EXPLORING LTE SECURITY WITH OPEN-SOURCE TOOLS, TESTING PROTOCOL EXPLOITS AND ANALYZING THEIR POTENTIAL IMPACT ON 5G NETWORKS

Roger Piqueras Jover

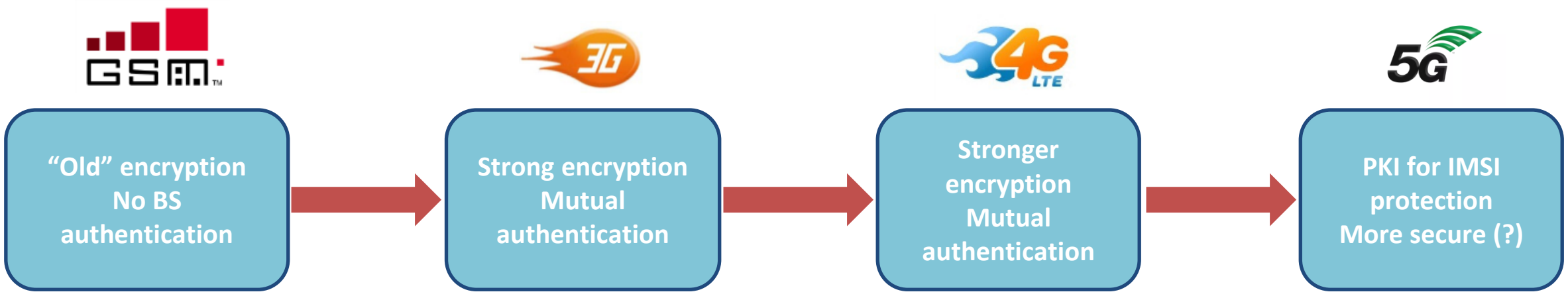
rpiquerasjov@bloomberg.net

ABOUT ME

- Recent dad who goes to a lot of live music shows, plays and watches too much soccer, and does some security research on the side
- Security Researcher (aka Senior Security Architect), Office of the CTO at Bloomberg
- Formerly (5 years) Principal Member of Technical Staff at AT&T Security Research
- Mobile/wireless network security research
  - Mostly LTE PHY and upper layers
- If it communicates wirelessly, I am interested in its security
  - BLE
  - 802.11
  - Zigbee, Zigwave
  - LoRaWAN
- More details
  - http://rogerpiquerasjover.net/  @rgoestotheshows

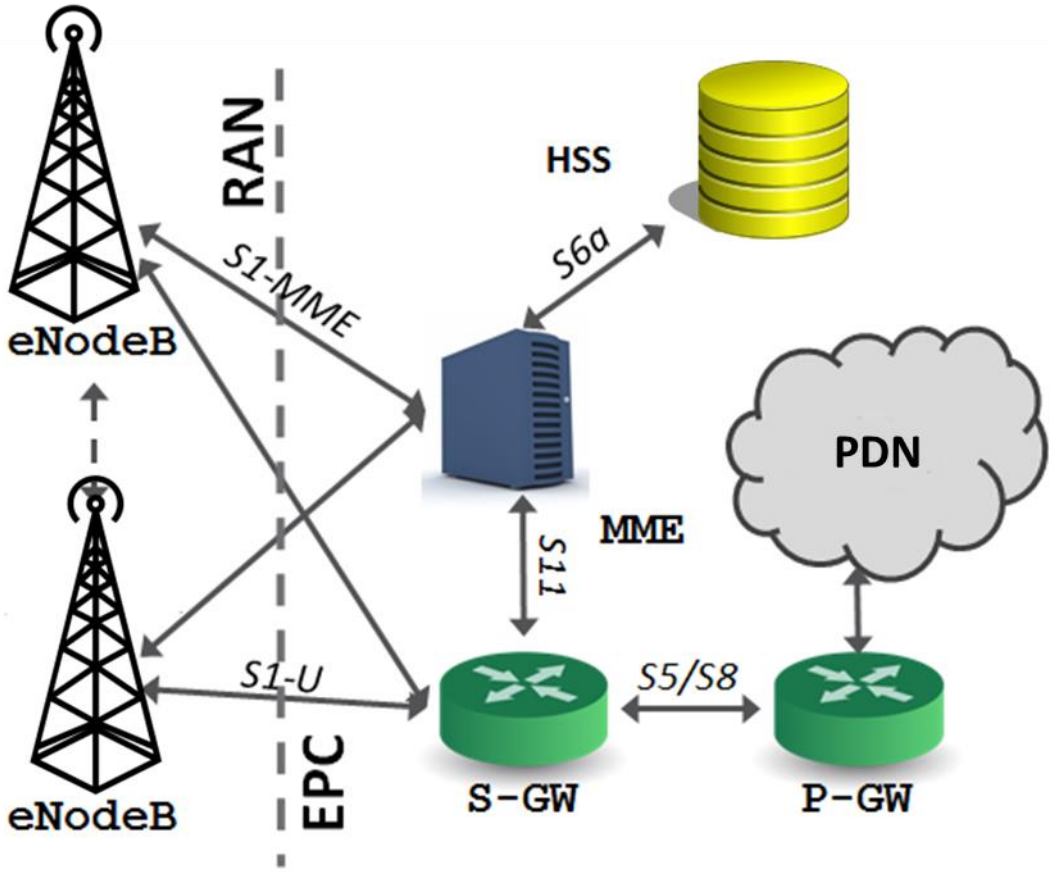
EXPLORING MOBILE NETWORK PROTOCOL SECURITY

The first mobile networks were not designed with a strong security focus (no support for encryption in 1G!!!)

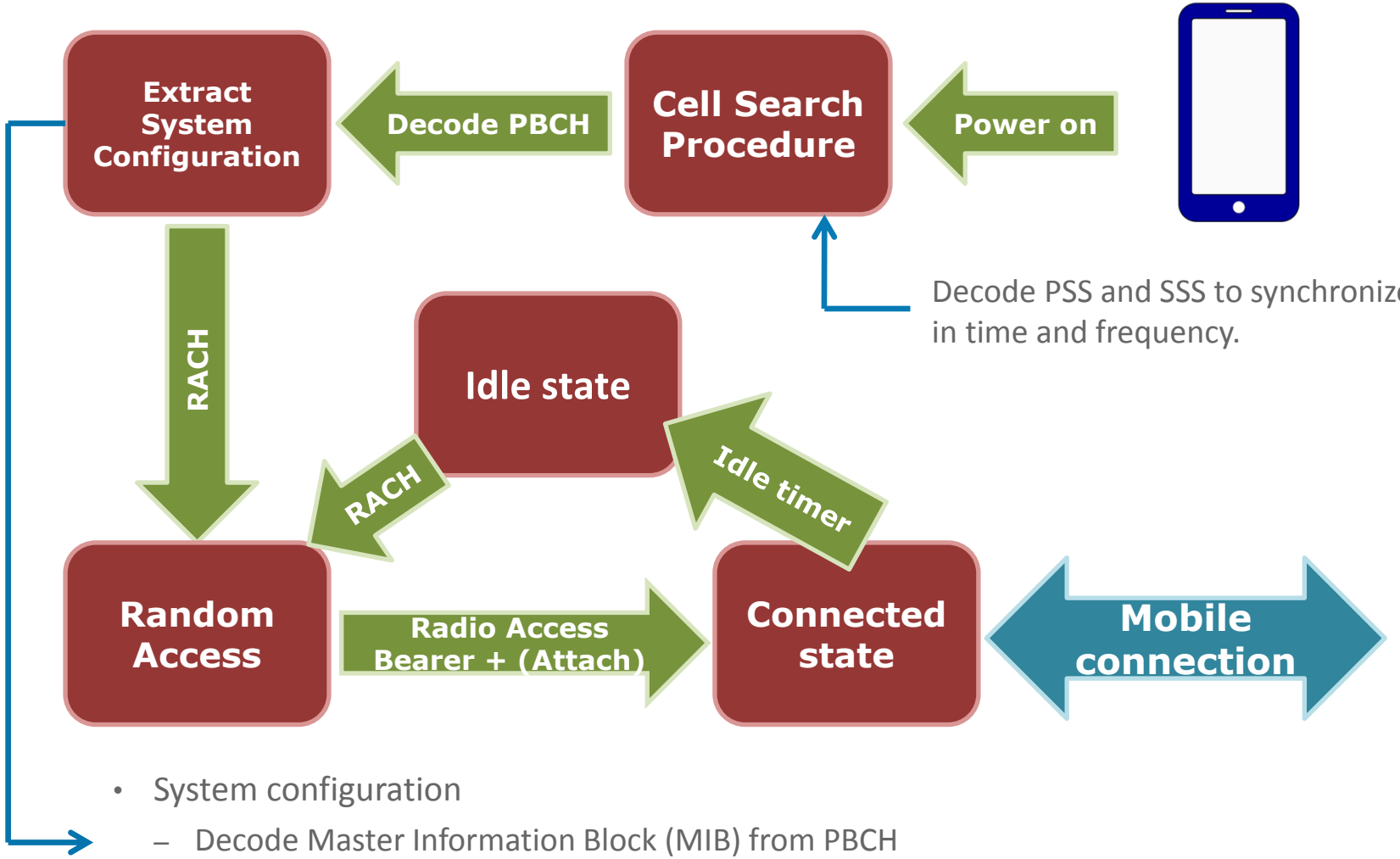


LTE BASICS

LTE MOBILE NETWORK ARCHITECTURE

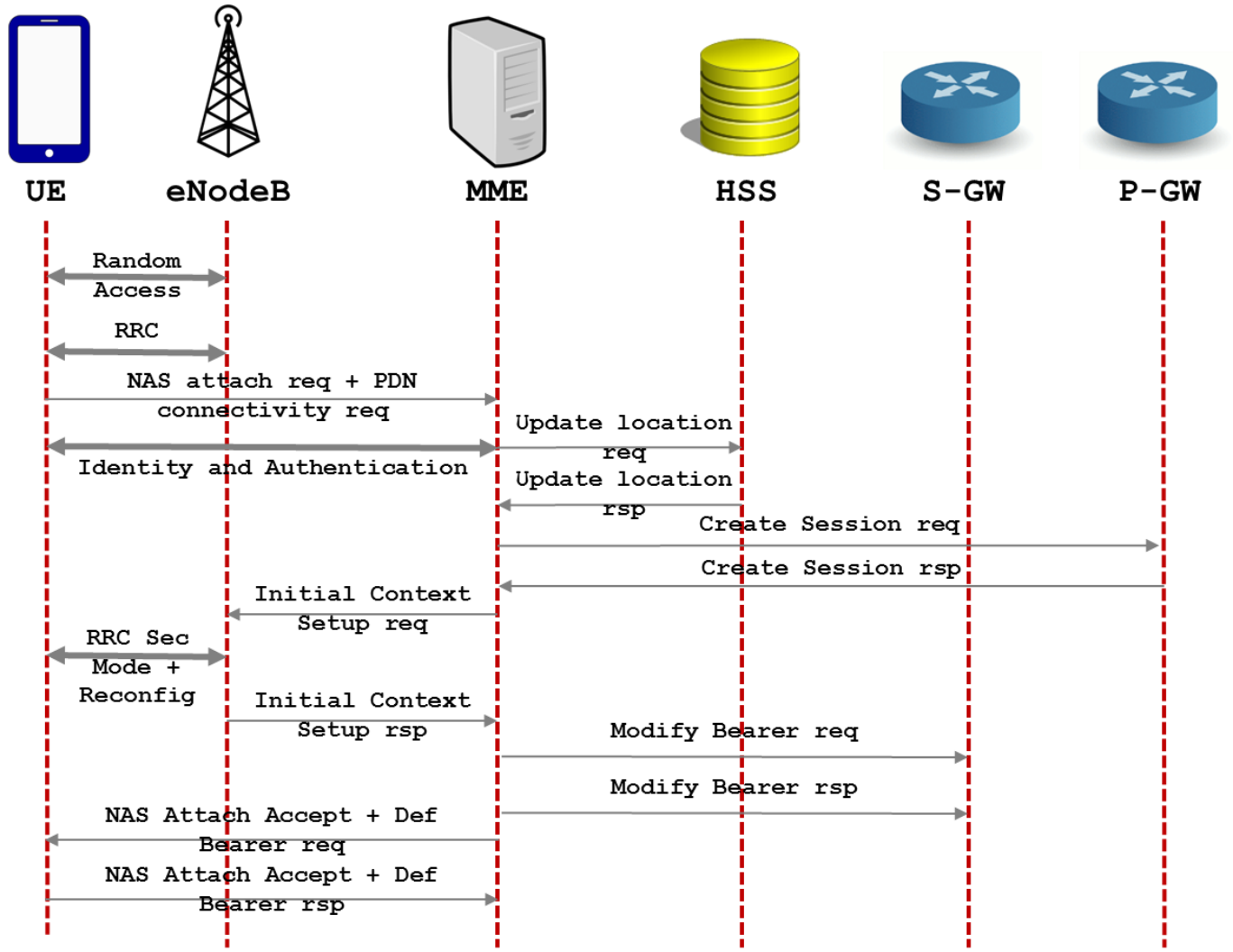


LTE CELL SELECTION AND CONNECTION

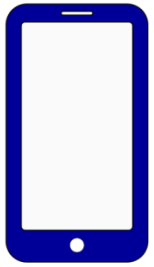


- System configuration
  - Decode Master Information Block (MIB) from PBCH
  - Decode System Information Blocks (SIBs) from PDSCH

LTE NAS ATTACH PROCEDURE



MOBILE NETWORK USER/DEVICE IDENTIFIERS



IMEI – “Serial number” of the device

IMSI – secret id of the SIM that should never be disclosed
TMSI – temporary id used by the network once it knows who you are

MSISDN – Your phone number.

LTE (IN)SECURITY RATIONALE

LTE (IN)SECURITY RATIONALE

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 RATIONALE

IntelliJudge

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. I can sniff these messages and I can transmit them pretending to be a legitimate base station.

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 RATIONALE

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.

Spoiler alert – This also potentially applies to 5G. No viable solution proposed in the specifications yet.

(more on this later)

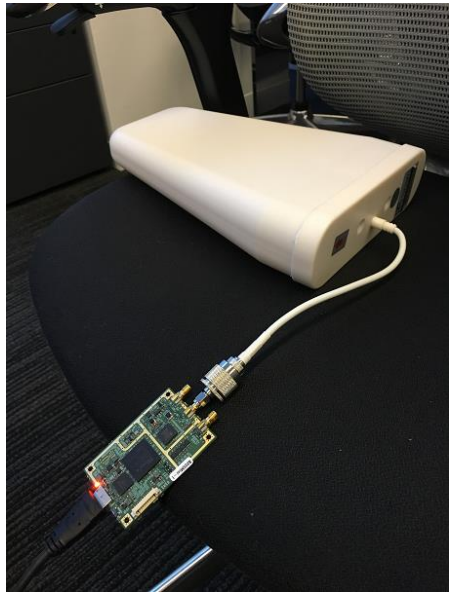
EXPLORING LTE SECURITY WITH SOFTWARE-RADIO

TOOLSET

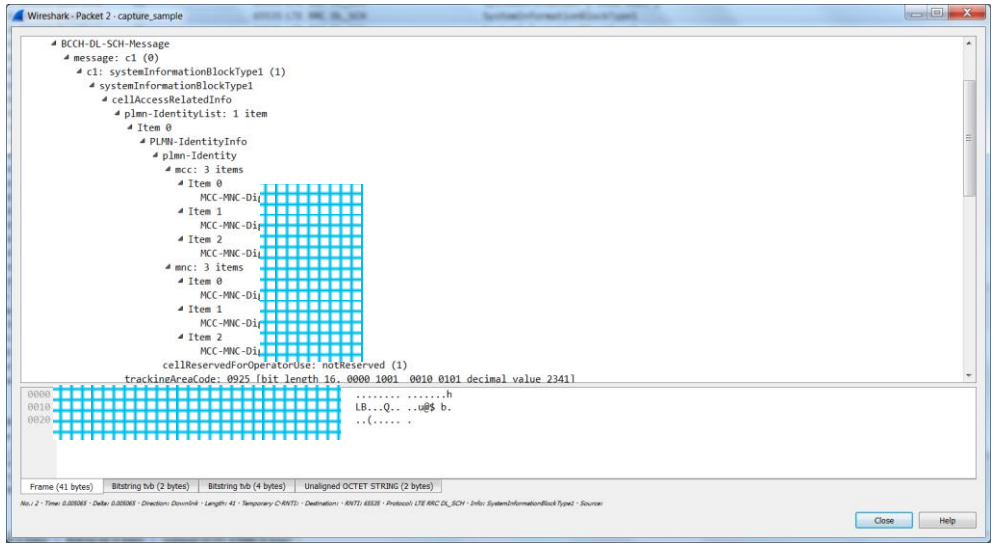
- LTE open source implementation (eNB+UE)
  - Modified srsLTE – https://github.com/srsLTE
    - **First available UE stack implementation!!!!!!**
    - LTE sniffer
  - Modifications to source for protocol exploit experimentation
- HW setup
  - USRP B210/USRP mini for active rogue base station
  - BUDGET: USRP B210 ($1100) + GPSDO ($625) + LTE Antenna (2x$30) = $1785
  - Machine running Ubunutu 16

All LTE active radio experiments MUST be performed inside a faraday cage!!!

SNIFFING BASE STATION CONFIGURATION



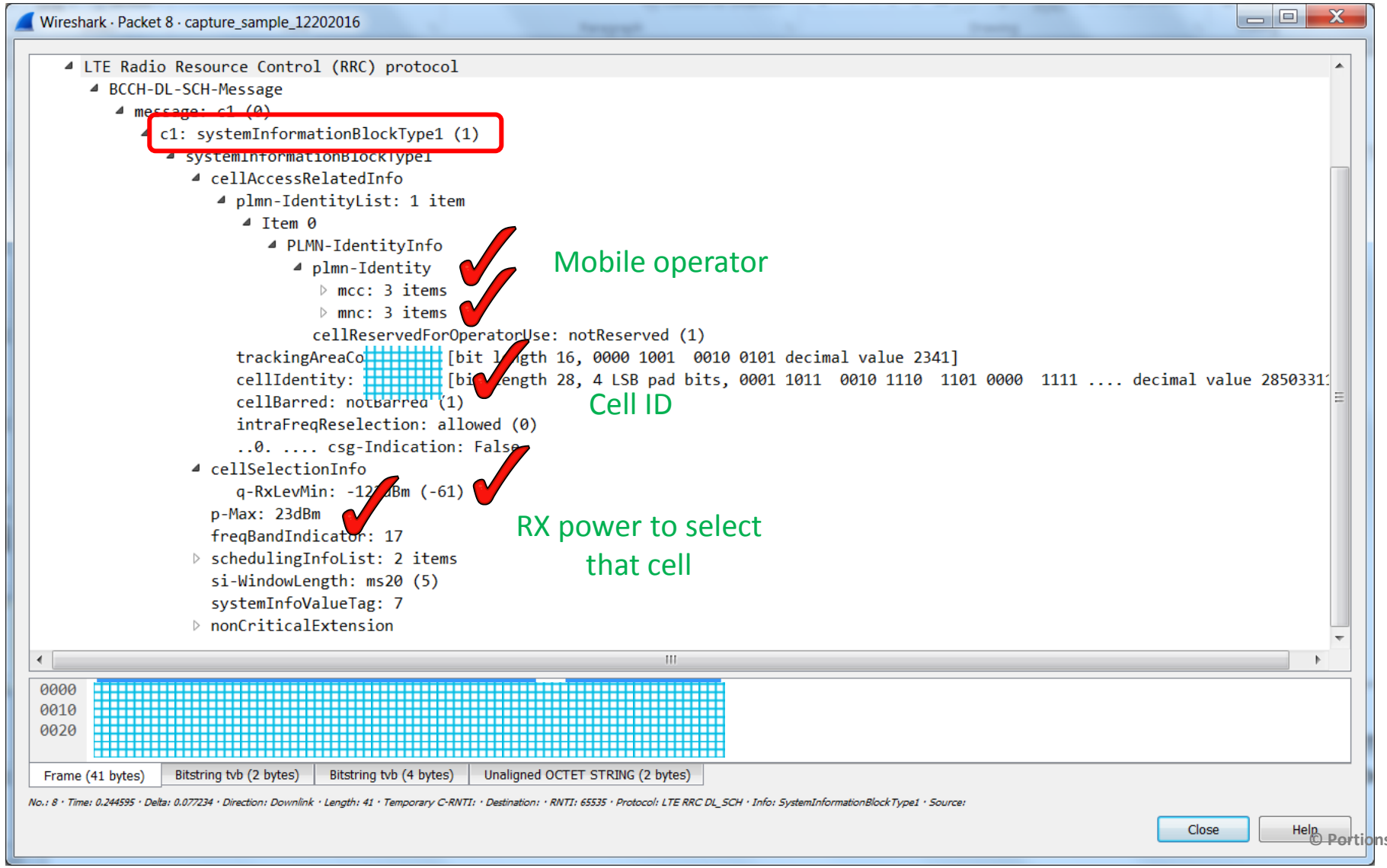
- Base station configuration broadcasted in the clear in MIB and SIB messages.
- srsLTE + AirScope
  - Dump everything on pcap
- Very useful information that could be leveraged by and adversary
  - Optimal tx power for a rogue base station
  - High priority frequencies to force priority cell reselection
  - Tracking Area of the legitimate cell (use a different one in your rogue eNodeB to force TAU update messages)
  - Mapping of signaling channels
  - Paging channel mapping and paging configuration
- Broadcast message scanning tools available in both srsLTE and openLTE



LTE/LTE-A Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation. Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, Jeffrey H. Reed. IEEE Communications Magazine. Special issue on Critical Communications and Public Safety Networks. April 2016.

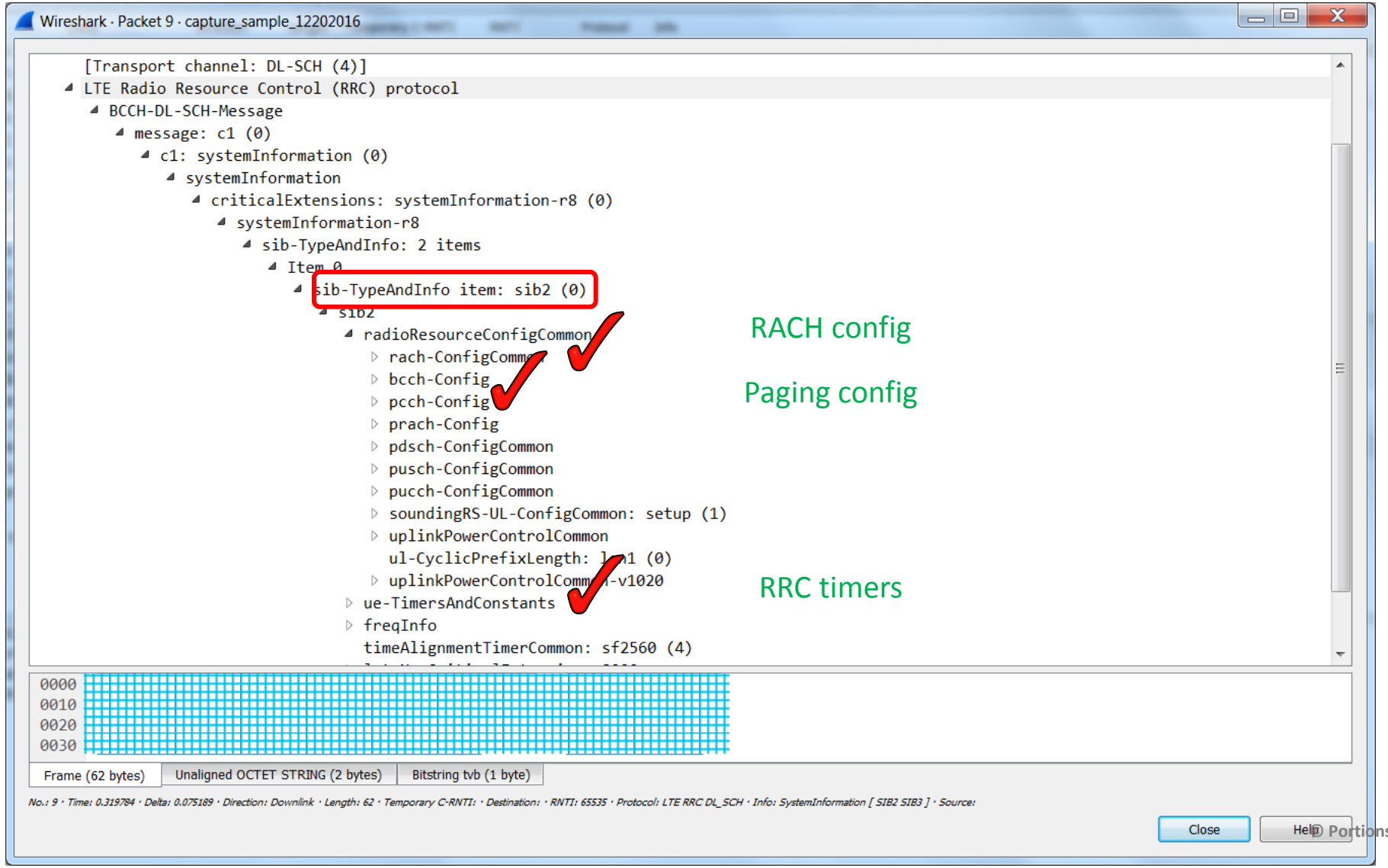
SNIFFING BASE STATION CONFIGURATION

LTE PDSCH SIB1 packet



SNIFFING BASE STATION CONFIGURATION

LTE PDSCH SIB2/3 packet



SNIFFING BASE STATION CONFIGURATION

- MIB/SIB messages are necessary for the operation of the network
  - Some things must be sent in the clear (i.e. a device connecting for the first time)
  - But perhaps not everything
- Things an attacker can learn from MIB and SIB messages
  - Optimal tx power for a rogue base station (no need to set up your USRP to its max tx power)
  - High priority frequencies to force priority cell reselection
  - Mobile operator who owns that tower
  - Tracking Area of the legitimate cell (use a different one in your rogue eNodeB to force TAU update messages)
  - Mapping of signaling channels
  - Paging channel mapping and paging configuration
  - Etc

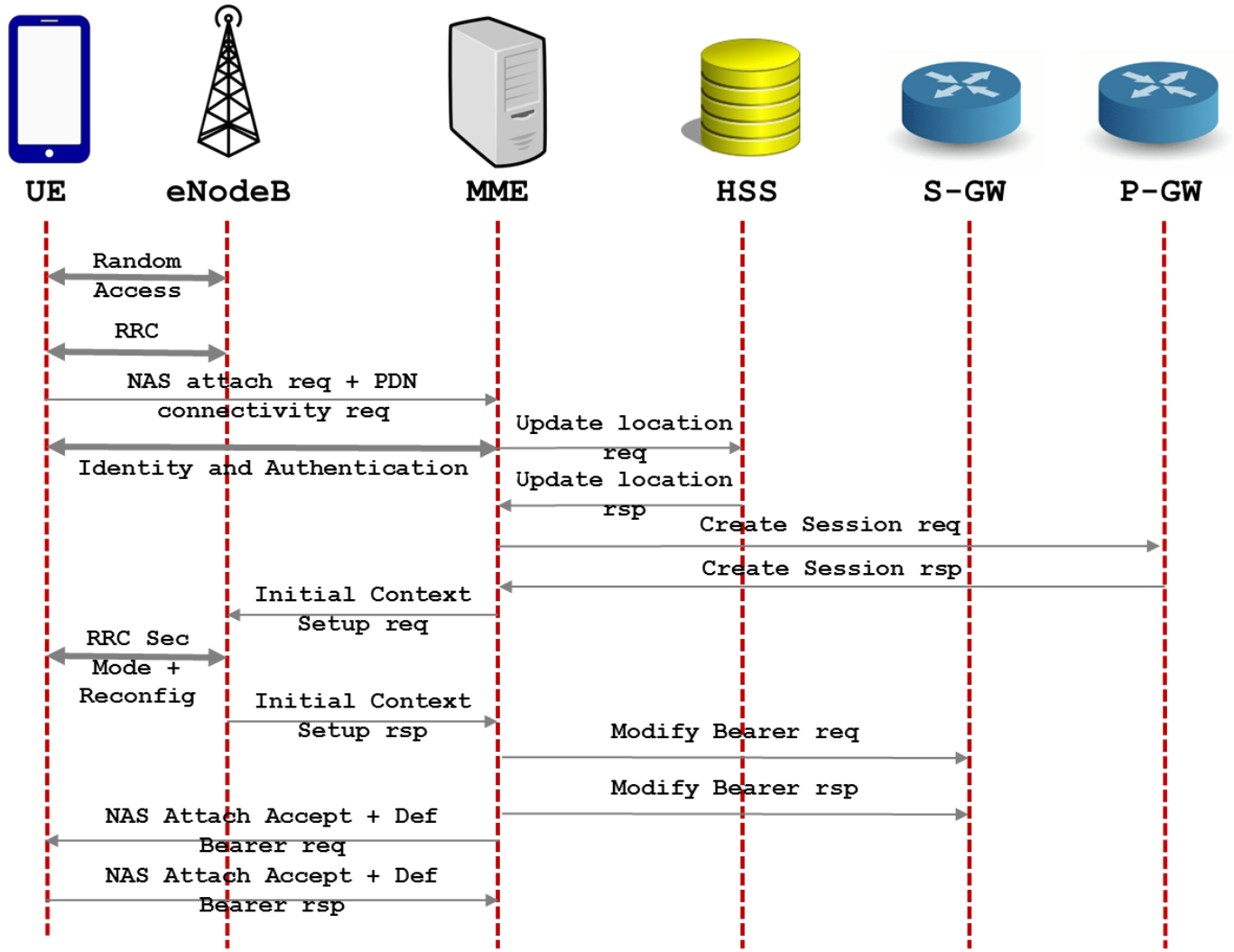
LTE/LTE-A Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation. Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, Jeffrey H. Reed. **IEEE Communications Magazine.** Special issue on Critical Communications and Public Safety Networks. April 2016.

LOW-COST LTE IMSI CATCHER (STINGRAY)

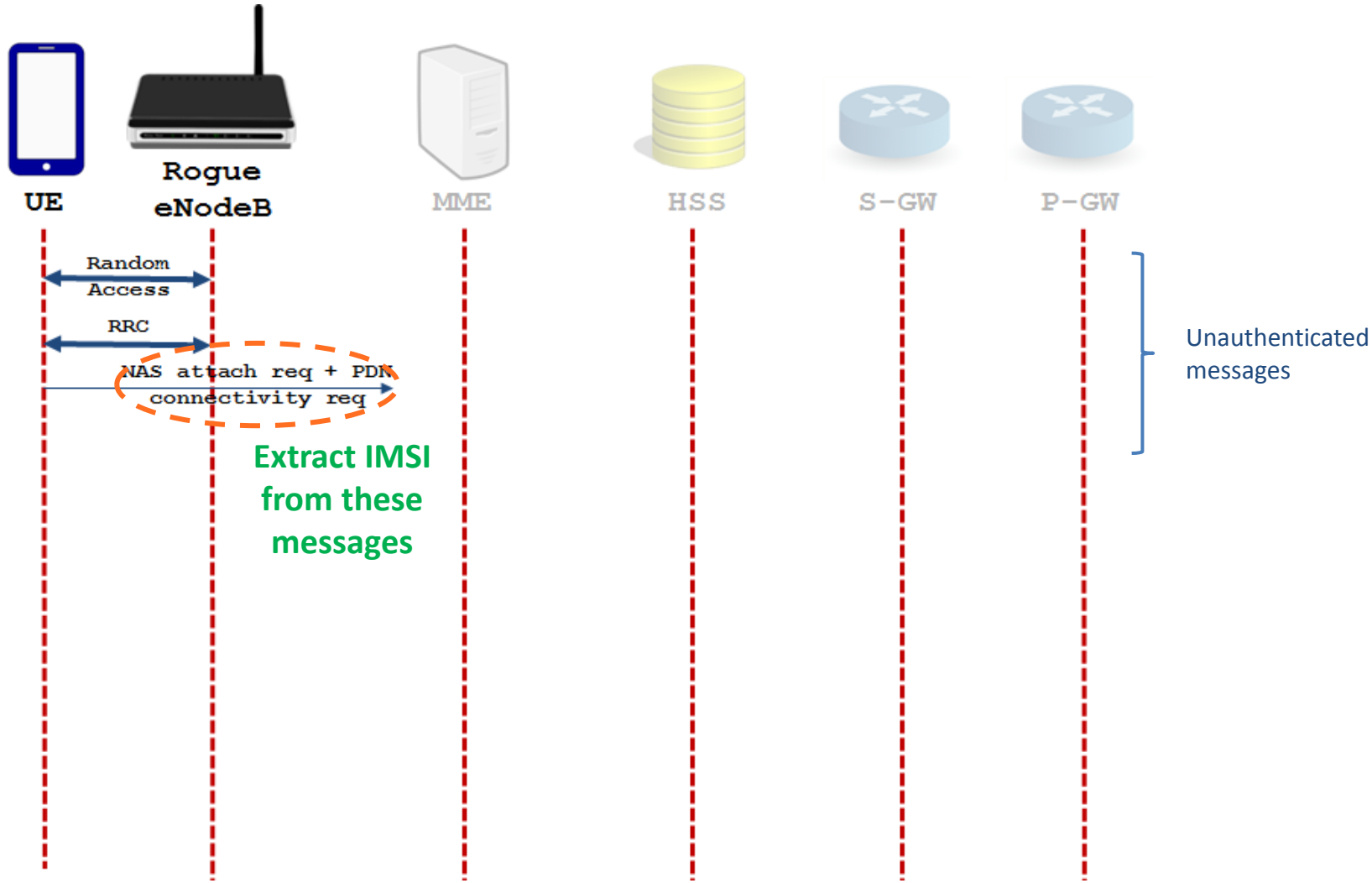
- Despite common assumptions, in LTE the IMSI is always transmitted in the clear at least once
  - If the network has never seen that UE, it must use the IMSI to claim its identity
  - A UE will trust *any* eNodeB that claims it has never seen that device (pre-authentication messages)
  - IMSI can also be transmitted in the clear in error recovery situations (very rare)

- Implementation
  - USRP B210 + Ubuntu 16 + gnuradio 3.7.2
  - LTE base station – srsLTE (slightly modified)
    - Added feature to record IMSI from Attach Request messages
  - Send attach reject after IMSI collection
  - Very simple to implement
    - Mjølsnes, Stig F., and Ruxandra F. Olimid. "Easy 4G/LTE IMSI Catchers for Non-Programmers." In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, pp. 235-246. Springer, Cham, 2017.

IMSI CATCHERS(STINGRAY)



IMSI CATCHERS(STINGRAY)



LOW-COST LTE IMSI CATCHER (STINGRAY)

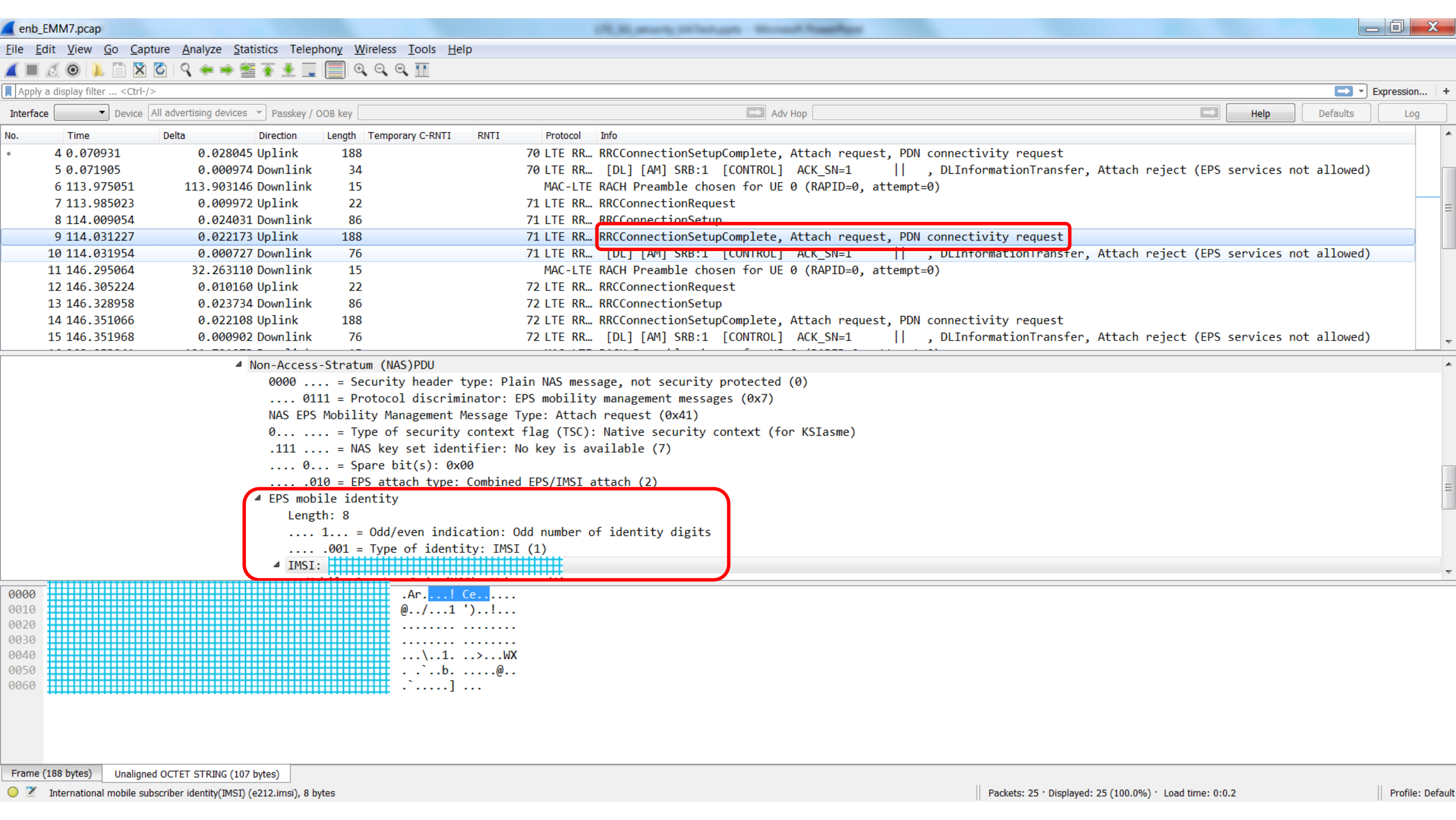
- AttachRequest message processing
  - s1ap_nas_transport.cc

```
//Get attach type from attach request
if(attach_req.eps_mobile_id.type_of_id == LIBLTE_MME_EPS_MOBILE_ID_TYPE_IMSI)
{
  m_s1ap_log->console("Attach Request -- IMSI-style attach request\n");
  m_s1ap_log->info("Attach Request -- IMSI-style attach request\n");
  handle_nas_imsi_attach_request(enb_ue_s1ap_id, attach_req, pdn_con_req, reply_buffer, reply_flag, enb_sri);
}
else if(attach_req.eps_mobile_id.type_of_id == LIBLTE_MME_EPS_MOBILE_ID_TYPE_GUTI)
{
  m_s1ap_log->console("Attach Request -- GUTI-style attach request\n");
  m_s1ap_log->info("Attach Request -- GUTI-style attach request\n");
  handle_nas_guti_attach_request(enb_ue_s1ap_id, attach_req, pdn_con_req, nas_msg, reply_buffer, reply_flag, enb_sri);
}
else
{
  m_s1ap_log->error("Unhandle Mobile Id type in attach request\n");
  return false;
}
```

LOW-COST LTE IMSI CATCHER (STINGRAY)

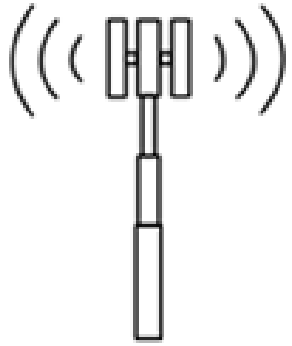
- Export/save IMSI when processing AttachRequest message

```
s1ap_nas_transport::handle_nas_imsi_attach_request(uint32_t enb_ue_s1ap_id,
                                                   const LIBLTE_MME_ATTACH_REQUEST_MSG_STRUCT &attach_req,
                                                   const LIBLTE_MME_PDN_CONNECTIVITY_REQUEST_MSG_STRUCT &pdn_con_req,
                                                   srslte::byte_buffer_t *reply_buffer,
                                                   bool* reply_flag,
                                                   struct sctp_sndrcvinfo *enb_sri)
{
  uint8_t     k_asme[32];
  uint8_t     autn[16];
  uint8_t     rand[16];
  uint8_t     xres[8];

  ue_ctx_t ue_ctx;
  ue_emm_ctx_t *emm_ctx = &ue_ctx.emm_ctx;
  ue_ecm_ctx_t *ecm_ctx = &ue_ctx.ecm_ctx;

  //Set UE's EMM context
  uint64_t imsi = 0;
  for(int i=0;i<=14;i++){
    imsi += attach_req.eps_mobile_id.imsi[i]*std::pow(10,14-i);
  }
```

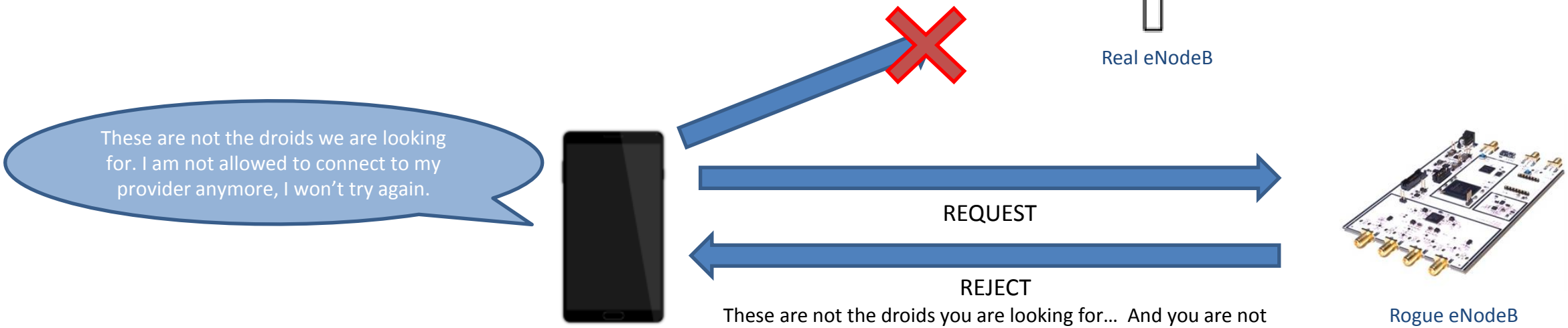

enb_EMM7.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Interface Device All advertising devices Passkey / OOB key Adv Hop Help Defaults Log
No. Time Delta Direction Length Temporary C-RNTI RNTI Protocol Info
4 0.070931 0.028045 Uplink 188 70 LTE RR… RRCConnectionSetupComplete, 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)
6 113.975051 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… RRCConnectionRequest
8 114.009054 0.024031 Downlink 86 71 LTE RR… RRCConnectionSetup
9 114.031227 0.022173 Uplink 188 71 LTE RR… RRCConnectionSetupComplete, 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… RRCConnectionRequest
13 146.328958 0.023734 Downlink 86 72 LTE RR… RRCConnectionSetup
14 146.351066 0.022108 Uplink 188 72 LTE RR… RRCConnectionSetupComplete, 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)
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:
0000 .Ar. ...! Ce.. ....
0010 @../...1 ')..!...
0020 ....
0030 ....
0040 ...\..1. ..>...WX
0050 . .`..b. .....@..
0060 .`.....] ...
Frame (188 bytes)
Unaligned OCTET STRING (107 bytes)
International mobile subscriber identity(IMSI) (e212.imsi), 8 bytes
Packets: 25 · Displayed: 25 (100.0%) · Load time: 0:0.2
Profile: Default

DEVICE AND SIM TEMPORARY LOCK

- Attach reject and TAU (Tracking Area Update) reject messages not encrypted/integrity-protected
- Spoofing this messages one can trick a device to
  - Believe it is not allowed to connect to the network (blocked)
  - Believe it is supposed to downgrade to or only allowed to connect to GSM



Real eNodeB

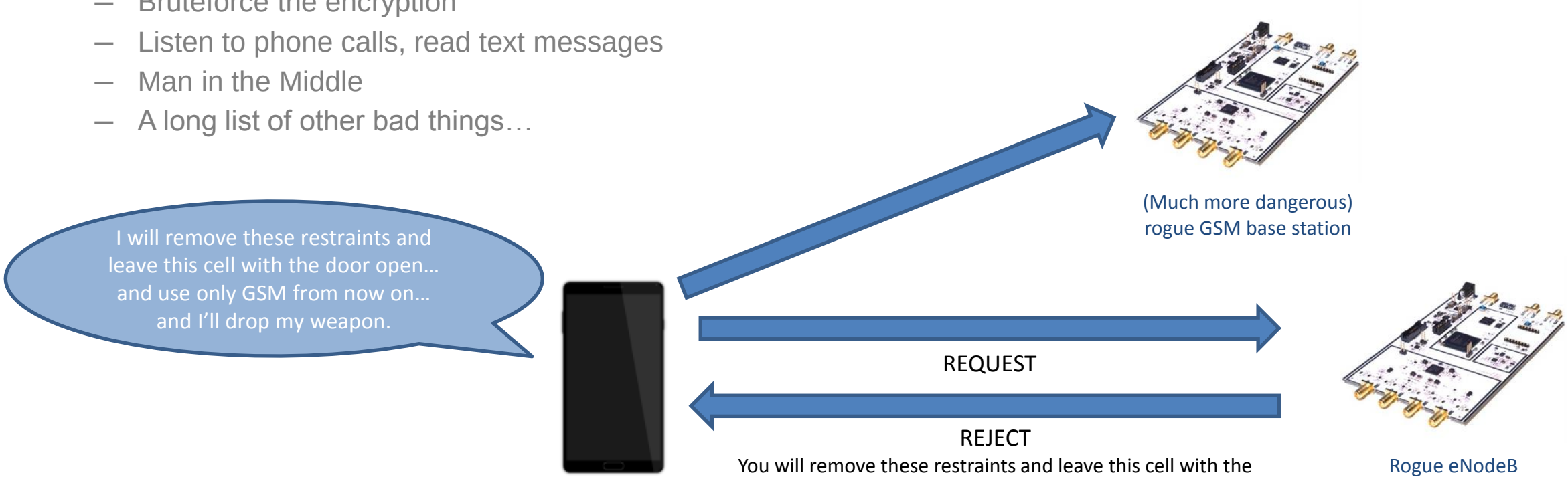


Jover, Roger Piqueras. "LTE security, protocol exploits and location tracking experimentation with low-cost software radio." *arXiv preprint arXiv:1607.05171* (2016).

SOFT DOWNGRADE TO GSM

- Use similar techniques to “instruct” the phone to downgrade to GSM
  - Only GSM services allowed OR LTE and 3G not allowed

- Once at GSM, the phone to connects to your rogue base station
  - Bruteforce the encryption
  - Listen to phone calls, read text messages
  - Man in the Middle
  - A long list of other bad things…



Jover, Roger Piqueras. "LTE security, protocol exploits and location tracking experimentation with low-cost software radio." *arXiv preprint arXiv:1607.05171* (2016).

enb_EMM7.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

Interface Device All advertising devices Passkey / OOB key Adv Hop Help Defaults Log

No.	Time	Delta	Direction	Length	Temporary C-RNTI	RNTI	Protocol	Info
2	0.009992	0.009992	Uplink	22		70	LTE RR…	RRCConnectionRequest
3	0.042886	0.032894	Downlink	86		70	LTE RR…	RRCConnectionSetup
4	0.070931	0.028045	Uplink	188		70	LTE RR…	RRCConnectionSetupComplete, 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	113.975051	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…	RRCConnectionRequest
8	114.009054	0.024031	Downlink	86		71	LTE RR…	RRCConnectionSetup
9	114.031227	0.022173	Uplink	188		71	LTE RR…	RRCConnectionSetupComplete, 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…	RRCConnectionRequest
13	146.328958	0.023734	Downlink	86		72	LTE RR…	RRCConnectionSetup

```
    rrc-TransactionIdentifier: 0
  ▲ criticalExtensions: c1 (0)
    ▲ c1: dlInformationTransfer-r8 (0)
      ▲ dlInformationTransfer-r8
        ▲ dedicatedInfoType: dedicatedInfoNAS (0)
          ▲ dedicatedInfoNAS: 074407
            ▲ 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 reject (0x44)
              ▲ EMM cause
                  Cause: EPS services not allowed (7)
MAC: 0x00000000 [Matches calculated result]
```

```
0000
```

.D.

Frame (34 bytes) | Unaligned OCTET STRING (3 bytes)

Non-Access-Stratum (NAS)PDU (nas-eps), 3 bytes | Packets: 25 · Displayed: 25 (100.0%) · Load time: 0:0.2 | Profile: Default

DEVICE TEMPORARY LOCK AND SOFT DOWNGRADE

- Some results
  - The blocking of the device/SIM is only temporary
  - Device won’t connect until rebooted
  - SIM won’t connect until reboot
  - SIM/device bricked until timer T3245 expires (24 to 48 hours!)
  - Downgrade device to GSM and get it to connect to a rogue BS

- If the target is an M2M device, it could be a semi-persistent attack
  - Reboot M2M device remotely?
  - Send a technician to reset SIM?
  - Or just wait 48 hours for your M2M device to come back online…

Shaik, Altaf, et al. "Practical attacks against privacy and availability in 4G/LTE mobile communication systems." arXiv preprint arXiv:1510.07563 (2015).

OTHER ATTACH/TAU REJECT EXPLOITS

- 3GPP defines a number of possible EMM Cause Codes
  - Let's try them all and see what happens…

Table 9.9.3.9.1: EMM cause information element

Cause value (octet 2)

Bits 8	7	6	5	4	3	2	1	
0	0	0	0	0	0	1	0	IMSI unknown in HSS
0	0	0	0	0	0	1	1	Illegal UE
0	0	0	0	0	1	0	1	IMEI not accepted
0	0	0	0	0	1	1	0	Illegal ME
0	0	0	0	0	1	1	1	EPS services not allowed
0	0	0	0	1	0	0	0	EPS services and non-EPS services not allowed
0	0	0	0	1	0	0	1	UE identity cannot be derived by the network
0	0	0	0	1	0	1	0	Implicitly detached
0	0	0	0	1	0	1	1	PLMN not allowed
0	0	0	0	1	1	0	0	Tracking Area not allowed
0	0	0	0	1	1	0	1	Roaming not allowed in this tracking area
0	0	0	0	1	1	1	0	EPS services not allowed in this PLMN
0	0	0	0	1	1	1	1	No Suitable Cells In tracking area
0	0	0	1	0	0	0	0	MSC temporarily not reachable
0	0	0	1	0	0	0	1	Network failure
0	0	0	1	0	0	1	0	CS domain not available
0	0	0	1	0	0	1	1	ESM failure
0	0	0	1	0	1	0	0	MAC failure
0	0	0	1	0	1	0	1	Synch failure
0	0	0	1	0	1	1	0	Congestion
0	0	0	1	0	1	1	1	UE security capabilities mismatch
0	0	0	1	1	0	0	0	Security mode rejected, unspecified
0	0	0	1	1	0	0	1	Not authorized for this CSG
0	0	0	1	1	0	1	0	Non-EPS authentication unacceptable
0	0	1	0	0	0	1	1	Requested service option not authorized
0	0	1	0	0	1	1	1	CS service temporarily not available
0	0	1	0	1	0	0	0	No EPS bearer context activated
0	1	0	1	1	1	1	1	Semantically incorrect message
0	1	1	0	0	0	0	0	Invalid mandatory information
0	1	1	0	0	0	0	1	Message type non-existent or not implemented
0	1	1	0	0	0	1	0	Message type not compatible with the protocol state
0	1	1	0	0	0	1	1	Information element non-existent or not implemented
0	1	1	0	0	1	0	0	Conditional IE error
0	1	1	0	0	1	0	1	Message not compatible with the protocol state
0	1	1	0	1	1	1	1	Protocol error, unspecified

Any other value received by the mobile station shall be treated as 0110 1111, "protocol error, unspecified". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified".

FUZZING MOBILE NETWORK PROTOCOLS

- LTEFUZZ v0.1
  - Try each value of EMM Reject Cause one by one
  - Rinse and repeat
- Some observed interesting behaviors
  - Cellular modem in UE stops working (crash?)
  - Weird reconnection + reattach attempt
  - IMSI + IMEI disclosure
  - Constant retransmission/reattempt
    - Battery drain substantially fast but I need to test more
  - Induction of handover attempts to secondary eNB
- Currently triaging and reliably reproducing results
- Collaboration with 2 academic labs (any students interested?)

Table 9.9.3.9.1: EMM cause information element

Cause value (octet 2)

Bits 8	7	6	5	4	3	2	1	
0	0	0	0	0	0	1	0	IMSI unknown in HSS
0	0	0	0	0	0	1	1	Illegal UE
0	0	0	0	0	1	0	1	IMEI not accepted
0	0	0	0	0	1	1	0	Illegal ME
0	0	0	0	0	1	1	1	EPS services not allowed
0	0	0	0	1	0	0	0	EPS services and non-EPS services not allowed
0	0	0	0	1	0	0	1	UE identity cannot be derived by the network
0	0	0	0	1	0	1	0	Implicitly detached
0	0	0	0	1	0	1	1	PLMN not allowed
0	0	0	0	1	1	0	0	Tracking Area not allowed
0	0	0	0	1	1	0	1	Roaming not allowed in this tracking area
0	0	0	0	1	1	1	0	EPS services not allowed in this PLMN
0	0	0	0	1	1	1	1	No Suitable Cells In tracking area
0	0	0	1	0	0	0	0	MSC temporarily not reachable
0	0	0	1	0	0	0	1	Network failure
0	0	0	1	0	0	1	0	CS domain not available
0	0	0	1	0	0	1	1	ESM failure
0	0	0	1	0	1	0	0	MAC failure
0	0	0	1	0	1	0	1	Synch failure
0	0	0	1	0	1	1	0	Congestion
0	0	0	1	0	1	1	1	UE security capabilities mismatch
0	0	0	1	1	0	0	0	Security mode rejected, unspecified
0	0	0	1	1	0	0	1	Not authorized for this CSG
0	0	0	1	1	0	1	0	Non-EPS authentication unacceptable
0	0	1	0	0	0	1	1	Requested service option not authorized
0	0	1	0	0	1	1	1	CS service temporarily not available
0	0	1	0	1	0	0	0	No EPS bearer context activated
0	1	0	1	1	1	1	1	Semantically incorrect message
0	1	1	0	0	0	0	0	Invalid mandatory information
0	1	1	0	0	0	0	1	Message type non-existent or not implemented
0	1	1	0	0	0	1	0	Message type not compatible with the protocol state
0	1	1	0	0	0	1	1	Information element non-existent or not implemented
0	1	1	0	0	1	0	0	Conditional IE error
0	1	1	0	0	1	0	1	Message not compatible with the protocol state
0	1	1	0	1	1	1	1	Protocol error, unspecified

Any other value received by the mobile station shall be treated as 0110 1111, "protocol error, unspecified". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified".

CONNECTION HIJACKING IN LTE

- LTE layer 2 encryption and integrity protection
  - Packets with known structure
  - AES Counter Mode (AES-CTR)
  - 16 bit checksum in the IP-UDP DNS request packets

- Protocol exploit
  - Track user (RNTI)
  - Identify DNS requests
  - MitM DNS requests (some “radio” challenges)
  - Apply mask to flip bits on destination IP address
  - Forward DNS requests to malicious DNS server

Rupprecht, David, Katharina Kohls, Thorsten Holz, and Christina Pöpper. "Breaking LTE on Layer Two.“ To be presented at IEEE Security and Privacy 2019.

EXPLORING UPLINK PROTOCOL SECURITY

SRSUE

- First open-source implementation of the mobile device stack
  - https://github.com/srsLTE/srsLTE/tree/master/srsue
  - First commit May 2017

- Platform to experiment with UL pre-authentication messages

- Now researchers can analyze exploits in the eNodeB and the mobile core network
  - eNodeB and core network (MME+HSS) fuzzing!

CONNECTION DETACH HANDSHAKE

- Procedure through which the UE disconnects from the network
  - Switch off UE
  - Airplane mode
  - Remove SIM
- Can be UE initiated and does not require ACK from network (!!!)
- Authentication/integrity protection (???)

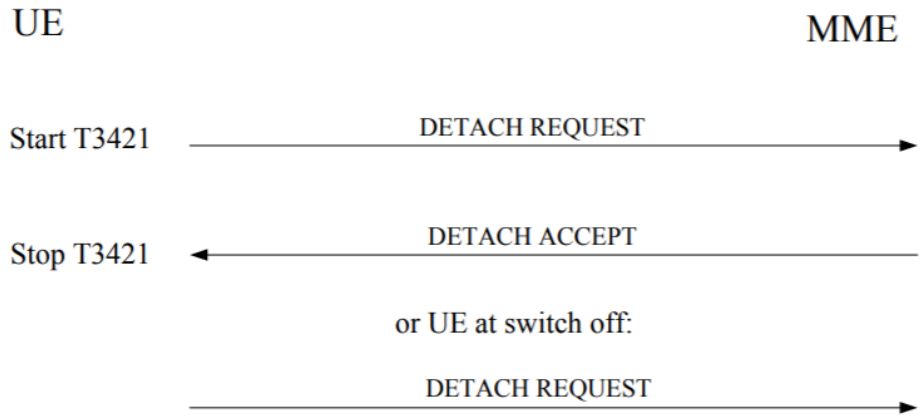


Figure 5.5.2.2.1.1: UE initiated detach procedure

3GPP TS 24.301 V13.7.0 (2016-09). Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS);

CONNECTION DETACH HANDSHAKE

- NAS detach request message
  - Includes EPS mobile identity
  - Can be GUTI or IMSI
  - It can even be the IMEI
- In some cases it does not require integrity protection
  - It can be spoofed!

5.5.2.2.1 UE initiated detach procedure initiation

The detach procedure is initiated by the UE by sending a DETACH REQUEST message (see example in figure 5.5.2.2.1.1). The Detach type IE included in the message indicates whether detach is due to a "switch off" or not. The Detach type IE also indicates whether the detach is for EPS services only, for non-EPS services only, or for both. If the UE has a mapped EPS security context as the current EPS security context, the UE shall set the type of security context flag to "mapped security context". Otherwise, the UE shall set the type of security context flag to "native security context".

If the UE has a valid GUTI, the UE shall populate the EPS mobile identity IE with the valid GUTI. If the UE does not have a valid GUTI, the UE shall populate the EPS mobile identity IE with its IMSI.

If the UE does not have a valid GUTI and it does not have a valid IMSI, then the UE shall populate the EPS mobile identity IE with its IMEI.

4.4.4.3 Integrity checking of NAS signalling messages in the MME

Except the messages listed below, no NAS signalling messages shall be processed by the receiving EMM entity in the MME or forwarded to the ESM entity, unless the secure exchange of NAS messages has been established for the NAS signalling connection:

- EMM messages:
  - ATTACH REQUEST;
  - IDENTITY RESPONSE (if requested identification parameter is IMSI);
  - AUTHENTICATION RESPONSE;
  - AUTHENTICATION FAILURE;
  - SECURITY MODE REJECT;
  - DETACH REQUEST;
  - DETACH ACCEPT;
  - TRACKING AREA UPDATE REQUEST.

NOTE 1: The TRACKING AREA UPDATE REQUEST message is sent by the UE without integrity protection, if the tracking area updating procedure is initiated due to an inter-system change in idle mode and no current EPS security context is available in the UE. The other messages are accepted by the MME without integrity protection, as in certain situations they are sent by the UE before security can be activated.

3GPP TS 24.301 V13.7.0 (2016-09). Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS);

CONNECTION DETACH HANDSHAKE

- In some cases it does not require integrity protection
  - It can be spoofed!

In mobile protocol security it only takes finding one single security edge case supported by the standard to make the entire house of cards fall apart.

THERE'S MORE…

Once a current EPS security context exists, until the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving EMM entity in the MME shall process the following NAS signalling messages, even if the MAC included in the message fails the integrity check or cannot be verified, as the EPS security context is not available in the network:

- ATTACH REQUEST;
- IDENTITY RESPONSE (if requested identification parameter is IMSI);
- AUTHENTICATION RESPONSE;

3GPP

- AUTHENTICATION FAILURE;
- SECURITY MODE REJECT;
- DETACH REQUEST (if sent before security has been activated);
- DETACH ACCEPT;

REMOTE DEVICE DETACH

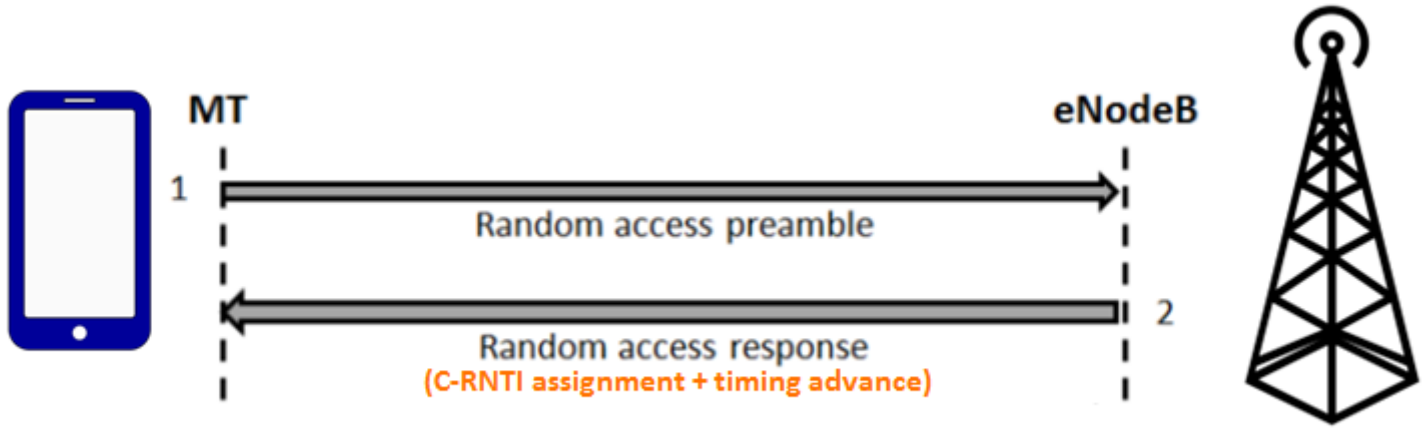
- Set up
  - Test smartphone (victim)
  - Linux box #1
    - USRP B210 running srsUE (adversary)
  - Linux box #2
    - USRP B210 running srsENB
    - Open source LTE EPC
- Run RRC handshake and spoof Detach Request message with victim's identity
- Knock out victim from network remotely
  - Though in the lab it is not "remotely"
- Testing it in a real network would be easy
  - But not legal
  - Next tests → commercial picocell
- **Might not work in a real network if inter-layer integrity checks are well implemented**

Raza, Muhammad Taqi, Fatima Muhammad Anwar, and Songwu Lu. "Exposing LTE Security Weaknesses at Protocol Inter-Layer, and Inter-Radio Interactions." In International Conference on Security and Privacy in Communication Systems, pp. 312-338. Springer, Cham, 2017.

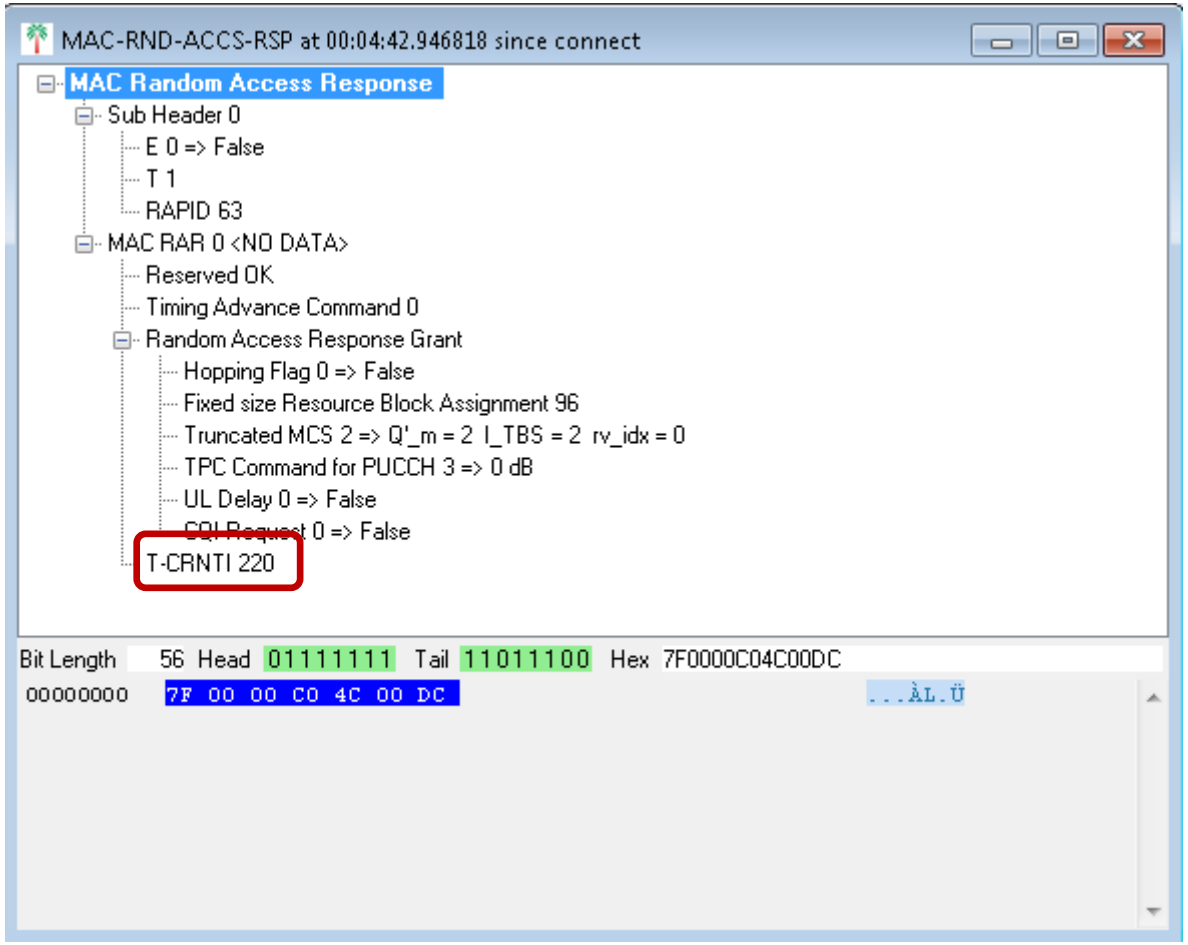
LTE LOCATION LEAKS

LOCATION LEAKS AND DEVICE TRACKING - RNTI

- RNTI
  - PHY layer id sent in the clear in EVERY SINGLE packet, both UL and DL
  - Identifies uniquely every UE within a cell
    - Changes infrequently
    - Based on several captures in the NYC and Honolulu areas
  - No distinguishable behavior per operator or per base station manufacturer
  - Assigned by the network in the MAC RAR response to the RACH preamble



LOCATION LEAKS AND DEVICE TRACKING - RNTI

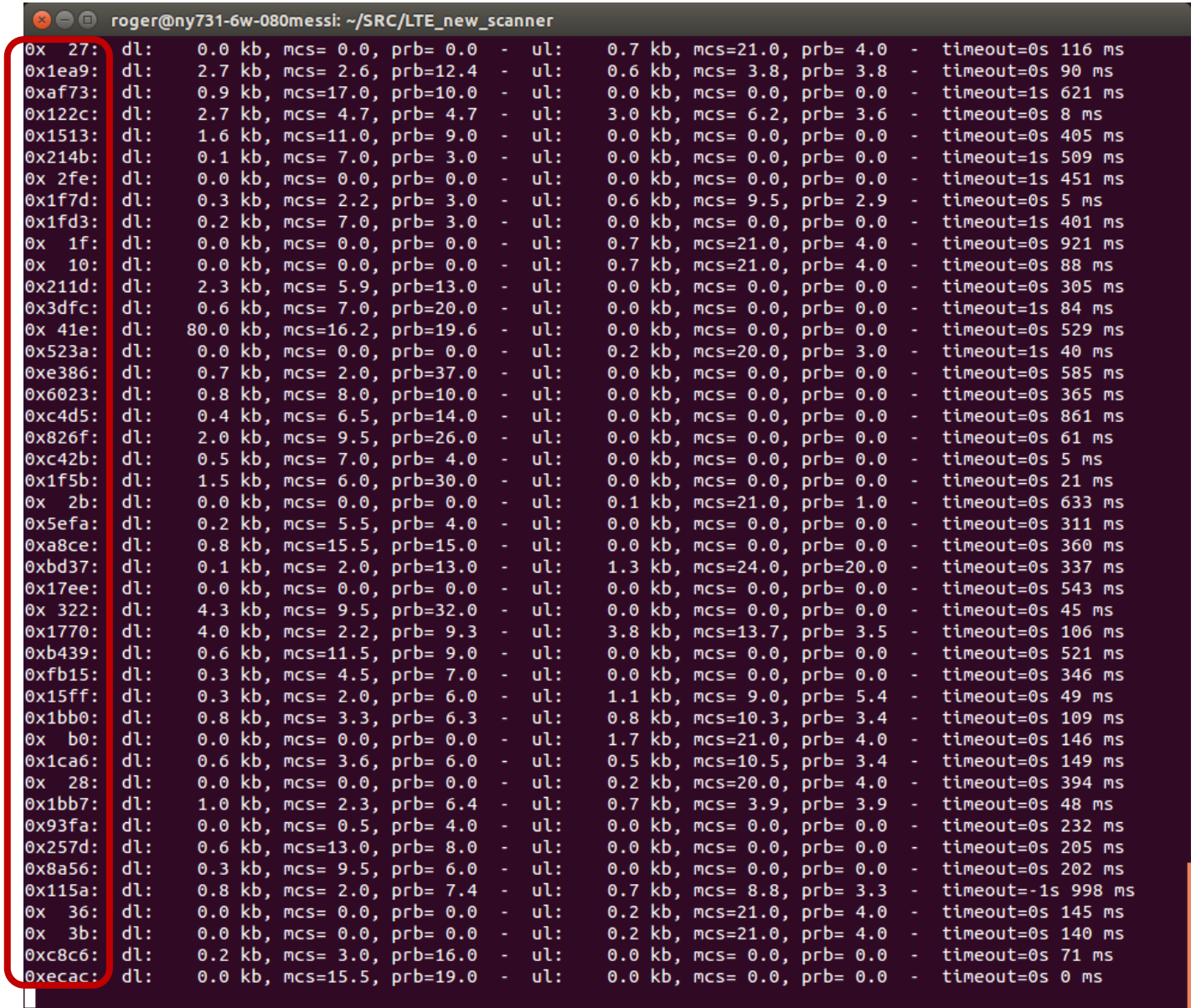


LOCATION LEAKS AND DEVICE TRACKING - RNTI

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		6	OK
RRCConnectionSetup	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
RRCConnectionSetupComplete	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
RRCConnectionReconfiguration	00:02:26.957868	D		1001	19841		84	OK
RRCConnectionReconfigurationC...	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
RRCConnectionSetup	00:02:27.003868	D		1006	1[illegible]3		24	OK
Unknown Data	00:02:27.020868	D		1007	1[illegible]1		1428	1
Ciphered RRC	00:02:27.021868	D		1007	1[illegible]5		2	OK

RNTI TRACKING WITH OPEN-SOURCE TOOLS

RNTIs being tracked within this cell (srsLTE)



RNTI LOCATION LEAKS AND DEVICE TRACKING

- Unprotected RRC Connection Reconfiguration message for handover should **not** occur
  - eNBs that used to have this issue have since been configured correctly

- According to 3GPP TR 33.899 V1.3.0 (2017-08)
  - RNTI tracking is not a privacy issue because RNTI is not a long lived id
    - But I keep seeing in the lab the RNTI of my devices not changing for hours…
  - TMSI can be mapped to RNTI, but TMSI is also short lived id
    - But the TMSI changes rather infrequently as well…

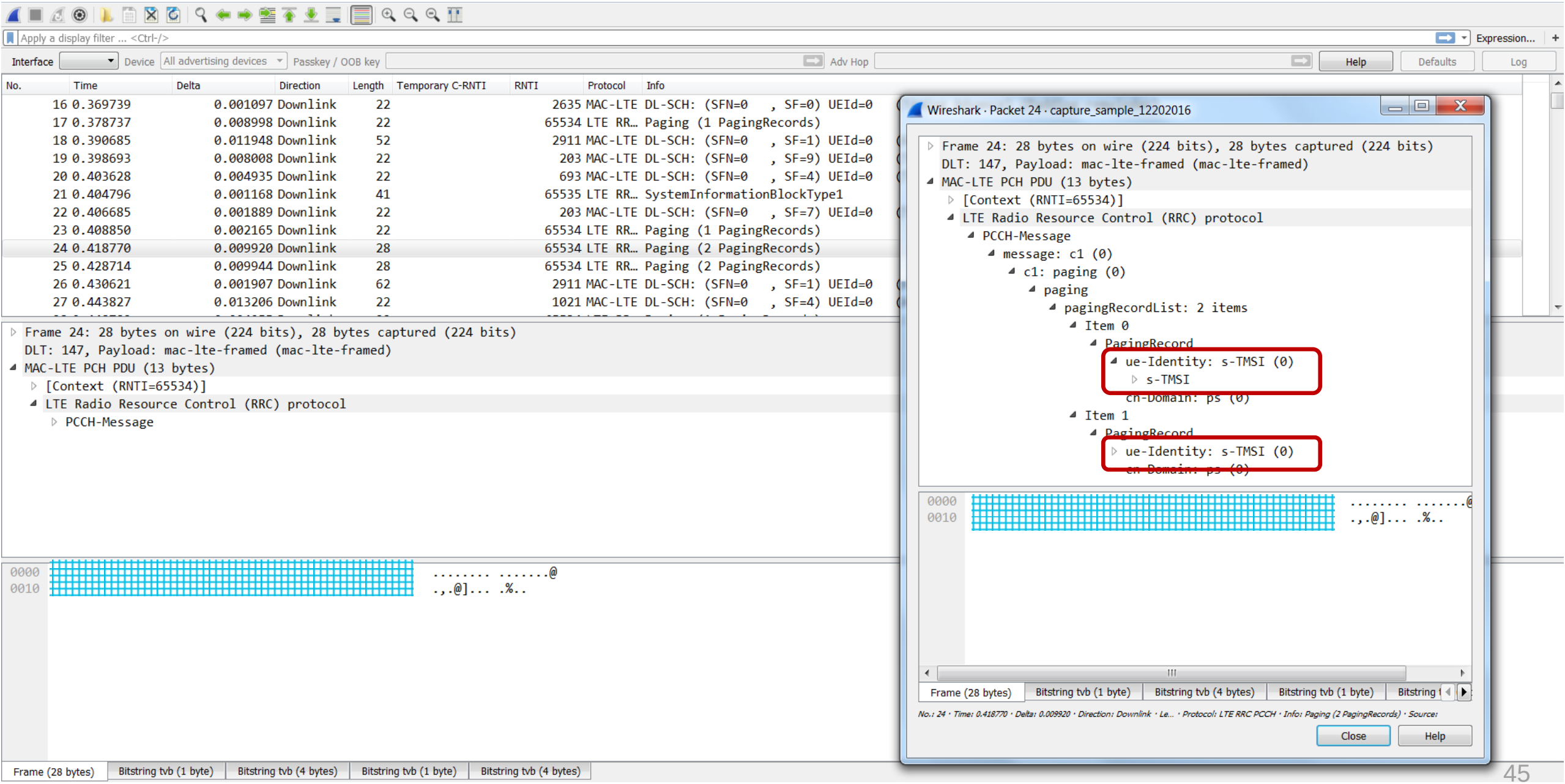
- LTE hijacking paper shows it is indeed possible!
  - https://alter-attack.net/media/breaking_lte_on_layer_two.pdf

Rupprecht, David, Katharina Kohls, Thorsten Holz, and Christina Pöpper. "Breaking LTE on Layer Two.“ To be presented at IEEE Security and Privacy 2019.

OTHER POTENTIAL LTE LOCATION LEAKS

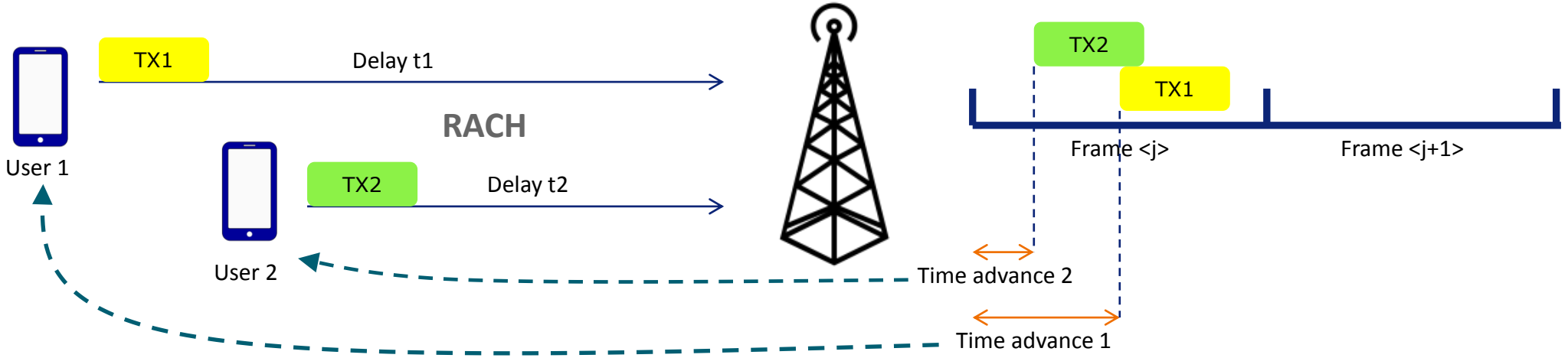
- Paging messages sent in the clear
  - Known location tracking techniques based on sniffing paging messages
  - Silent text message to target IMSI/TMSI/MSISDN
  - If a paging is sniffed, the UE is in the same Tracking Area as the sniffer
  - If connection establishment is sniffed, the UE is in the same cell as the sniffer

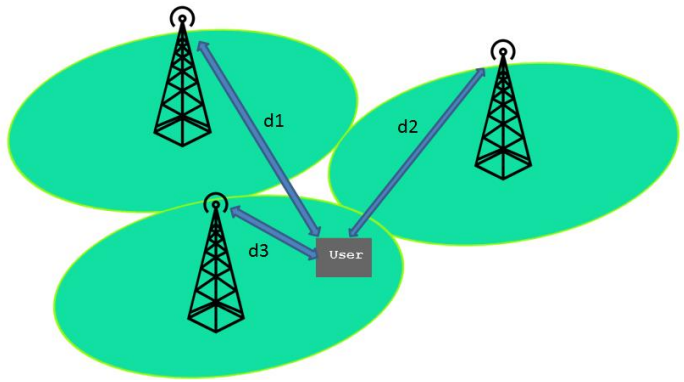
Khan, Haibat, Benjamin Dowling, and Keith M. Martin. "Identity Confidentiality in 5G Mobile Telephony Systems."


Apply a display filter ... <Ctrl-/>
Expression...
Interface
Device
All advertising devices
Passkey / OOB key
Adv Hop
Help
Defaults
Log
No. Time Delta Direction Length Temporary C-RNTI RNTI Protocol Info
16 0.369739 0.001097 Downlink 22 2635 MAC-LTE DL-SCH: (SFN=0 , SF=0) UEId=0
17 0.378737 0.008998 Downlink 22 65534 LTE RR… Paging (1 PagingRecords)
18 0.390685 0.011948 Downlink 52 2911 MAC-LTE DL-SCH: (SFN=0 , SF=1) UEId=0
19 0.398693 0.008008 Downlink 22 203 MAC-LTE DL-SCH: (SFN=0 , SF=9) UEId=0
20 0.403628 0.004935 Downlink 22 693 MAC-LTE DL-SCH: (SFN=0 , SF=4) UEId=0
21 0.404796 0.001168 Downlink 41 65535 LTE RR… SystemInformationBlockType1
22 0.406685 0.001889 Downlink 22 203 MAC-LTE DL-SCH: (SFN=0 , SF=7) UEId=0
23 0.408850 0.002165 Downlink 22 65534 LTE RR… Paging (1 PagingRecords)
24 0.418770 0.009920 Downlink 28 65534 LTE RR… Paging (2 PagingRecords)
25 0.428714 0.009944 Downlink 28 65534 LTE RR… Paging (2 PagingRecords)
26 0.430621 0.001907 Downlink 62 2911 MAC-LTE DL-SCH: (SFN=0 , SF=1) UEId=0
27 0.443827 0.013206 Downlink 22 1021 MAC-LTE DL-SCH: (SFN=0 , SF=4) UEId=0
Frame 24: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
DLT: 147, Payload: mac-lte-framed (mac-lte-framed)
MAC-LTE PCH PDU (13 bytes)
[Context (RNTI=65534)]
LTE Radio Resource Control (RRC) protocol
PCCH-Message
0000
0010
Frame (28 bytes)
Bitstring tvb (1 byte)
Bitstring tvb (4 bytes)
Bitstring tvb (1 byte)
Bitstring tvb (4 bytes)
Wireshark · Packet 24 · capture_sample_12202016
Frame 24: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
DLT: 147, Payload: mac-lte-framed (mac-lte-framed)
MAC-LTE PCH PDU (13 bytes)
[Context (RNTI=65534)]
LTE Radio Resource Control (RRC) protocol
PCCH-Message
message: c1 (0)
c1: paging (0)
paging
pagingRecordList: 2 items
Item 0
PagingRecord
ue-Identity: s-TMSI (0)
s-TMSI
cn-Domain: ps (0)
Item 1
PagingRecord
ue-Identity: s-TMSI (0)
cn-Domain: ps (0)
0000
0010
Frame (28 bytes)
Bitstring tvb (1 byte)
Bitstring tvb (4 bytes)
Bitstring tvb (1 byte)
No.: 24 · Time: 0.418770 · Delta: 0.009920 · Direction: Downlink · Le... · Protocol: LTE RRC PCCH · Info: Paging (2 PagingRecords) · Source:
Close
Help

OTHER POTENTIAL LTE LOCATION LEAKS

- Simple location inference
  - Eavesdrop MAC RAR messages
  - Time Advance → distance from eNodeB
  - Very low resolution unless one captures MAC RARs from multiple base stations





Tri-lateration of user's location with eavesdropped MAC-RAR messages

5G SECURITY

5G STANDARDS

- 5G largely a marketing buzz word
  - But there's some actual very interesting technology behind
  - First deployments and tests already happening
- Release 15 of the 3GPP standards
  - December 2017
  - First release of 5G – New Radio + 5G System
- Most changes at the PHY layer
  - mmWave
  - Massive MIMO
- Work to address some protocol exploits
  - IMSI obfuscation and encryption
  - PKI for IMSI concealing
- Security standards published in March 2018
  - 3GPP TS 33.501 V1.0.0 (2018-03)

IMSI PROTECTION

- IMSI encrypted (concealed) with public key of home operator
  - Probabilistic asymmetric encryption
  - Same IMSI encrypted multiple times results in different ciphertexts (to avoid tracking)

- IMSI catching much harder

- Challenges
  - What happens if private key of home operator is “lost” or needs to be rotated?
    - New SIM?
    - New public key burned in SIM?
    - “*Outside of the scope of the 3GPP specifications*”

SUPI – THE NEW IMSI

- SUPI – Subscription Permanent Identifier
  - New IMSI in 5G
  - SUCI (SUbscription Concealed Identifier) – Encrypted SUPI

- Challenges
  - "*If the home network has not provisioned the public key in USIM, the SUPI protection in initial registration procedure is not provided. In this case, the null-scheme shall be used by the ME.*"
    - Null cipher still supported
  - "*In case of an unauthenticated emergency call, privacy protection for SUPI is not required.*"
    - Can a rogue base station fool a UE to initiate such an emergency call?

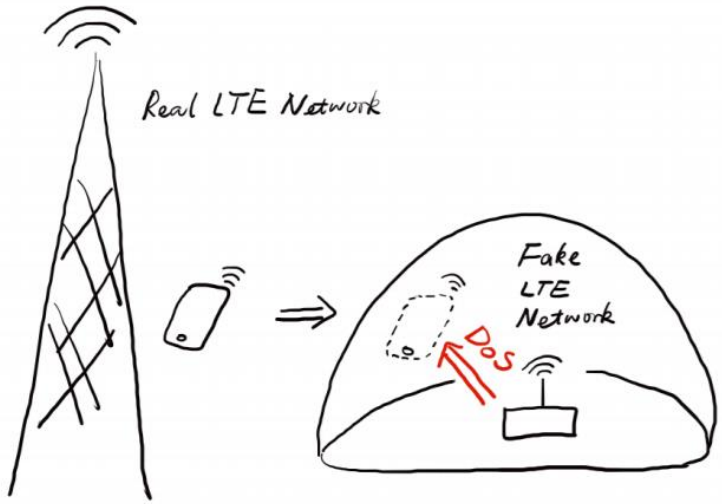
PROTOCOL EXPLOITS IN 5G

- Most LTE protocol exploits caused by implicit trust in pre-authentication messages
  - RRC, MAC, NAS layers
- 5G aims to tackle known exploits in LTE
  - E.g. AttachReject DoS and downgrade to GSM mentioned explicitly
- Leverage public key of home operator?
  - Does not work with roaming devices
  - Public key from all operators?
    - Not scalable
    - Unrealistic
- How are the 5G security specifications preventing exploiting pre-authentication messages?
  - **As of now, 5G appears to be vulnerable to pre-authentication message protocol exploits**

PROTOCOL EXPLOITS IN 5G

- I am not the only one claiming this…

Fake 5G Base Station may still Exist



DoS attack examples:
- ✓ You are an illegal cellphone!
- ✓ Here is NO network available. You could shut down your modem.

The root cause is the initial broadcasting message from network can not be proved to be trustable.

NO PKI infrastructure solution reaches agreement in 3GPP.

Huang Lin (360 Radio Security Research Institute). "5G Security Enhancement". Hack in the Box 2018..

“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

- 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.”

NULL CIPHERING

- Supported ciphering modes
  - **NEA0 - Null ciphering algorithm**
  - 128-NEA1 - 128-bit SNOW 3G based algorithm
  - 128-NEA2 - 128-bit AES based algorithm
  - 128-NEA3 - 128-bit ZUC based algorithm

- **Null ciphering** is a supported option
  - **Same for null integrity**
  - Potential security edge cases
  - Bidding down attacks
    - Public key of home operator burned in SIM
    - How to authenticate a bidding down request at a foreign (roaming) network?

- Note null ciphering support often a requirement for Lawful Interception

POTENTIAL SECURITY EDGE CASES

- *“In case the UE registers for Emergency Services and receives an Identifier Request, the UE shall use the null-scheme for generating the SUCI in the Identifier Response.”*
- *“If the UE receives a NAS security mode command selecting NULL integrity and ciphering algorithms, the UE shall accept this as long as the IMS Emergency session progresses.”*
- *“If the authentication failure is detected in the AMF then the UE is not aware of the failure in the AMF, but still needs to be prepared, according to the conditions specified in TS 24.301, to accept a NAS SMC from the AMF requesting the use of the NULL ciphering and integrity algorithms.”*
- *“If the AMF cannot identify the subscriber, or cannot obtain authentication vector (when SUPI is provided), the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.”*
- …

5G SECURITY - ARE WE THERE YET?

NAS integrity activation:

"Replay protection shall be activated when integrity protection is activated, except when the NULL integrity protection algorithm is selected."

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

Q&A

http://rogerpiquerasjover.net ----  @rgoestotheshows

FURTHER READING

FURTHER READING

- Shaik, Altaf, et al. "Practical attacks against privacy and availability in 4G/LTE mobile communication systems." arXiv preprint arXiv:1510.07563 (2015).
- Jover, Roger Piqueras. LTE Security and Protocol Exploits. ShmooCon 2016.
- Jover, Roger Piqueras, Joshua Lackey, and Arvind Raghavan. "Enhancing the security of LTE networks against jamming attacks." EURASIP Journal on Information Security 2014.1 (2014): 1-14.
- Jover, Roger Piqueras. "Security attacks against the availability of LTE mobility networks: Overview and research directions." Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on. IEEE, 2013.
- M. Lichtman, R. Piqueras Jover, M. Labib, R. Rao, V. Marojevic,and J. H. Reed, "LTE/LTE-A Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation," Communications Magazine, IEEE, vol. 54,no. 4, 2016.
- Engel, Tobias. "SS7: Locate. Track. Manipulate." FTP: http://events. ccc. de/congress/2014/Fahrplan/system/attachments/2553/or iginal/31c3-ss7-locate-track-manipulate. pdf. 2014.
- Kumar, Swarun, et al. "LTE radio analytics made easy and accessible." ACM SIGCOMM Computer Communication Review. Vol. 44. No. 4. ACM, 2014.
- Spaar, Dieter. "A practical DoS attack to the GSM network." In DeepSec (2009).
- Kune, Denis Foo, et al. "Location leaks on the GSM Air Interface." ISOC NDSS (Feb 2012) (2012).
- Jermyn, Jill, et al. "Scalability of Machine to Machine systems and the Internet of Things on LTE mobile networks." World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a. IEEE, 2015.
- Lichtman, Marc, et al. "Vulnerability of LTE to hostile interference." Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE. IEEE, 2013.

FURTHER READING

- Golde, Nico, Kévin Redon, and Jean-Pierre Seifert. "Let me answer that for you: Exploiting broadcast information in cellular networks." Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13). 2013.
- Mulliner, Collin, Nico Golde, and Jean-Pierre Seifert. "SMS of Death: From Analyzing to Attacking Mobile Phones on a Large Scale." USENIX Security Symposium. 2011.
- Bhattarai, Sudeep, et al. "On simulation studies of cyber attacks against lte networks." Computer Communication and Networks (ICCCN), 2014 23rd International Conference on. IEEE, 2014.
- Ghavimi, Fayezeh, and Hsiao-Hwa Chen. "M2M Communications in 3GPP LTE/LTE-A Networks: Architectures, Service Requirements, Challenges, and Applications." Communications Surveys & Tutorials, IEEE 17.2 (2015): 525-549.
- Nakarmi, Prajwol Kumar, Oscar Ohlsson, and Michael Liljenstam. "An Air Interface Signaling Protection Function for Mobile Networks: GSM Experiments and Beyond." Trustcom/BigDataSE/ISPA, 2015 IEEE. Vol. 1. IEEE, 2015.
- Khosroshahy, Masood, et al. "Botnets in 4G cellular networks: Platforms to launch DDoS attacks against the air interface." Mobile and Wireless Networking (MoWNeT), 2013 International Conference on Selected Topics in. IEEE, 2013.
- Bailey, D. "War Texting: Weaponizing Machine to Machine." Black-Hat USA (2011).
- Nohl, Karsten, and Sylvain Munaut. "Wideband GSM sniffing." In 27th Chaos Communication Congress. 2010.
- Prasad, Anand. "3GPP SAE-LTE Security." NIKSUN WWSMC (2011).
- Jermyn, Jill, Gabriel Salles-Loustau, and Saman Zonouz. "An analysis of dos attack strategies against the LTE RAN." Journal of Cyber Security 3.2 (2014): 159-180.
- Bailey, Don, and Nick DePetrillo. "The Carmen Sandiego Project." Proc. of BlackHat (Las Vegas, NV, USA, 2010) (2010).

FURTHER READING

- Hussain, Syed Rafiul, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE." In Symposium on Network and Distributed Systems Security (NDSS), pp. 18-21. 2018.
- Rupprecht, David, Katharina Kohls, Thorsten Holz, and Christina Pöpper. "Breaking LTE on Layer Two." In Breaking LTE on Layer Two, p. 0. IEEE..
- Hussain, Syed Rafiul, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE." In Symposium on Network and Distributed Systems Security (NDSS), pp. 18-21. 2018..
- Jover, Roger Piqueras, and Vuk Marojevic. "Security and Protocol Exploit Analysis of the 5G Specifications." arXiv preprint arXiv:1809.06925 (2018).
- Raza, Muhammad Taqi, Fatima Muhammad Anwar, and Songwu Lu. "Exposing LTE Security Weaknesses at Protocol Inter-Layer, and Inter-Radio Interactions." In International Conference on Security and Privacy in Communication Systems, pp. 312-338. Springer, Cham, 2017.
- Khan, Haibat, Benjamin Dowling, and Keith M. Martin. "Identity Confidentiality in 5G Mobile Telephony Systems." 2018.
- Mjølsnes, Stig F., and Ruxandra F. Olimid. "Easy 4G/LTE IMSI Catchers for Non-Programmers." In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, pp. 235-246. Springer, Cham, 2017.
- Khan, M., Ginzboorg, P., Järvinen, K. and Niemi, V., 2018. Defeating the Downgrade Attack on Identity Privacy in 5G. arXiv preprint arXiv:1811.02293.
- Basin, David, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. "A Formal Analysis of 5G Authentication." In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 1383-1396. ACM, 2018.