Ain't Nothin' but a G Thang

The Evolution of Cellular Networks

Tracy Mosley

hackerpinup

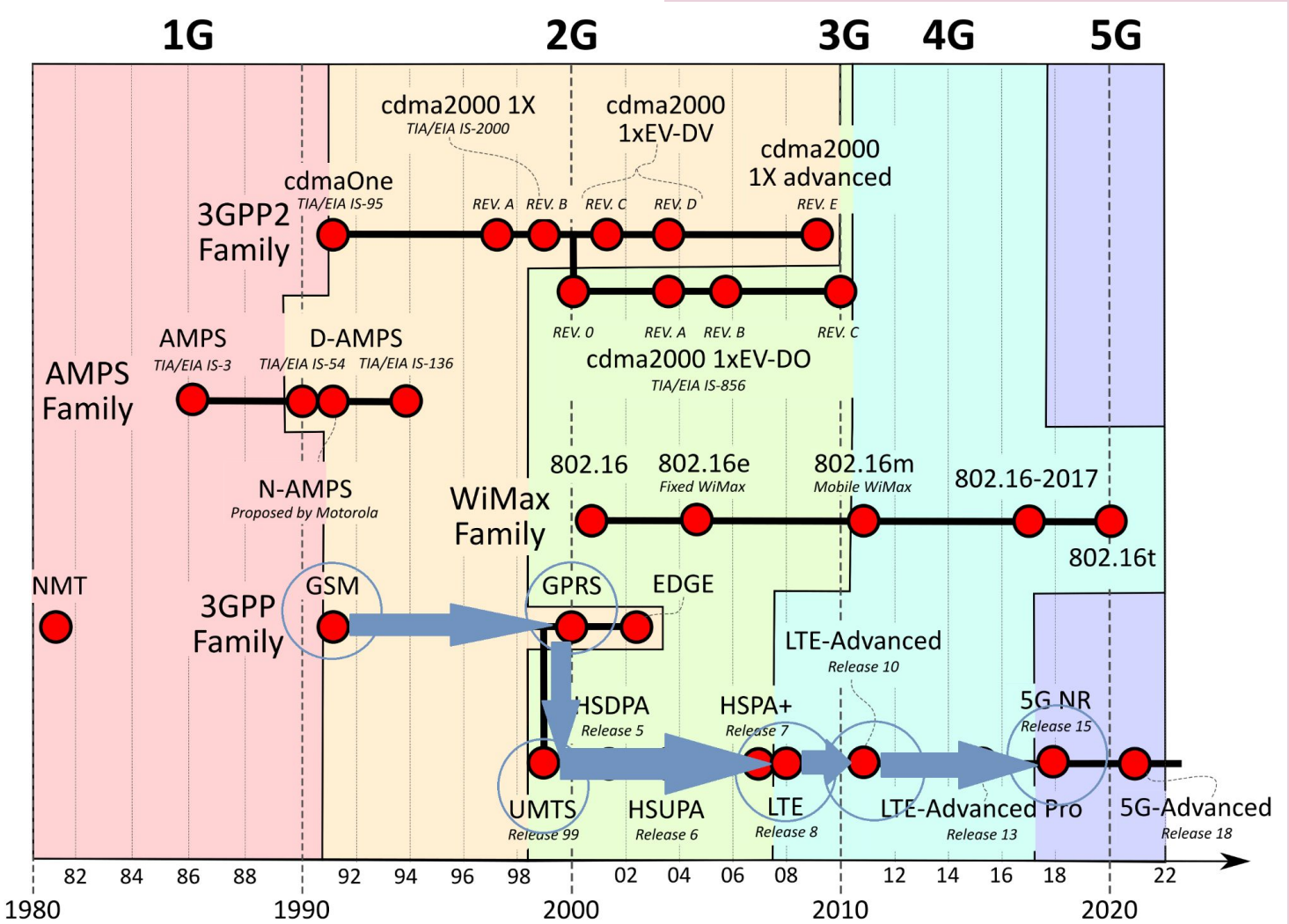
hackerpinup@infosec.exchange

Who am I?

- Vulnerability Researcher at Trenchant
- RE and embedded dev
- Telco focused
- ~10 years of experience
- Computer Engineering Degree

What to cover

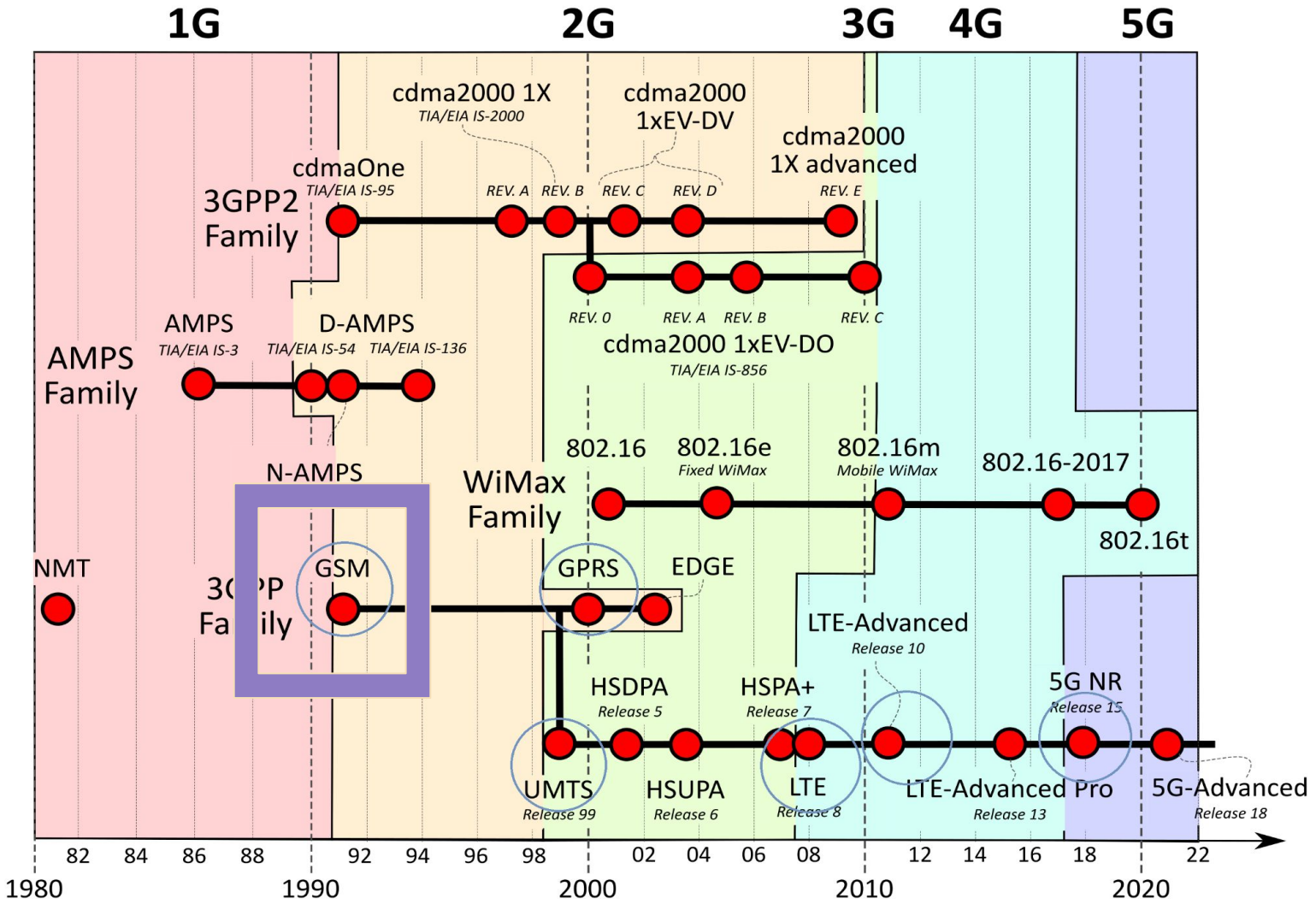
- 2G: GSM. Digital Technology! Voice and Data. Circuit Switched.
- GPRS: Both Circuit and Packet Switched!
- 3g: UMTS.
- LTE: Evolved packet core!
- 4G: LTE Advanced. VoLTE, IPv6, IMS.
- 5G: NR. Virtualization. Network slicing. Functionality generally split into “functions” instead of devices.


1G
2G
3G
4G
5G
cdma2000 1X
TIA/EIA IS-2000
cdma2000
1xEV-DV
cdma2000
1X advanced
cdmaOne
TIA/EIA IS-95
REV. A
REV. B
REV. C
REV. D
REV. E
3GPP2
Family
REV. 0
REV. A
REV. B
REV. C
cdma2000 1xEV-DO
TIA/EIA IS-856
AMPS
TIA/EIA IS-3
D-AMPS
TIA/EIA IS-54
TIA/EIA IS-136
AMPS
Family
802.16
802.16e
Fixed WiMax
802.16m
Mobile WiMax
802.16-2017
802.16t
N-AMPS
Proposed by Motorola
WiMax
Family
NMT
GSM
GPRS
EDGE
3GPP
Family
LTE-Advanced
Release 10
HSDPA
Release 5
HSPA+
Release 7
5G NR
Release 15
UMTS
Release 99
HSUPA
Release 6
LTE
Release 8
LTE-Advanced Pro
Release 13
5G-Advanced
Release 18
82
84
86
88
92
94
96
98
02
04
06
08
12
14
16
18
22
1980
1990
2000
2010
2020

Basic Cellular Concepts

- **POTS**
  - Plain Old Telephone Service
- **PSTN**
  - Public Switched Telephone Network
- Circuit Switched
- **PDN**
  - Public Data Network
- **RRC**
  - Radio Resource Control
- **RAB**
  - Radio Access Bearer

Rachel Brosnahan stars as Midge in Amazon Studios' *The Marvelous Mrs. Maisel*. (Amazon Studios)


1G
2G
3G
4G
5G
cdma2000 1X
TIA/EIA IS-2000
cdma2000
1xEV-DV
cdma2000
1X advanced
cdmaOne
TIA/EIA IS-95
REV. A
REV. B
REV. C
REV. D
REV. E
3GPP2
Family
REV. 0
REV. A
REV. B
REV. C
cdma2000 1xEV-DO
TIA/EIA IS-856
AMPS
TIA/EIA IS-3
D-AMPS
TIA/EIA IS-54
TIA/EIA IS-136
AMPS
Family
N-AMPS
802.16
802.16e
Fixed WiMax
802.16m
Mobile WiMax
802.16-2017
802.16t
WiMax
Family
NMT
GSM
GPRS
EDGE
LTE-Advanced
Release 10
HSDPA
Release 5
HSPA+
Release 7
5G NR
Release 15
UMTS
Release 99
HSUPA
Release 6
LTE
Release 8
LTE-Advanced Pro
Release 13
5G-Advanced
Release 18
82
84
86
88
92
94
96
98
02
04
06
08
12
14
16
18
22
1980
1990
2000
2010
2020

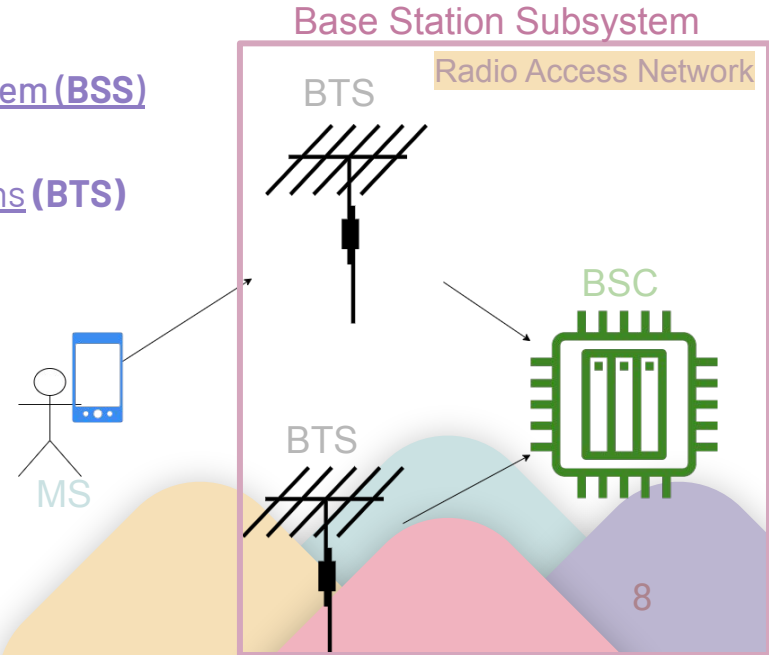
2G

GSM

- Calls
- SMS
- ETSI and GSM standardizing!
- SS7 for signaling

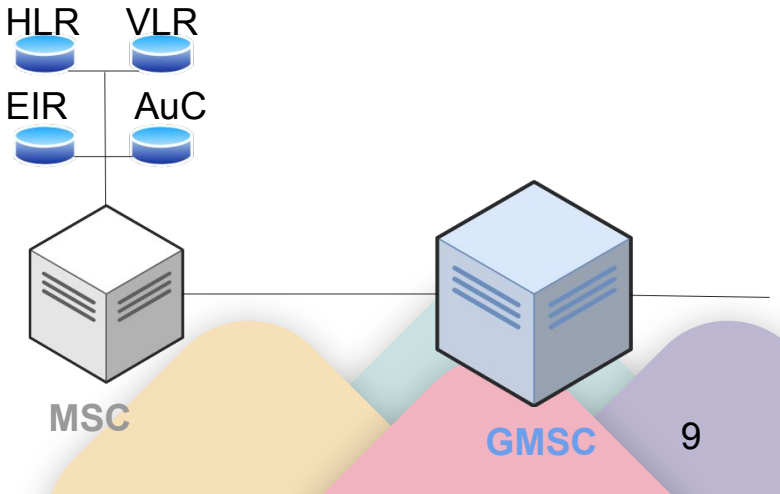
2G - GSM - Network Architecture

- Mobile Equipment **(ME)** or Mobile Station **(MS)**
  - This is usually the whole device in your hand when you're making a call.
- Radio Access Network **(RAN)**
  - In GSM it is the same as the Base Station Subsystem **(BSS)**
    - **BSS** contains
      - One or more Base Transceiver Stations **(BTS)**
      - Base Station Controller **(BSC)**



2G - GSM - Network Architecture

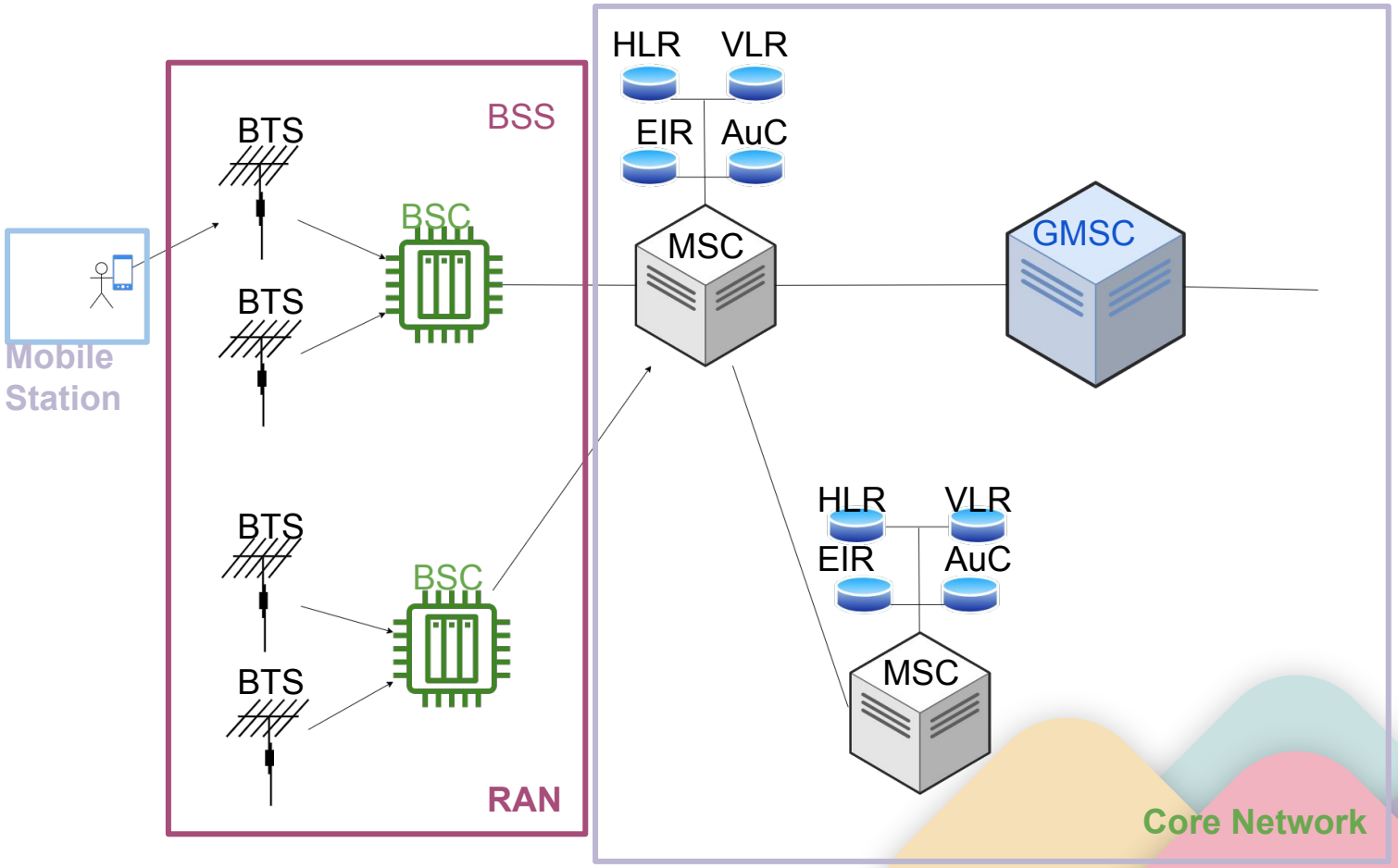
- Mobile Switching Center **(MSC)**
  - Handles the call switching, handover, registration, authentication.
- Home Location Register **(HLR)**
  - Large DB of user information for “local” users
- Visitor Location Register **(VLR)**
  - Large DB of user info for visiting users
- Authentication Center **(AuC)**
  - **Secret keys stored here**
- Equipment Identity Register **(EIR)**
  - Large DB of valid equipment on the network.
- Gateway Mobile Switching Center (GMSC)

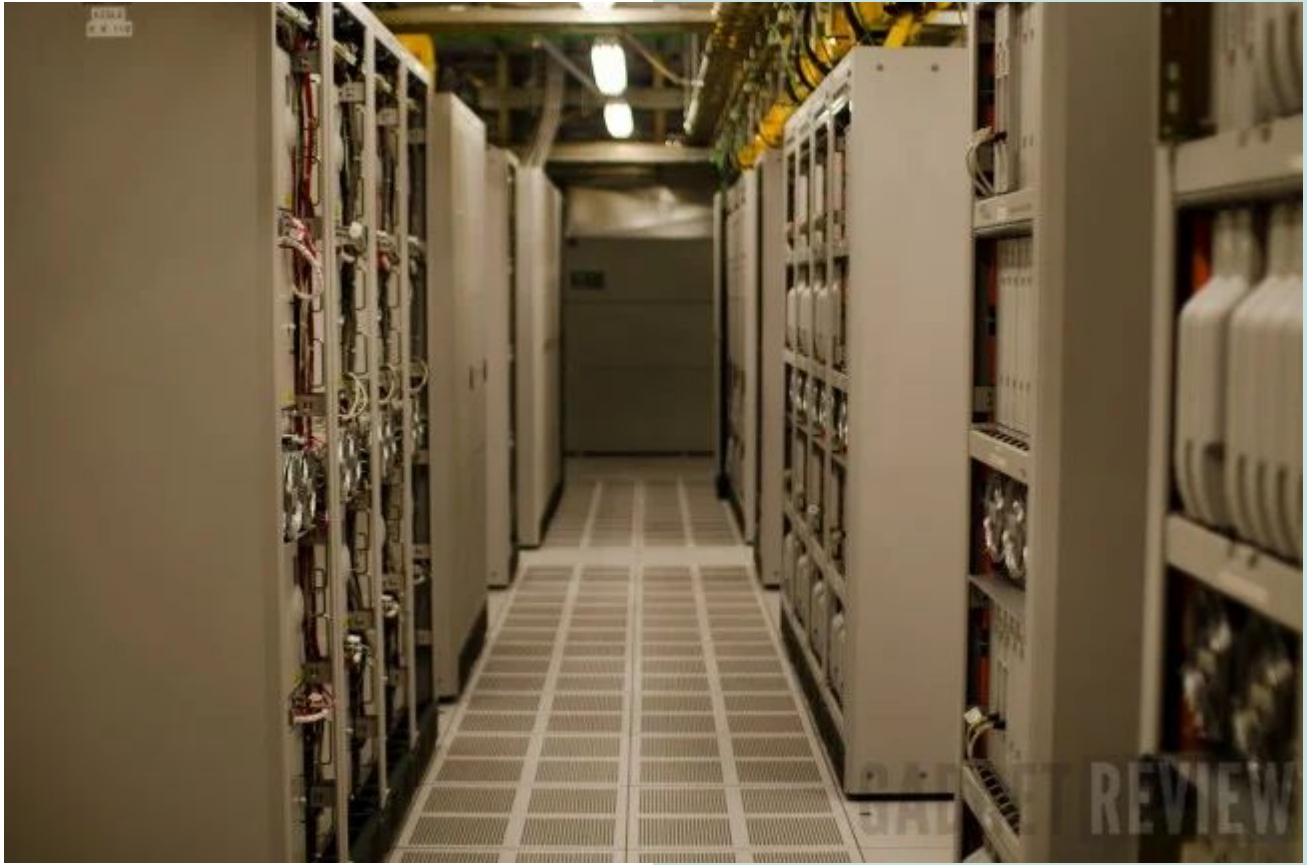



NOKIA


Flexi BSC
Nokia Siemens Networks

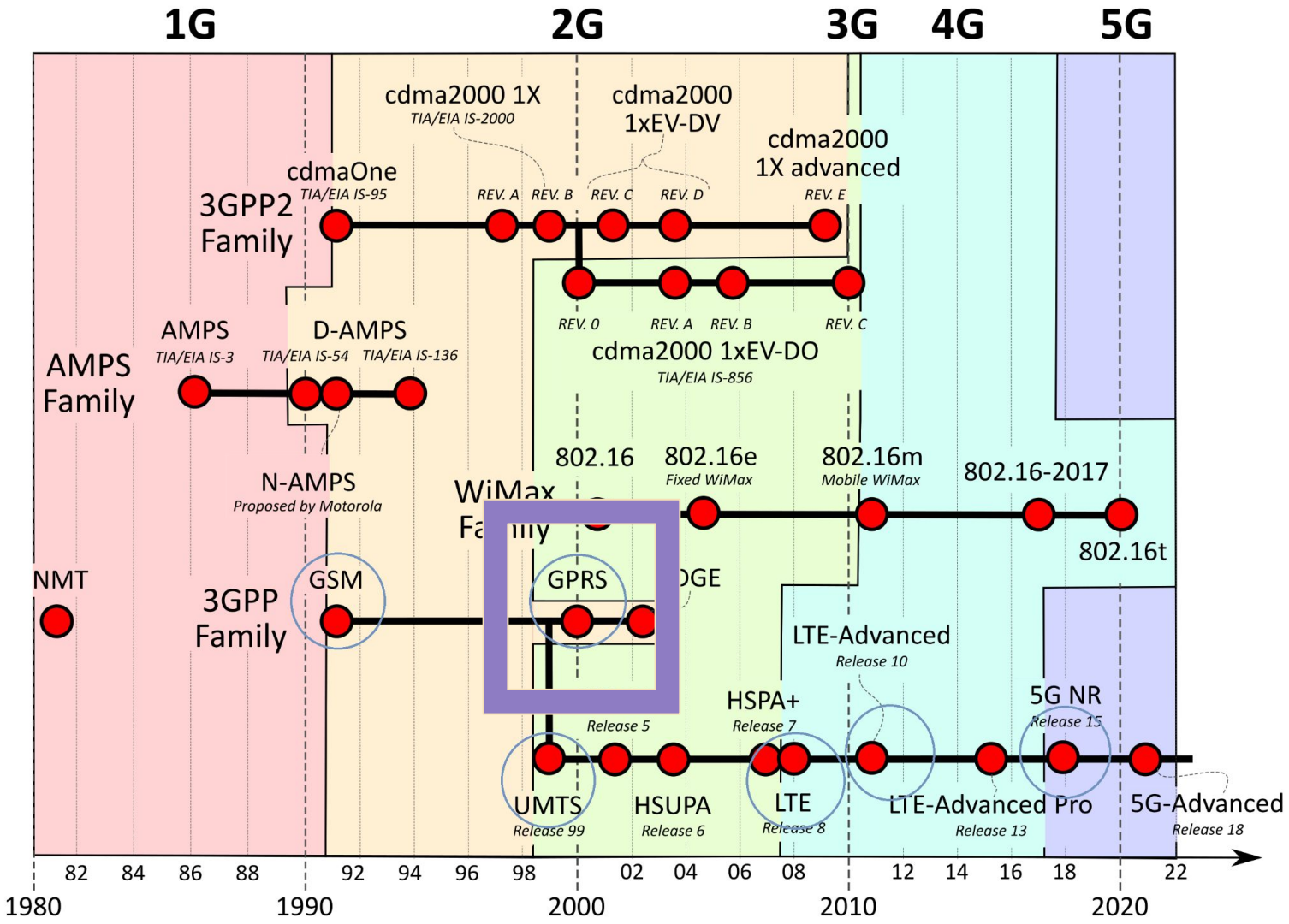
2G - GSM


HLR
VLR
EIR
AuC
BSS
BTS
BTS
BSC
MSC
GMSC
Mobile
Station
BTS
BTS
BSC
HLR
VLR
EIR
AuC
MSC
RAN



2G - GSM - Attack Vectors

- No mutual Authentication
  - IMSI-catchers / Stingray attacks
    - Rogue BTS
  - BTS determines encryption scheme!
- A5/1 is easily broken. A5/2 slightly harder but still weak.
- Jamming
- Network based attacks based on outbound signaling protocol
- Clear text tx after BTS


1G
2G
3G
4G
5G
cdma2000 1X
TIA/EIA IS-2000
cdma2000
1xEV-DV
cdma2000
1X advanced
cdmaOne
TIA/EIA IS-95
REV. A
REV. B
REV. C
REV. D
REV. E
3GPP2
Family
REV. 0
REV. A
REV. B
REV. C
cdma2000 1xEV-DO
TIA/EIA IS-856
AMPS
TIA/EIA IS-3
D-AMPS
TIA/EIA IS-54
TIA/EIA IS-136
AMPS
Family
802.16
802.16e
Fixed WiMax
802.16m
Mobile WiMax
802.16-2017
802.16t
N-AMPS
Proposed by Motorola
WiMax
Family
NMT
GSM
GPRS
3GPP
Family
LTE-Advanced
Release 10
HSPA+
Release 7
5G NR
Release 15
Release 5
UMTS
Release 99
HSUPA
Release 6
LTE
Release 8
LTE-Advanced Pro
Release 13
5G-Advanced
Release 18
82
84
86
88
92
94
96
98
02
04
06
08
12
14
16
18
22
1980
1990
2000
2010
2020

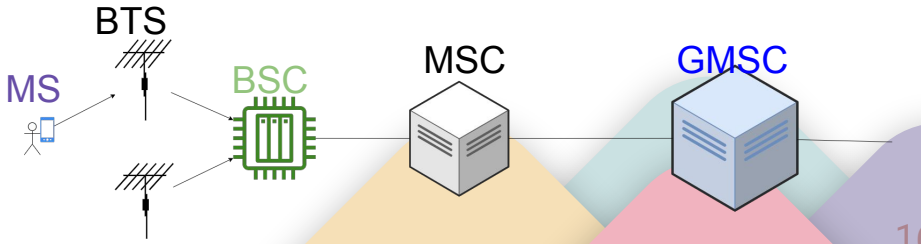
2.5G

GPRS

- Packet Switched + Circuit Switched
  - GSM + IP
- More Services!
  - MMS
  - Push-To-Talk over cellular
  - 4+1 or 3+2 timeslots

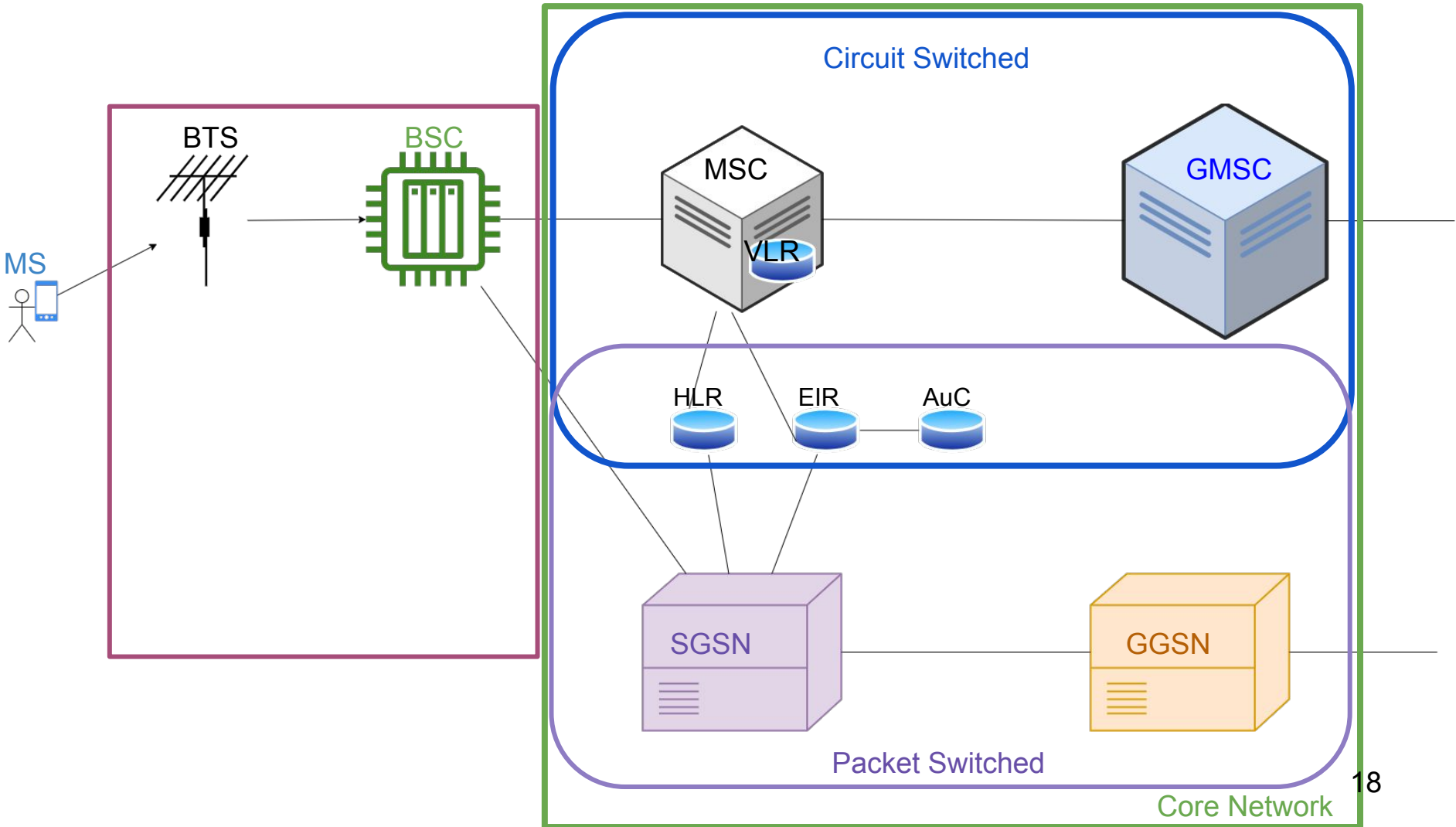
2.5G/GPRS - Network Architecture

- Front part mostly the same
  - Mobile Station **(MS)** / User Endpoint **(UE)**
    - Same thing. Now we also consider the Mobile Equipment **(ME)**.
  - BSS remains the same
    - **BTS** and **BSC** still there
- Circuit Switched Mobile GateWay **(CS-MGW)**
  - Hands it off to the known MSC.
- **MSC** functionality of before is needed for both portions of the network
  - Still feeds into the GMSC



2.5G/GPRS - Network Architecture

- GPRS Support Nodes
  - Serving GPRS Support Node (SGSN)
    - location, sec and access controls, mobility management and charging
    - communicates with other **SGSN** or **MME** (mobility management Entities) in same network and/or reaches out to the **GGSN**.
  - GPRS Gateway Support Note (GGSN)
    - a router in the subnetwork.
    - Converts incoming IP traffic into GSM and hands that off to the **SGSN**.
- Border Gateway and/or Charging Gateway
  - GGSN often contains this functionality


Circuit Switched
BTS
BSC
MSC
VLR
GMSC
MS
HLR
EIR
AuC
SGSN
GGSN
Packet Switched
Core Network

Mitigations from 2G

- Mutual Authentication for Packet Switched Portion
- Authentication between MS and SGSN
- Some level of Ciphering algorithm for SGSN.
  - PDU still transmitted in plain text.
- SGSN identity verification.

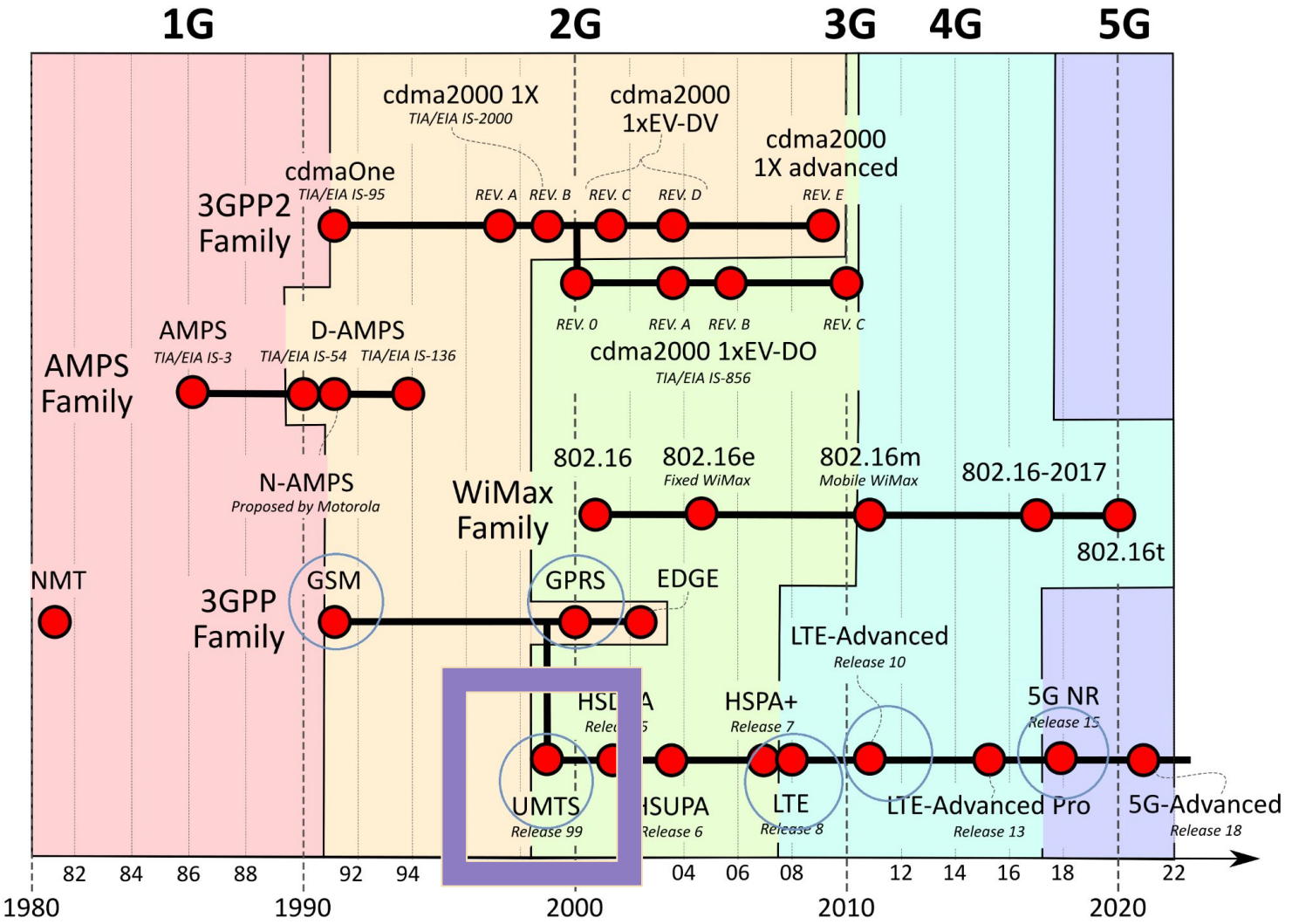
2.5G/GPRS Attack Vectors

- Same known rogue BTS flaws
- Some implementations without any encryption
  - Italy and Denmark according to P1
- Nokia GGSN attack
  - non-standard IP options in a packet over the Gi interface
- GTP weaknesses
  - GPRS Tunnelling Protocol has no encryption for User Plane or Control Plane.
  - Infra attacks, overbilling, protocol anomaly attacks
- Cisco GGSN ASR 5000
  - Improper Wireless Session Protocol (WSP) packet handling
    - Portal Page bypass
  - Improper HTTP packet handling
    - Send requests through GGSN without Verifying!

3G

UMTS

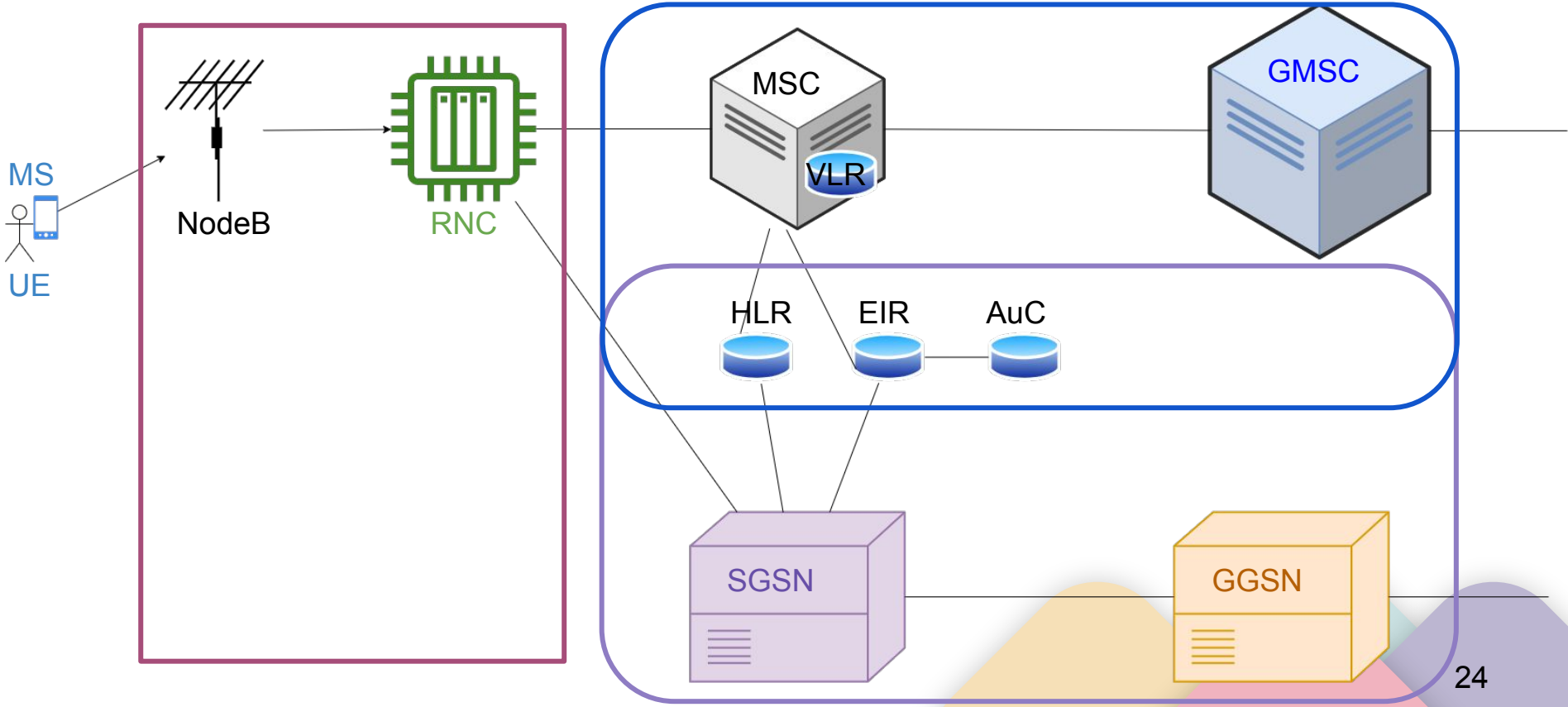
- More internet functionality!
- Video Chat!
- Mobile Broadband!
- SIGTRAN


1G
2G
3G
4G
5G
cdma2000 1X
TIA/EIA IS-2000
cdma2000
1xEV-DV
cdma2000
1X advanced
cdmaOne
TIA/EIA IS-95
REV. A
REV. B
REV. C
REV. D
REV. E
3GPP2
Family
REV. 0
REV. A
REV. B
REV. C
cdma2000 1xEV-DO
TIA/EIA IS-856
AMPS
TIA/EIA IS-3
D-AMPS
TIA/EIA IS-54
TIA/EIA IS-136
AMPS
Family
N-AMPS
Proposed by Motorola
802.16
802.16e
Fixed WiMax
802.16m
Mobile WiMax
802.16-2017
802.16t
WiMax
Family
NMT
3GPP
Family
GSM
GPRS
EDGE
LTE-Advanced
Release 10
HSPA+
Release 7
5G NR
Release 15
UMTS
Release 99
HSUPA
Release 6
LTE
Release 8
LTE-Advanced Pro
Release 13
5G-Advanced
Release 18
82
84
86
88
92
94
04
06
08
12
14
16
18
22
1980
1990
2000
2010
2020

3G - UMTS -Network Architecture

- Kept most of GPRS
- RAN is now called UTRAN **(UMTS terrestrial Radio Access Network)**
- NodeB
    - This is literally the same basic placement in the network and functionality as the
- Radio Network Controller **(RNC)**
    - In charge of all NodeBs for radio management.
    - Some Mobility Management
    - User data encryption

3G - UMTS - Architecture

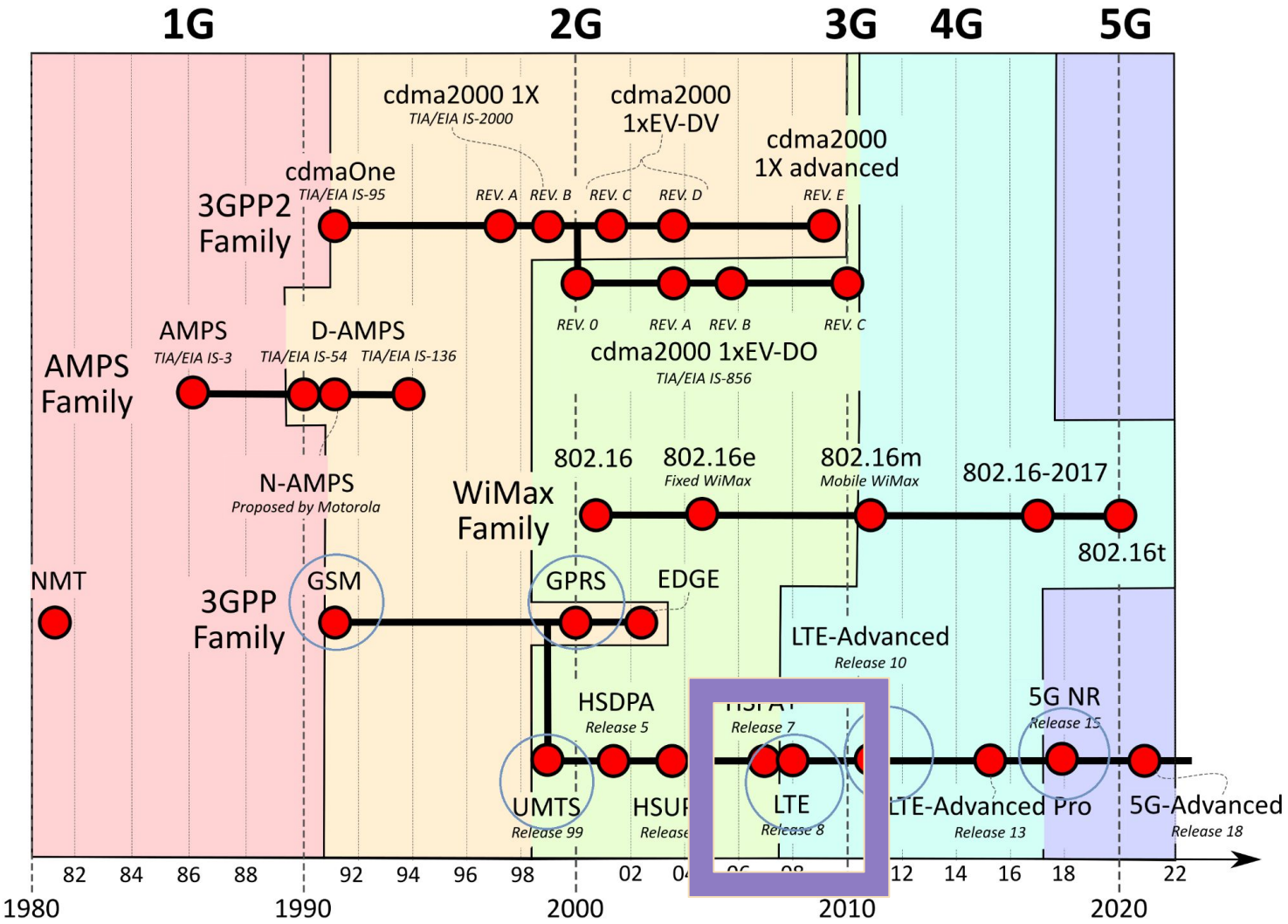


Mitigations from 2.5G

- (Attempts at) IMSI catcher mitigation
- Radio Access Link preserves IMSI confidentiality
- User Location confidentiality
- Signaling plane and user plane now have confidentiality requirements in the specs!
- Security should now be shown to the user
    - eg when hand off occurs to 2G
- True Mutual Auth!?

3G - UMTS - Attack Vectors

- Rogue **NodeB** (BTS) can still happen
- Remote IMSI Attack
  - Integrity keys between **UE** and **RNC** are generated in the Core Network and tx unencrypted to RNC, and sometimes between RNCs
  - Integrity of user data is not defined
- Signaling Plane **RAB**
- Mobile Network Operators receiving **UE** capabilities plain-text
- **HLR** overloading using SQN
- Cisco ASR 5000 Series GGSN
  - Not properly handling TCP packets

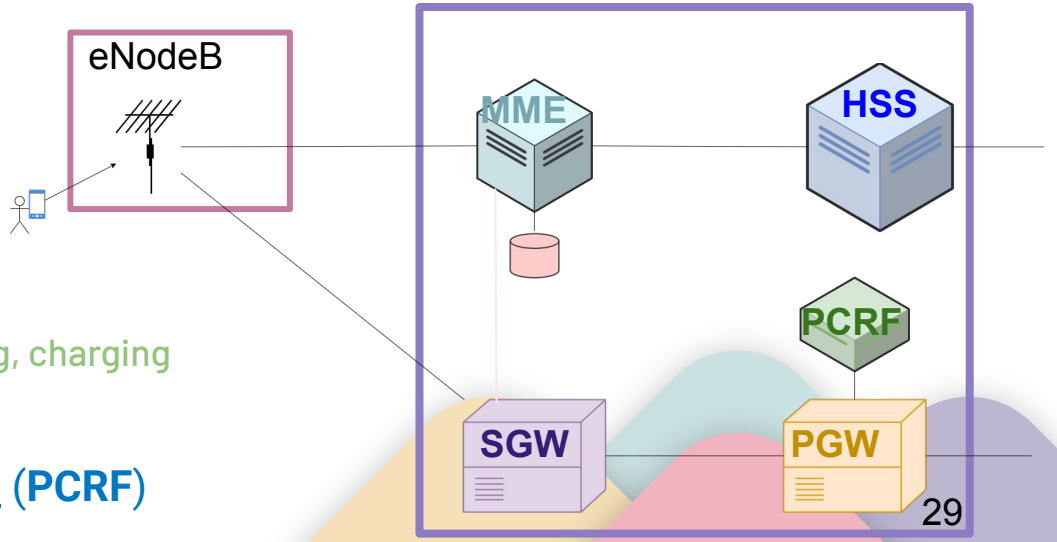

1G
2G
3G
4G
5G
cdma2000 1X
TIA/EIA IS-2000
cdma2000
1xEV-DV
cdma2000
1X advanced
cdmaOne
TIA/EIA IS-95
REV. A
REV. B
REV. C
REV. D
REV. E
3GPP2
Family
REV. 0
REV. A
REV. B
REV. C
cdma2000 1xEV-DO
TIA/EIA IS-856
AMPS
TIA/EIA IS-3
D-AMPS
TIA/EIA IS-54
TIA/EIA IS-136
AMPS
Family
N-AMPS
Proposed by Motorola
802.16
802.16e
Fixed WiMax
802.16m
Mobile WiMax
802.16-2017
802.16t
WiMax
Family
NMT
3GPP
Family
GSM
GPRS
EDGE
LTE-Advanced
Release 10
HSDPA
Release 5
Release 7
5G NR
Release 15
UMTS
Release 99
LTE
Release 8
LTE-Advanced Pro
Release 13
5G-Advanced
Release 18
82
84
86
88
92
94
96
98
02
12
14
16
18
22
1980
1990
2000
2010
2020

LTE

- 3.95G? 4G? Guess it’s called 4G now?
- Core network is now Evolved Packet Core aka System Architecture Evolution
- VoLTE, carrier adopted improvements
- Diameter

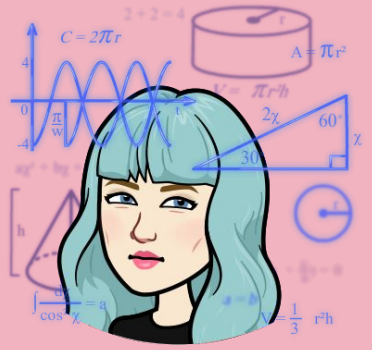
LTE - Network Architecture

- eNodeB
- Mobility Management Entity (**MME**)
  - replaces the RNC
  - Directs to appropriate SGW.
- Home Subscriber Server (**HSS**)
  - HLR and AuC combined
- Signal Gateway (**SGW**)
  - Routes and Forwards packets.
- PDN Gateway (**PGW**)
  - policy enforcement, packet filtering, charging
  - Gateway to the outside
- Policy and Charging Rules Function (**PCRF**)



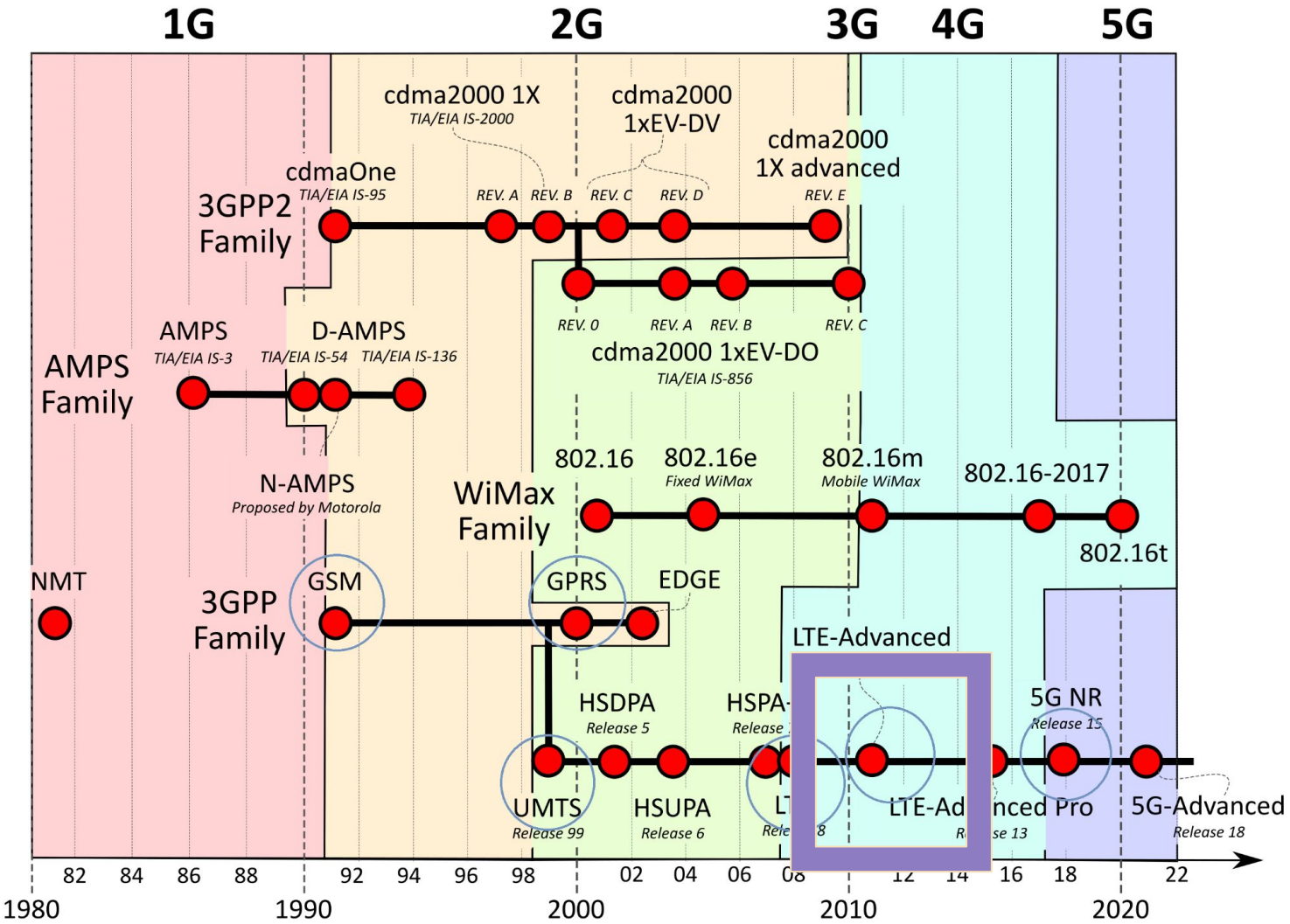
Mitigations

- eNodeB security?!
- IMEI is not sent to eNodeB until NAS (non-access stratum) security established
- EEA0
  - Null X algorithm (Null ciphering algorithm, Null integrity protection algorithm
- Mobility Management is now split apart and in its own entity for MME



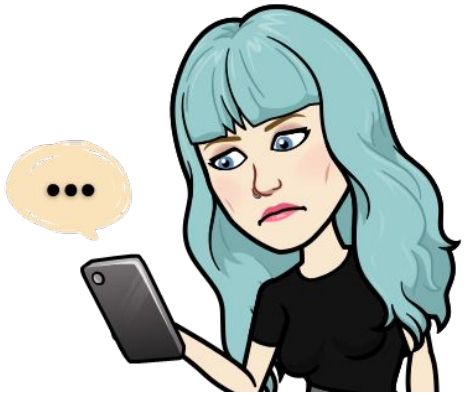
LTE - Attack Vectors

- LTEinspector
  - LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE by Hussain, Chowdhurry, Mehnaz and Bertino paper on these attacks.
    - Authentication Relay Attacks
    - Paging Channel Hijacking Attack
    - Panic Attack
- Bidding Down Attacks
  - Capabilities downgraded in quality.
  - Service can be downgraded to 3g or 2g
- Actual Implementation Errors for Identifiers
- Cisco PGW 2200 Remote DOS


1G
2G
3G
4G
5G
cdma2000 1X
TIA/EIA IS-2000
cdma2000
1xEV-DV
cdma2000
1X advanced
cdmaOne
TIA/EIA IS-95
REV. A
REV. B
REV. C
REV. D
REV. E
3GPP2
Family
REV. 0
REV. A
REV. B
REV. C
cdma2000 1xEV-DO
TIA/EIA IS-856
AMPS
TIA/EIA IS-3
D-AMPS
TIA/EIA IS-54
TIA/EIA IS-136
AMPS
Family
N-AMPS
Proposed by Motorola
802.16
802.16e
Fixed WiMax
802.16m
Mobile WiMax
802.16-2017
802.16t
WiMax
Family
NMT
3GPP
Family
GSM
GPRS
EDGE
LTE-Advanced
HSDPA
Release 5
HSPA-
Release
5G NR
Release 15
UMTS
Release 99
HSUPA
Release 6
LTE-Ad
nced Pro
Release 13
5G-Advanced
Release 18
82
84
86
88
92
94
96
98
02
04
06
08
12
14
16
18
22
1980
1990
2000
2010
2020

4G

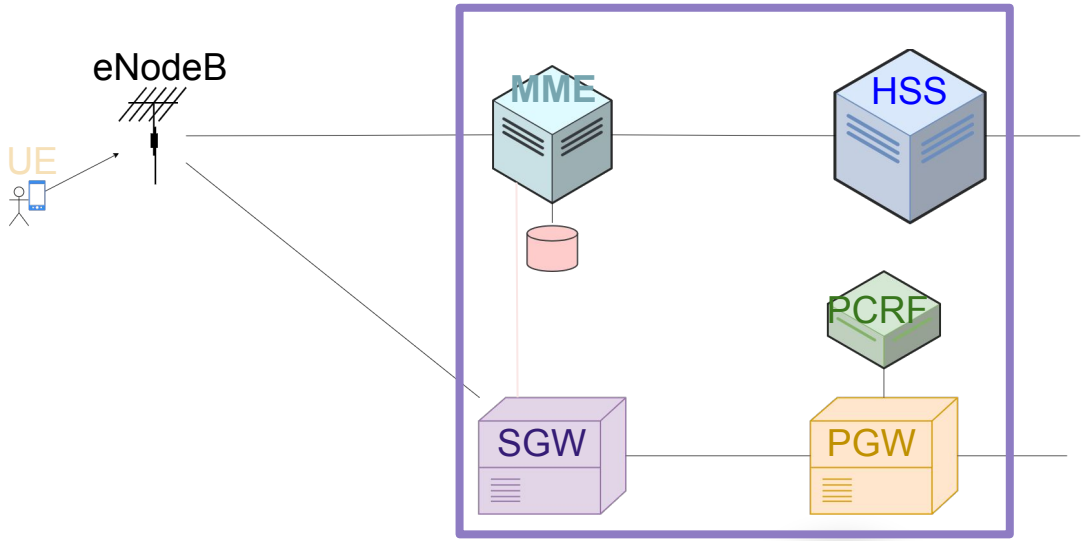
LTE Advanced, LTE Advanced Pro



- IPv6 expansions
- Adaptive modulation
- Time varying channel
- Voice over LTE
- Carrier Aggregation (LTE Advanced) and enhanced carrier aggregation (LTE Advanced Pro)
- IP Multimedia Subsystem

4G - LTE Adv - Network Architecture

- Same as 3.95G
- UE
- eNodeB
- MME
- HSS
- SGW
- PGW
- PCRF



Mitigations from LTE and Prior

- All radio interface data shall be encrypted
- AKA procedure for mutual auth between **UE** and **EPC**
- Different session keys for encryption and integrity protection
- CU-DU to make up eNodeB possible
- MNO may provide confidentiality in Radio Resource Control (RRC) signaling.
- Secondary authentication (for data network outside MNO)

4G - LTE Adv - Attack Vectors

- Still have IMSI catchers!
- Signaling vulns of Diameter
- VoIP SPIT Flooding
  - Syn flooding
  - UDP flooding
  - P2P/M2M attacks
- Router Vulns

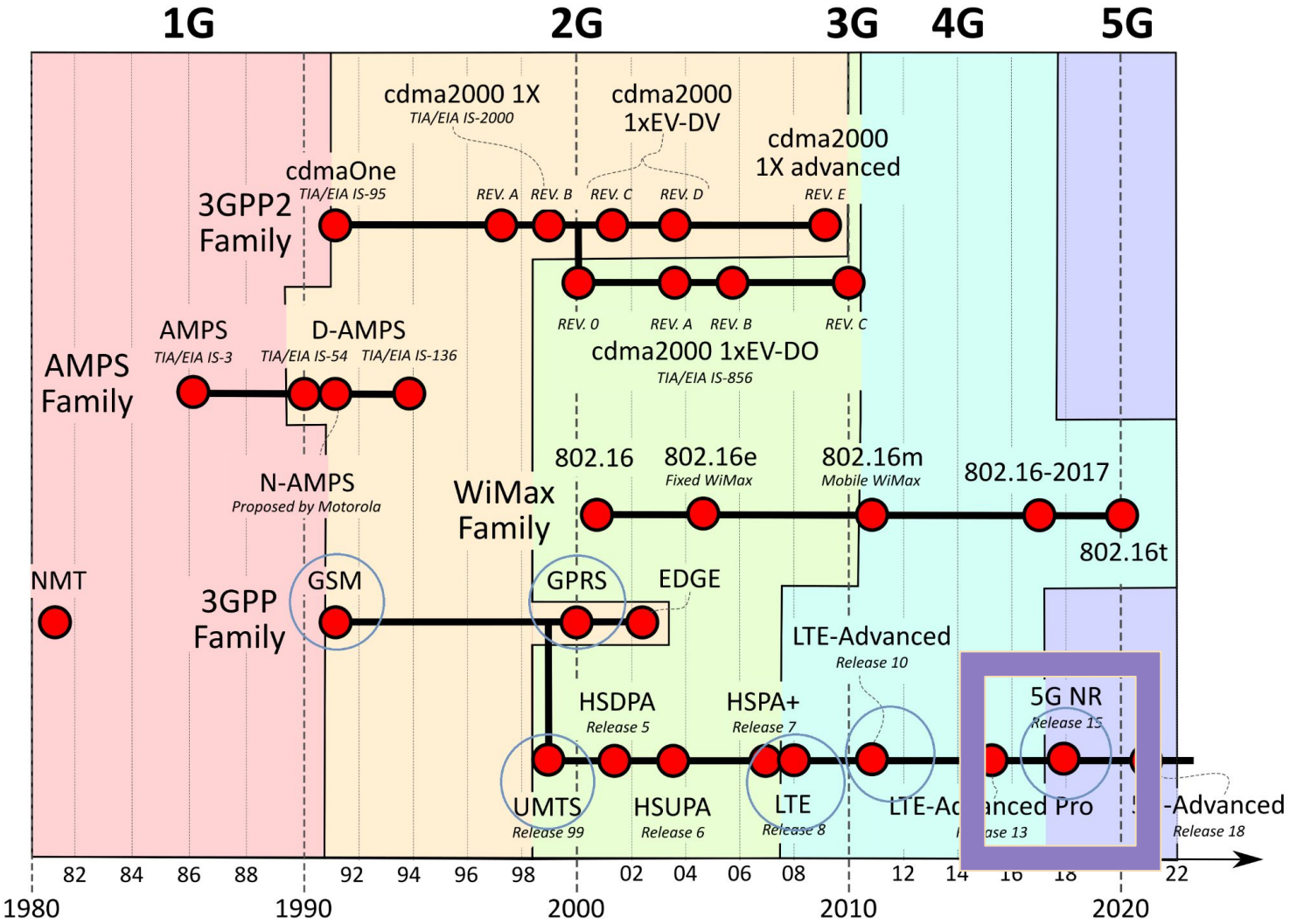
4G - LTE Adv - Attack Vectors

- Cisco ASR 5000 PGW DoS
- MME vuln
  - P1 HITB talk on keys being hardcoded
- MML Interface exposed to the wide internet on some routers
- Bidding down attacks
  - VoLTE can be denied

5G

Not just for telephony!

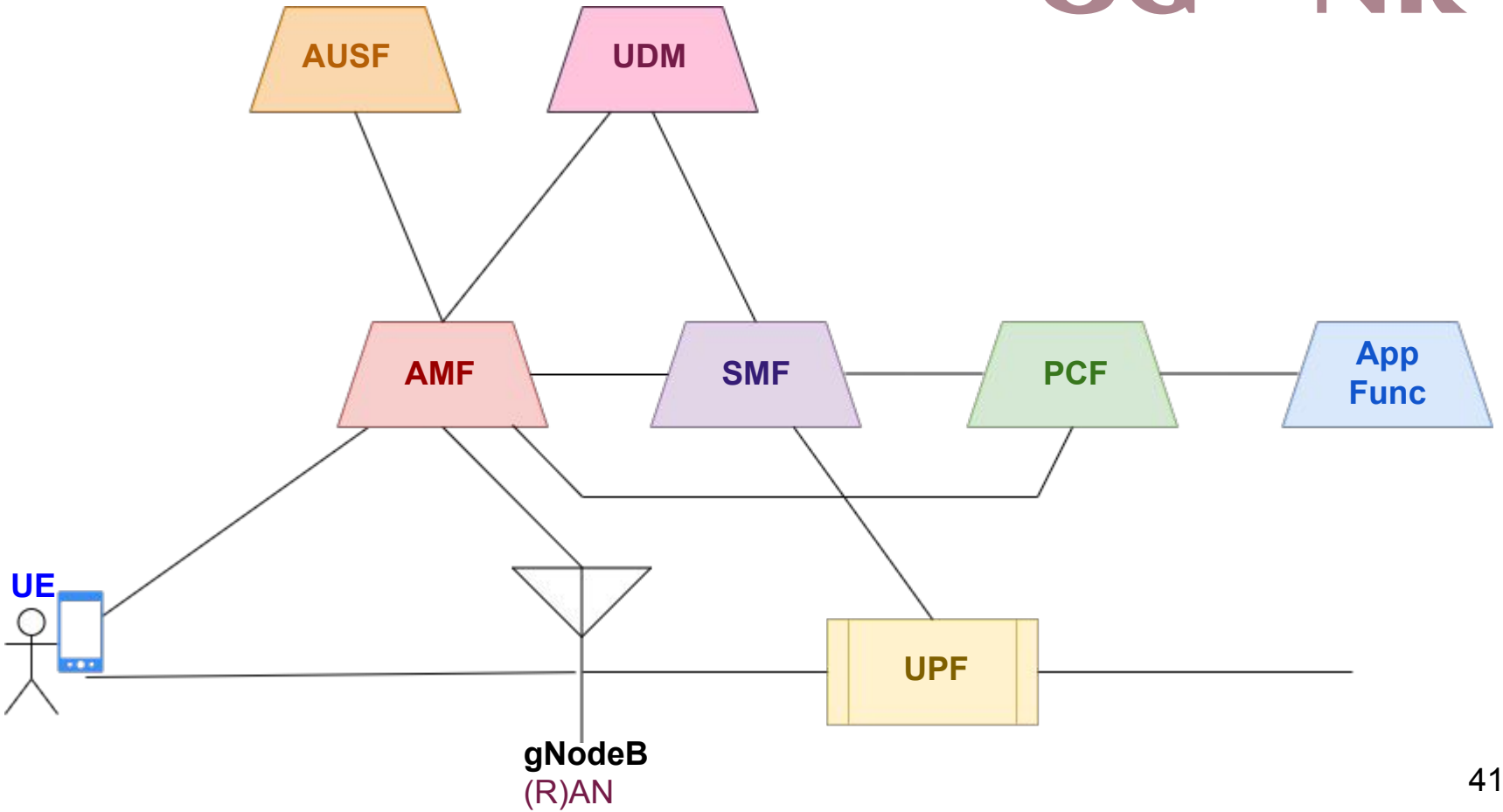
- Network Function Virtualization
- Management and Orchestration is now officially part of the core network
- New concept of Network Slicing
  - Different devices have different needs!
- Renaming the eNodeB to **gNodeB** just cuz!


1G
2G
3G
4G
5G
cdma2000 1X
TIA/EIA IS-2000
cdma2000
1xEV-DV
cdma2000
1X advanced
cdmaOne
TIA/EIA IS-95
REV. A
REV. B
REV. C
REV. D
REV. E
3GPP2
Family
REV. 0
REV. A
REV. B
REV. C
cdma2000 1xEV-DO
TIA/EIA IS-856
AMPS
TIA/EIA IS-3
D-AMPS
TIA/EIA IS-54
TIA/EIA IS-136
AMPS
Family
N-AMPS
Proposed by Motorola
802.16
802.16e
Fixed WiMax
802.16m
Mobile WiMax
802.16-2017
WiMax
Family
802.16t
NMT
GSM
GPRS
EDGE
3GPP
Family
LTE-Advanced
Release 10
HSDPA
Release 5
HSPA+
Release 7
5G NR
Release 15
UMTS
Release 99
HSUPA
Release 6
LTE
Release 8
LTE-Ad
ase 13
anced Pro
-Advanced
Release 18
82
84
86
88
92
94
96
98
02
04
06
08
12
14
16
18
22
1980
1990
2000
2010
2020

5G - NR - Network Architecture

- Access and Mobility Management Function **(AMF)**
- Session Management Function **(SMF)**
  - PDU management, pcf interaction for data network profile
  - UPF selection, IP address allocation if IP based
- User Plane Function **(UPF)**
  - Also would have been in **MME**
  - Anchor for NG-RAN mobility and QoS flow, Policy enforcement
- Unified Data Management **(UDM)**
  - Access authorization, Data network profiles
  - Registration and Mobility Management
- Policy Control Function **(PCF)**
  - Dynamic policy decisions and conditions.

5G - NR



5G - NR


SERVICES
NDDP
PLATFORM
SPECTRUM
ANALYZER
Baseband 6502
Baseband 6303
Baseband C608
Baseband P614
Radio 2205
Radio 2242
Radio 4412
Radio 4407
Radio 8808
AIR 6468

Mitigations from 4G

- Initial NAS message confidentiality!
- Subscription Concealed Identifier (**SUCI**) and Subscription Permanent Identifier (**SUPI**) to protect IMSI
- Security and Mobility separated in the core network
- 256bit keys supported
  - ("prepared to" in 4G docs, now "must")
- Mutual auth between Network Exposure Function (**NEF**) and Application Function (**AF**)
- Inter-PLMN UP Security (IPUPS) in UPF at perimeter to protect user plane messages (GTP-U).
- **AUSF** and **UE** now have SoR counter to mitigate replay attacks.
- Security Anchor Function (**SEAF**) allows AKA to skip full reauth

5G Attack Vectors

- RA and CN don't require authentication. Location sniffing attack
  - Place sniffing tool near target UE
    - Monitor for plaintext AuthReq msg
    - The message contains RAND and AUTN
  - Build an AuthReq message using that RAND and AUTN.
  - Broadcast fake message.
    - MAC check fails if not target UE
    - Victim UE passes MAC, fails SEQ
    - If all messages fail MAC verification, the UE is not nearby. If one SEQ failure, it is nearby.

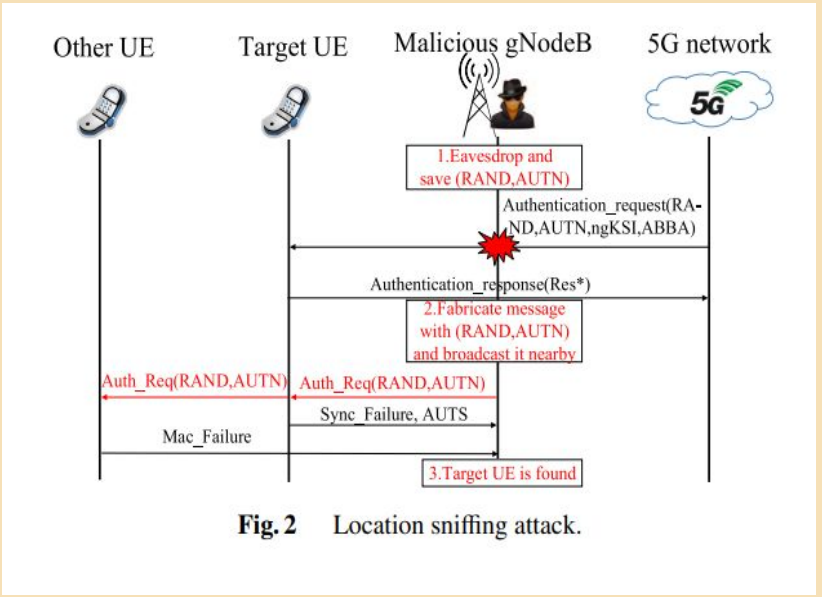


Fig. 2 Location sniffing attack.

https://www.jstage.jst.go.jp/article/transinf/E103.D/8/E103.D_2019FOL0001/_pdf

5G Attack Vectors

- Attach Req Injection
- Battery Draining
  - NB-IOT and LTE-M devices in particular can be drained like 5x faster than expected
- AKA Attack
- Sending malformed packets can trigger crashes in 5g cores. Yes, still.
- Network Slicing Vuln
  - Deloitte gave a talk at RSA about this.
  - Navigate up a network slice looking for other vulnerable devices.
- Multi-Access Edge Computing (MEC)
- HTTP/2 Attacks
  - Stream Reuse
  - Closed Stream
- End-to-end China Unicom

Review

- 2G: Digital Technology! Voice and Data. Circuit Switched. User, BSS, MSC, GMSC.
- GPRS: Both Circuit and Packet Switched! Added the SGSN and GGSN.
- 3G: UMTS NodeB, RNC, kept SGSN and GGSN.
- LTE: Evolved packet core! eNodeB, Mobility Management, Signal Gateway and PDN Gateway.
- 4G: VoLTE, IPv6, IMS. Kept devices same.
- 5G: Virtualization. Network slicing. gNodeB. Functionality generally split into "functions" instead of devices.

References

- Most used image came from https://en.wikipedia.org/wiki/Cellular_network
- Device images came from vendor websites
- The Critical Hole at the Heart of Our Cell Phone Networks, Zetter https://www.wired.com/2016/04/the-critical-hole-at-the-heart-of-cell-phone-infrastructure/
- Taking up the Gauntlet - SS7 Attacks in Ukraine, Cathal Mc Daid, https://blog.adaptivemobile.com/russia-ukraine-telecom-monitoring
- https://www.cnvd.org.cn/flaw/show/CNVD-2014-00546 Cisco ASR 5000 Series Devices GPRS Support Node Security Bypass Vulnerability
- https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-cisco-pdng-dos-KmzwEy20.html Cisco Packet Data Network Gateway IPsec ICMP Denial of Service Vulnerability
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160621-asr Cisco ASR 5000 Series Packet Data Network Gateway Denial of Service Vulnerability
- LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE, Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, Elisa Bertino
- Nokia warns 5G security 'breaches are the rule, not the exception' , Kapko, https://www.cybersecuritydive.com/news/5g-security-breaches/636693/
- 5G Network Attacks Projects, https://networksimulationtools.com/5g-network-attacks-projects
- P1 security Archives, https://www.p1sec.com/corp/category/p1-security/
- A Vulnerability in 5G Authentication Protocols and Its Countermeasure (2020). Xinxin HU, Caixia LIU, Shuxin LIU, Jinsong LI, and Xiaotao CHENGHU. IEICE Transactions on Information and Systems. E103.D. 1806-1809. 10.1587/transinf.2019FOL0001.
- Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li and Elisa Bertino. https://homepage.divms.uiowa.edu/~comarhaider/publications/LTE-torpedo-NDSS19.pdf

References

- On the Detection of Signaling DoS Attacks on 3G WiMax Wireless Networks. Patrick P.C. Lee, Tian Bu , Thomas Woo https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=cb5197dfceb76fe6ac37909c6ef935285f9e0cc7
- Statement of Vulnerabilities in ZTE MF910 and MF65+ Products. ZTE. 2019. https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1010203
- ZTE MF910 – An end of life router, running lots of vivacious hidden code. Richter, Pentest Partners. https://www.pentestpartners.com/security-blog/zte-mf910-an-end-of-life-router-running-lots-of-vivacious-hidden-code
- LTE Pwnage: Hacking HLR/HSS and MME Core Network Elements P1 Security. Presented at HITBSecConf2013. Amsterdam. https://conference.hitb.org/hitbsecconf2013ams/materials/D1T2%20-%20Philippe%20Langlois%20-%20Hacking%20HLR%20HSS%20and%20MME%20Core%20Network%20Elements.pdf
- Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui L,, Elisa Bertino.
- New 4G LTE Network Attacks Let Hackers Spy, Track, Spoof and Spam. Swati Khandelwal. The Hacker News, Mar 05, 2018. https://thehackernews.com/2018/03/4g-lte-network-hacking.html
- GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier. Byeongdo Hong, Sangwook Bae, Yongdae Kim. Presented at the Network and Distributed System Security Symposium. https://syssec.kaist.ac.kr/pub/2018/hong_ndss_2018.pdf
- A first look on the effects and mitigation of VoIP SPIT flooding in 4G mobile networks. Bou-Harb, Elias & Debbabi, Mourad & Assi, Chadi. (2012). 982-987. 10.1109/ICC.2012.6364233.
- Cheating VoIP Security by Flooding the SIP. Irfan Shakeel. Jan 20, 2016. https://resources.infosecinstitute.com/topics/hacking/cheating-voip-security-by-flooding-the-sip/

More References!

- New Vulnerabilities in 5G Networks. Altaf Shaik* , Ravishankar Borgaonkar. Presented at Black Hat Briefings. https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf
- Cisco PGW 2200软体交换机多个安全漏洞 May 2010. CNVD -2010-0844. https://www.cnvd.org.cn/flaw/show/CNVD-2010-0844
- LTE核心网存在拒绝服务漏洞. Jan 2021. CNVD-2020-71678. https://www.cnvd.org.cn/flaw/show/CNVD-2020-71678
- Cisco Gateway GPRS Support Node TCP Invalid Packet Vulnerability. Cisco. CVE-2015-4201. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150619-CVE-2015-4201
- https://www.mpirical.com/ for 5G trainings
- Signalling Security Analysis: Is HTTP/2 Secure in 5G Core Network? Xinxin Hu, Caixia Liu, Shuxin Liu, Wei You, Yu Zhao; 2018 10th International Conference on Wireless Communications and Signal Processing. Hangzhou, China, 2018. doi: 10.1109/WCSP.2018.8555612.
- Bookworm Game: Automatic Discovery of LTE Vulnerabilities Through Documentation Analysis; Yi Chen, Yepeng Yao, XiaoFeng Wang, Dandan Xu, Chang Yeue , Xiaozhong Lui, Kai Chen, Haixu Tang, Bauxu Liu. 2021 IEEE Symposium on Security and Privacy IEEE publication
- ESF Potential Threats to 5G Network Slicing, NSA, CISA. https://www.cisa.gov/news-events/alerts/2023/07/17/nsa-cisa-release-guidance-security-considerations-5g-netw
- New Vulnerabilities in 5G Networks-Blackhat Briefings Altaf Shaik* , Ravishankar Borgaonkar. https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdfork-slicing
- Statement of Vulnerabilities in ZTE MF910 and MF65+ Products. ZTE. 20 February 2019. https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1010203
- Potential Threat Vectors to 5G Infrastructure - U.S. Department of Defense. May 2021. https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF

Questions?

Thank you!!!

- My cowor[illegible]edback and