LTE Security Disabled—Misconfiguration in Commercial Networks

Merlin Chlosta
merlin.chlosta@rub.de
Ruhr University Bochum
Germany

David Rupprecht
david.rupprecht@rub.de
Ruhr University Bochum
Germany

Thorsten Holz
thorsten.holz@rub.de
Ruhr University Bochum
Germany

Christina Pöpper
christina.poepper@nyu.edu
NYU Abu Dhabi
United Arab Emirates

ABSTRACT

Long Term Evolution (LTE) is the de-facto standard for mobile communication. It provides effective security features but leaves room for misunderstandings in its configuration and implementation. In particular, providers face difficulties when maintaining network configurations.

In this paper, we analyze the security configuration of commercial LTE networks. We enhance the open baseband srsLTE with support for commercial networks and perform a subsequent analysis. In more detail, we test the security algorithm selection in a total of twelve LTE networks in five European countries. We expose four misconfigured networks and multiple cases of implementation issues. Three insecure networks fail to enforce integrity protection and encryption, which enables an adversary to impersonate victims towards the network. We provide a proof-of-concept attack in a live network, where the adversary obtains an IP address at the victim's cost. Our work is an appeal to security as a holistic state, which requires not only secure specifications but also secure configurations.

ACM Reference Format:
Merlin Chlosta, David Rupprecht, Thorsten Holz, and Christina Pöpper. 2019. LTE Security Disabled—Misconfiguration in Commercial Networks. In *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19), May 15–17, 2019, Miami, FL, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3317549.3324927

1 INTRODUCTION

LTE is the latest deployed mobile communication standard, offering high-speed, low-latency Internet access and packet-based telephony. It is used by millions of people worldwide and has become an integral component of our daily communication. The security goals of LTE aim to provide mutual authentication, integrity and confidentiality of traffic, and location privacy.

These security goals and their consideration in the specification evolved from the lessons learned of previous cellular generations. Flaws and resulting attack vectors of earlier generations can only be avoided in the specification of future generations. One central example is the first digital mobile generation GSM (2G) that is vulnerable to Man-in-the-Middle (MitM) attacks and passive decryption; LTE overcomes these flaws by employing mutual authentication and by using strong cryptographic algorithms. Hence, uncovering specification flaws in current mobile generations is a crucial accelerator for new, more secure standards.

However, overcoming well-known vulnerabilities in the specification does not guarantee a secure deployment. The specification defines mandatory security features, whereas their realization is up to the provider. For example, integrity protection might be disabled for emergency calls – but poses a security risk in any other scenario [2, Sec. 4.4.4]. This introduces a discrepancy between the assumed theoretical security (specification) and the actual situation (configuration). Commercial LTE networks are large-scale systems with a complex infrastructure for wide-area coverage. Configuration management is not standardized and often vendor-specific. We assume that this, if accompanied by human error, may result in configuration issues.

In this paper, we evaluate security-relevant parameters of commercial LTE networks and identify states of misconfiguration that disagree with the specified security aims. Using an active approach, we can modify the security parameters of the connecting phone and thereby test the acceptance by the network. So far, security configuration testing of LTE networks has only been explored with commercial basebands or passive approaches [9, 10] that do not allow the modification of parameters and thus are unsuitable for querying selected network settings. Recently, Kim et al. [15] extensively test user and network-side equipment with open source basebands but do not consider configuration issues. Rupprecht et al. [22] found flaws in the user-side selection of security algorithms.

We focus on the security algorithm selection of the network as an integral component of LTE security. One of the consequences of an incorrect configuration is that attackers could perform a MitM attack and impersonate users against the network. Due to dense roaming agreements between providers, misconfiguration has global implications. It is thus essential to ensure the deployment of secure configurations in current LTE and future (5G) mobile networks. In particular, we make the following contributions:

- We develop a low-cost LTE network testing tool to identify configuration flaws based on the open baseband srsLTE.
- We actively test the infrastructure-side security algorithm selection of twelve European commercial LTE networks.
- We identify four misconfigured networks and multiple cases of non-compliant behavior. Three networks are vulnerable to an *impersonation attack*, which we demonstrate.

We address operator networks with an alias composed by the country code and an index, e. g., DE-1 for the German operator we tested first. It does *not* refer to the Mobile Network Code (MNC).

WiSec '19, May 15–17, 2019, Miami, FL, USA

ACM ISBN 978-1-4503-6726-4/19/05…$15.00
https://doi.org/10.1145/3317549.3324927

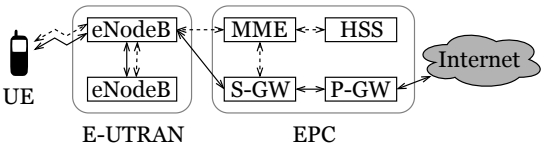

Figure 1: LTE Network Overview.

2 TECHNICAL BACKGROUND

We briefly review the LTE network architecture and relevant mobility procedures with a focus on security mechanisms. We only cover the components and procedures required for a basic connection setup, i. e., connecting and registering on the network.

2.1 LTE Network

The LTE network serves connectivity to the user devices, called User Equipment (UE). An operator's network is often called Public Land Mobile Network (PLMN), which also includes technologies other than LTE. Figure 1 shows a network overview.

User Equipment (UE). The UE is the user device, often a smartphone. It is associated with the permanent International Mobile Subscriber Identity (IMSI) and a permanent key stored on the Universal Subscriber Identity Module (USIM). The frequently changing Temporary Mobile Subscriber Identity (TMSI) replaces the IMSI after successful network registration for privacy reasons.

Evolved NodeB (eNodeB). eNodeBs provide radio access to the LTE network by spanning *cells* within the signal range. UEs usually select the eNodeB with the highest signal strength and quality. *Rogue cells*, which are operated by an attacker and not connected to the legitimate core network, thereby lure users into their cells. The Radio Access Network (RAN), or E-UTRAN in LTE, is the wide-area network of eNodeBs that provides wireless access.

Evolved Packet Core (EPC). Within LTE's backend *core* network, the Mobility Management Entity (MME) is central for user management. It provides mutual authentication to the UE, selects security algorithms, and keeps track of user locations. The Home Subscriber Server (HSS) stores user credentials, i. e., the IMSI and permanent keys. Gateways (S-GW and P-GW) route Internet traffic.

2.2 Procedures and Security

LTE separates the management of UE into the Access Stratum (AS) and Non-Access Stratum (NAS). The AS covers management on the radio layer between UE and eNodeB using the Radio Resource Control (RRC) protocol, while the NAS protocol handles the connection management between UEs and core network (MME). The following covers the interaction of both layers for basic connection establishment and the roaming scenario.

2.2.1 Attach Procedure & AKA. The UE must perform an initial attach procedure to access the LTE network, initiating all protocol layers from the radio layer up to IP. For our propose, we assume that the UE and the eNodeB already established a radio connection. Figure 2 depicts the *initial* attach procedure, which runs as follows.

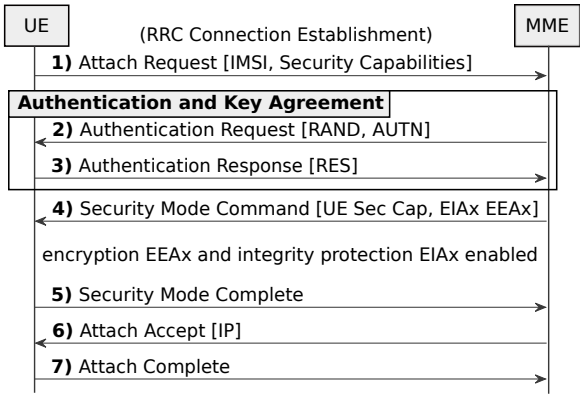

Figure 2: LTE Attach Procedure including the AKA.

The UE initially sends the Attach Request **(1)** with IMSI or TMSI for identification and the supported security algorithms (Security Capabilities). The following Authentication and Key Agreement (AKA) establishes mutual authentication. The MME sends an Authentication Request **(2)** containing a random nonce (RAND) and an authentication token (AUTN). The UE verifies the authentication token, computes and returns the response RES **(3)**, which is verified by the network. For enabling the security mechanisms, the network sends the already integrity protected Security Mode Command **(4)**, indicating the selected security algorithms and a replay of the original UE Security Capabilities to prevent algorithm downgrade attacks. The UE acknowledges with a Security Mode Complete **(5)**. The network finally assigns an IP address with Attach Accept **(6)**, which the UE confirms **(7)**.

2.2.2 Security Algorithms. LTE supports three algorithms for ciphering and integrity protection, referred to as EPS Encryption Algorithm (EEA) and EPS Integrity Algorithm (EIA). EIA1 and EEA1 use the Snow3G cipher, EIA2 and EEA2 rely on AES. Every UE, eNodeB and core network shall support Snow3G and AES. A later LTE release adds optional ZUC support (EIA3, EEA3). The *null*-algorithms EIA0 and EEA0 disable security, i.e., data is sent unprotected. This enables emergency calls without valid USIM and thereby without valid keys. During normal operation, integrity protection for the signaling plane is mandatory, whereas encryption is optional but encouraged [1]. Integrity protection is crucial to ensure the authenticity of exchanged messages. It continuously proves that both parties are in possession of valid keys. AS and NAS are not required to select the same algorithms.

2.2.3 Roaming. Roaming allows users to *visit* the PLMN of foreign operators (VPLMN) without having a USIM of that operator. Figure 3 visualizes the relation between the networks and the user. During the attach procedure, the VPLMN asks the user's Home PLMN (HPLMN) to provide credentials for the user, which requires cooperation between the operators [1, Sec. 6.1.2]. This procedure is interesting for security since the home operator authenticates the user, but the visited network is responsible for securing the connection to the user. The Home PLMN can by no means detect which security algorithms are enforced by the VPLMN.

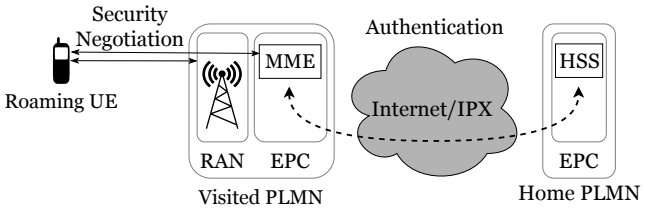

Figure 3: Authentication and Security Algorithm Negotiation in a Roaming Scenario. The UE is customer of the HPLMN.

3 SECURITY ALGORITHM SELECTION

We focus on the selection of security algorithms in the attach procedure as a fundamental element of LTE security that depends both on operator configuration and implementation support. The UE and network negotiate security algorithms during the attach procedure (see Section 2.2.1). If the UE requests unsupported algorithms, the network should deny access. Similarly, a standard-compliant UE terminates the connection if the network dictates insecure or unsupported algorithms. We implement a UE that requests insecure algorithms and does *not* terminate insecure connections—thus, it enables the detection of network-supported configurations.

We introduce the test implementation and the experiments conducted. Later, we present security issues found in four out of twelve tested networks and describe and perform an end-to-end attack on a commercial UE in a live network, in which the attacker obtains an IP address at the victim's cost. Furthermore, we show several cases of non-compliant network behavior, which indicates bugs in the eNodeB implementation.

3.1 Implementation

Our test setup builds upon the UE component srsUE of the open baseband srsLTE [8] with an Ettus B210 USRP and a USIM card reader. Prior to our work, the srsUE baseband could not access commercial networks, in particular, it did not feature encryption (AES, Snow3G) and could not read USIM cards. In collaboration with the srsLTE developers, both features were added to the project.

To test an operator's configuration, we perform the attach procedure for each possible set of supported algorithms (*Security Capabilities*) and observe the network's choice. In particular, we allow the UE to use the *null-encryption* and *null-integrity*. We expect two cases to emerge: (*i*) The network accepts the list of capabilities and signals the chosen algorithms in a Security Mode Command message, or (*ii*) the network denies access. To comply with the standards, the network must explicitly reject illegal or unsupported Security Capabilities with a NAS Attach Reject message. If the network accepts the configuration, we record the selected algorithms for AS and NAS. Regarding the srsLTE software, the supported algorithms are encoded as a bit array (8-bit) that can be arbitrarily manipulated.

For automated testing of networks, we created a slightly modified version of the srsUE. To establish unprotected connections to the LTE network, several protection mechanisms within the UE must be disabled. Therefore, the test setup does not check the Security Mode Command replay and does not verify the Message Authentication Code (MAC). Outgoing messages with EIA0 have the MAC set to zeros. For unknown indicated ciphers, we select EIA0 and EEA0.

At the application level, the srsUE iterates through all possible combinations of Security Capabilities and receives feedback from the lower layers (NAS, RRC) while the physical layer remains synchronized with the cell. In this way, we do not need to re-synchronize for a new test case and thus increase the speed of automated testing. For the evaluation PCAP traces and log files are written to disk.

3.2 Experiments

The experiment requires successful authentication to the network. Hence, we use several commercial USIM cards which usually belong to roaming partners of the network under test. Note that using roaming USIM cards does not affect the experiment since the serving network is responsible for the security algorithm selection [7].

We conducted tests for twelve networks in Austria, Czech Republic, Germany, Spain, and France over several months in 2018. Practical issues arise during the actual experiments, such as lack of mobile coverage in conference hotels, the need for a matching USIM card and *regional* differences due to varying eNodeB vendors (see the Results paragraph). Therefore, later experiments are conducted with a car and rooftop-mounted antennas.

3.3 Results

We observe different selection policies, e. g., regarding the ZUC support or preference of Snow3G or AES. In our analysis, we concentrate on the *non*-compliant behavior, first configuration issues and then bugs in the MME or eNodeB implementation. Table 1 shows security-relevant results for all operators. The checkmarks indicate the support of an algorithm.

The providers AT-1, CZ-1, DE-2, and ES-2 require particular attention since they allow *non-encrypted and non-integrity* protected signaling. This behavior is prohibited by the LTE standard, which requires NAS and RRC control-plane integrity protection [2, Sec. 4.4.4]. Section 4 presents the implications of this insecure configuration, including a proof-of-concept impersonation attack.

While testing the security algorithms field, we observe that several of the tested LTE networks show non-compliant behavior. Table 1 references the behavior by its number:

- **(1) Fallback to insecure configurations:** The network prohibits the use of EEA0 if requested explicitly. If the UE indicates that no cipher is supported at all, the network selects EEA0 by default, falling back to an insecure configuration.
- **(2) Illegal values for algorithm indication:** The network signals the unassigned spare value *EIA7* in place of EIA0. This violates the LTE standard and may prohibit detection of EIA0 support during a security assessment. We found this issue to differ regionally, i. e., we observed that base stations in one region all abide the standard, while base stations in other areas show this issue.
- **(3) Missing support for AES or Snow3G:** Networks must support both AES and Snow3G [2, Sec. 5.1.3.2]. Some tested networks fail to accept Snow3G or AES on either AS or NAS.

Table 1: Acceptance of Null-Algorithms in LTE Networks

Result		Network											
		AT-1	AT-2	CZ-1	CZ-2	CZ-3	DE-1	DE-2	DE-3	ES-1	ES-2	ES-3	FR-1
EEA0	AS	✓	–	✓	–	✓	–	✓	–	✓	✓	✓	–
	NAS	✓	–	–	–	✓	–	✓	–	✓	✓	–	–
EIA0	AS	✓	–	✓	–	–	–	✓	–	–	✓	–	–
	NAS	✓	–	✓	–	–	–	✓	–	–	✓	–	–
Bugs		1		1, 2								3	

– / ✓: algorithm not allowed / algorithm allowed
Detected bugs, see Section 3.3 for details
Red highlights vulnerable configurations (impersonation attack)

While the use of insecure security algorithms indicates a misconfiguration, the non-compliant behavior, e. g., the use of spare-bits, means a faulty implementation at the network components.

4 IMPERSONATION ATTACK

Mutual authentication between the network and the UE relies on the AKA *and* subsequent integrity protection of control data. If a network allows null-integrity along with null-encryption, it exposes users to impersonation attacks.

Scenario. A commercial network allows null-integrity and null-encryption for normal operation. The victim UE belongs to that network *or any roaming partner of the affected, insecure operator.*

Attacker Model. The adversary uses a UE component and an eNodeB component for a MitM attack. She impersonates the commercial network towards the victim UE and the victim UE towards the network. Note that the adversary does not possess any information about the victim UE, especially neither IMSI nor cryptographic keys. She can lure the UE to connect to her cell with similar techniques that commercially IMSI catchers implement (e.g., UE usually select the eNodeB with the highest signal strength and quality, or cells on priority frequencies). The attacker does not have to target a specific UE if her goal is only to obtain an IP address without authorization, which results in billing fraud [21].

Attack Procedure. In LTE, the attach procedure including the AKA is not secured by any transport security mechanism and can be intercepted and manipulated by a MitM attacker. If the network selects the null algorithms, the attacker does not require valid keys to communicate with the network. Thus she can impersonate the benign UE. The attacker enforces the selection of null algorithms due to the misconfiguration we observed. Figure 4 depicts the attack procedure, and the steps are as follows:

(1) The benign UE connects to the attacker and sends an Attach Request, containing the IMSI and Security Capabilities. **(2)** The attacker forwards the Attach Request but modifies the supported algorithms to EIA0 and EEA0 only. **(3)** The commercial network starts the AKA with an Authentication Request containing the challenge and network authentication (RAND and AUTN). **(4)** The attacker forwards the Authentication Request to the victim UE. **(5)** The AUTN authenticates the commercial network; thus, the UE generates the Authentication Response RES. **(6)** The attacker forwards the Authentication Response to the network and thereby authenticates herself to the commercial network. **(7)** The attacker

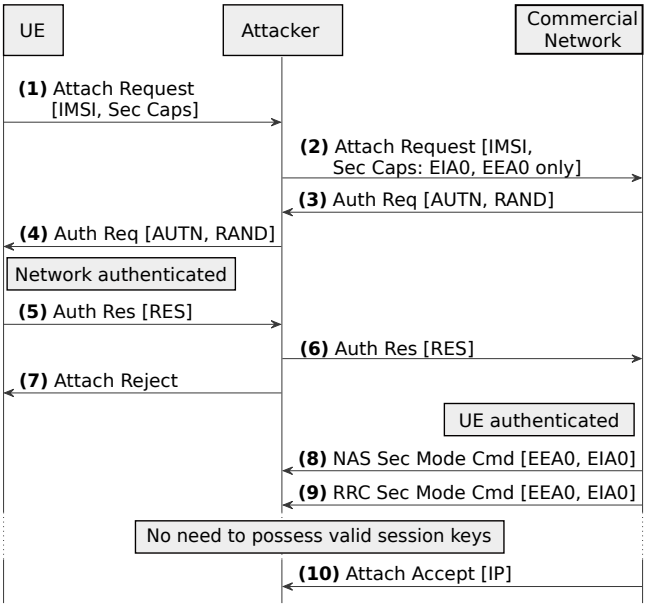

Figure 4: Impersonation attack exploiting the selection of EIA0 and EEA0 in a commercial network.

rejects the UE's attach request with a permanent reject reason, prohibiting it from re-attaching to the network until restart [24]. **(8-9)** Based on the modified Security Capabilities, the network selects EIA0 and EEA0 on the RRC and NAS layer for further communication. Therefore, the communication does not require possession of valid keys. Attacker and network exchange user and control data in plaintext, without any integrity protection and encryption. **(10)** The network finally accepts the Attach Request and assigns an IP connection to the attacker. The attacker is now able to use the LTE network for data services, while the connection is associated with the victim's identity (IMSI).

Note that in case the UE connects with Attach Request but identifies with TMSI, the attacker requests the IMSI with an Identity Request. If the UE connects with Service Request or Tracking Area Update, the attacker denies access with reason Implicitly Detached, forcing the UE to re-attach with Attach Request [2, Sec. 5.5.3.3.5].

Implementation Details. We implement the impersonation attack using the srsLTE stack [8] with separate UE and eNodeB components and a simple communication protocol in-between using sockets to exchange the victim's IMSI and the authentication data. The attacker's eNodeB and the victim UE are located in a shielding box to prevent attacks on other users.

While both attacker components run on the same computer during the experiment, the components can be separated to run on two separate setups, communicating over the Internet. Internet communication introduces a delay that could interfere with the timers that the attach procedure and AKA depend on. To test the viability of separated attacker components, we add an additional delay between the attacker UE and eNodeB component (see Figure 5), i. e., between steps (1) and (2), (3) and (4), and between (6) and (7) in Figure 4.

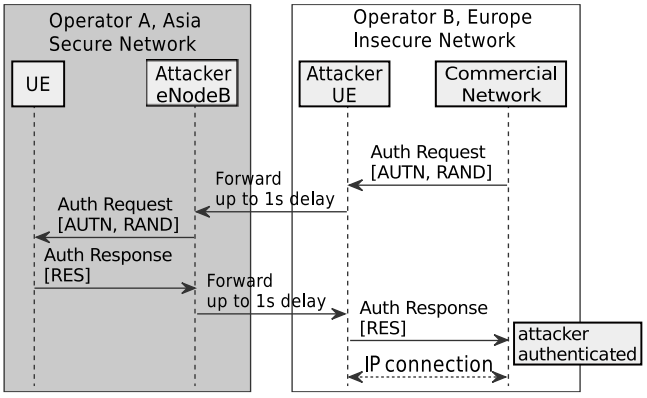

Figure 5: Impersonation attack in roaming context.

Proof of Concept in Live Network. We perform the attack in the commercial DE-2 network and a commercial UE as a victim, equipped with a standard DE-2 USIM card. After running the above procedure, the attacker UE successfully establishes an IP connection over the LTE network and can surf the Internet, while the commercial UE is denied access.

For delays up to one second between each step in the communication between the attacker UE and eNodeB component (i. e., three seconds additional delay in total), we can successfully and reliably establish the IP connection for the attacker. This implies that both attacker components can be in different locations, communicating over the Internet. In the discussion, we further go into the implications of global roaming cooperations.

5 DISCUSSION

We expose severe misconfigurations in four of the twelve tested networks accompanied by implementation bugs of eNodeBs. In the following, we discuss the global impact of misconfigured networks, directions for future work, and ethical considerations of our work.

Global Impact. Even operators with secure configurations are affected by their roaming partners because the *serving network* is responsible for the choice of security algorithms. This requires two attacker components, an eNodeB component in the vicinity of the victim and another UE component in the vulnerable network. In this way, an adversary can steal the authentication vector from users that reside within the secure network, relay the authentication procedure over the Internet, and inject it into the insecure network of the roaming partner (cf. Figure 5).

The protocol allows margins of multiple seconds between the authentication messages [2, Table 10.2.2], while we empirically confirmed delays of up to one second. This is enough time to forward messages around the world and conduct the attack globally. Given the density of roaming agreements, we assume that already a few vulnerable operators pose a threat to users *worldwide*. Each of the examined networks has more than 200 cooperating LTE networks, visible through public lists [19]. We expect that detection and mitigation of impersonation attacks become more challenging in this scenario since all roaming partners of one network operator must deploy a secure configuration to prevent attacks.

Future Work. Focusing on the selection of security algorithms serves as one example of detecting insecure configurations. While we found misconfigured networks in regard of the selection of security algorithms, plenty of other security-relevant parameters are configurable by the network provider, e. g., re-authentication at inter-generation (LTE to GSM) or eNodeB handovers, or the use of packet data passwords (APN settings). Failing to configure these parameters correctly opens up new attack vectors and amplifies existing ones. In the future, further tests can be quickly implemented for a comprehensive security assessment of networks.

5G Deployment. Similar to LTE, some of the upcoming 5G security features are up to the provider's configuration. The fundamental problems of the current generation are continuing in 5G. The persistent discrepancy between the specified and the configured security, therefore, requires a different approach. Our proposed security testing extends the providers' toolset and improves the resilience of the deployment process. We argue that only active testing can overcome the prevalent discrepancy in current and future networks. 5G brings up new security features, e. g., IMSI encryption, that only fulfill their purpose given a flawless configuration.

Ethical Considerations. Testing in commercial networks requires special care since it must not interfere with normal operations. We took several precautions to avoid negative side-effects. Our system relies on standard-compliant messaging and procedures only, which any commercial UE must use to obtain network access. Prior to testing in commercial networks, we performed tests in an operator's laboratory, observing network-side logfiles and PCAP traces of base stations and the MME. Thereby we verify that our equipment abides the LTE standard and shows no unexpected behavior. The test purely probes for the network configuration with the method designated by the standard. This is independent of the equipment of the operator, thus we consider it safe to perform tests in other networks in this particular case. Experiments involving attacks on our smartphones took place in a shielding box to prevent any interference.

Responsible Disclosure. Before submission, we have contacted all affected providers and the GSM Association (GSMA) security group to resolve the issue, following the guidelines of responsible disclosure. All vulnerable networks now utilize a secure configuration. The process of finding the reasons for the non-compliant network behavior is on-going and left to the responsible parties. This resulted in change requests to the LTE and 5G standards, clarifying the handling of null-integrity [3, 4].

6 RELATED WORK

Providers can configure the frequent reallocation of temporary identifiers and hinder de-anonymization attacks. Hong et al. [9, 10] evaluated such configuration by using a non-modifiable baseband. In contrast to their work, we can actively modify the content of messages. Li et al. [16] and Kim et al. [14] perform active configuration testing in VoLTE networks, which allow a hidden channel for free data transmission. While their work focuses on the IP layer above LTE, we focus on the LTE specific layers.

Various studies have assessed the security of mobile stack implementations. Security testing of the protocol state machines discovered that faulty implementations could result in the acceptance

of forbidden security algorithms [18, 22]. The latter is most similar to our work, testing the acceptance of forbidden security algorithms on the UE-side, while we focus on the network side. Recently, Kim et al. [15] presented a systematical approach for detecting implementation flaws, leading to 36 vulnerabilities in phones and network components. Our work focuses on the configuration of live networks and show that operators fail to configure the network securely. Their AKA bypass attack abuses insecure UE implementations to eavesdrop on the user, while our attacker obtains an IP address from the network at the victim's cost.

Our impersonation attack uses a rogue base station to steal a valid authentication token. Shaik et al. [24] demonstrated that a rogue base station could locate victims or deny network access. Localization attacks are improved by side-channels based on paging injection [5, 12]. Hussain et al. [11] presented a systematic approach for finding LTE specification flaws that can be exploited by a rogue base station. Users can be steered to rogue base stations by jamming attacks [13, 17]. While prior rogue base stations focused on localization or downgrades, we used them for the impersonation attack. Recently, Rupprecht et al. [23] demonstrated a transparent layer-two relay to manipulate DNS requests and redirect users to malicious websites. In contrast, we impersonate users towards the network by relaying NAS messages. Prior research focused on rogue base station detection, that could detect the eNodeB component of MitM attacker [6, 20].

7 CONCLUSION

The LTE specification overcomes the flaws of previous generations with new security measures. Unfortunately, the specification leaves room for misunderstandings in the implementation and configuration. This leads us to a situation in which the erroneous configuration of providers easily compromises the *claimed* security.

We analyzed the configuration of twelve commercial LTE networks concerning the security algorithm selection, and we found severe configuration issues. Those issues allow an impersonation attack in three networks. We implemented the impersonation attack as a proof-of-concept and demonstrated that an attacker obtains an IP connection associated with the victim's identity. Such a misconfiguration has global implications due to the density of roaming agreements. Our findings motivate ongoing and permanent security testing of deployed and future mobile generations. Our contributions support providers in the secure deployment and configurations of mobile networks.

8 ACKNOWLEDGEMENT

We thank all anonymous reviewers for their helpful comments, and the team of Software Radio Systems for their LTE software. This work was supported by the German Federal Ministry of Education and Research with the SysKit project (FKZ: 16KIS0664) and the BERCOM project (FKZ: 13N13741).

REFERENCES

[1] 3GPP. 2011. *3GPP System Architecture Evolution (SAE); Security architecture.* TS 33.401. http://www.3gpp.org/ftp/Specs/html-info/33401.htm

[2] 3GPP. 2011. *Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3.* TS 24.301. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/ftp/Specs/html-info/24301.htm

[3] 3GPP. 2019. C1-191700 - Handling when the UE indicated security capabilities are invalid or unacceptable. https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionUid=C1-191700. [Online; accessed April 8, 2019].

[4] 3GPP. 2019. C1-191702, - Handling when the UE indicated security capabilities are invalid or unacceptable. https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionUid=C1-191702. [Online; accessed April 8, 2019].

[5] Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Kévin Redon, and Ravishankar Borgaonkar. 2012. New Privacy Issues in Mobile Telephony: Fix and Verification. In *ACM Conference on Computer and Communications Security (CCS)*.

[6] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. 2014. IMSI-Catch Me If You Can: IMSI-Catcher-Catchers. In *ACM Annual Computer Security Applications Conference (ACSAC)*.

[7] Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller, and Valtteri Niemi. 2012. *LTE Security.* John Wiley & Sons.

[8] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D. Sutton, Pablo Serrano, Cristina Cano, and Doug J. Leith. 2016. srsLTE: An Open-source Platform for LTE Evolution and Experimentation. In *Wireless Network Testbeds, Experimental Evaluation, and Characterization (WiNTECH)*. ACM.

[9] Byeongdo Hong, Sangwook Bae, and Yongdae Kim. 2018. GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier. In *Symposium on Network and Distributed System Security (NDSS)*. ISOC.

[10] B. Hong, S. Park, H. Kim, D. Kim, H. Hong, H. Choi, J. P. Seifert, S. J. Lee, and Y. Kim. 2018. Peeking over the Cellular Walled Gardens - A Method for Closed Network Diagnosis. *IEEE Transactions on Mobile Computing* (2018).

[11] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In *Symposium on Network and Distributed System Security (NDSS)*. ISOC.

[12] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. 2019. Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. In *Symposium on Network and Distributed System Security (NDSS)*. ISOC.

[13] Roger Piqueras Jover. 2013. Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions. In *Symposium on Wireless Personal Multimedia Communications (WPMC)*. IEEE.

[14] Hongil Kim, Dongkwan Kim, Minhee Kwon, Hyungseok Han, Yeongjin Jang, Dongsu Han, Taesoo Kim, and Yongdae Kim. 2015. Breaking and Fixing VoLTE : Exploiting Hidden Data Channels and Misimplementations. In *ACM Conference on Computer and Communications Security (CCS)*.

[15] Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim. 2018. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. In *IEEE Symposium on Security & Privacy (SP)*. IEEE.

[16] Chi-Yu Li, Guan-Hua Tu, Songwu Lu, Xinbing Wang, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu, and Xinbing Wang. 2015. Insecurity of Voice Solution VoLTE in LTE Mobile Networks. In *ACM Conference on Computer and Communications Security (CCS)*.

[17] Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, and Jeffrey H. Reed. 2016. LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation. *IEEE Communications Magazine* 54, 4 (2016).

[18] Benoit Michau and Christophe Devine. 2016. How to not Break LTE Crypto. In *ANSSI Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*.

[19] Mobile World Live. 2018. GSM Roaming and Coverage Maps. https://maps.mobileworldlive.com/. [Online; accessed April 8, 2019].

[20] Peter Ney, Ian Smith, Gabriel Cadamuro, and Tadayoshi Kohno. 2017. SeaGlass: Enabling City-wide IMSI-Catcher Detection. In *Privacy Enhancing Technologies (PETS)*. De Gruyter Open.

[21] David Rupprecht, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, and Christina Pöpper. 2018. On Security Research towards Future Mobile Network Generations. *IEEE Communications Surveys & Tutorials* (2018).

[22] David Rupprecht, Kai Jansen, and Christina Pöpper. 2016. Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness. In *Workshop on Offensive Technologies (WOOT)*. USENIX Association.

[23] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2019. Breaking LTE on Layer Two. In *IEEE Symposium on Security & Privacy (SP)*.

[24] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2016. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. In *Symposium on Network and Distributed System Security (NDSS)*. ISOC.