area Update Request	× w/o jammer / w/ jammer	= Positive

No operator dependency (as

Lessons learned & what do to next

➔5G will most likely not fix location privacy

⇨SUCI protection still to come… and OPTIONAL (sic!)

➔Some protocol vulnerabilities will hardly be fixed

➔Discussed in 3GPP
but there are **security vs usability vs availability trade-offs**

➔And downgrade attacks are still possible

➔As the result of the need for flexibility and backward compatibility

➔So what?

3GPP battle against Fake BS

➔user-assisted detection of rogue base station.

⇨measurement reports: UE → network

➔include security-related values and use measurements for detection!

➔detection algorithms: left to the implementation

⇨But comprehensive Release 16 study started:

➔TR 33.809, “Study on 5G security enhancements against false base stations”

5G threats? increased attack surface…

➔ **[the new 5G technical features – SDN/NFV, slicing, MEC, etc]** ***will give additional prominence to the complexity of the telecoms supply chain in the security analysis, with various existing or new players, such as integrators, service providers or software vendors, becoming even more involved in the configuration and management of key parts of the network. This is likely to intensify further the reliance of mobile network operators on these third-party suppliers. In addition, the distribution of responsibilities will also become more complex, with the specific challenge that some new players lack familiarity with the mission-critical aspects of telecom networks. This source of risk will become even more important with the advent of network slicing, the differing security requirements per slice and the subsequent increase in attack surface.***

[quote from EU 5G cybersecurity Risk assessment report, 10/2019]

➔ ***And new threaths as well***

⇨ Massive coordinated IoT attacks

→Remember Mirai, 2016?!

→What if IoT botnet controlled by a foreign country?

⇨ Cloud/virtualization vulnerabilities: may play havoc with our softwarization plans!

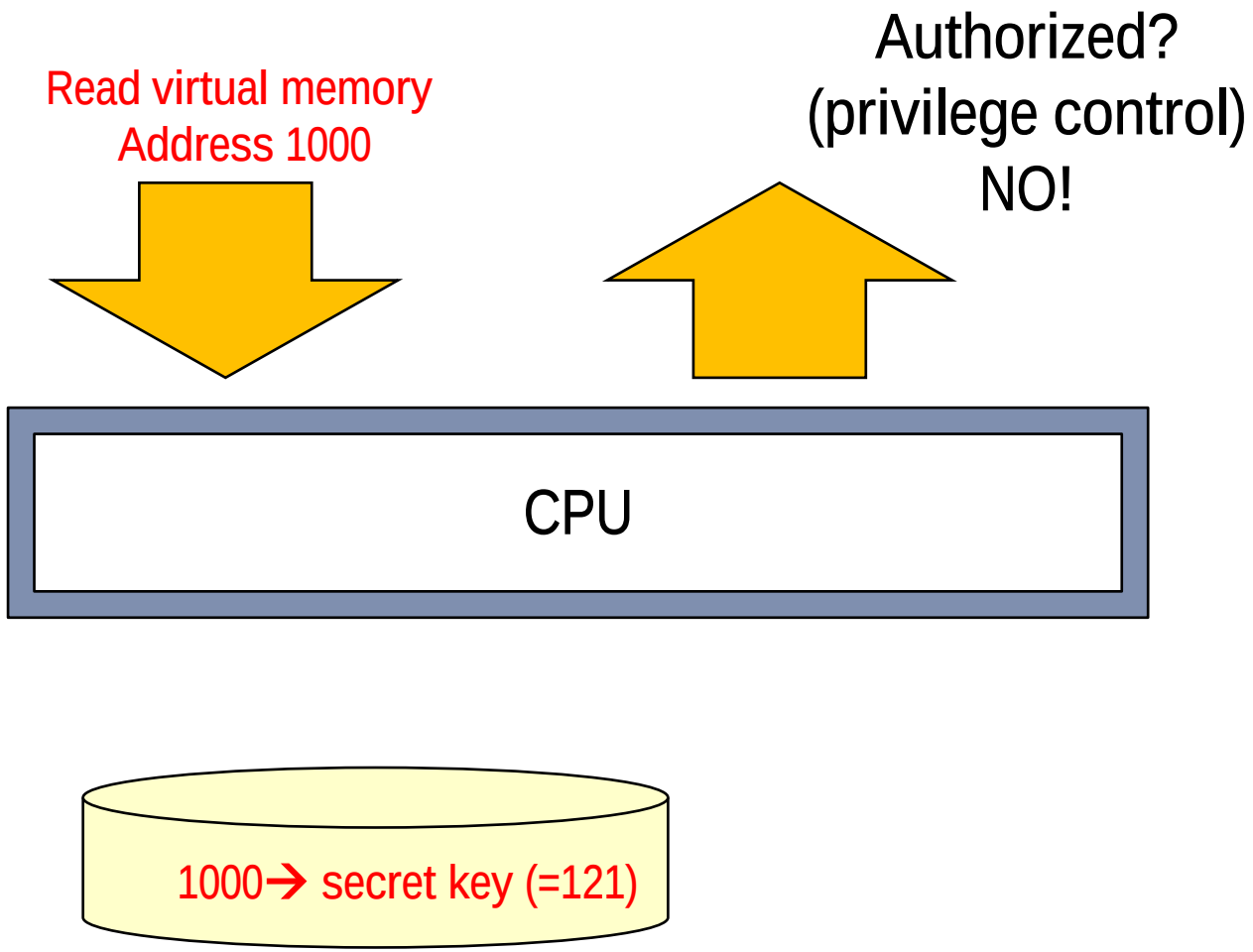
→Spectre, Meltdown, Foreshadow were NOT NEARLY isolated cases!

→A fundamental CPU design issue → transient execution attacks

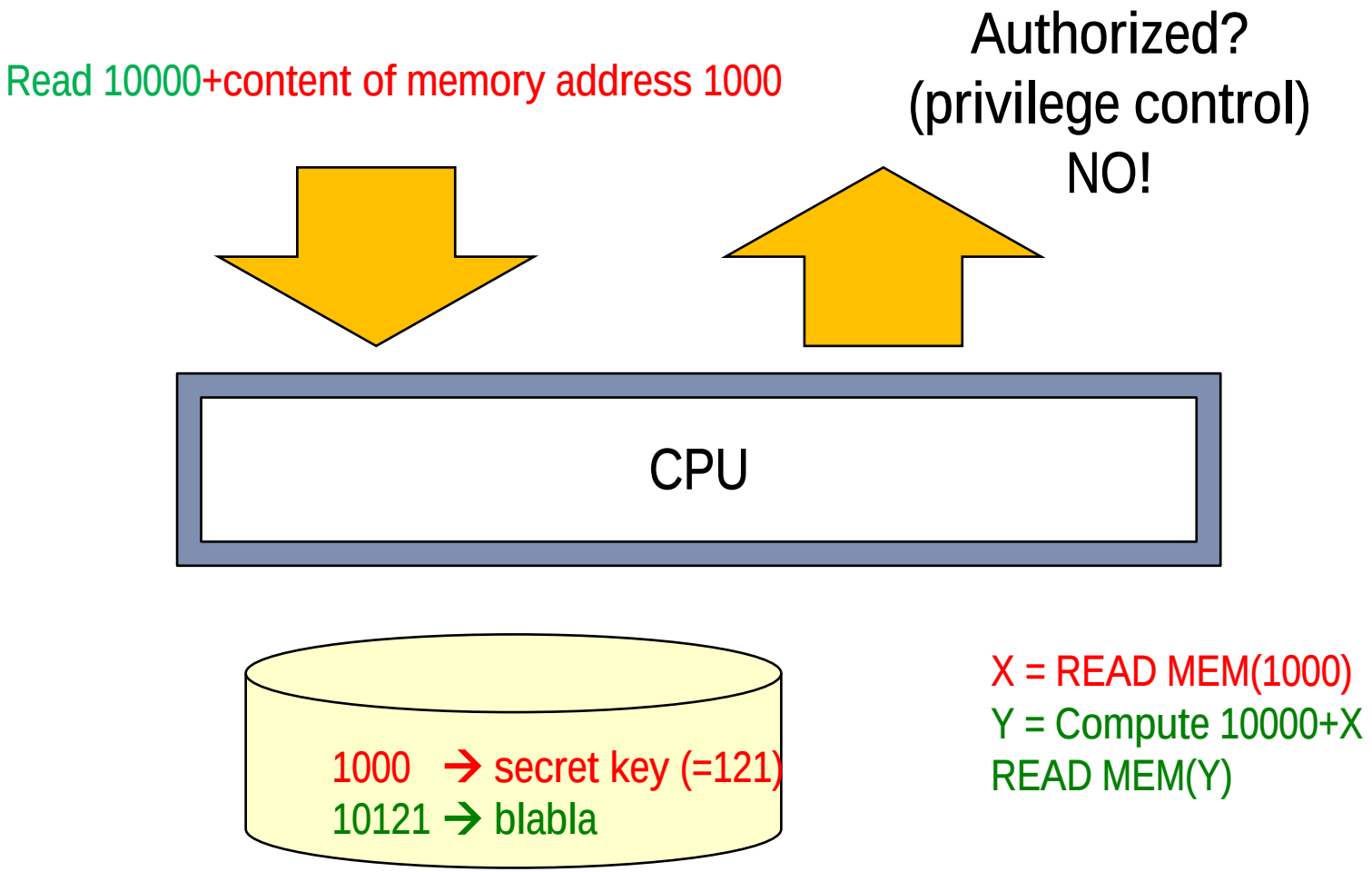
Further technical details in 5G Italy 5G Security & Privacy book chapter

our own foreshadow-VMM demo @ https://www.youtube.com/watch?v=sJuzQP6D9zY

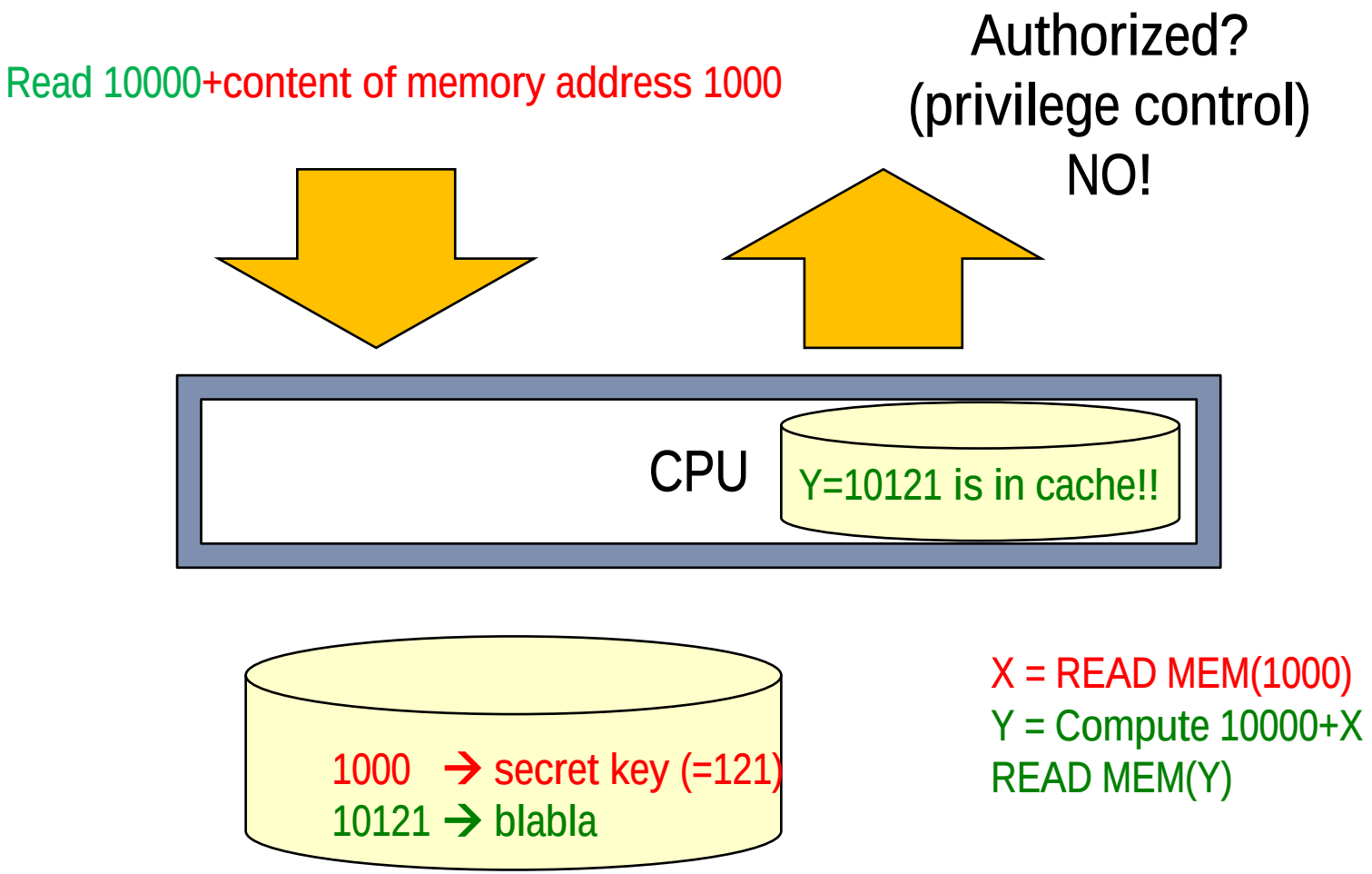
Transient execution attacks: just a sketch (baseline idea of Meltdown)



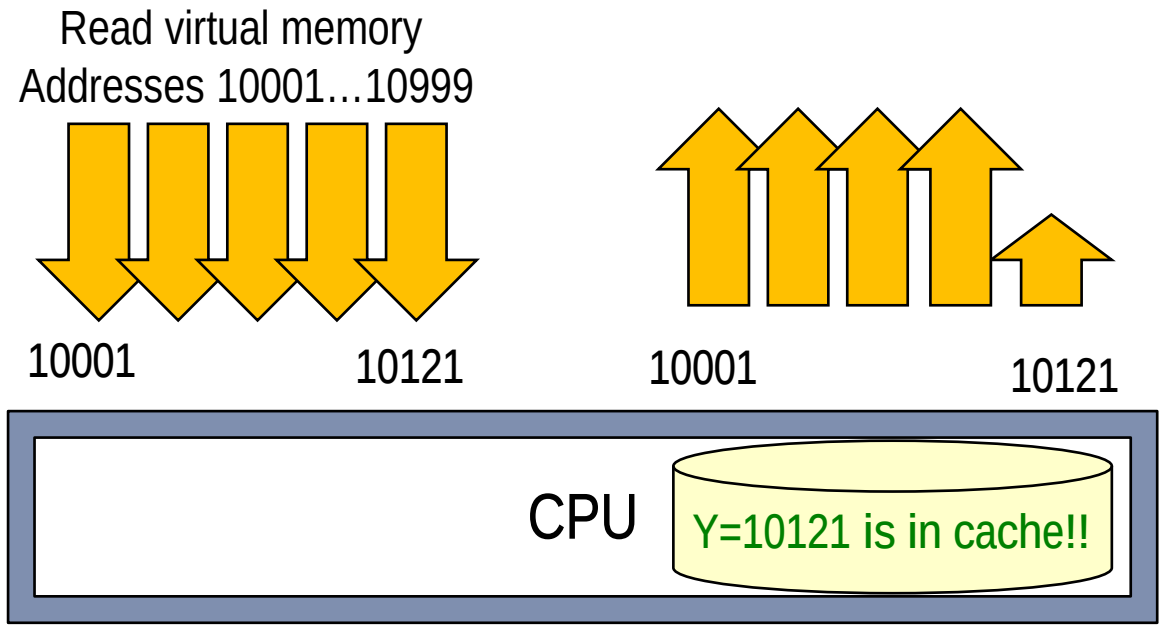
More sophisticated instructions are available

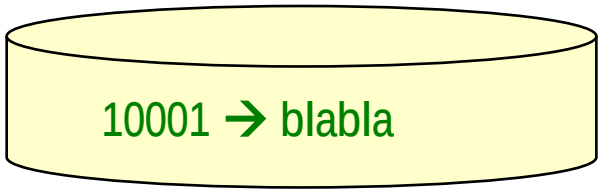


But… CPUs do a lot of caching! (irrespective of privilege management)



We have now a TIME channel!





Slow response: data in main memory

FAST response: data in cache

→ Secret key = 121!!

Today's focus:
5G systems' security only??

Mobile/IoT security

Applications

Device manufacturing security

… … …

… … … Interworking

Hardware

Firmware

Malware

Implementation

… … …

… … … Risk management

5G security

… … …

Side channels

… … …

Incremental deployment

… … …

No 5G security if implementation is insecure!

Assessing implementation security: not nearly easy!

➔**See e.g. ROBOT 2018, Usenix Security (and many, many, other)**

- ⇨Based on very old (1998) RSA vulnerability, corrected in 2000
  - ➔Bleichenbacker Oracle
- ⇨Creative forms of TLS «protocol fuzzying» made it pop up again in major sites
  - ➔Including facebook, Cisco, Radware, etc

Security assurance frameworks

➔**3GPP SCAS**

⇨Under standardization, focus on core network functions

➔**GSMA NESAS**

⇨More general, tilored to Manufacturers

➔**???**

➔**Crucial issue for centers such as CVCN!**

And what about backdoors/bug-doors?

Not nearly a new 5G concern → remember Greek Wiretapping case, 2004/05!

My own 2 cents:

Need for a more open

Vulnerability assessment process!

Thank you! Q&A?