The impact of open-source testbeds on cellular security research

Roger Piqueras Jover

Software Engineer - Google

02/08/2022

About me

- Things I do…
  - Fatherhood
  - SWE at Google
  - Wireless Security Research
  - Soccer, live rock/punk-rock/metal music, geek
- Mobile/wireless security research
  - Started 12 years ago with LTE
  - History of breaking things communicating over 802.11, BLE, ZigBee…
  - 5G security
- Random trivia/achievements I am proud of
  - Watched every single game live on TV during World Cup 2006 and 2010
  - Seen the band Bad Religion live 23 times
- More
  - http://rogerpiquerasjover.net/  @rgoestotheshows

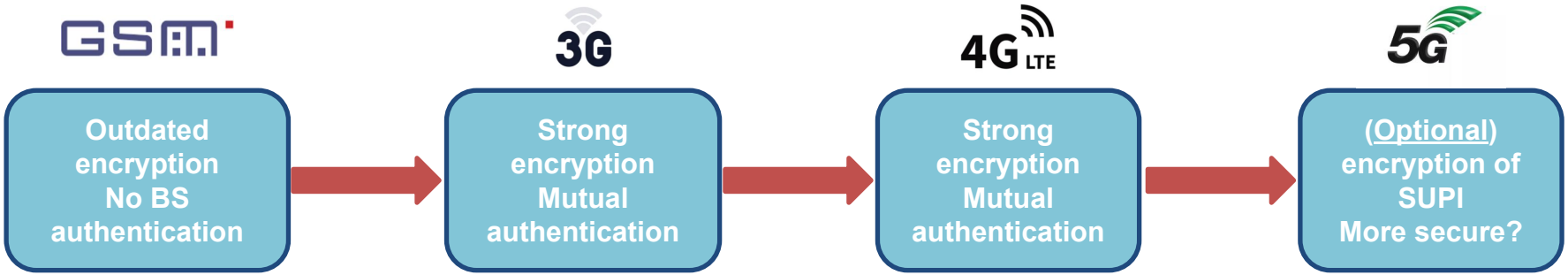
> The opinions and ideas discussed in this talk are mine. They do not necessarily reflect my employer's and are not related to my day job.

The impact of open source on mobile security research.

Roger Piqueras Jover - May 2016

https://www.linkedin.com/pulse/impact-open-source-mobile-security-research-roger-piqueras-jover/

MOBILE NETWORK SECURITY RETROSPECTIVE



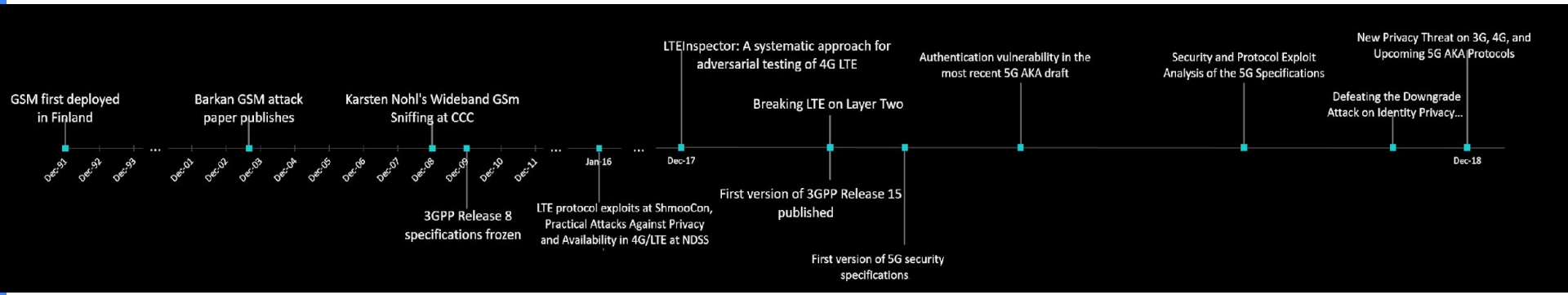
Ask Karsten Nohl and Sylvain Munaut…

Interestingly, research mostly skipped 3G…

Researchers found vulnerabilities: eg. Rabi Borgaonkar, David Rupprecht, Syed Rafiul Hussain, Yongdae Kim, myself…

Researchers identified security issues pre-deployment: eg. Rabi Borgaonkar, David Rupprecht, Syed Rafiul Hussain, Yongdae Kim, myself…

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 ~4 years
- 5G
  - Release 15 published 12/2017, 5G security specifications 03/2018, vulnerabilities found since 2018

SECURITY RESEARCH RAPIDLY MATURING

- Cellular security research ramping up rapidly!

18 years from deployment to first demonstrated vulnerabilities

8 years from standards to first demonstrated vulns, 3 years from deployment to first demonstrated vulns

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

srsRAN

openLTE

OpenAirInterface

Ruhr Universität Bochum

KAIST

TU Berlin

Purdue University

VATech

openLTE

- First open-source implementation of the LTE stack
  - The one that started it all!
  - By Ben Wojtowicz
  - First commit December 31, 2011 (Happy new year!)

- **December 31, 2011**: Initial release (version 00.01) of matlab/octave files for LTE FDD downlink transmission and reception. This includes PSS, SSS, CRS, and PBCH. The receiver has been tested against a live LTE recording and the transmitter has been tested against the receiver.

  - Abandoned in 2017… then major update/refactoring on Valentine's Day 2021 (I like you too!)

- **February 14, 2021**: Version 0.21.0 is available. This version includes a massive reformat, a new RRC library, migration of LTE_fdd_dl_file_gen and LTE_fdd_dl_file_scan from python to c++, turbo decoder improvements, and many bug fixes

I probably would not be here (career-wise) right now if it wasn't for openLTE…

SRSRAN, FORMERLY KNOWN AS SRSLTE

- Open-source implementation of the LTE stack, including the UE stack
  - The one most people use (at least most people I know of!)
  - By the Software Radio Systems team (https://www.srs.io/)
  - First commit in 2014: 11k lines of code for an LTE cell search function
  - Very well documented, great community support
  - GNU AGPL license (https://github.com/srsran/srsRAN/blob/master/LICENSE)
  - Pro-tip: Enable Google Scholar notifications for keywords “security” and “srsLTE”

I probably would not be here (career-wise) right now if it wasn’t for srsLTE...

OPEN AIR INTERFACE

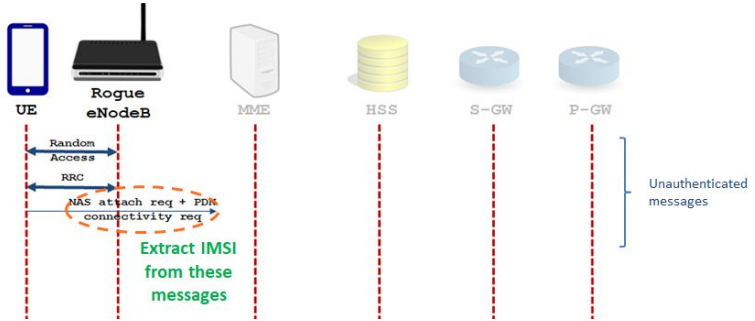
- Released in 2014 under the French non-profit OpenAirInterface Software Alliance
  - EURECOM project
  - Under OAI Public License (modified Apache v2.0 license) - https://openairinterface.org/?page_id=698
  - Code is free to use for non-commercial/academic research purposes

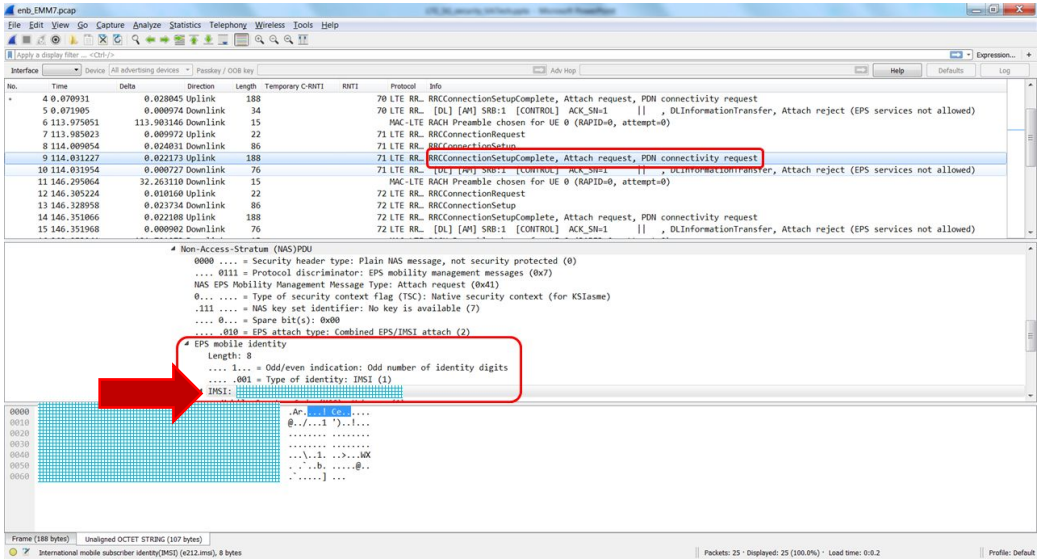
```
openairinterface5g
├── ci-scripts: Meta-scripts used by the OSA CI process. Contains also configuration files used day-to-day by CI.
├── cmake_targets: Build utilities to compile (simulation, emulation and real-time platforms), and generated build files
├── common : Some common OAI utilities, other tools can be found at openair2/UTILS
├── doc : Contains an up-to-date feature set list
├── LICENSE
├── maketags : Script to generate emacs tags
├── nfapi : Contains the NFAPI code. A local Readme file provides more details.
├── openair1 : 3GPP LTE Rel-10/12 PHY layer + PHY RF simulation. A local Readme file provides more details.
├── openair2 : 3GPP LTE Rel-10 RLC/MAC/PDCP/RRC/X2AP + LTE Rel-14 M2AP implementation.
    ├── COMMON
    ├── DOCS
    ├── ENB_APP
    ├── LAYER2/RLC/ with the following subdirectories: UM_v9.3.0, TM_v9.3.0, and AM_v9.3.0.
    ├── LAYER2/PDCP/PDCP_v10.1.0.
    ├── NETWORK_DRIVER
    ├── PHY_INTERFACE
    ├── RRC/LITE
    ├── UTIL
    ├── X2AP
    ├── M2AP
    ├── MCE_APP
├── openair3: 3GPP LTE Rel10 for S1AP, NAS GTPV1-U for both ENB and UE.
    ├── COMMON
    ├── DOCS
    ├── GTPV1-U
    ├── NAS
    ├── S1AP
    ├── M3AP
    ├── SCTP
    ├── SECU
    ├── UDP
    ├── UTILS
└── targets: Top-level wrappers for unitary simulation for PHY channels, system-level emulation (eNB-UE with and without
```

Cellular security research with OSS testbeds - Some examples

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



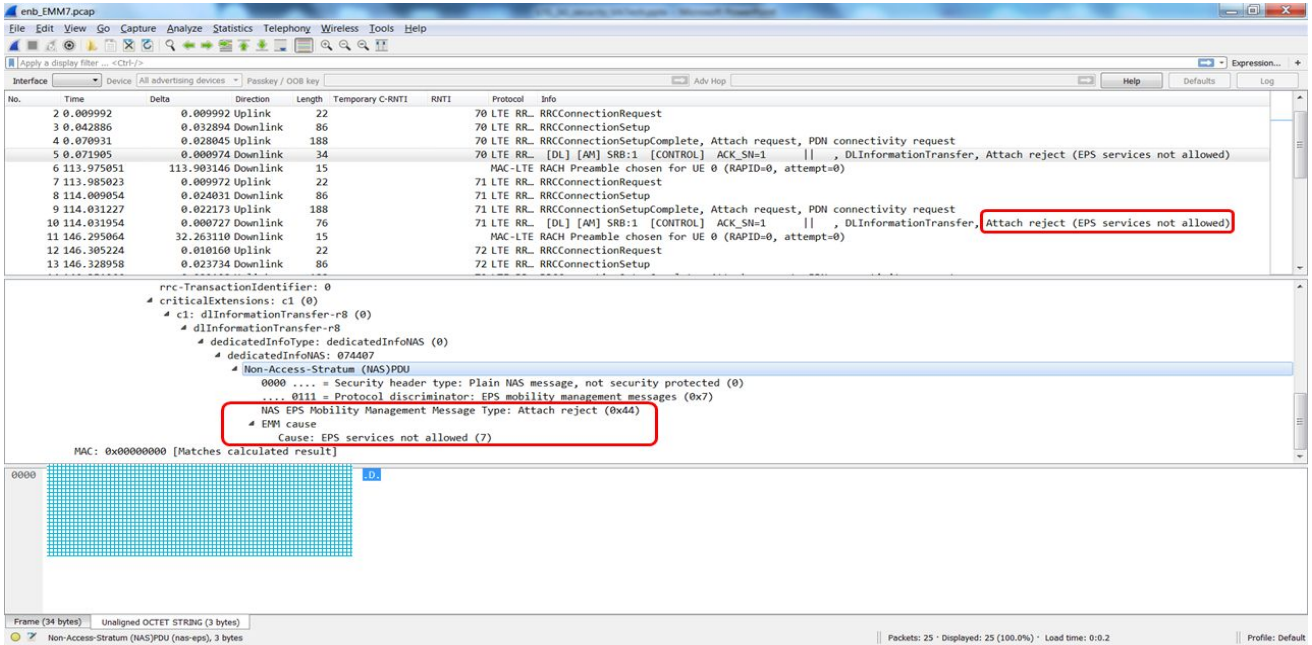


Roger Piqueras Jover. LTE protocol exploits. ShmooCon 2016.

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.

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



Roger Piqueras Jover. LTE protocol exploits. ShmooCon 2016.

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.

DNS SPOOFING AND TRAFFIC HIJACK OVER LTE

- aLTEr Attack
  - Leverages RNTI-based tracking/fingerprinting
  - Poor implementation of AES cipher leads to cipher text modification attack
  - Flip bits in encrypted DNS responses, modify plain-text IP in DNS response predictably and hijack user's traffic

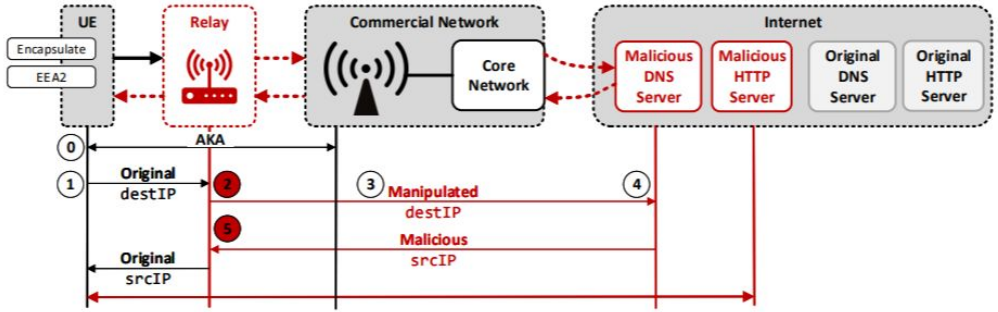


Fig. 4. ALTER: Overview of the DNS redirection attack. We deploy a malicious relay as a MitM between the UE and the commercial network and alter the destination IP address of a DNS request to redirect messages to our malicious DNS server. Eventually, the UE connects to the malicious HTTP server.

Rupprecht, David, Katharina Kohls, Thorsten Holz, and Christina Pöpper. "Breaking LTE on layer two." In IEEE Symposium on Security & Privacy (SP). 2019.

DIGITAL CERTIFICATES IN CELLULAR NETWORKS

- X509 certs in cellular
  - SIBx broadcast messages and security-critical messages (*TAUpdateReject*, *AttachReject*, etc)
- Working prototype on srsRAN
  - Trimmed down certificates

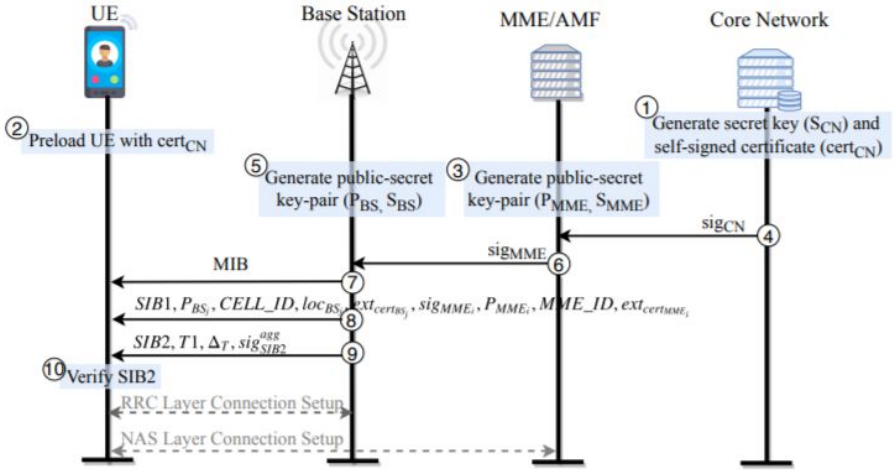


Figure 8: Optimized PKI Scheme.

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.

Looking ahead - 5G testbeds

OSS 5G SECURITY TESTBEDS

- Open Air Interface
  - Partial implementation of 5G RAN (mainly PHY + MAC + RLC)
  - COTS UE connection over 5G NSA (with LTE EPC)

- srsRAN
  - Very good documentation (https://docs.srsran.com/en/latest/)
  - COTS UE connection over 5G NSA (with LTE EPC)
    - https://docs.srsran.com/en/latest/app_notes/source/5g_nsa_cots/source/index.html
  - NSA UE (srsUE) connection with commercial NSA gNB
    - https://docs.srsran.com/en/latest/app_notes/source/5g_nsa_amari/source/index.html

- openLTE
  - open5G: Open source implementation of the 3GPP 5G specifications
    - https://open5g.sourceforge.io/
  - NRARFCN_recorder, GSCN_recorder, GSCN_scan

PLENTY OF COMMERCIAL OPTIONS

(Incomplete list with testbeds I am aware of in absolutely no particular order)

- Radisys - https://www.radisys.com/connect/connectran/5g
- Yate - https://yatebts.com/products/
- AWS Private 5G Networks - https://aws.amazon.com/private5g/
- Parallel Wireless - https://www.parallelwireless.com/technologies/5g/
- LimeMicro “network in a box” - https://limemicro.com/products/systems/
- Mavenir - https://www.mavenir.com/solutions/evolve-5g/
- Accelleran - https://accelleran.com/
- Etc…

Wrapping up...

INTERESTED IN CELLULAR SECURITY?

- Strong SW engineering and development skills? Experience in LTE, 5G and open-source testbeds? Experience with Android Platform and/or Telephony?
  - My team is hiring; let's chat! Apply here:
    - https://www.linkedin.com/jobs/view/software-engineer-iii-security-privacy-android-at-google-2891245381
  - ~~Summer'22 - Security Engineer Summer Internship; apply here~~ (reach out for summer 2023!)
- Academic teams working in cellular security?
  - Android Security and Privacy grant that aims to foster collaboration between Android and academia
  - Application deadline ~early Fall
- Google is hiring! And we have many wireless-related teams
  - Fi, Android, Chrome, Pixel, Cloud 5G, Nest, Fitbit…

Thank You