

5G protocol vulnerabilities and exploits

Roger Piqueras Jover
@rgoestotheshows

ABOUT ME

- Things I do...
 - Fatherhood
 - Senior Security Architect in the Office of the CTO at Bloomberg LP
 - Wireless Security Research
 - Soccer, live rock/punk-rock/metal music, geek
- Mobile/wireless security research
 - Started 10 years ago with LTE
 - History of breaking/breaking-into things communicating over 802.11, BLE, ZigBee...
 - 5G security
- Random trivia/achievements
 - Saw every single game live on TV during World Cup 2006 and 2010
 - Seen the band Bad Religion live 22 times
- Very happy to be back at the ShmooCon stage 4 years later!
- More
 - <http://rogerpiquerasjover.net/>



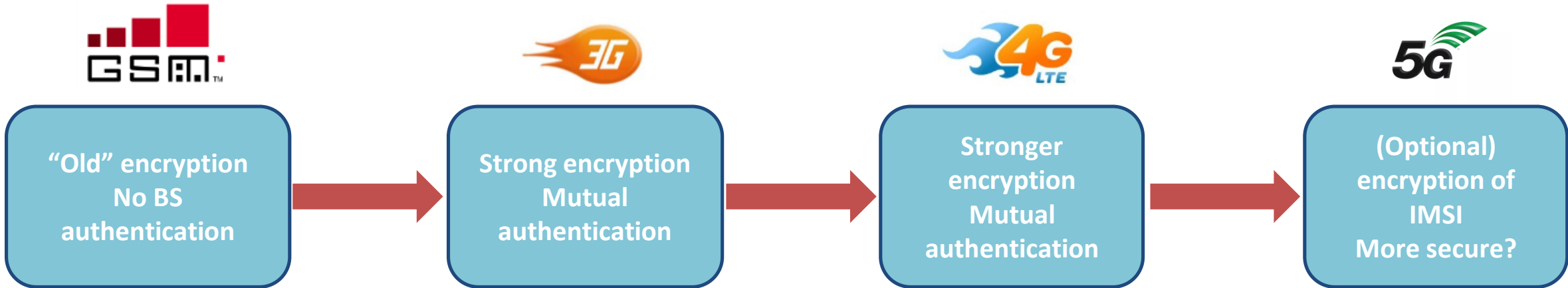
@rgoestotheshows

This work is unrelated to my day job. All opinions and views expressed here are my own.

WHAT AM I GOING TO TALK ABOUT?



MOBILE NETWORK SECURITY RETROSPECTIVE



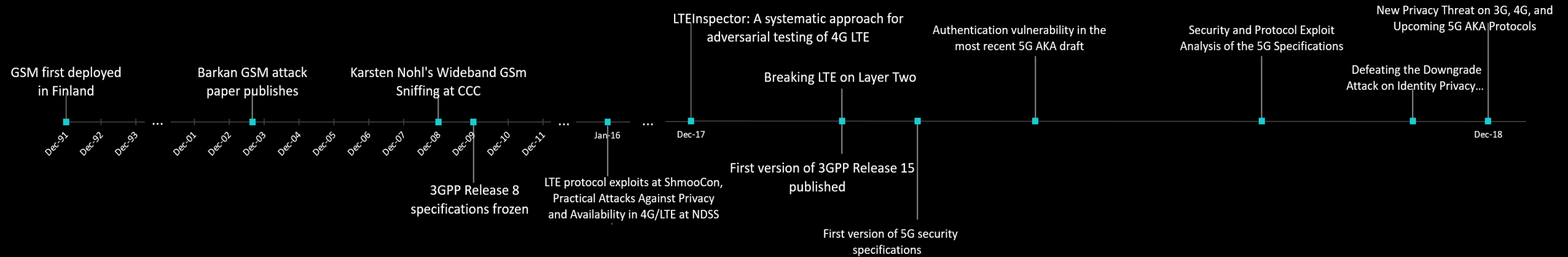
Ask Karsten Nohl and Sylvain Munaut...

Interestingly, research mostly skipped 3G...

Broken in a number of ways. Ask Rabi Borgaonkar, David Rupperecht, Syed Rafiul Hussain, Yongdae Kim, myself...

So much buzz! Has security improved?

MOBILE NETWORK SECURITY RETROSPECTIVE



- GSM
 - Deployment 1991, first crypto attacks 2004, first system attack 2009
 - Osmocombb, OpenBTS, OpenBSC, etc
- LTE
 - Standards 2008, deployment 2012, first system attacks early 2016
 - OpenLTE (12/31/2012), srsLTE (06/15/2015)
 - Lots of excellent research papers over the last 3 years
- 5G
 - Release 15 published 12/2017, 5G security specifications 03/2018, many vulnerabilities found since 2018

SECURITY RESEARCH RAPIDLY MATURING

- Cellular security research ramping up rapidly!



18 years from deployment to first attacks



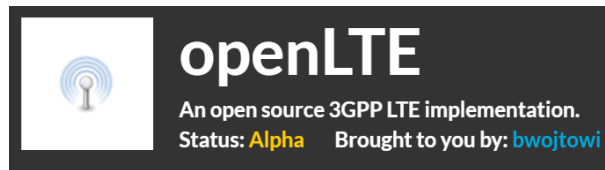
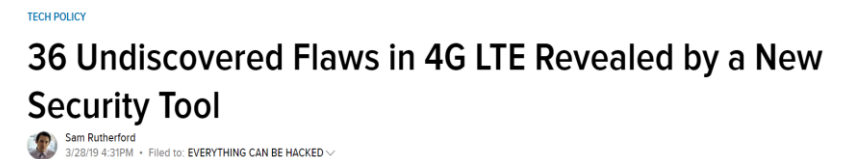
8 years from standards to first attacks, 3 years from deployment to first attacks



A number of vulnerabilities identified even before deployment!

WHAT HAS CHANGED BETWEEN THEN AND NOW?

- Research ecosystem maturing
 - Maturity of open-source tools
 - Excellent work from academia over the last few years
 - Cellular security research hitting mainstream media

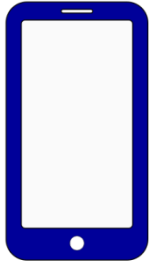


MOBILE NETWORK SECURITY RETROSPECTIVE

- A topic that I am very interested in...
 - <https://www.linkedin.com/pulse/reflection-history-cellular-security-research-outlook-piqueras-jover>
 - <https://www.eff.org/deeplinks/2019/06/history-cellular-network-security-doesnt-bode-well-5g>
 - <https://softhandover.wordpress.com/2018/12/06/the-current-state-of-affairs-in-5g-security/>
 - <https://www.linkedin.com/pulse/impact-open-source-mobile-security-research-roger-piqueras-jover/>
 - <https://arxiv.org/abs/1904.08394>

LTE protocol security redux...

SOME BASIC JARGON



IMEI – “Serial number” of the device



IMSI – secret id of the SIM that should never be disclosed

SUPI – Subscriber Unique Private Identifier (“5G IMSI”)

SUCI – Subscriber Unique Concealed Identifier (SUPI encrypted with operator’s public key)

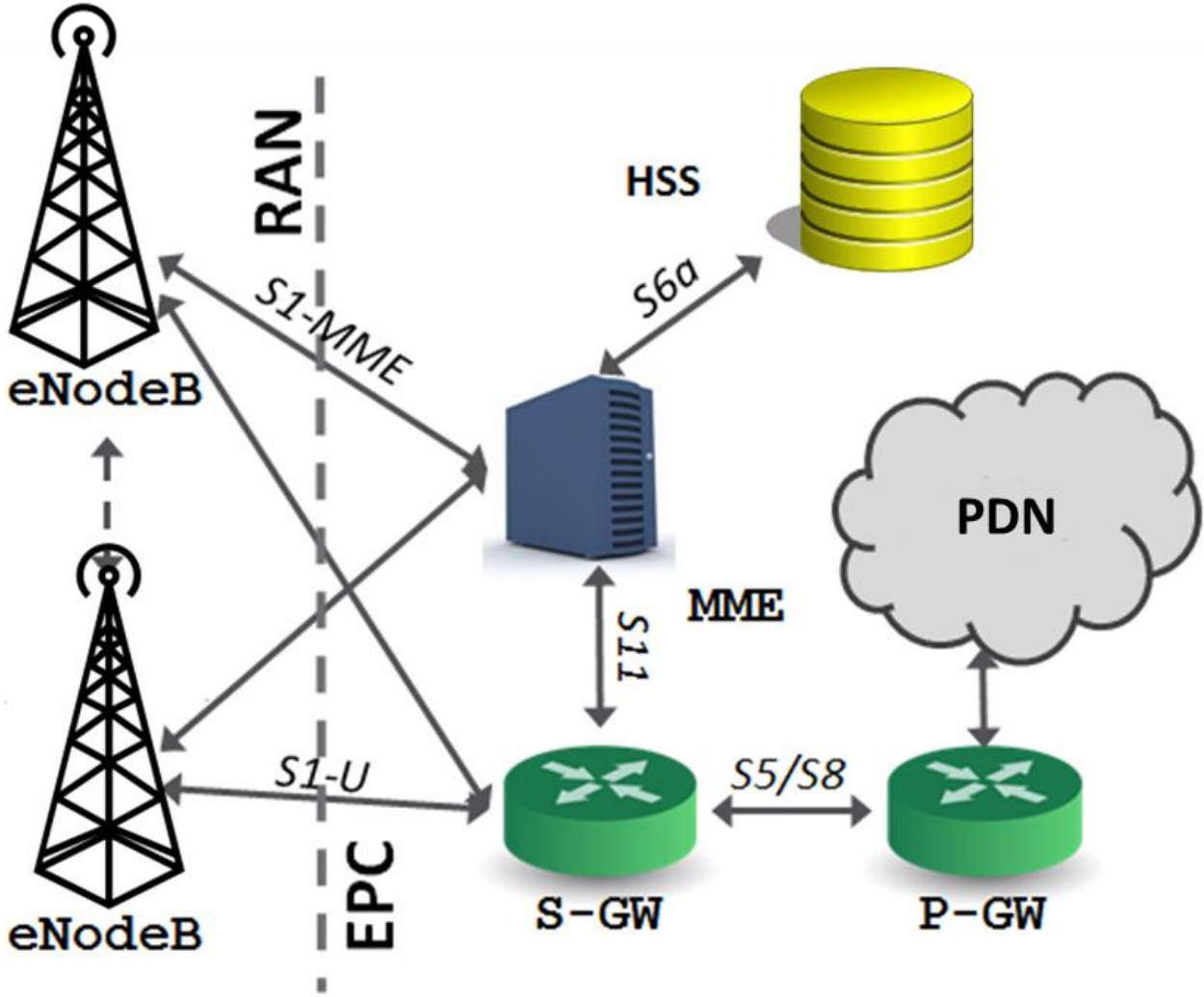
TMSI – temporary id used by the network once it knows who you are



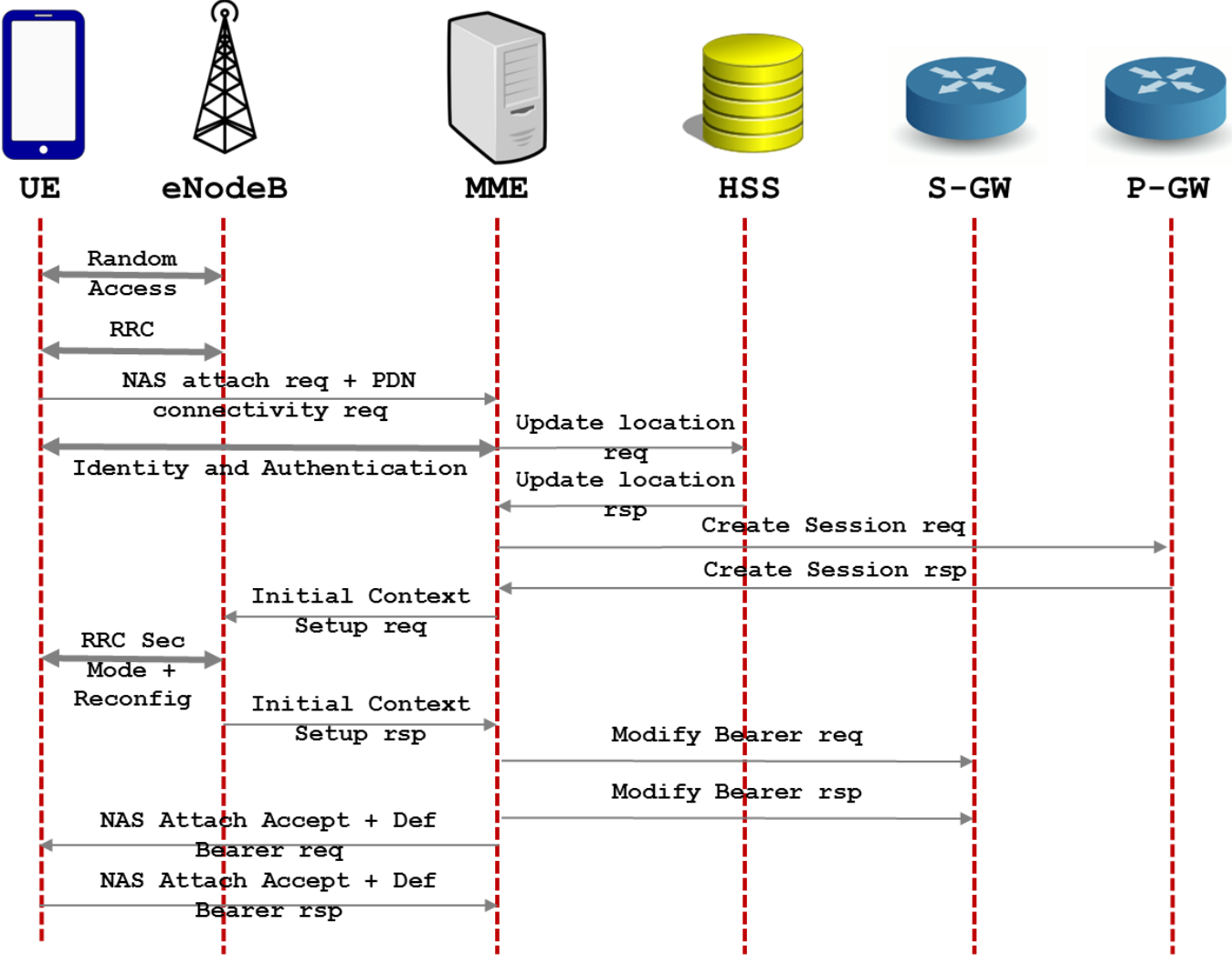
XYZ-867-5309

MSISDN – Your phone number.

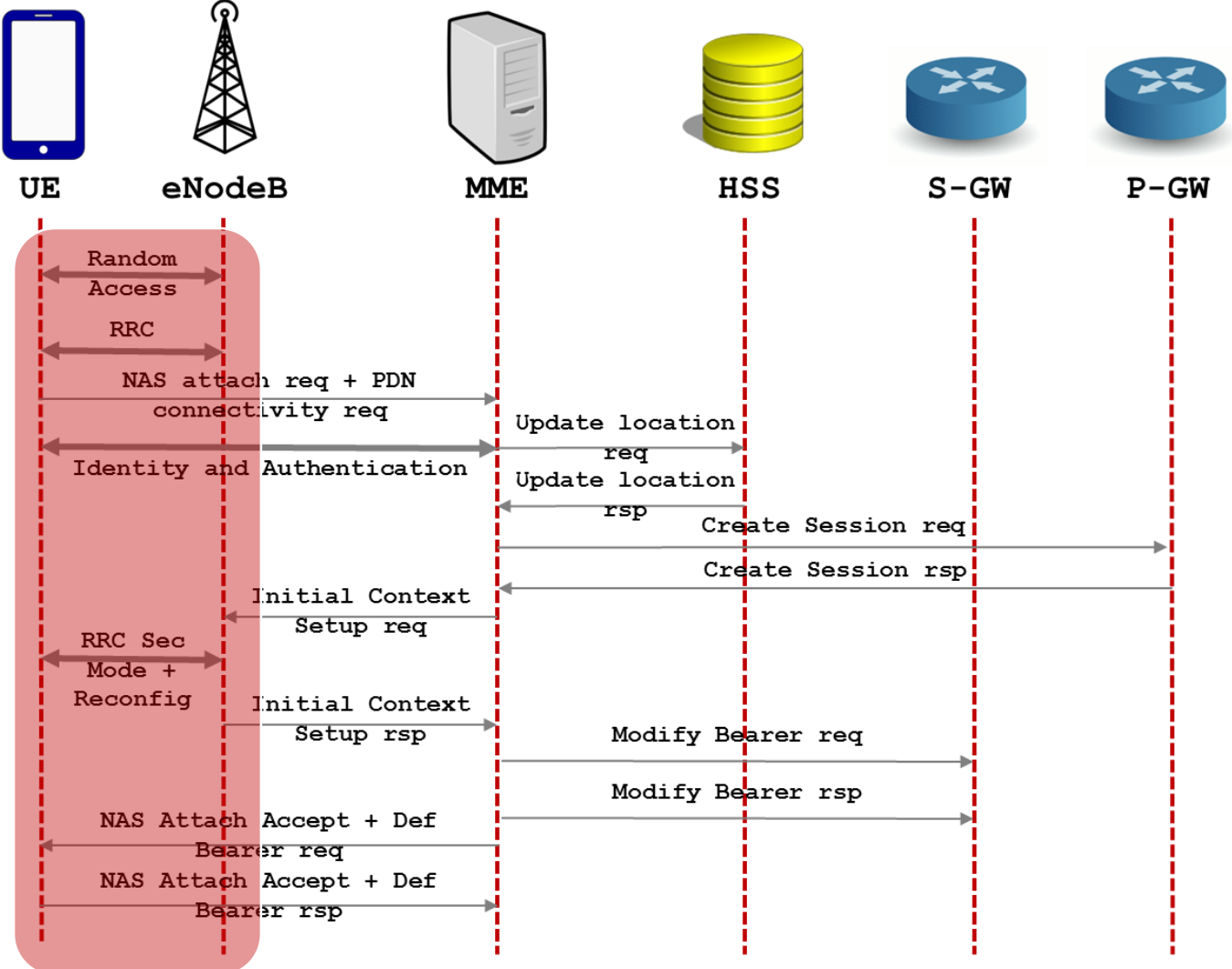
LTE ARCHITECTURE



LTE ATTACH PROCEDURE



LTE ATTACH PROCEDURE



LTE ATTACH PROCEDURE

Name	Start time	DI/UI	Cell	Cell ID	Frame	Subf	RCE	Power	Length	Errs	Retrans	Decr	Valid	Sf RSSI	SINR
RACH	01:32:03.954999	U			440	1	-16.64	-57.98	0						16.64
MAC Random Access Response	01:32:03.958999	D			440	5	-16.41	-45.73	7	OK				-39.20	16.41
RRCConnectionRequest	01:32:03.964999	U			441	1	-23.85	-51.14	6	OK					23.85
RRCConnectionSetup	01:32:03.979999	D			442	6	-15.11	-42.21	26	OK				-38.72	15.11
RRCConnectionSetupComplete	01:32:04.013999	U			446	0			56	OK					
Attach Request	01:32:04.013999	U			446	0	-25.25	-49.36	53	OK					25.25
PDN Connectivity Request	01:32:04.013999	U			446	0	-25.25	-49.36	36	OK					25.25
DLInformationTransfer	01:32:04.088999	D			453	5			39	OK					
Authentication Request	01:32:04.088999	D			453	5	-15.00	-41.33	36	OK				-38.44	15.00
ULInformationTransfer	01:32:04.225999	U			467	2			22	OK					
Authentication Response	01:32:04.225999	U			467	2	-20.80	-53.66	19	OK					20.80
DLInformationTransfer	01:32:04.267999	D			471	4			17	OK					
Security Protected NAS Message	01:32:04.267999	D			471	4	-15.52	-44.04	14	OK		Not...	No...	-39.22	15.52
Security Mode Command	01:32:04.267999	D			471	4	-15.52	-44.04	8	OK				-39.22	15.52
ULInformationTransfer	01:32:04.285999	U			473	2			22	OK					
Security Protected NAS Message	01:32:04.285999	U			473	2	-22.49	-52.16	19	OK		No...	No...		22.49
Unknown NAS	01:32:04.285999	U			473	2	-22.49	-52.16	13	OK					22.49
DLInformationTransfer	01:32:04.327999	D			477	4			12	OK					
Security Protected NAS Message	01:32:04.327999	D			477	4	-14.73	-45.68	9	OK		No...	No...	-39.27	14.73
Unknown NAS	01:32:04.327999	D			477	4	-14.73	-45.68	3	OK				-39.27	14.73
ULInformationTransfer	01:32:04.345999	U			479	2			24	OK					
Security Protected NAS Message	01:32:04.345999	U			479	2	-21.36	-53.39	21	OK		No...	No...		21.36
Unknown NAS	01:32:04.345999	U			479	2	-21.36	-53.39	15	OK					21.36
SecurityModeCommand	01:32:04.472999	D			491	9			3	OK					
Ciphered RRC	01:32:04.495999	U			494	2			2	OK		No...	No...		
Ciphered RRC	01:32:04.501999	D			494	8			3	OK		No...	No...		
Ciphered RRC	01:32:04.515999	U			496	2			18	OK		No...	No...		
Ciphered RRC	01:32:04.536999	D			498	3			165	OK		No...	No...		
Ciphered RRC	01:32:04.575999	U			502	2			2	OK		No...	No...		
Ciphered RRC	01:32:04.575999	U			502	2			16	OK		No...	No...		
Ciphered RRC	01:32:04.604999	D			505	1			30	OK		No...	No...		
Ciphered data	01:32:14.426997	U			463	3			96	OK		No...			
Ciphered data	01:32:14.475997	U			468	2			40	OK		No...			
Ciphered data	01:32:14.513997	U			472	0			96	OK		No...			

RACH handshake between UE and eNB

RRC handshake between UE and eNB

Connection setup (authentication, set-up of encryption, tunnel set-up, etc)

Encrypted traffic

LTE (IN)SECURITY REDUX

Count	Name	Start time	DI/UI	Cell ID	Frame	RNTI	RCE	Power	Errs
1	RACH	00:04:42.942818	U		651		-6.42	-64.65	
2	MAC Random Access Response	00:04:42.946818	D		651		-8.50	-45.23	OK
3	RRCConnectionRequest	00:04:42.952818	U		652		-19.19	-56.46	OK
4	RRCConnectionSetup	00:04:42.967818	D		653		-9.07	-43.18	OK
5	RRCConnectionSetupComplete	00:04:43.001818	U		657				OK
6	Attach Request	00:04:43.001818	U		657				OK
7	PDN Connectivity Request	00:04:43.001818	U		657		-17.59	-60.11	OK
8	DLInformationTransfer	00:04:43.080818	D		664				OK
9	Authentication Request	00:04:43.080818	D		664		-8.86	-42.27	OK
10	ULInformationTransfer	00:04:43.213818	U		678				OK
11	Authentication Response	00:04:43.213818	U		678		-12.51	-65.43	OK
12	DLInformationTransfer	00:04:43.258818	D		682				OK
13	Security Protected NAS Message	00:04:43.258818	D		682		-8.90	-44.51	OK
14	Security Mode Command	00:04:43.258818	D		682		-8.90	-44.51	OK
15	ULInformationTransfer	00:04:43.273818	U		684				OK
16	Security Protected NAS Message	00:04:43.273818	U		684		-11.14	-64.93	OK
17	Unknown NAS	00:04:43.273818	U		684		-11.14	-64.93	OK
18	DLInformationTransfer	00:04:43.318818	D		688				OK
19	Security Protected NAS Message	00:04:43.318818	D		688		-8.88	-45.69	OK
20	Unknown NAS	00:04:43.318818	D		688		-8.88	-45.69	OK
21	ULInformationTransfer	00:04:43.333818	U		690				OK
22	Security Protected NAS Message	00:04:43.333818	U		690		-11.82	-63.66	OK
23	Unknown NAS	00:04:43.333818	U		690		-11.82	-63.66	OK
24	SecurityModeCommand	00:04:43.451818	D		702				OK
25	Ciphered RRC	00:04:43.479818	D		704				OK
26	Ciphered RRC	00:04:43.503818	U		707				OK
27	Ciphered RRC	00:04:43.524818	D		709				OK
28	Ciphered RRC	00:04:43.563818	U		713				OK
29	Ciphered RRC	00:04:43.563818	U		713				OK
30	Ciphered RRC	00:04:43.594818	D		716				OK
31	Ciphered data	00:04:52.021817	D		535				OK
32	Ciphered data	00:04:52.021817	D		535				OK
33	Ciphered data	00:04:52.113817	U		544				OK
34	Ciphered data	00:04:52.153817	U		548				OK

Unencrypted and unprotected.
These messages can be intercepted
and spoofed with open-source tools
and low-cost radios

Other things sent in the clear:

- Base station config (broadcast messages)
- Measurement reports
- Measurement report requests
- (Sometimes) GPS coordinates
- HO related messages
- Paging messages
- Etc

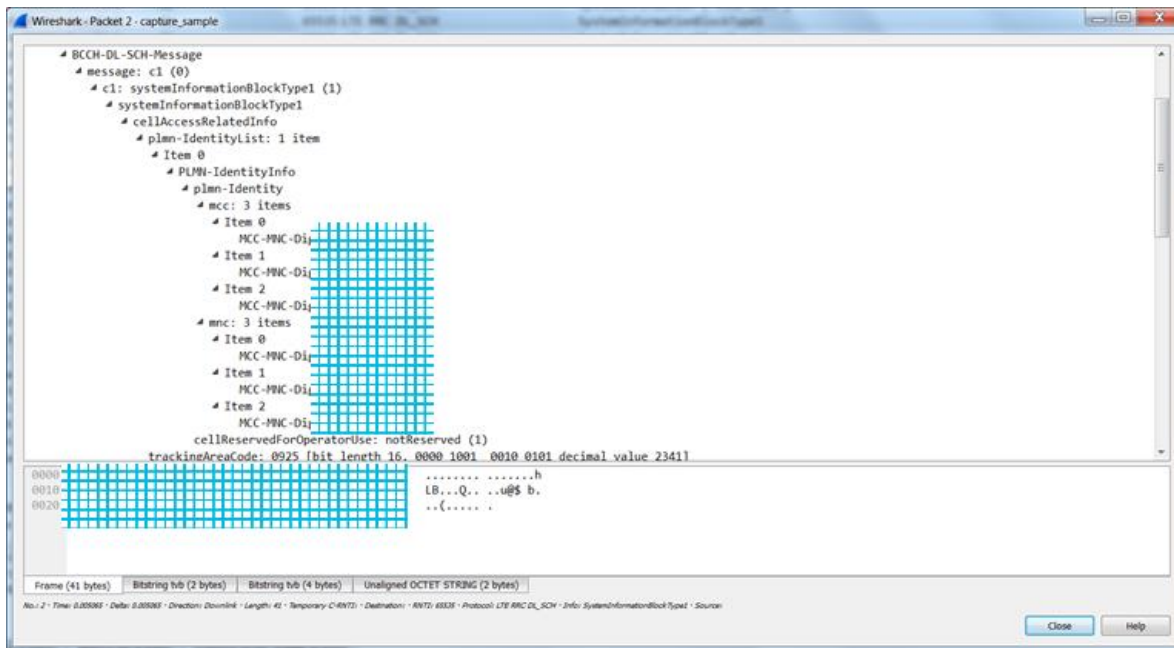
LTE (IN)SECURITY REDUX

Regardless of mutual authentication and strong encryption, a mobile device engages in a substantial exchange of unprotected messages with **any** LTE base station (malicious or not) that advertises itself with the right broadcast information.

The vast majority of vulnerabilities identified in LTE are based on exploiting these pre-authentication messages.

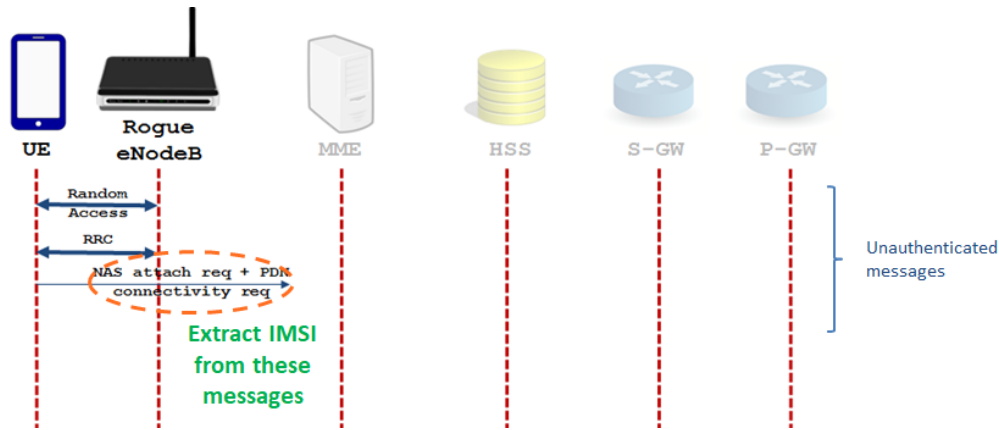
SNIFFING BASE STATION CONFIGURATION

- Capturing MIB and SIB broadcast messages
 - Identify base stations of a given operator
 - Identify ad-hoc base stations for first responders, etc
 - Optimal TX power for rogue base station
 - High priority frequencies
 - Etc



IMSI CATCHING

- Until late 2015, it was wrongly assumed to not be possible in LTE
 - Just a few lines of extra code in srsLTE
 - Not too long ago operators would still page devices using the IMSI in some cases



Wireshark packet capture screenshot showing a list of packets and a detailed view of a Non-Access-Stratum (NAS) PDU. The packet list shows several packets, including 'RRConnectionSetupComplete, Attach request, PDN connectivity request' and 'Attach reject (EPS services not allowed)'. The detailed view shows the structure of the NAS PDU, including the 'EPS mobile identity' field. A red box highlights the 'EPS mobile identity' field, which contains the IMSI. A red arrow points to the hex dump of the IMSI field.

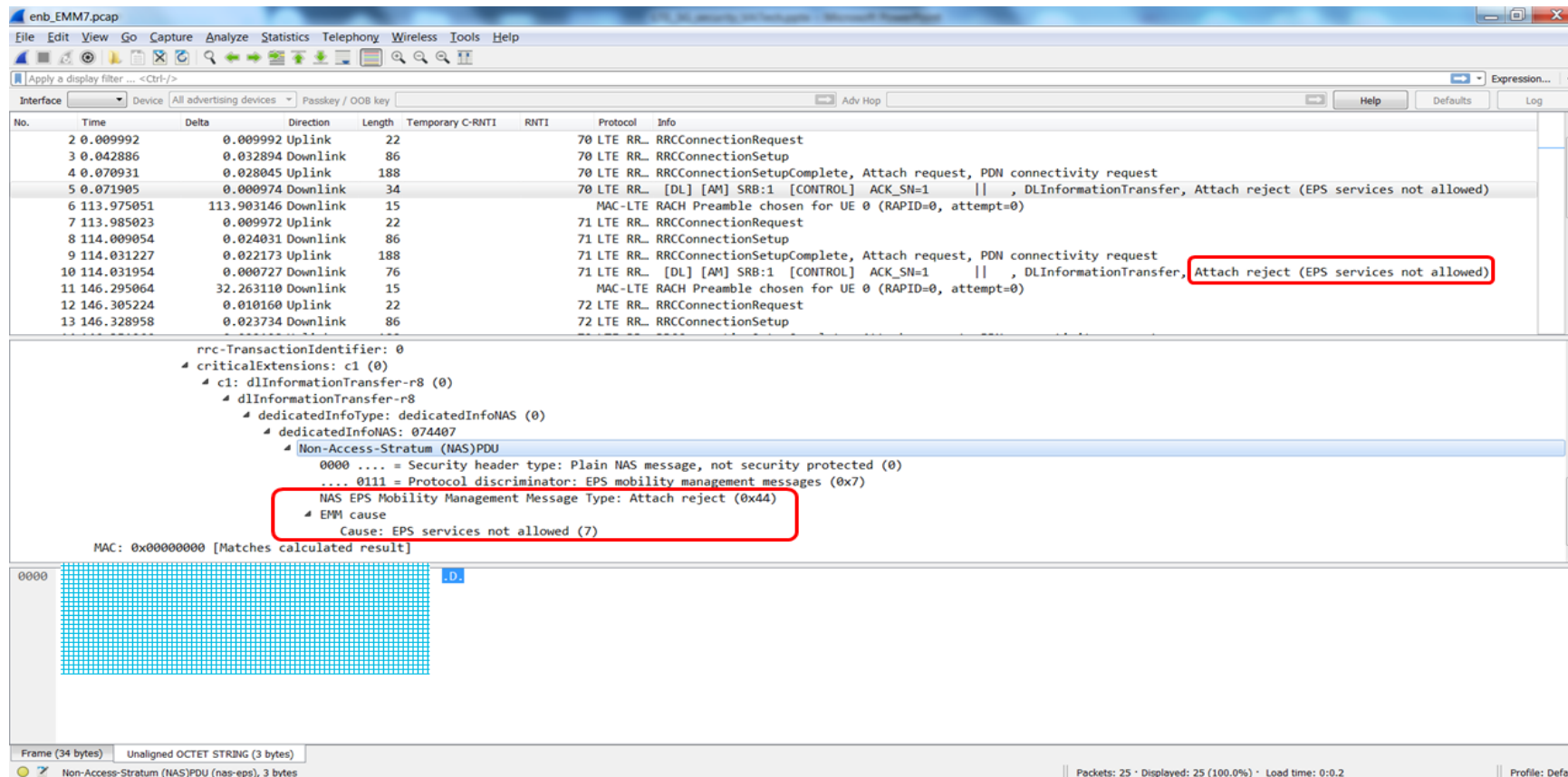
No.	Time	Delta	Direction	Length	Temporary C-RNTI	RNTI	Protocol	Info
4	0.070931	0.028045	Uplink	188			70 LTE RR_	RRConnectionSetupComplete, Attach request, PDN connectivity request
5	0.071905	0.000974	Downlink	34			70 LTE RR_ [DL] [AM] SRB:1 [CONTROL] ACK_SN=1	DLInformationTransfer, Attach reject (EPS services not allowed)
6	113.975951	113.903146	Downlink	15			MAC-LTE RACH Preamble	chosen for UE 0 (RAPID=0, attempt=0)
7	113.985023	0.009972	Uplink	22			71 LTE RR_	RRConnectionRequest
8	114.009054	0.024031	Downlink	86			71 LTE RR_	RRConnectionSetup
9	114.031227	0.022173	Uplink	188			71 LTE RR_	RRConnectionSetupComplete, Attach request, PDN connectivity request
10	114.031954	0.000727	Downlink	76			71 LTE RR_ [DL] [AM] SRB:1 [CONTROL] ACK_SN=1	DLInformationTransfer, Attach reject (EPS services not allowed)
11	146.295064	32.263110	Downlink	15			MAC-LTE RACH Preamble	chosen for UE 0 (RAPID=0, attempt=0)
12	146.305224	0.010160	Uplink	22			72 LTE RR_	RRConnectionRequest
13	146.328958	0.023734	Downlink	86			72 LTE RR_	RRConnectionSetup
14	146.351066	0.022108	Uplink	188			72 LTE RR_	RRConnectionSetupComplete, Attach request, PDN connectivity request
15	146.351968	0.000902	Downlink	76			72 LTE RR_ [DL] [AM] SRB:1 [CONTROL] ACK_SN=1	DLInformationTransfer, Attach reject (EPS services not allowed)

```

4 Non-Access-Stratum (NAS)PDU
  0000 .... = Security header type: Plain NAS message, not security protected (0)
  .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
  NAS EPS Mobility Management Message Type: Attach request (0x41)
  0... .... = Type of security context flag (TSC): Native security context (for KSIasme)
  .111 .... = NAS key set identifier: No key is available (7)
  .... 0... = Spare bit(s): 0x00
  .... .010 = EPS attach type: Combined EPS/IMSI attach (2)
  * EPS mobile identity
    Length: 8
    .... 1... = Odd/even indication: Odd number of identity digits
    .... .001 = Type of identity: IMSI (1)
    IMSI: [REDACTED]
  
```

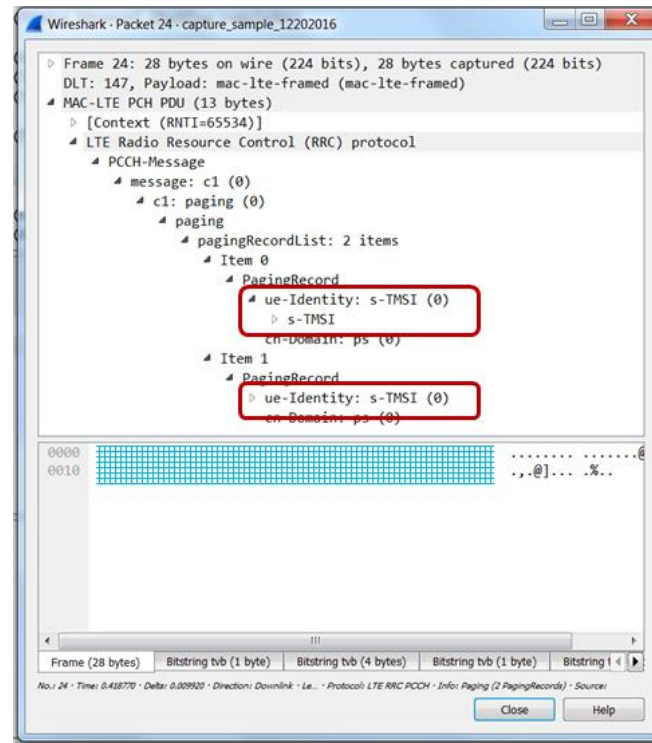
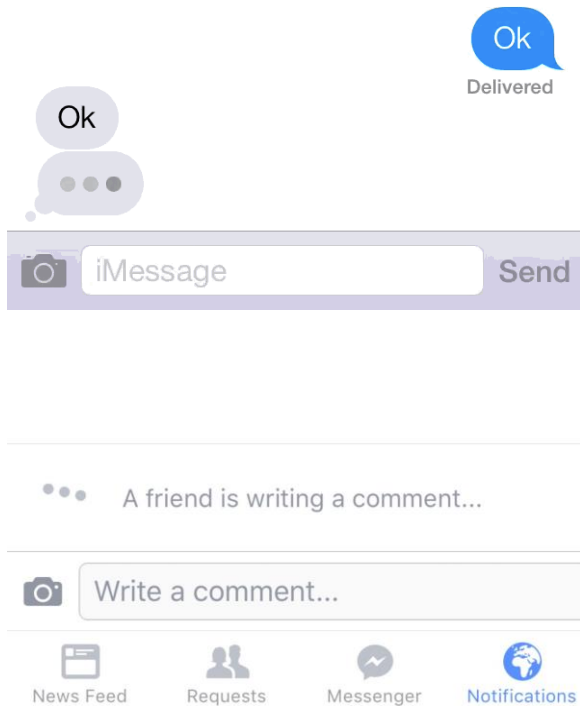
DEVICE DoS AND SILENT DOWNGRADE TO GSM

- Rogue base station replying with Attach Reject and/or TAU Reject messages
 - Brick a mobile device until reboot or toggle of airplane mode
 - Silent downgrade to GSM

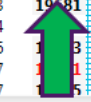


DEVICE TRACKING

- Silent paging leveraging social networks (eg Whatsapp and FB Messenger)
- TMSI+RNTI-based tracking
- Device/identity fingerprinting capturing LTE traffic



Name	Start time	DI/UI	Cell ID	Frame	RNTI	UE Identity	Length	Errs
RACH	00:02:26.830866	U		988			0	
MAC Random Access Response	00:02:26.834868	D		989	8		7	OK
RRCConnectionRequest	00:02:26.840866	U		989	19841		5	OK
RRCCConnectionSetup	00:02:26.853868	D		991	19841		24	OK
Ciphered data	00:02:26.855868	D		991	19681		1280	OK
Ciphered data	00:02:26.856868	D		991	19681		1280	OK
Ciphered data	00:02:26.857868	D		991	19681		1280	OK
Ciphered data	00:02:26.858868	D		991	19681		1280	OK
Unknown Data	00:02:26.871868	D		992	12381		52	1
Unknown Data	00:02:26.871868	D		992	12381		109	1
RRCCConnectionSetupComplete	00:02:26.874866	U		993	19841		7	OK
Service Request	00:02:26.874866	U		993	19841		4	OK
Ciphered data	00:02:26.894868	D		995	19681		1280	OK
Ciphered data	00:02:26.895868	D		995	19681		1280	OK
Ciphered data	00:02:26.900868	D		995	19681		1280	OK
Ciphered data	00:02:26.901868	D		995	19681		1280	OK
Ciphered data	00:02:26.902868	D		995	19681		1280	OK
SecurityModeCommand	00:02:26.909868	D		996	19841		3	OK
Ciphered data	00:02:26.931868	D		998	19681		1280	OK
Ciphered data	00:02:26.932868	D		998	19681		1280	OK
SecurityModeComplete	00:02:26.932866	U		998	19841		2	OK
Ciphered data	00:02:26.933868	D		999	19681		1280	OK
Ciphered data	00:02:26.934868	D		999	19681		1280	OK
Ciphered data	00:02:26.952868	D		1000	19681		1280	OK
Ciphered data	00:02:26.953868	D		1001	19681		1280	OK
Ciphered data	00:02:26.954868	D		1001	19681		1280	OK
Ciphered data	00:02:26.955868	D		1001	19681		1280	OK
RRCCConnectionReconfiguration	00:02:26.957868	D		1001	19841		34	OK
RRCCConnectionReconfigurationC...	00:02:26.972866	U		1002	19841		2	OK
IP Data (IPv4 UDP)	00:02:26.972866	U		1002	19841		70	OK
Ciphered data	00:02:26.974868	D		1003	19681		1280	OK
Ciphered data	00:02:26.975868	D		1003	19681		404	OK
MAC Random Access Response	00:02:26.984868	D		1004			7	OK
RRCCConnectionSetup	00:02:27.003868	D		1006			24	OK
Unknown Data	00:02:27.020868	D		1007			1428	1
Ciphered RRC	00:02:27.021868	D		1007			2	OK



Shaik, Altaf, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. "Practical attacks against privacy and availability in 4G/LTE mobile communication systems." In Network and Distributed System Security Symposium. Internet Society, 2016.

Jover, Roger Piqueras. "LTE protocol exploits." Shmocon 2016 (2016).

DNS SPOOFING AND TRAFFIC HIJACK OVER LTE

- aLTER Attack
 - Leverages my RNTI-based tracking/fingerprinting
 - For the record, 3GPP TR 33.899 V1.3.0 (2017-08) ignored me and claimed RNTI tracking was not a security issue...
- Poor implementation of AES cipher leads to cipher text modification attack
 - Flip bits in encrypted DNS responses, modify plain-text IP in DNS response and hijack user's traffic
 - How to tell DNS requests/responses apart from other encrypted traffic?
 - RNTI-based tracking, of course, which was clearly never a security issue...

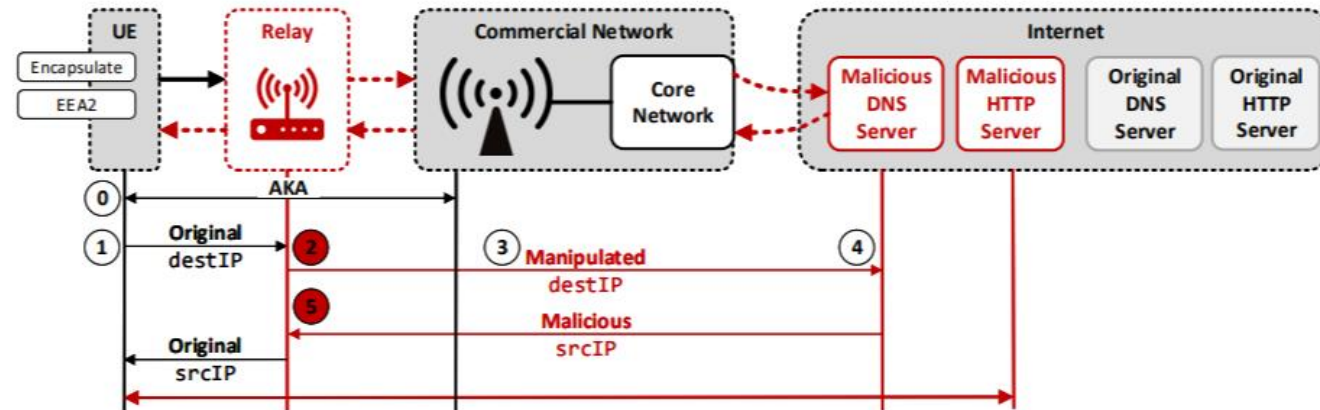


Fig. 4. ALTER: Overview of the DNS redirection attack. We deploy a malicious relay as a MitM between the UE and the commercial network and alter the destination IP address of a DNS request to redirect messages to our malicious DNS server. Eventually, the UE connects to the malicious HTTP server.

UL FUZZING AND EXPLOITS WITHOUT ROGUE BS!

- IMSI extraction based on paging traffic and paging occasion analysis
- Signal overshadowing
 - No need to set up a rogue base station to inject malicious LTE pre-authentication messages
- LTE uplink fuzzing!
 - Open-source tools and low-cost hardware to inject arbitrary traffic into cellular networks
 - NAS-layer traffic hits the MME
 - MME/core network fuzzing?

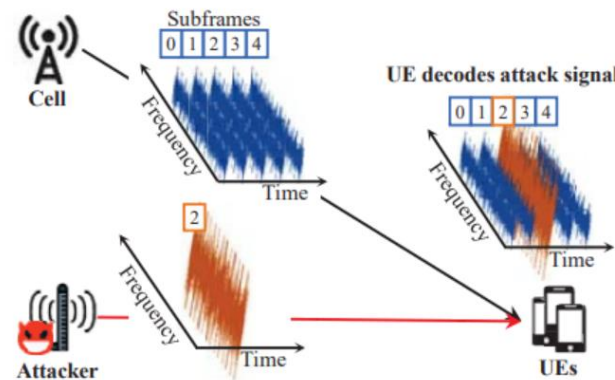
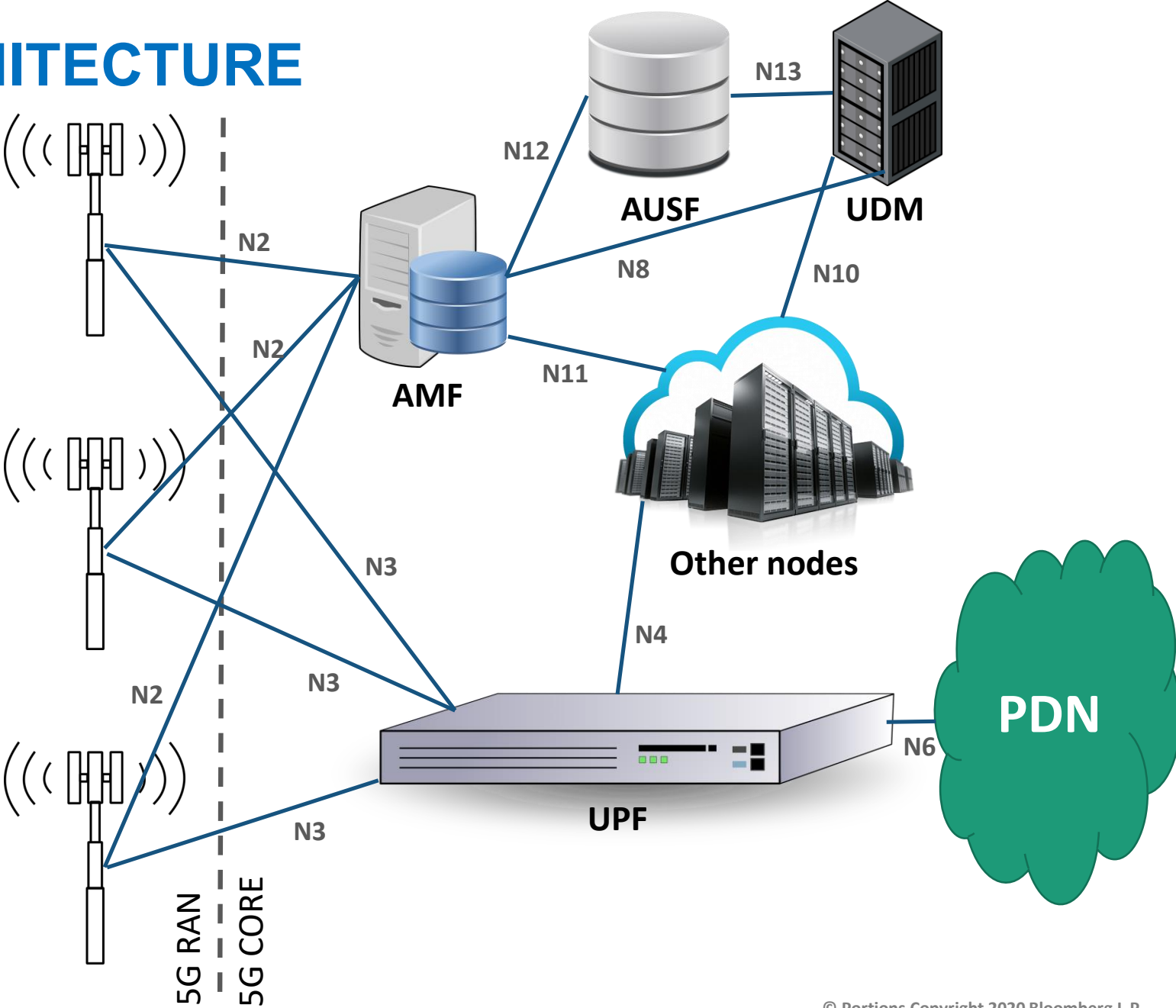
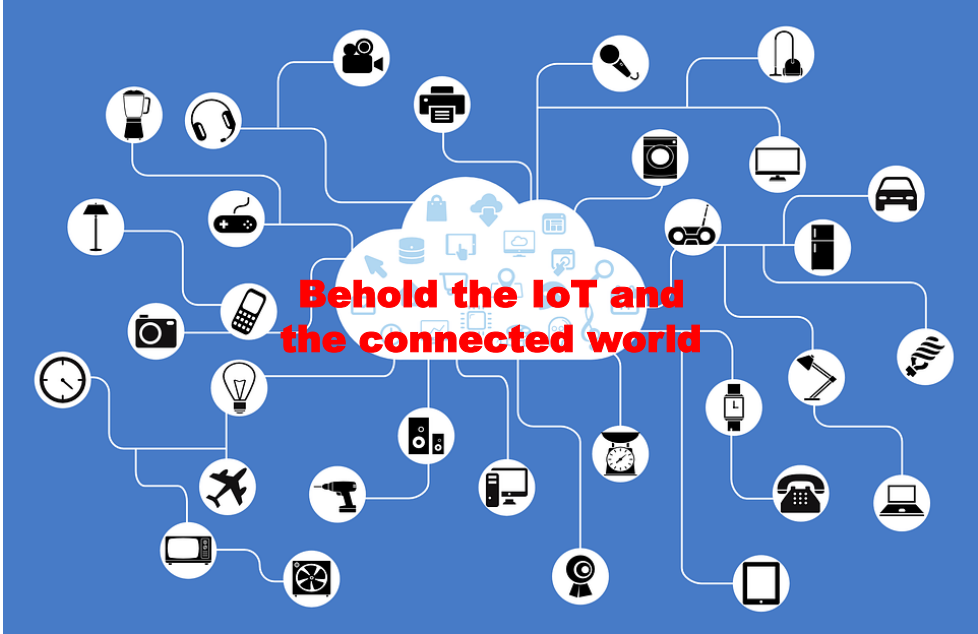


Figure 3: Overshadowing attack at a glimpse: By exploiting the fixed transmission timings of LTE subframes, the attacker injects a crafted subframe (in brown) that precisely *overshadows* the legitimate subframe (in blue) without errors.

Yang, Hojoon, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim.
"Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE." In 28th USENIX Security Symposium (USENIX Security 19), pp. 55-72. 2019..

How do things look like in 5G?

(SIMPLIFIED) 5G ARCHITECTURE



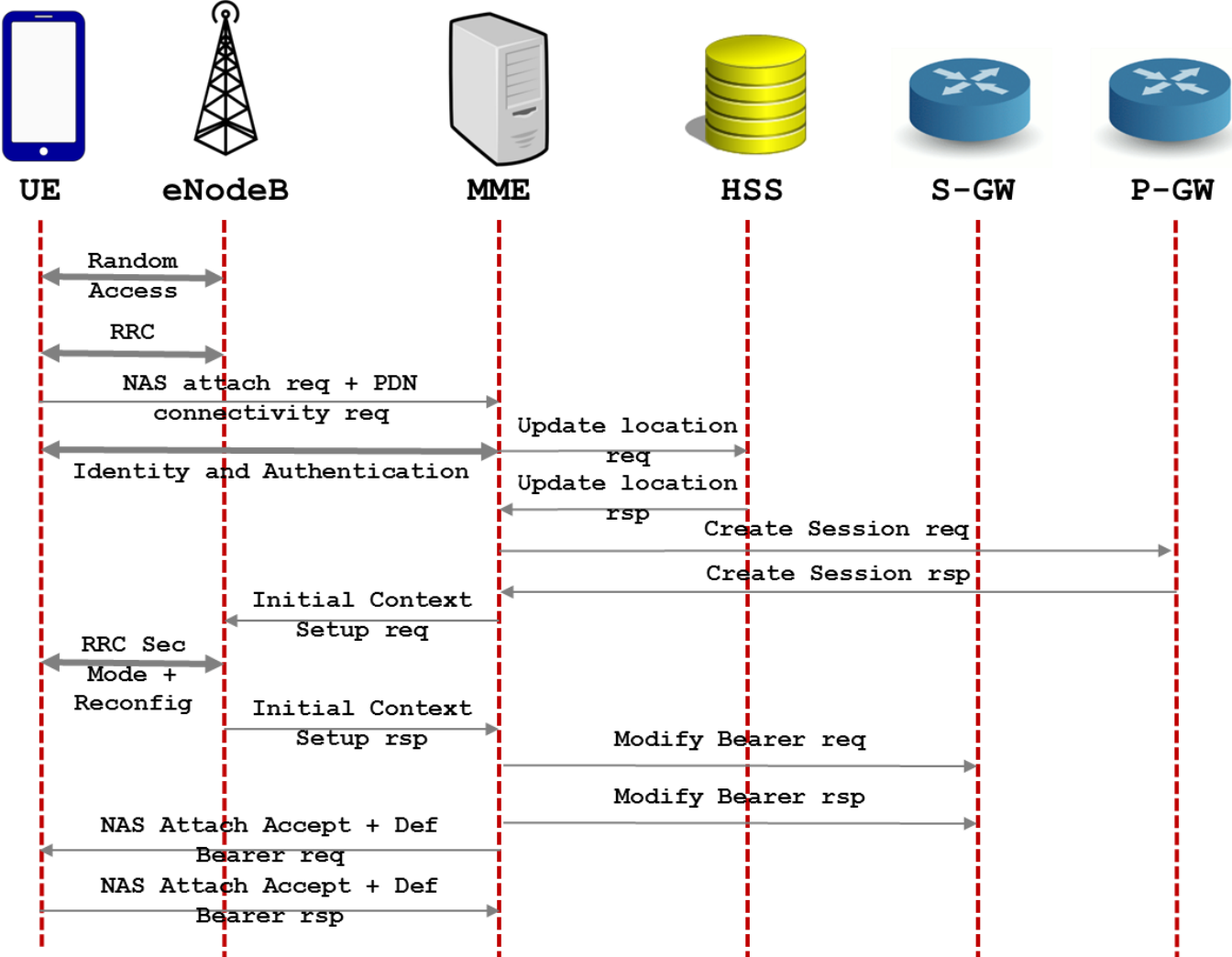
5G ATTACH PROCEDURE

- Two types of deployment and operation of 5G
 - Non-standalone mode (NSA)
 - 5G-NR RAN deployment
 - LTE core infrastructure
 - Everything like LTE but using the 5G high throughput RAN
 - Architecture like LTE plus 5G gNodeB (base station)
 - Standalone mode (SA)
 - Actual standalone 5G deployment
 - Architecture like the one in the previous figure

5G NSA ATTACH PROCEDURE

- Start with basic LTE NAS attach...

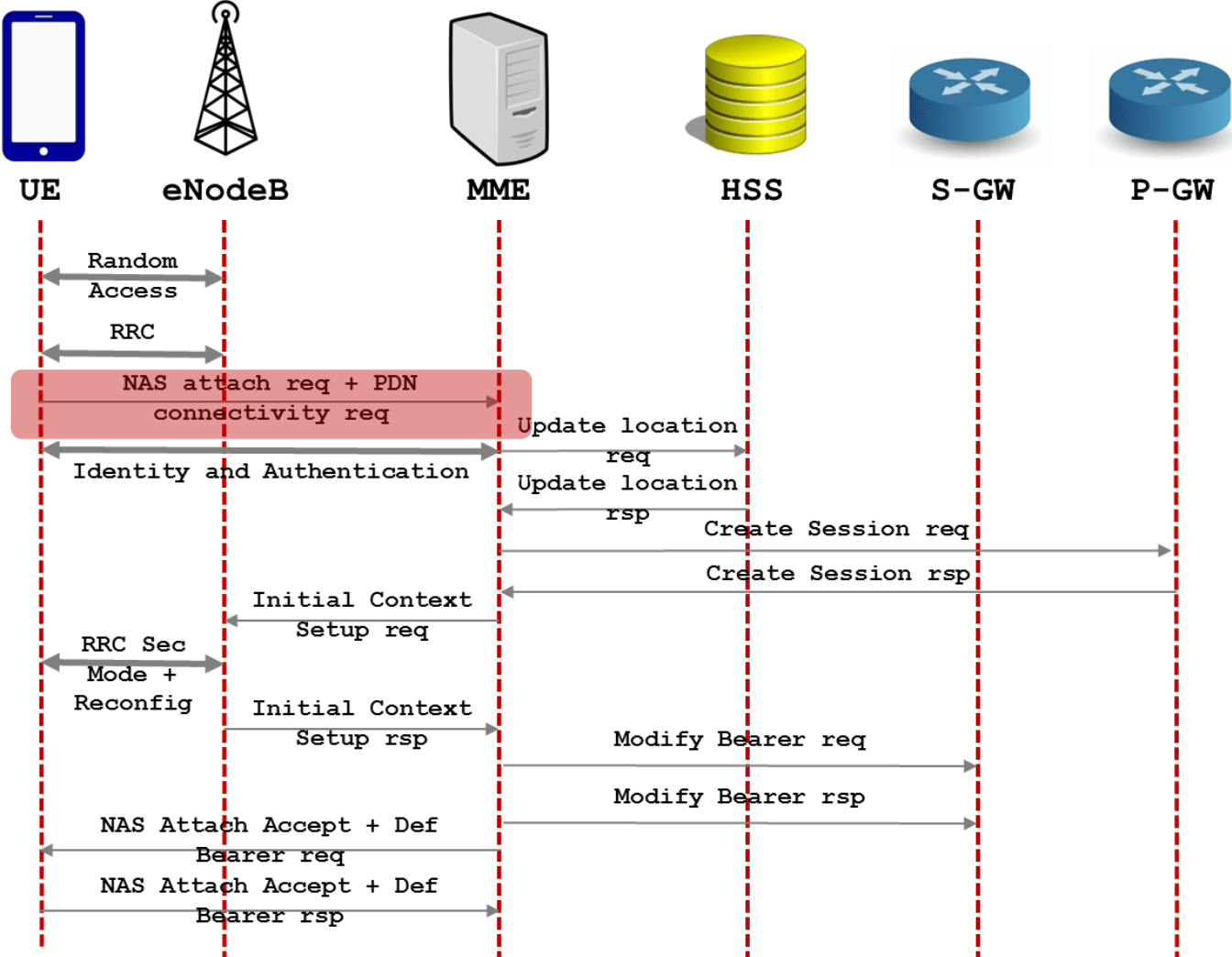
UE signals to LTE core that it supports 5G NR via DCNR bit in AttachRequest message



5G NSA ATTACH PROCEDURE

- Start with basic LTE NAS attach...

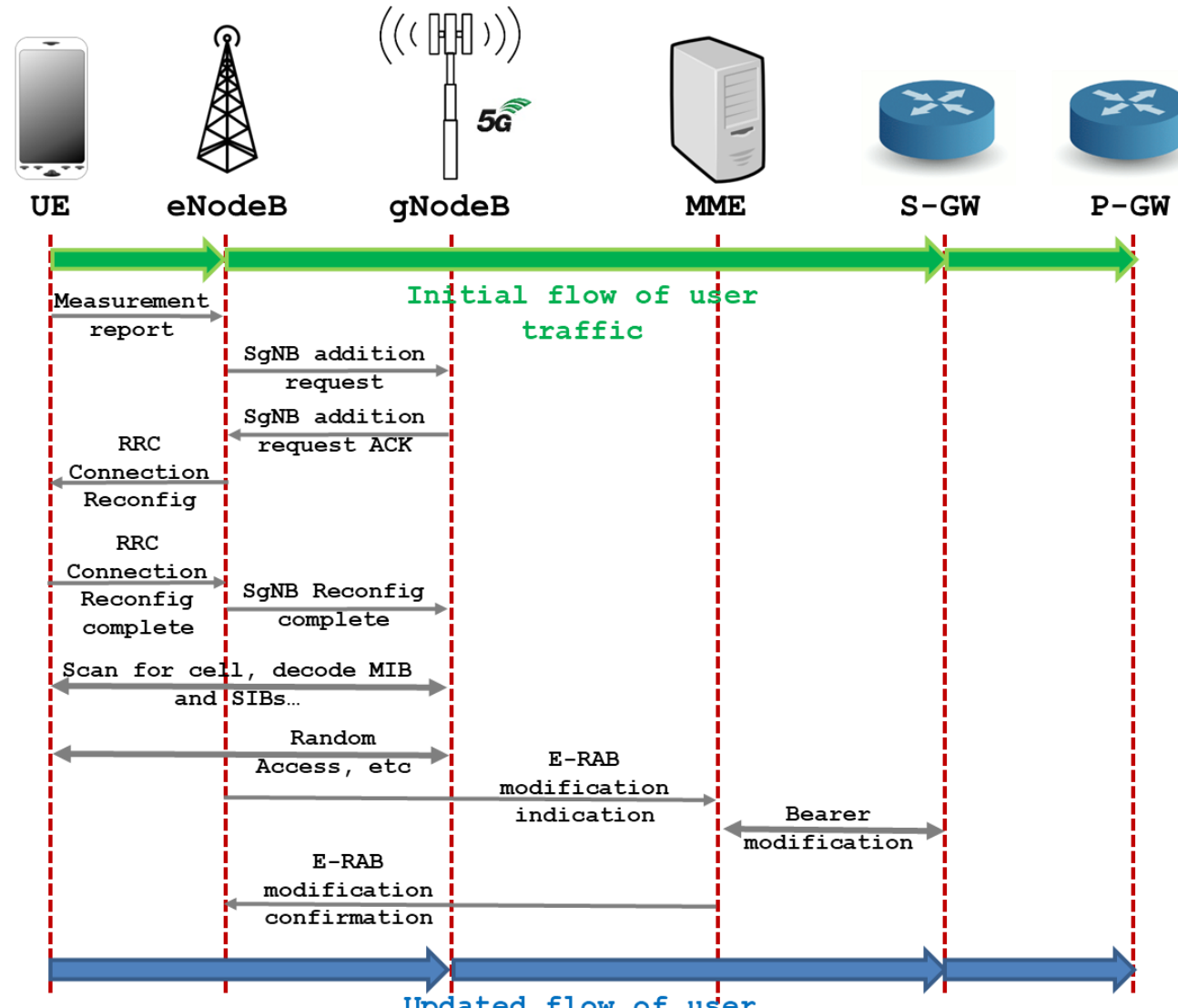
UE signals to LTE core that it supports 5G NR via DCNR bit in AttachRequest message (unprotected message)



As shown earlier, the initial NAS Attach on LTE is **unprotected**.

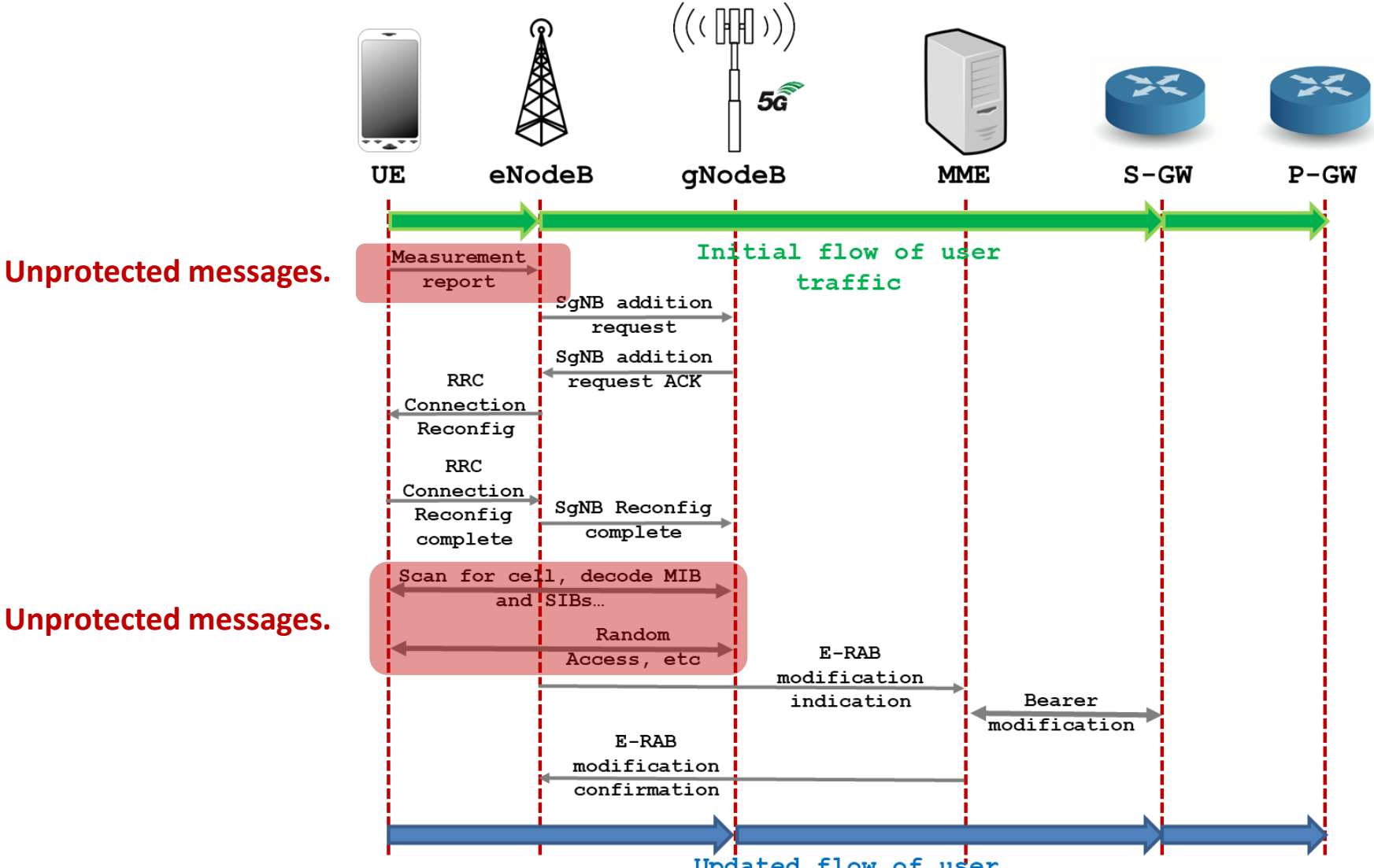
5G NSA ATTACH PROCEDURE

- Then switch 5G-NR RAN...

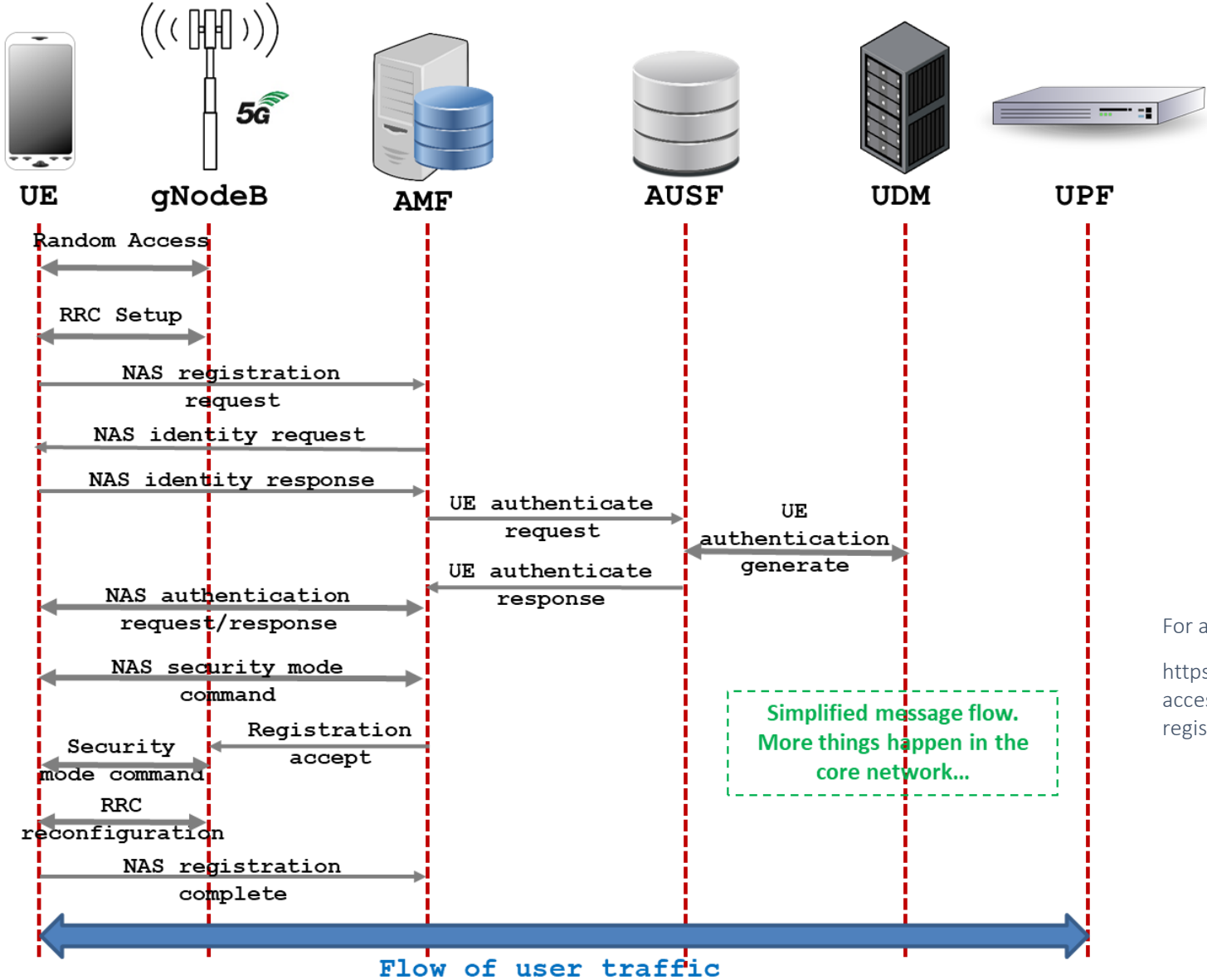


5G NSA ATTACH PROCEDURE

- Then switch 5G-NR RAN...

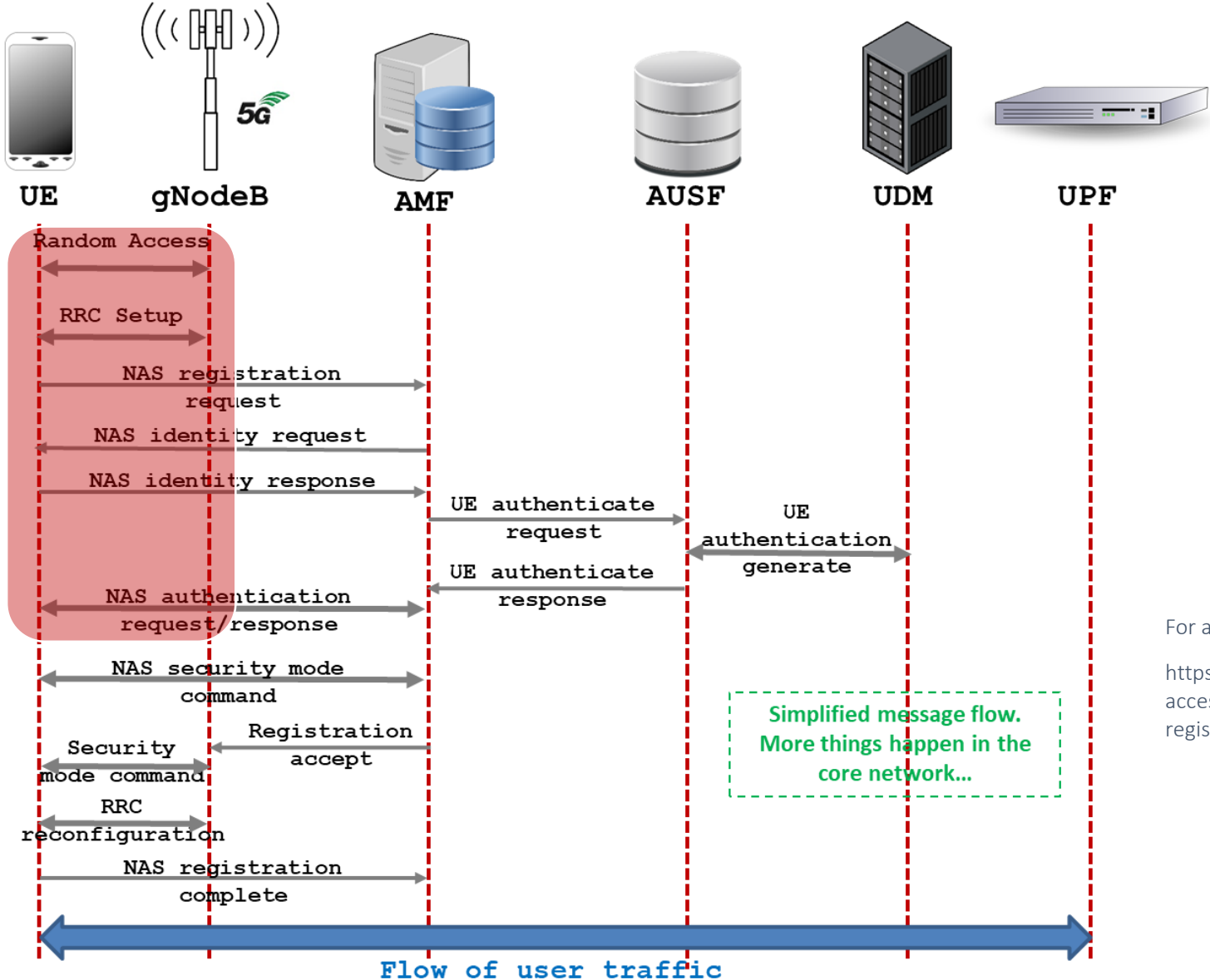


5G SA ATTACH PROCEDURE



For a more detailed message flow:
<https://www.eventhelix.com/5G/standalone-access-registration/5g-standalone-access-registration.pdf>

5G SA ATTACH PROCEDURE



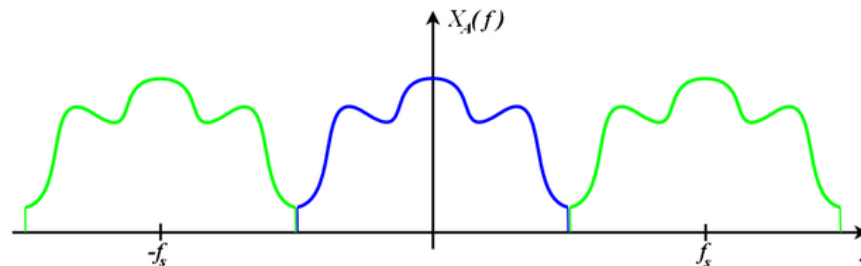
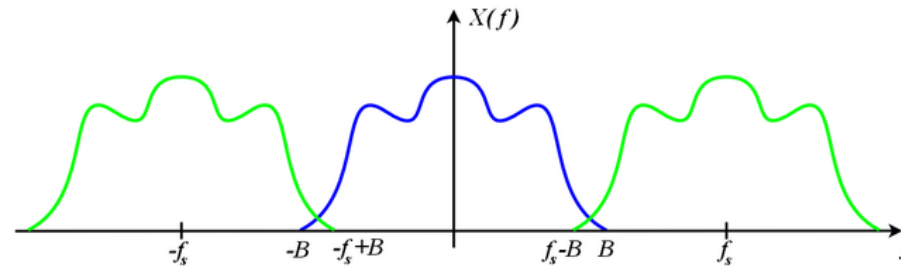
Unprotected messages.

For a more detailed message flow:
<https://www.eventhelix.com/5G/standalone-access-registration/5g-standalone-access-registration.pdf>

Gearing up to explore 5G's security...

CHALLENGES IN CAPTURING AND ANALYZING 5G TRAFFIC

- You cannot exploit any of these protocol vulnerabilities with any (known) open-source tool or standard SW radios
 - Any statement otherwise is incorrect
 - Technology is just not there yet, but soon will be
 - Eg. 5G 100MHz BW
 - Recall Nyquist and Shannon
 - Your lab PC already sometimes struggles to tx/rx at 32Mps to/from your USRP for LTE 10MHz
 - Imagine 5G at 2xBW!



CHALLENGES IN CAPTURING AND ANALYZING 5G TRAFFIC

- Open-source 5G protocol stack
 - Exciting ongoing work
 - Commercial tools that cover the network core and/or parts of the NR-RAN

Note: This list is not intended to be complete or in any particular order, but just a sample of existing options.



- srsLTE already implements some 5G features since release 19.12 very useful for early fuzz tests of the 5G core protocol
 - 5G RRC (https://github.com/srsLTE/srsLTE/blob/master/lib/include/srslte/asn1/rrc_nr_asn1.h)
 - 5G NGAP (https://github.com/srsLTE/srsLTE/blob/master/lib/include/srslte/asn1/ngap_nr_asn1.h)

CHALLENGES IN CAPTURING AND ANALYZING 5G TRAFFIC

- Software radio
 - A high end USRP X series has a BW of up to 120MHz
 - You know when you mess up with gnuradio and start saving raw IQ samples on disk?
 - Imagine at, say, 200Msps
 - HUGE capture files
 - Expensive to process
 - On a standard PC, forget about processing them in real time
 - Yes, **no SDR-based 5G sniffing yet**



RELEASE 15 TRAFFIC CAPTURES FOR ANALYSIS

- All 5G captures shown here are from real Release15 5G lab mobile devices and base stations
- Captured with Sanjole 5G Wavejudge
 - Traffic analysis processing raw 5G IQ samples on Wavejudge's SW
- 5G test and experimentation HW still in early stages of product life
 - High price
 - In constant development
- Capture limitations
 - Max capture duration of a couple of seconds at best (HUGE file anyways)
 - No real-time processing (no Wireshark-like traffic capture)
 - Hard to get an entire attach plus user traffic flow in such a short capture

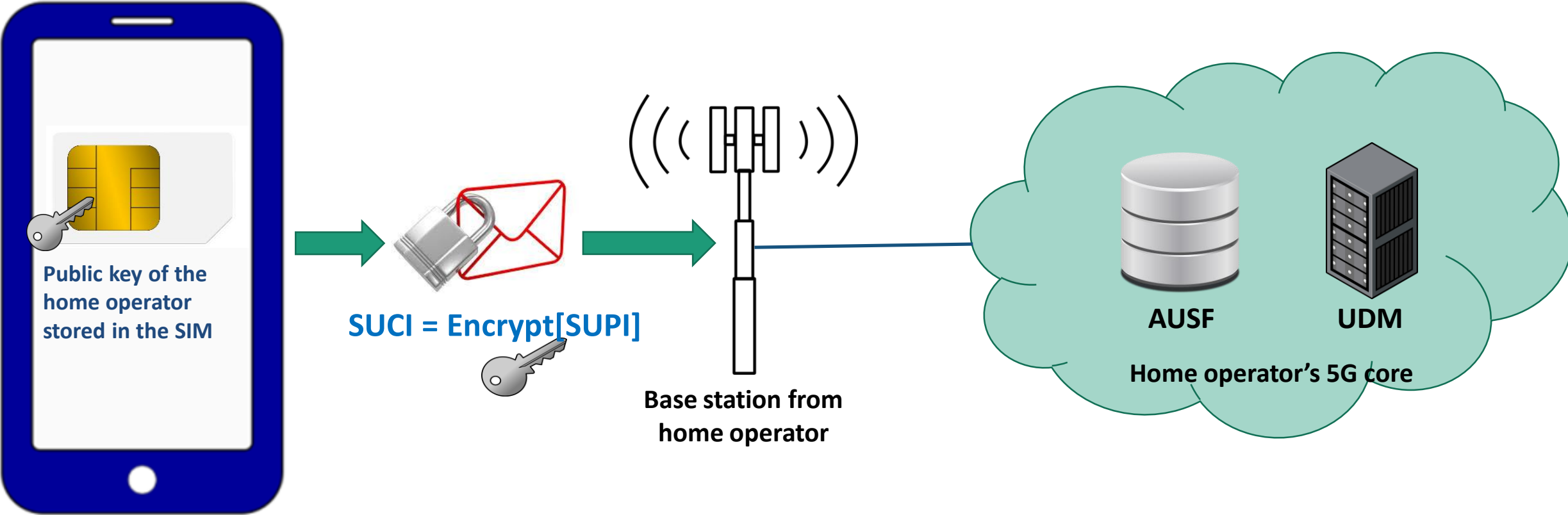


If you are a prospect PhD student or PostDoc and would like to have access to such 5G security analysis equipment, come talk to me after the talk or send me an email.

5G protocol security analysis

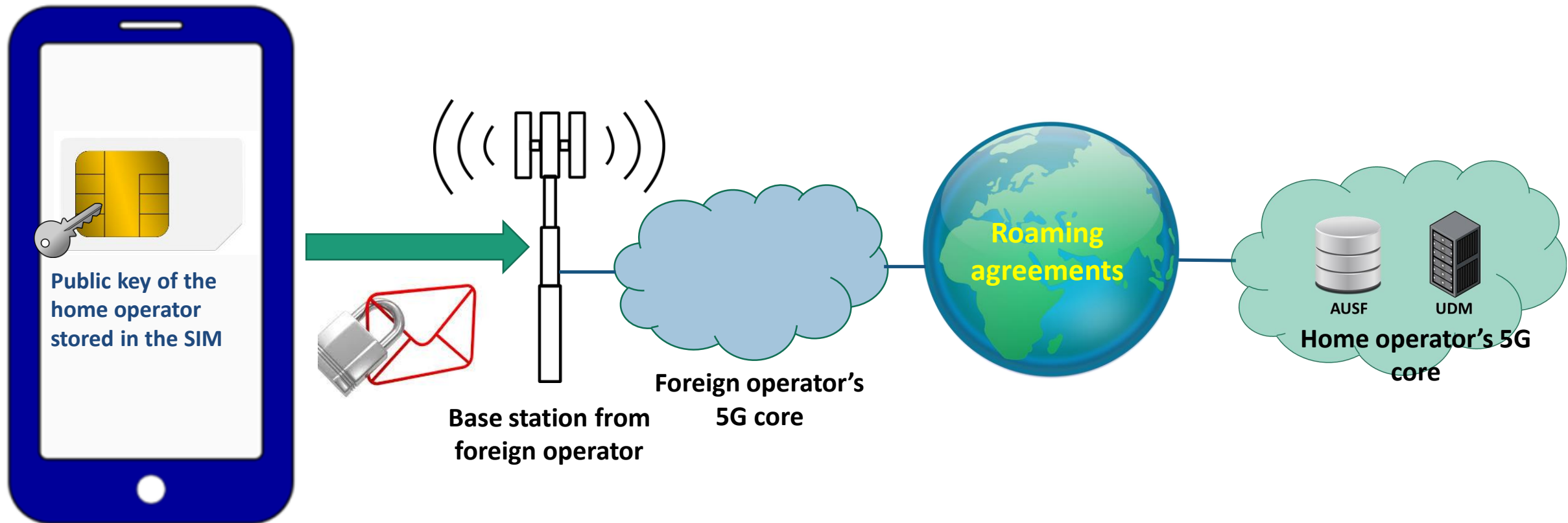
5G IMSI PROTECTION – SUPI/SUCI

- New unique secret identifier
 - SUPI (Subscriber Unique Private Identifier)
- (OPTIONAL) Feature to encrypt the SUPI in flight
 - SUCI (Subscriber Unique Concealed Identifier)



5G IMSI PROTECTION – SUPI/SUCI

- SUPI encryption also works in roaming scenarios
 - Devices authenticate only with their home operator
 - Only the home operator has the key material shared between the SIM and the operator
- If this is implemented, IMSI/SUPI catching not possible in 5G...



5G IMSI PROTECTION – SUPI/SUCI

- SUPI encryption also works in roaming scenarios
 - Devices authenticate only with their home operator
 - Only the home operator has the key material shared between the SIM and the operator
- If this is implemented, IMSI/SUPI catching not possible in 5G...
 - **Yeah, not so fast... Broken too.**
- Flaws on LTE and 5G paging protocol
 - Trigger paging messages and intercept
 - Derive Paging Occasion
 - Bruteforce the IMSI or SUPI

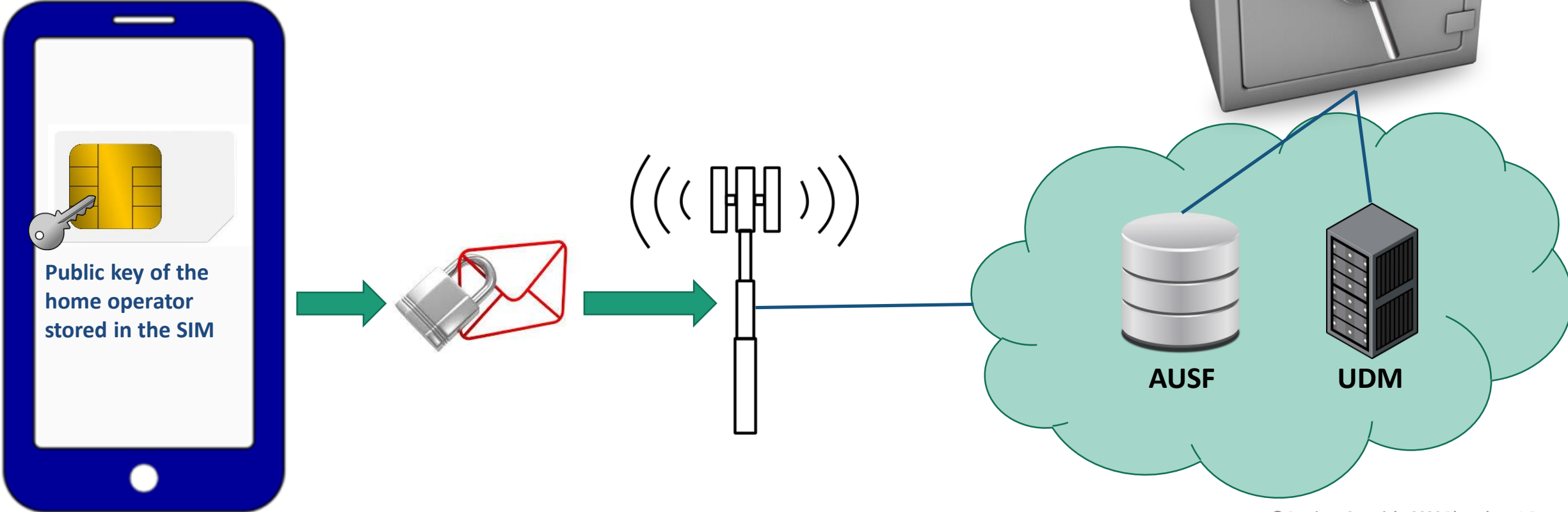
New flaws in 4G, 5G allow attackers to intercept calls and track phone locations

Zack Whittaker @zackwhittaker / 11:39 am EST • February 24, 2019

Hussain, Syed Rafiul, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information." In NDSS. 2019..

5G SUPI PROTECTION?

- Optional feature
 - Optional features in previous cellular generations were generally left unimplemented
- So many key architectural elements left “outside of the scope” of the 3GPP specs
 - Key management, key distribution, key rotation, key storage...
 - Likely a deterrent from actual implementation



“OUT OF SCOPE”

This works for most wireless security specifications:

**Ctrl+F for {“scope”, “out of scope”, “out of the scope”, etc}
In mobile communication standard documents**

3GPP TS 33.501 - Security architecture and procedures for 5G system

- 5.2.5 – Subscriber privacy
 - “The provisioning and updating of the home network public key is out of the scope of the present document. It can be implemented using, e.g. the Over the Air (OTA) mechanism.”
- 12.2 – Mutual authentication
 - “The structure of the PKI used for the certificate is out of scope of the present document.”
- C.3.3 – Processing on home network side
 - “How often the home network generates new public/private key pair and how the public key is provisioned to the UE are out of the scope of this clause.”
- Many more...

5G NSA ATTACH PROCEDURE

The screenshot displays a network analysis tool interface for a 5G NSA attach procedure. The main window is divided into several sections:

- Left Panel:** Configuration options for 'Cell 1: DL on RX 1', including 'Use N Cell ID', 'Single Symbol', and slot configurations (slots 3-19).
- WaveJudge Messages List Table:**

Name	Start Time	P	D	Error Chec.	# Bytes	RNTI	Frame N.	Code
MIB	0019.18	1	D	OK	3			
PRACH	0023.67	1	U				250	5
MAC Random Access Response	0026.18	1	D	OK	10	129		
RRCSetupRequest	0028.18	1	U	OK	6	372		
MIB	0039.18	1	D	OK	3			
RRCSetup	0055.68	1	D	OK	58	372		
MIB	0059.18	1	D	OK	3			
MIB	0079.18	1	D	OK	3			
SIB1	0084.18	1	D	OK	123	65535		
RRCSetupComplete	0088.68	1	U	OK	100	372		
MIB	0099.18	1	D	OK	3			
UECapabilityEnquiry	0100.18	1	D	OK	21	372		
DLInformationTransfer	0114.18	1	D	OK	7	372		
MIB	0119.18	1	D	OK	3			
SIB2,3,4	0124.18	1	D	OK	36	65535		
UECapabilityInformation	0138.68	1	U	OK	259	372		
MIB	0139.18	1	D	OK	3			
- Constellation Diagrams:** Four plots showing 'Rel Amplitude UI' for 'Constellation: Cell 1 DL/UL All layers All'. A summary below indicates: Carrier Freq Err: 0.063 kHz = 0.025 ppm; Sampling Freq Err: 3.410 Hz = 0.023 ppm.
- Power dBm:** 'Time Domain Power: RX 5G 1 All' plot showing power levels over time (0-120 ms).
- 2D Power:** '2D Power: RX 5G 1 DL All' plot showing power across frequency (20-130 ms).
- EVM dB:** 'EVM Per Subcarrier: RX 5G 1 All' plot showing Error Vector Magnitude across subcarriers (-1600 to -1100).

5G NSA ATTACH PROCEDURE

Name	Start Ti...	Cell ID	Frame N...	D...	Error Chec...	# Bytes	RNTI
MIB	0019.18			D	OK	3	
PRACH	0023.67	8	250	U			
MAC Random Access Response	0026.18			D	OK	10	129
RRCSetupRequest	0028.18			U	OK	6	372
MIB	0039.18			D	OK	3	
RRCSetup	0055.68			D	OK	58	372
MIB	0059.18			D	OK	3	
MIB	0079.18			D	OK	3	
SIB1	0084.18			D	OK	123	65535
RRCSetupComplete	0088.68			U	OK	100	372
MIB	0099.18			D	OK	3	
UECapabilityEnquiry	0100.18			D	OK	21	372
DLInformationTransfer	0114.18			D	OK	7	372
MIB	0119.18			D	OK	3	
SIB2,3,4	0124.18			D	OK	36	65535
UECapabilityInformation	0138.68			U	OK	259	372
MIB	0139.18			D	OK	3	

Unencrypted and unprotected. These messages can be intercepted and spoofed.

Other things sent in the clear:

- Base station config (broadcast messages)
- Some measurement reports
- Some measurement report requests
- Paging messages
- Etc

Sounds familiar?

5G (IN)SECURITY RATIONALE

Regardless of mutual authentication and strong encryption, a 5G mobile device engages in a substantial exchange of unprotected messages with *any* 5G base station (malicious or not) that advertises itself with the right broadcast information.

5G (IN)SECURITY RATIONALE

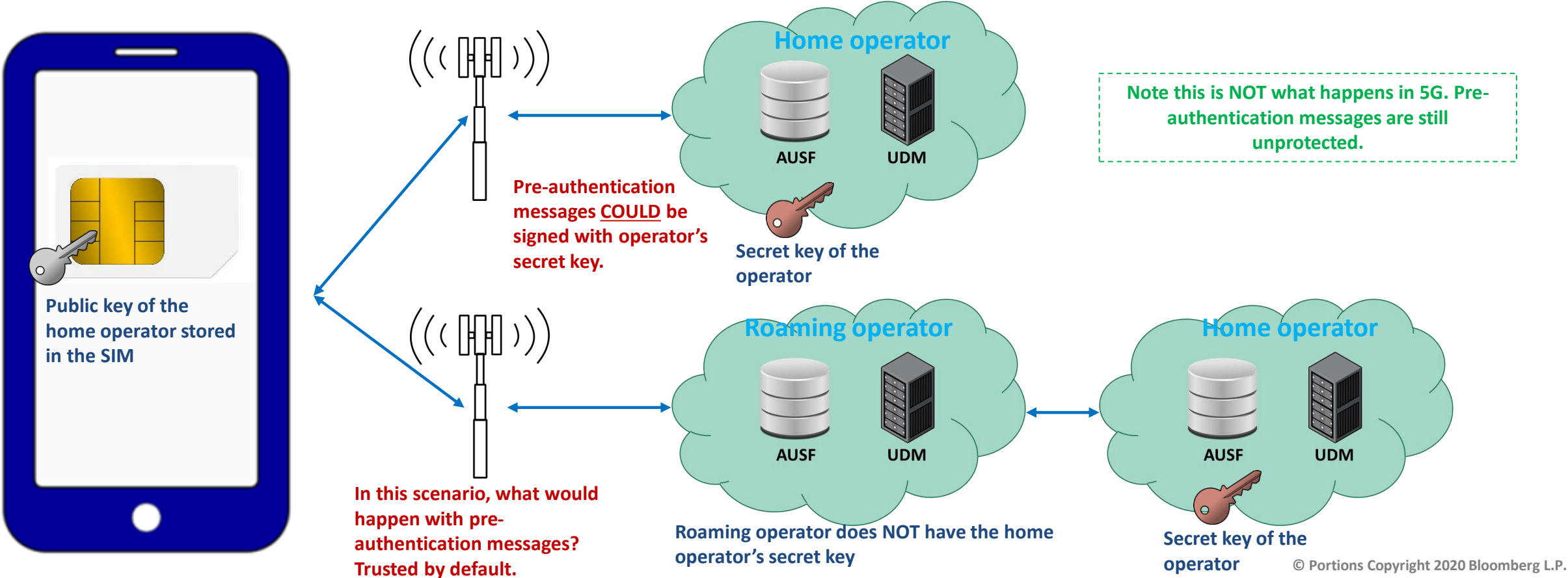
Regardless of mutual authentication and strong encryption, a 5G mobile device engages in a substantial exchange of unprotected messages with *any* 5G base station (malicious or not) that advertises itself with the right broadcast information.

Abusing these messages causes most LTE protocol exploits to still apply in 5G, renders SUPI encryption potentially useless and allows to track 5G devices.

Are we there yet? The long path to securing 5G mobile communication networks
<https://www.linkedin.com/pulse/we-yet-long-path-securing-5g-mobile-communication-piqueras-jover>

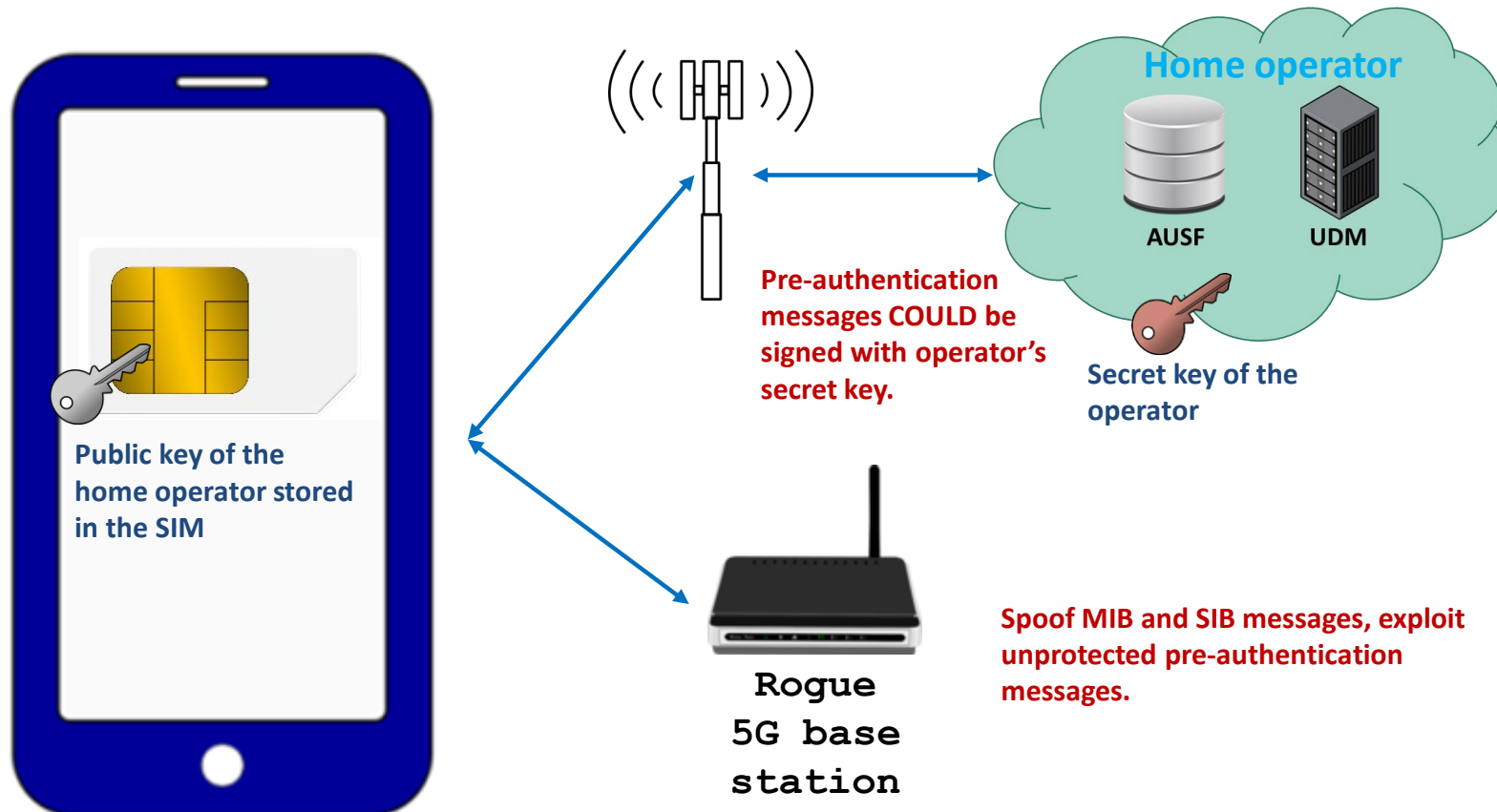
5G (IN)SECURITY RATIONALE

- 5G still does not provide any means to verify the validity of a base station before communicating with it
 - Operator’s public key in the SIM works for SUPI encryption
 - It does NOT work to prevent pre-authentication message-based exploits



5G (IN)SECURITY RATIONALE

- 5G still does not provide any means to verify the validity of a base station before communicating with it
 - Operator's public key in the SIM works for SUPI encryption
 - It does NOT work to prevent pre-authentication message-based exploits



Note this is NOT what happens in 5G. Pre-authentication messages are still unprotected.

5G RNTI-BASED TRACKING

- RNTI-based device tracking and fingerprinting
 - Again, for the record, 3GPP TR 33.899 V1.3.0 (2017-08) claimed RNTI tracking was not a security issue in LTE...
 - Combination of RNTI with other layer 2 identities

Process interval: 0 ms | 140.2013333: ms

WaveJudge Messages List

Name	Start Ti...	Cell ID	Frame N...	D...	Error Chec	# Bytes	RNTI
MIB	0019.18			D	OK	3	
PRACH	0023.67	8	250	U			
MAC Random Access Response	0026.18			D	OK	10	129
RRCSetupRequest	0028.18			U	OK	6	372
MIB	0039.18			D	OK	3	
RRCSetup	0055.68			D	OK	58	372
MIB	0059.18			D	OK	3	
MIB	0079.18			D	OK	3	
SIB1	0084.18			D	OK	123	65535
RRCSetupComplete	0088.68			U	OK	100	372
MIB	0099.18			D	OK	3	
UECapabilityEnquiry	0100.18			D	OK	21	372
DLInformationTransfer	0114.18			D	OK	7	372
MIB	0119.18			D	OK	3	
SIB2,3,4	0124.18			D	OK	36	65535
UECapabilityInformation	0138.68			U	OK	259	372
MIB	0139.18			D	OK	3	

MAC Random Access Response at 26.18 ms

- MAC Random Access Response
 - Sub Header 0
 - E 1 => True
 - T 0
 - Reserved OK
 - BI 0 => 5 ms
 - Sub Header 1
 - E 0 => False
 - T 1
 - RAPID 4
 - Reserved OK
 - Timing Advance Command 0
 - UL Grant
 - Frequency Hopping Flag 0 => False
 - Msg3 PUSCH Frequency Resource Allocation 548
 - Msg3 PUSCH Time Resource Allocation 0
 - MCS 2
 - TPC Command for Msg3 PUSCH 3
 - CSI Request 0 => False
 - T-CRNTI 372
 - Padding OK

Bit Length 80 Head 10000000 Tail 00000000 Hex 80440000224026017400
00000000 80 44 00 00 22 40 26 01 74 00

“Demo” time

Let’s look at some captures of real 5G traffic...

UE CAPABILITY INQUIRY

- Known vulnerability in LTE
 - Fingerprint the type of device based solely on the capabilities disclosed in this unprotected messages
 - Bidding down attacks, battery drain...
 - Implemented in LTE with SW radio and open-source LTE stack
- Also possible in 5G

New Vulnerabilities in 5G Networks



Altaf Shaik | M.Sc., Technical University of Berlin and Kaitiaki Labs

Ravishankar Borgaonkar | Dr., SINTEF Digital

Location: South Pacific

Date: Wednesday, August 7 | 1:30pm-2:20pm

Format: 50-Minute Briefings

Tracks:  Mobile,  Network Defense

POSTED: 9 AUG, 2019 | 2 MIN READ | [FEATURE STORIES](#)

BlackHat 2019: Don't Assume that 5G Networks Can't Get Hacked

5G security roadmap?

THE CURRENT STATE OF AFFAIRS IN 5G SECURITY

- An increasing number of vulnerabilities identified before 5G even goes live
 - This can be a good thing, things can still be fixed...
 - Topic that fascinates me
 - <https://softhandover.wordpress.com/2018/12/06/the-current-state-of-affairs-in-5g-security/>
 - Jover, Roger Piqueras. "The current state of affairs in 5G security and the main remaining security challenges." arXiv preprint arXiv:1904.08394 (2019).

The current state of affairs in 5G security

December 6, 2018 in 5G, LTE, security, wireless

- Martin Dehnel-Wild and Cas Cremers: [Authentication vulnerability in the most recent 5G AKA draft](#). [February 2018]
- Roger Piqueras Jover, Vuk Marojevic: [Security and Protocol Exploit Analysis of the 5G Specifications](#). [September 2018]
- Basin, David and Dreier, Jannik and Hirschi, Lucca and Radomirovic, Sa\{v\}s}a and Sasse, Ralf and Stettler, Vincent: [A Formal Analysis of 5G Authentication](#). [October 2018]
- Adrien Koutsos: [The 5G-AKA Authentication Protocol Privacy](#). [November 2018]
- Mohsin Khan, Philip Ginzboorg, Kimmo Järvinen, Valteri Niemi: [Defeating the Downgrade Attack on Identity Privacy in 5G](#). [November 2018]
- Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park, and Altaf Shaik: [New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols](#). [December 2018]
- Cas Cremers, Martin Dehnel-Wild: [Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion](#). Network and Distributed Systems Security (NDSS) Symposium 2019. [December 2018]

THE CURRENT STATE OF AFFAIRS IN 5G SECURITY

- Formal verification analysis of the 5G specifications
 - A number of new theoretical protocol vulnerabilities identified
 - Really exciting work going on in this area!
 - All vulnerabilities identified exist due to pre-authentication messages and other unprotected control traffic

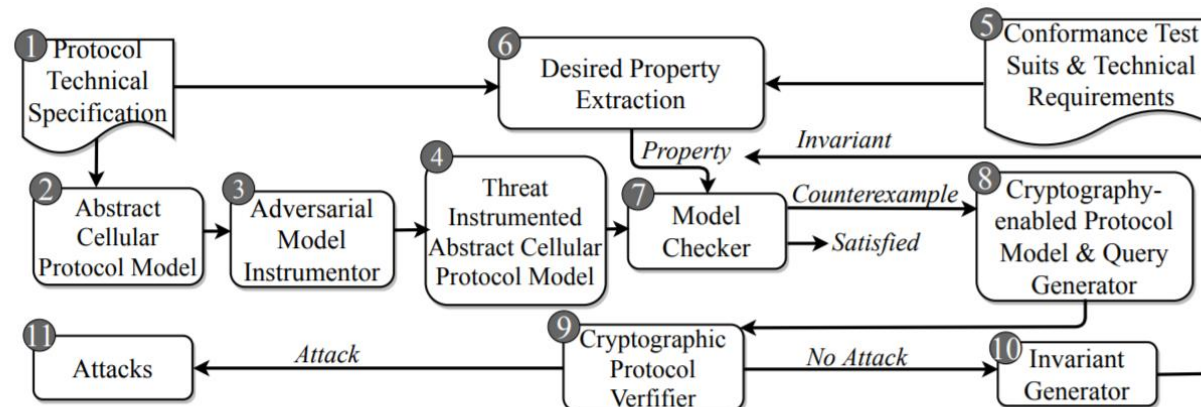
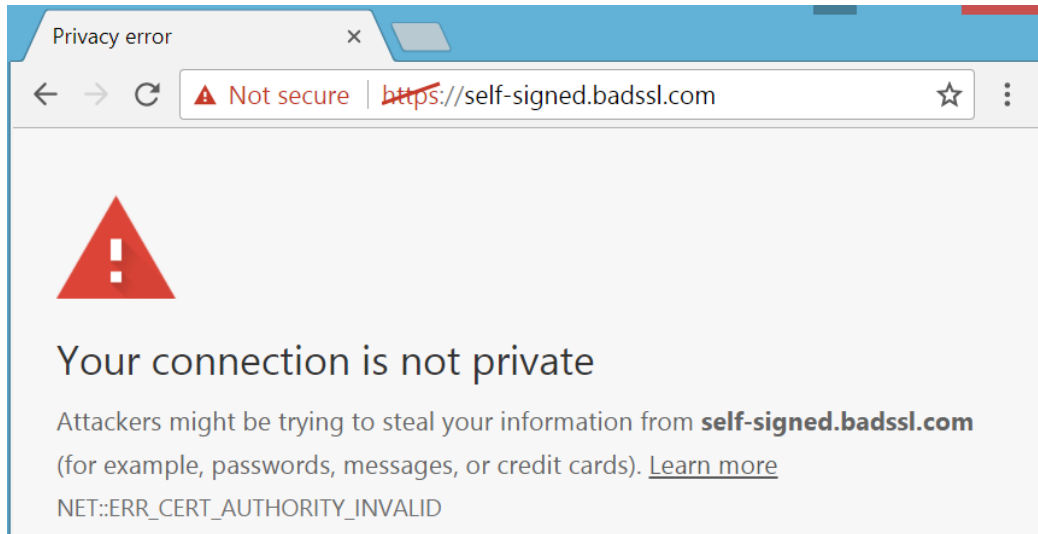


Figure 3: 5GReasoner Architecture.

ROOT CAUSE FOR MOST VULNERABILITIES

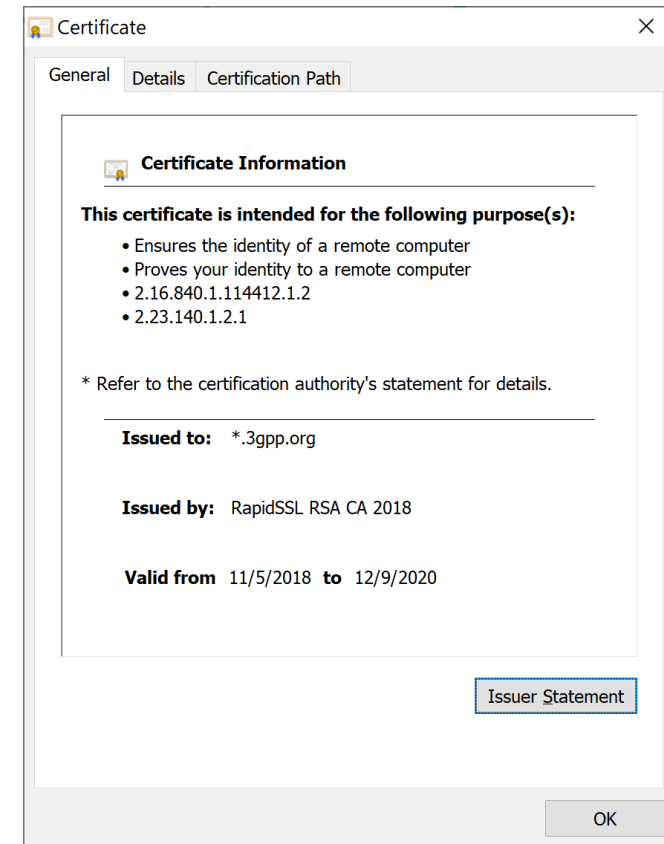
- How do we fix the challenge with pre-authentication messages?
 - It has been a big security challenge in cellular throughout all Gs



You would not trust a self-signed certificate on an eCommerce site and type in your login or credit card number. Why would you trust a plain-text MIB/SIB message that claims a given tower is your operator?

5G SECURITY ROADMAP?

- How do we fix the challenge with pre-authentication messages?
 - It has been a big security challenge in cellular throughout all Gs
 - Using public keys without defining how to manage them, rotate them, etc is NOT the right way
- PKI and Digital Certificates?
 - Mature technology
 - Makes the Internet “trustworthy” to use
 - And by that I mean that I am personally ok to type my cc number in a reliable site with a valid cert...



5G SECURITY ROADMAP?

- PKI and Digital Certificates in cellular?
 - Why not?
 - Probably not a single root CA
 - Each country runs and admin its own root CA?
 - Each operator runs a sub CA?
 - Flexibility for operators worldwide to decide who do they trust and who they don't
 - List of root CAs loaded in your browser \leftrightarrow List of root CAs loaded on your SIM
- It is not easy
 - Global effort standards+industry
 - Cert revocation? (your phone is not always "online")
- But it is definitively possible!

DIGITAL CERTIFICATES IN CELLULAR NETWORKS?

- X509 certs in cellular
 - Just a few messages need to be signed
 - Perhaps SIB messages and RRC handshake plus responses to AttachRequest and TAURequest etc?
- Hussain, Syed Rafiul, Mitziu Echeverria, Ankush Singla, Omar Chowdhury, and Elisa Bertino. "Insecure connection bootstrapping in cellular networks: the root of all evil." In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, pp. 1-11. ACM, 2019.
 - IMO, the greatest thing to happen in mobile network security research in years!

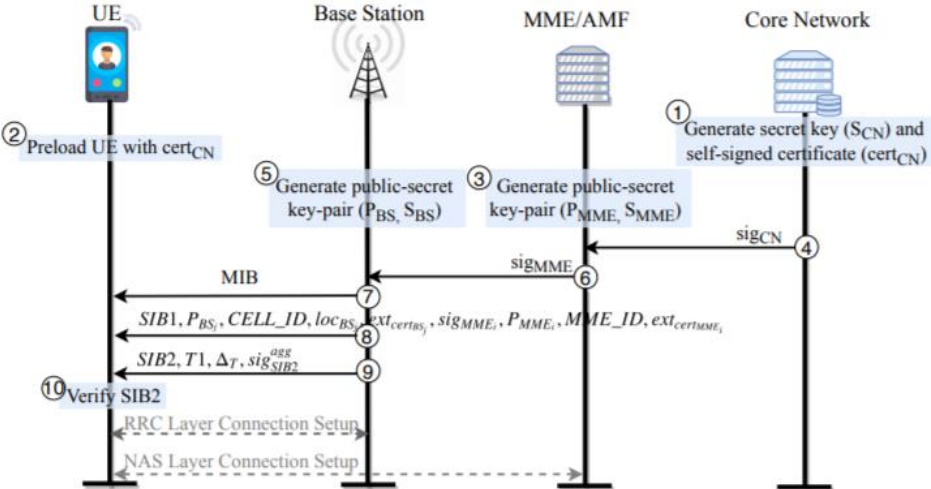


Figure 8: Optimized PKI Scheme.

Thanks!

If you are a PhD student, PostDoc, professor, etc. interested in 5G security and in using similar 5G security research equipment, contact me!

Roger Piqueras Jover
@rgoestotheshows
<http://rogerpiquerasjover.net/>