Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Exploit Vulnerabilities in 4G and 5G Cellular Access Network

Ahmed M. Elbadry Kamal[1], Mohamed Saad Zaghloul[1], Waleed K. Badawi[1], Roshdy A. Abdelrassoul[1,*]

[1] Electronics and Communications Engineering, Arab Academy for Science, Technology and Maritime Transport, Alexandria Governate 5528341, Egypt

ABSTRACT

Portable gadgets back different specialized highlights and administrations for up-and-coming 2G, 3G, 4G and 5G systems. For illustration, these determinations contain physical layer rate sorts, radio convention data, security calculations, carrier conglomeration groups, and benefit sorts such as GSM-R, Voice over LTE, Within the setting of portable security standardization, these organize determinations and administrations are alluded to as gadget capabilities and are traded with the organize amid the gadget enrolment stage. In this article, we investigate data around indicated gadget capabilities for 4G and 5G gadgets and their part in building up a secure interface between the gadget and the arrange. Our inquire about comes about appear the plausibility of the gadget being traded with the carrier some time recently the confirmation step without any ensures and not affirmed by the carrier. Therefore, we display three unused sorts of assaults that misuse data approximately the capabilities of unprotected gadgets in future 5G systems: Character assaults, sending assaults, and battery deplete assaults against versatile gadgets. Conduct verification of concept assaults utilizing reasonable equipment and computer program arrangements to survey their effect on commercial 4G gadgets and systems. We have detailed the distinguished vulnerabilities to pertinent benchmarks bodies and given countermeasures to relieve assaults against gadget capabilities in up-and-coming 5G systems.

Keywords:
Attacks; security; wireless; 5G

1. Introduction

Mobile networks have advanced, allowing for innovative applications and remote control of various devices, from small sensors to vehicles. 4G and 5G networks are designed to support various applications such as smart homes, basic framework, HD media conveyance, and robotized cars. Also, Limit Band IoT and LTE-M are revolutionizing the IoT showcase with an uncommon protocol suite for IoT applications. 3GPP outlines features in 4G and 5G standards to manage mobile network apps shared during device registration. Device capabilities dictate device-to-network communication, covering speed, frequency, security, and telephony. The network detects the app and connects the self-driving car with nearby vehicles using V2V support. Top smartphones support carrier aggregation

[*] *Corresponding author.*
E-mail address: roshdy@ieee.org

https://doi.org/10.37934/araset.53.2.252262

and MIMO for faster data rates, while IoT devices negotiate with the network for power usage. Proper app operation requires device capabilities. This article analyses 4G and 5G network security standards and finds that sharing device information during registration can be risky. 3 types of mobile attacks: identification, bidding down, battery draining. Our attacks can reveal device details, slow data rates, block VoLTE services, and quickly drain batteries on real LTE networks using commercial devices. LTE and upcoming 5G devices are vulnerable due to 3GPP specifications. Minor fixes have been recommended to SA3 and network administrators. [1,2] We anticipate 3GPP 5G will address the vulnerabilities exposed in this report, including a flaw in the specification that permits utility identity attacks through equipment exploitation during LTE device registration. The initial LTE NB-IoT protocol has a vulnerability that impacts battery life in low-power devices. Inexpensive testing can be conducted using existing hardware and software. Test attacks using commercial devices and mobile networks. Use 4G measures and 5G security suggestions to counter assaults.

2. Related Work

We review research on wireless security, including MitM, identity, and service availability, with a focus on privacy breaches of LTE subscribers via rogue base stations. Authors in [3] hijack DNS traffic by exploiting the unprotected LTE radio interface, while our attacks are simpler and don't require cryptography. 5G networks have vulnerabilities that need fixing, including MitM attacks in low-power wireless networks. Bluetooth pairing is explained in [4-6], whereas LoRa's spread factor affects power usage & bit rate [7] and is a static configuration compared to LTE. Sigfox [8] has a unique security model that is resistant to MitM attacks, except when utilizing the mobile network as the backbone link. IMSI can be exposed in LTE networks, while IMEI is kept private. Baseband can reveal IMEI to rogue stations, making LTE devices susceptible to attacks. [9,10] suggest identifying device type by using MAC layer data and network interaction for IoT or wired/WLAN connected mobile devices. They find vulnerable devices by checking a database and testing with real IoT devices.

Our study targets new mobile IoT technologies and recognizes devices by features, not IMEI or MAC address. Our technique detects multiple devices on 5G networks and authors in [11] recognize LTE supporters and areas utilizing brief identifiers. Randomization of these identifiers avoids following and has been broadly received by operators. Our fingerprinting methods stay the same, permitting us to associate fingerprints with IMSI and follow LTE clients. LTE service threats: accessibility and benefit downsizing attacks, demonstrated in [12], with vulnerable networks to malicious base station attacks. Hackers can contaminate internal data, causing call disruptions and service downgrade. However, their intrusion is temporary, and users can bounce back. We focus on UEs with less effort and cost for major damage. The author executes a DoS attack using LTE control messages. Inexperienced for network attacks like V3 vulnerability. NB-IoT is used for power-consuming attacks on commercial UEs. Table 2. shows a list of acronyms used in this paper.

3. UE Capabilities

A UE underpins many capabilities for distinctive LTE organizations and operations. They are classified into centre organize capabilities [13,14] and radio get to capabilities [15,16] and are worked out by the MME and the eNodeB separately. The centre organizes capabilities contain non-radio related capabilities, security calculations, communication highlights and whereas radio get to capabilities donate radio perspectives of the UE, such as supported repeat groups, get and transmit capabilities and etc. Progress, a UE can back different radio get to progress such as LTE, 3G, 2G, and CDMA and reports its capabilities to the organize in the midst of the enrolment strategy.

3.1 LTE Registration

In LTE, a standard enlistment is carried out with control plane messages. Once turned on, a UE sends an attach request to the MME to ask for voice/data services. This text discusses supporter characters like IMSI and TMSI, as well as the UE's centre organize capabilities. Connect Ask is sent in plaintext as the first message to the network. After identifying the subscriber, UE and network authenticate and establish security, including encryption and message integrity between UE and MME. MME asks eNodeB for UE's radio accessibility. UE sends capabilities via UE Capability Information message upon receiving query from eNodeB. eNodeB sends capabilities to MME and keeps them until UE exits network. RRC security established for encrypted message exchange between UE and eNodeB. Operators have different radio access and RRC security configurations. Successful UE registration occurs after receiving the Accept message, granting access to network services. LTE networks use Tracking Areas (TAs) with unique identifiers (TACs) for location division. A UE must perform a Tracking Area Update (TAU) when moving across TAs to update network position. UE sends TAU request to MME, process ends with TAU Accept message. UE updates network and performs TAU periodically when T3412 timer expires.

4. Vulnerabilities and Threat Model

This area reveals the vulnerabilities we found LTE conventions and usage. To begin with, we display a risk show and examine the vulnerabilities. Following that, we construct a test setup to abuse the vulnerabilities utilizing commercial gadgets and systems.

4.1 Threat Model

We characterize a danger demonstrate and characterize two sorts of enemies: passive and active. Both are familiar with authority the LTE protocol and provide access to the software and hardware required to intercept and decode LTE control channel messages over the air interface. Additionally, Active Devices offers two ways to set up a license-free LTE network. A first type of active adversary could manipulate her unauthorized eNodeB and exchange her messages with the victim's UE and her LTE control plane. The second type of active adversary acts as a "man in the middle" (MitM), forwarding traffic between the victim's UE and legitimate networks, and unencrypted her LTE control. You can also change/insert information into plain her messages.

4.2 Vulnerabilities

We identified three vulnerabilities in the LTE registration process. Use the UE's capabilities that are sent to the network during this time. The registration or TAU procedure is described as follows:

i. (V1) Both the primary centre arrange and radio get to capacities UEs can be obtained without requiring verification [7,17]. This permits for dynamic or detached rivals to get all the highlights of UE. Misuse this helplessness to illustrate a gadget sort recognizable proof attack Section5
ii. (V2) Moment, the MNO demands radio get to capabilities from the UE sometime recently RRC security. Set up as appeared in Figure 1. The result may be a completely useful UE. Sent in plaintext and can be seized by the other party capacity. We explore the dangers emerging from this helpless handle and illustrate a gadget offering attack in section 6.

iii. (V3) Third, the connect ask message is continuously sent decoded from the UE to the network [7], in spite of the fact that there may be judgment. Existing NAS security settings will be secured. U.E. Be that as it may, the enrolment handle will not be hindered. In case the MME judgment check falls flat. In such cases the substance of the Connect Ask message is powerless. Infusion or adjustment assault. In specific, centre-arranged capacities inside this message can be seized by people. Accomplice. We have found that adjusting certain centre arrange capacities can lead to control deplete attacks against NB-IoT. This will be explained in Section 7.

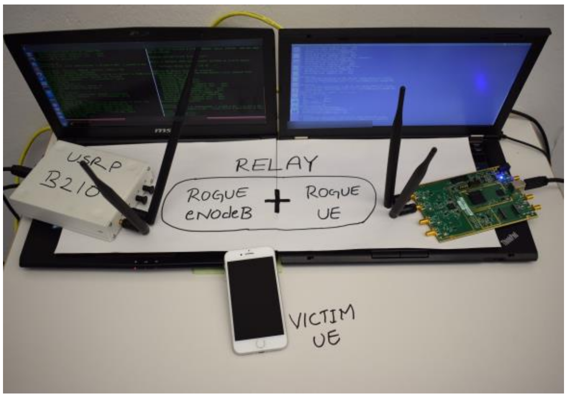

Fig. 1. LTE registration procedure

4.3 Experimental Setup

We construct a test format as appeared in Figure 2 to illustrate and authorize our assaults. Our outfit factors muster of two have i5 PCs exercising Linux OS and two radio modules made of All-inclusive Program Radio Peripheral B200(18). B200 could be a program represented radio that is ruled by a host-grounded computer program by means of a USB3 harbour age to achieve transmit and get missions. Another, our program factors are made exercising the open-source design srsLTE(19). Directly, we exercise srsUE program and srseNB to serve as a UE and eNodeB collectively. Help, we employed a test bed announced by a seller to achieve NB- IoT experiments. On this test bed, we have access to design, acclimate and fantasize LTE control airplane dispatches. For sequestration reasons we do not flash this test bed in this paper. As stressed in Figure 2 the computer program is executed on the have PC which controls the B200 to transmit and get LTE signals. To achieve our raids, we frame and work a mischief eNodeB and a phase-off which are point by point below.

i. <u>eNodeB operation isn't permitted:</u> A rogue eNodeB mimics a real eNodeB by recursively forging and sequencing the real network administrator's code. Use a TAC different from the current TA to include the UE within the working locale. Most importantly, it goes beyond the true eNodeB by delegating a little more advanced control and consequently receiving TAU-Ask messages from the UE. To achieve this, we modified the srseNB computer program and presented the rogue system to the UE. The rogue eNodeB in Figure 2 exchanges LTE control plane messages with UEs and, implausibly, forwards them to real organizations after the attack.

ii. <u>Relay Operation:</u> The relay comprises of an unauthorized User Equipment (UE) and an unauthorized Node B. The configuration of the rogue evolved Node B (eNodeB) is akin to the eNodeB discussed earlier and is directly linked to the rogue UE, which is located on a separate server. The rogue UE forwards the traffic between the victim UE and the legitimate network. We have adopted the same approach as described in [20] to ensure a stable connection between the legitimate UE and the network. However, we have utilized certain frequencies for the operation of the rogue eNodeB that differ from those of the legitimate operator, thereby preventing our rogue UE from connecting to our own rogue eNodeB. For the configuration depicted in Figure 2, we have employed a modified srseNB, as mentioned earlier, and a modified srsUE to receive and forward control plane messages (RRC and NAS) between the legitimate network and the victim UE core. The primary modification pertains to the merging of the srsUE and srseNB segments. Additionally, we have utilized directional antennas and power amplifiers to enhance the signal conditions between the unauthorized UE and the legitimate network. Similar to this transitional configuration, we have a UE shard and an eNodeB shard in our NB-IoT test platform, which we also refer to as transitions in our tests.

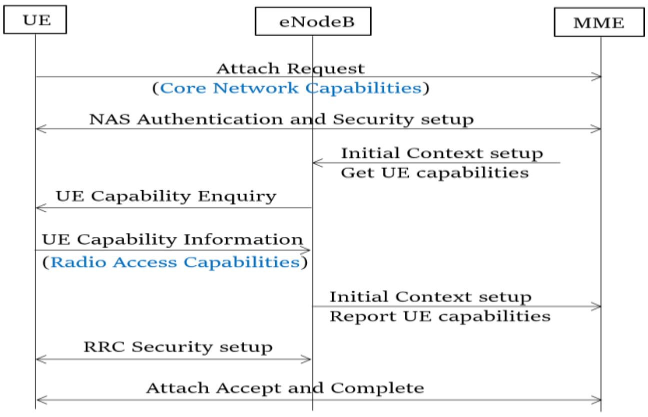

Fig. 2. Experimental setup

5. Device-Type Identification

This section introduces methodologies for identifying device types on a mobile network and intelligently estimating underlying applications. The initial focus is on exploring User Equipment (UE) capabilities and their application in commercial devices and applications. Subsequently, our reference model is discussed, which employs a range of known devices and techniques to differentiate between various devices and applications. Finally, the reference model is utilized to execute a Mobile Network Map (MNmap) attack, and the consequences of such an attack are deliberated.

5.1 Understanding UE Capabilities

"Device type refers to device-specific details such as manufacturer, model, software, and application. Mobile-enabled device manufacturing involves baseband vendors, device manufacturers, and application developers." Baseband vendors tune UE capabilities based on the 3GPP standard and specifications. They offer a subset of the many optional capabilities in distinct ways. UE capabilities vary for different applications. For instance, telephony is a must for cell phones. Trackers need GPS always, phones not. Cars need GPS and V2X for self-driving [21]. Modem features depend on the application, correlating with UE capabilities. We analyse UE capabilities and create a model to identify mobile device types.

5.2 Mobile Network Mapping (MNmap)

The goal of this attack is to identify devices on the wireless network by analysing their capabilities. An adversary can exploit an unauthorized eNodeB in our setup to obtain these capabilities (both core and radio) since the UE transfers them to the network without authentication. Passive adversaries may have UE core network capabilities, but not radio capabilities. For granular identification, both core and radio capabilities are needed, so we focus on active adversaries. We test an unknown UE and use our reference model to identify its device type. When the UE sends a TAU Request message, we extract core network capabilities and send a UE Capability Query. UE responds with its capability information. We extract its radio capabilities and release it to a legitimate network with RRC release message. Our model-based Intel XMM7480 baseband identified an unknown device as a voice-focused phone/tablet with Cat 6 support. Searched Intel XMM7480 smartphones & tablets, confirmed iPhone 7. Goal 2: spot potential device vulnerabilities. MNmap can gather vulnerability info from external sources like Huawei, Qualcomm, Google, Apple, and Samsung, and use it for targeted attacks. The device fingerprints can also be combined with the IMSI fixed identifier for subscriber tracking. Despite clear bans on IMSI transmission in all cases for 5G, unique device type information can still allow for device and user fingerprinting among neighbouring devices.

5.3 Evaluation and Challenges

Our benchmark model is also applicable to other baseband manufacturers. Determining the vendor and chipset model is easy with the specified parameters in the appendix. We tested 10 unknown UEs and identified their type at level four, using our fingerprinting method. These devices are similar to our reference model. MNmap uses a reference model and public database to identify device type, thus requiring a broader and varied reference model to accurately determine device type. Identifying phones, tablets, routers, and automotive devices is simple with our reference model. However, mobile IoT devices are challenging to recognize due to limited capabilities and similar applications, making aggregation a complex task. An issue is identifying the application's OS version as the baseband model and mobile OS version do not correlate and update at the same time. Additionally, some UEs' USIM cards can control feature accessibility. Bands are activated and deactivated by the operator and identified through USIM settings for MNmap attack consideration.

6. Device Bidding Down

This section describes a submission attack on a UE, where the functionality of the UE is hijacked. We first discuss the possibilities to be exploited and then a test attack and evaluate it on commercial networks. Finally, we present the feasibility and implications of this attack.

6.1 LTE Radio Access Capabilities

UE shares radio capabilities with eNodeB, which configures and plans data/signalling based on received capabilities. Explaining capabilities used in attacks and LTE network, starting with UE category. Used to determine bit allocation on radio channels to the UE in downlink and uplink. Higher category = more bits allocated. UE data rate determines theoretical maximum download speeds. UE Cat 6 = 300 Mbps, UE Cat 1 = 10 Mbps. 3GPP introduced CA and MIMO to increase network capacity and provide higher bit rates. CA and MIMO boost bit rate, but use different methods: CA increases bandwidth, MIMO uses multi-antenna tech. To benefit, UE needs network support. Bands are radio frequencies used by the UE. Multiple band support is necessary for handovers and roaming across regions. Commercial UEs usually support various bands by region. Bands 3, 7, and 20 operate in Europe, while North America prefers bands 2, 4, and 12. VoLTE. LTE uses VoLTE for voice calls, which requires radio access capabilities such as RoHC, UM, SPS, and interval grouping. UEs without TTI cannot use VoLTE and must use circuit switched calling.

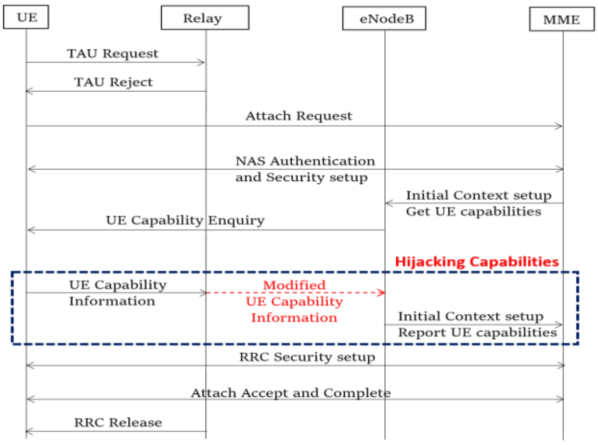
UE
Relay
eNodeB
MME
TAU Request
TAU Reject
Attach Request
NAS Authentication and Security setup
Initial Context setup Get UE capabilities
UE Capability Enquiry
Hijacking Capabilities
UE Capability Information
Modified UE Capability Information
Initial Context setup Report UE capabilities
RRC Security setup
Attach Accept and Complete
RRC Release

Fig. 3. MITM capability hijacking attack

6.2 Capability Hijacking

We MitM attack to capture UE's radio access during registration, altering iPhone 7's capability via carrier settings. Cat 12 device with Intel XMM7480 baseband boosts speeds to 600Mbps, supports CA, MIMO, and LTE bands. Refer to Figure 4 for the assault stream. TAC is changed to initiate the attack from a separate area than the iPhone 7. The TAU process is rejected by the relay with a message. To start a new registration process on iPhone 7, send an Attachment Request message after deleting the current security context and temporary identities. We deceive the network with a fabricated UE part to enable secure access setup and UE registration. Relay sends request to iPhone 7 for text response. UE capabilities modified upon receipt: changed to Cat 1, VoLTE mandatory, bands limited to active one. We send the altered UE capability message to the network for iPhone 7's security and registration. Then, we notify the network to release UE with RRC Release Notice. eNodeB shares modified capabilities with MME for future transactions without redoing UE capacity transaction. iPhone 7 gets slower speeds after attack, switches to 3G during calls due to no 4G support. UE loses services and high-speed data assigned to USIM plan.

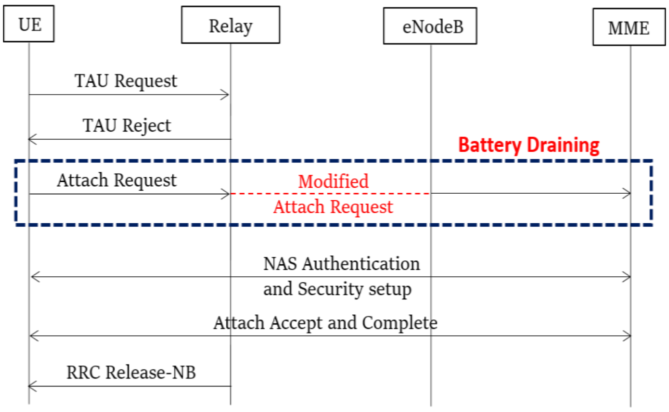

Fig. 4. MitM Control deplete assault devices

6.3 Experiments and Evaluation

Beneath ordinary conditions, the iPhone 7 download information rate (for the Tip top USIM arrange) is 27 Mbit/s. Agreeing to a speed test [22], the iPhone 7's information speed dropped to 3.7 Mbit/s during the attack. We tested it on two commercial networks and found that the top speed we got was 5 Mbps.

We repeated our tests in conjunction with other Gigabyte LTE Cat 16 devices capable of accelerating up to 1 Gbps, namely a Nighthawk M1 Mobile Router [4] and a Samsung Galaxy S8 phone, our tests have revealed that despite the theoretical download speeds of 1 Gbps supported by Cat 16 devices, actual speeds during low traffic hours are observed to be between 35-38 Mbps (after 9:00pm:00). However, following an attack, downstream speeds plummet to 2.9 Mbps, and during rush hour (10am:00), speeds are further reduced to 1 Mbit/s. Despite our test SIM card boasting high service quality and data rate, the bottleneck remains in the wireless layer. Consequently, an elite subscriber profile is rendered pointless if the UE radio is unable to support high speeds.

6.4 Feasibility and Impact

Possible shortened version: UE radio access without security setup allowed by some operators, leading to V2 vulnerability affecting 20 out of 30 carriers in 20 countries. UE radio access is crucial for RRC security, but it can make user services worse and enable MitM attacks. 10 networks implement RRC security to protect against MitM attacks during UE capability transactions. Messages are encrypted and registration capabilities are temporarily stored at the MME. Radio access is modified for UE data rates and services in this phase. Networks usually skip UE radio access in TAU procedures to conserve radio resources because of large message sizes (8188 bytes). During the trial, the network did not require radio access for a week due to the MME holding UE capabilities for several days. Additionally, some networks only need 3G for data transmission, resulting in prolonged LTE capability retention and potential impact on UE even if the attacker disrupts the relay. MitM reduces UE data rate, varying by type. Attack limits max rate, no minimum rate. Removing VoLTE may cause call rejection if UE or network lacks 2G/3G. UE will shift to 3G/2G if not compatible. Shortened: Shortening eras weakens UE, requiring reboots or re-registration after attacks. Report attacks via customer service or switch operators. V2V and industrial vehicles require low latency for good service, but UE loses access if it's disabled.

7. Device Power Drain

To begin with get it the control sparing highlights distinguished for IoT devices, then exploit V3 vulnerabilities During the NB-IoT and LTE-M UE registration process, a drain attack will then be performed to investigate the feasibility and associated impact issues.

7.1 Power Saving Function in LTE

3GPP shows baseband deactivation which stops radio, but apps/sensors can work according to device specs. The UE can request PSM by adding T3324 timer in Attachment or TAU Request message, which determines the duration of UE's dynamic state before entering PSM. UE monitors eNodeB channels for messages. PSM is only activated when the UE requests T3324 in attachment/TAU messages, it can only use PSM if the network has enabled T3324 IE on registration with a value other than "disabled". Responsibility for enabling or disabling PSM rests with both the UE and the network.

Expired T3412 will initiate TAU periodically for UE and extension T3412 can be used together with T3324 to save power. The UE prefers extension T3412 due to its longer idle time, which allows the transmitter in the PSM to remain operational for more than 10 years on 2 AA batteries.

7.2 Feasibility and Impact

LTE v12 vulnerability benefits low-power IoT devices. Manufacturers affected. Attack persists after relay shutdown until UE reaches T3412 or (T3412 ext.) timeout, with TAU timers measuring 10-15 days, contingent on SIM, app, and operator. LTE manufacturers with version 12 are vulnerable to attacks even after the relay is turned off. The attack continues until the UE T3412 or (T3412 ext.) timeout. TAU timers vary from 10-15 days depending on SIM subscription, IoT application, and operator setup. UE reconnects and re-registers safely. Timers T3324 and T3412 set at 30 seconds and 13 days. BC68 registers, enters PSM, and performs TAU every 13 days. After an attack, UE operates for 13 days with periodic TAU. Current usage rose because of network registration, BC68 doesn't have PSM and measures power from nearby cells. PSM saves power by turning off the baseband. NB-IoT devices can last 10+ years. on 5 Wh battery, says 3GPP. BC68 used 0 with PSM and drew 65mA for 64 days to fully utilize power. BC68 uses 3mA/5V, and lasts 333 hrs when hit, but battery life reduces by 5x with power-hungry attacks.

8. Discussion and Countermeasures

Table 1 lists vulnerabilities, attacks, and countermeasures. Here are 2 prevention methods for LTE and 5G network attacks. Our LTE-integrated solutions support 5G networks, safeguarding device capabilities. 3GPP should secure UE capabilities by limiting eNodeB access to the UE Capability Query message until RRC security is established to prevent MitM hijacking, which is difficult due to challenges in altering LTE standards. In phase two, the 5G vulnerability fix has been implemented, but attackers can still exploit it due to delays in baseband provider updates. Operators can update eNodeB settings to request UE capability info after RRC security is established. Limited access to security measures and testing variances may lead to implementation issues. Core network capabilities are accessible to anyone through plain text delivery. Attach req. Protected radio access relies on sensors and frequency. No sensors or messages were used in BC68 tests; all current was by baseband. Attacker can MNmap attack. Future work may include safeguards for core network capabilities. We ensure device capabilities and security algorithms for UE protection. our method is simplified for easy implementation. Security algorithms in the integrity-protected NAS secure-mode command message sent to the UE include timers and requested services for matching capabilities. Check UE capabilities to prevent attacks and downgrades and renegotiate if a mismatch is found. LTE v14 added network capability protection, but older versions like NB-IoT are still at risk. Radio problems will be fixed in 5G upgrades.

Table 1
Diagram of the attacks and vulnerabilities

Vulnerability	Problem in	Attack	Attack Mode	Impact	Mitigation
UE capabilities accessible without authentication (V1)	3GPP LTE protocols [15]	Mobile Network Mapping (MNmap)	Rogue eNodeB	Identification of devices (Model, OS)	Mandatory security protection for UE capabilities
UE radio capabilities	Operator’s eNodeB Configuration or	BiddingDown	MitM Relay	Decline of data rate,	

accessed before security setup (V2)	implementation		downgrade to 3G/2Gfor voice calls	
UE (NB-IoT) core capabilities not protected (V2)	3GPP LTE protocols [14]	Battery Draining	Excess power consumption on device	Core network capabilities mutually verified after NAS security setup

9. Conclusion

We have presented three vulnerabilities that exploit exposed UE capabilities on LTE networks and have evaluated them through an experimental setup. Our reference model has demonstrated the ability to determine the hardware and software characteristics of any mobile device. Furthermore, we have identified an LTE network configuration error among 20 service providers that resulted in multiple service downgrades and negatively impacted subscriber experience. Additionally, we have discussed battery-draining attacks on mobile IoT devices. We have also presented mitigations to prevent attacks and recommendations for the development of 5G phase 2. The impact of our findings has resulted in several operators reporting the deployment of vulnerabilities and taking remedial actions. Furthermore, the 3GPP SA3 body is considering adding protection to the UE.

Acknowledgement

This research was not funded by any grant.

References

[1] Yocam, Eric, Amjad Gawanmeh, Ahmad Alomari, and Wathiq Mansoor. "5G mobile networks: reviewing security control correctness for mischievous activity." *SN Applied Sciences* 4, no. 11 (2022): 304. https://doi.org/10.1007/s42452-022-05193-8

[2] Nair, Pramod. *Securing 5G and Evolving Architectures*. Addison-Wesley Professional, 2021.

[3] Rupprecht, David, Katharina Kohls, Thorsten Holz, and Christina Pöpper. "Breaking LTE on layer two." In *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 1121-1136. IEEE, 2019. https://doi.org/10.1109/SP.2019.00006

[4] Haataja, Keijo, and Pekka Toivanen. "Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures." *IEEE Transactions on Wireless communications* 9, no. 1 (2010): 384-392. https://doi.org/10.1109/TWC.2010.01.090935

[5] Haataja, Keijo MJ, and Konstantin Hypponen. "Man-in-the-middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures." In *2008 3rd International Symposium on Communications, Control and Signal Processing*, pp. 1096-1102. IEEE, 2008. https://doi.org/10.1109/ISCCSP.2008.4537388

[6] Kaltenberger, Florian, Aloizio P. Silva, Abhimanyu Gosain, Luhan Wang, and Tien-Thinh Nguyen. "OpenAirInterface: Democratizing innovation in the 5G Era." *Computer Networks* 176 (2020): 107284. https://doi.org/10.1016/j.comnet.2020.107284

[7] Yocam, Eric, Amjad Gawanmeh, Ahmad Alomari, and Wathiq Mansoor. "5G mobile networks: reviewing security control correctness for mischievous activity." *SN Applied Sciences* 4, no. 11 (2022): 304. https://doi.org/10.1007/s42452-022-05193-8

[8] Shaik, Altaf, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. "On the impact of rogue base stations in 4g/lte self organizing networks." In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pp. 75-86. 2018. https://doi.org/10.1145/3212480.3212497

[9] Miettinen, Markus, Samuel Marchal, Ibbad Hafeez, N. Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. "Iot sentinel: Automated device-type identification for security enforcement in iot." In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)*, pp. 2177-2184. IEEE, 2017. https://doi.org/10.1109/ICDCS.2017.283

[10] O'hanlon, Piers, Ravishankar Borgaonkar, and Lucca Hirschi. "Mobile subscriber wifi privacy." In *2017 IEEE Security and Privacy Workshops (SPW)*, pp. 169-178. IEEE, 2017. https://doi.org/10.1109/SPW.2017.14

[11] Connections the quarterly journal. “Semtech: AN1200.22 - LoRa Modulation Basics.” *Connections the quarterly journal*, (1970). https://connections-qj.org/article/semtech-an120022-lora-modulation-basics

[12] Shaik, Altaf, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. "Practical attacks against privacy and availability in 4G/LTE mobile communication systems." *arXiv preprint arXiv:1510.07563* (2015). https://doi.org/10.14722/ndss.2016.23236

[13] Sauter, Martin. *From GSM to LTE-advanced Pro and 5G: An introduction to mobile networks and mobile broadband*. John Wiley & Sons, 2017. https://doi.org/10.1002/9781119346913

[14] Watters, Paul, Nalin Asanka Gamagedara Arachchilage, David Maimon, and Richard Keith Wortley. "Cognition, Behavior and Cybersecurity." *Frontiers in Psychology* 12 (2021): 728132. https://doi.org/10.3389/fpsyg.2021.728132

[15] Yan, Zheng, Refik Molva, Wojciech Mazurczyk, and Raimo Kantola. "Network and system security." *Lecture Notes in Computer Science* (2017): 169-183. https://doi.org/10.1007/978-3-319-64701-2

[16] Akpakwu, Godfrey Anuga, Bruno J. Silva, Gerhard P. Hancke, and Adnan M. Abu-Mahfouz. "A survey on 5G networks for the Internet of Things: Communication technologies and challenges." *IEEE access* 6 (2017): 3619-3647. https://doi.org/10.1109/ACCESS.2017.2779844

[17] Yang, Xing, Lei Shu, Jianing Chen, Mohamed Amine Ferrag, Jun Wu, Edmond Nurellari, and Kai Huang. "A survey on smart agriculture: Development modes, technologies, and security and privacy challenges." *IEEE/CAA Journal of Automatica Sinica* 8, no. 2 (2021): 273-302. https://doi.org/10.1109/JAS.2020.1003536

[18] Brand, Ettus Research, a National Instruments. n.d. “USRP Software Defined Radio (SDR) Online Catalog.” *Ettus Research*. http://www.ettus.com/product/details

[19] Shaik, Altaf, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities." In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 221-231. 2019. https://doi.org/10.1145/3317549.3319728

[20] R.Borgaonkar, A.Shaik, N.Asokan, V.Niemi, J.P.Seifert. “LTE and IMSI catcher myths.” *Blackhat EU*. (2015). https://www.blackhat.com/docs/eu-15/materials/ eu-15-Borgaonkar-LTE-And-IMSI-Catcher-Myths.pdf

[21] Choung, Jae-Yong, Tahir Hameed, and Illyong Ji. "Role of formal standards in transition to the technology frontier: Korean ICT systems." *Telecommunications Policy* 35, no. 3 (2011): 269-287. https://doi.org/10.1016/j.telpol.2011.02.001

[22] Connections the quarterly journal. “Semtech AN120022 Lora Modulation Basics.” Connections the quarterly journal. (1970). https://connectionsqj.org/article/semtech-an120022-lora-modulation-basics