IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 17, 2019, accepted February 5, 2019, date of publication February 13, 2019, date of current version March 7, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2899254

Security and Protocol Exploit Analysis of the 5G Specifications

ROGER PIQUERAS JOVER[1], (Senior Member, IEEE), AND VUK MAROJEVIC[2], (Senior Member, IEEE)

[1]Bloomberg LP, New York, NY 10022, USA
[2]Department of Electrical and Computer Engineering, Mississippi State University, Starkville, MS 39762, USA

Corresponding author: Roger Piqueras Jover (rpiquerasjov@bloomberg.net)

ABSTRACT The third generation partnership project released its first 5G security specifications in March 2018. This paper reviews the proposed security architecture and its main requirements and procedures and evaluates them in the context of known and new protocol exploits. Although security has been improved from previous generations, our analysis identifies potentially unrealistic 5G system assumptions and protocol edge cases that can render 5G communication systems vulnerable to adversarial attacks. For example, null encryption and null authentication are still supported and can be used in valid system configurations. With no clear proposal to tackle pre-authentication message-based exploits, mobile devices continue to implicitly trust any serving network, which may or may not enforce a number of optional security features, or which may not be legitimate. Moreover, several critical security and key management functions are considered beyond the scope of the specifications. The comparison with known 4G long-term evolution protocol exploits reveals that the 5G security specifications, as of Release 15, Version 1.0.0, do not fully address the user privacy and network availability challenges.

INDEX TERMS Security, 5G, 3GPP Release 15, LTE, protocol exploit.

I. INTRODUCTION

The Third Generation Partnership Project (3GPP) published its fifteenth release of the mobile communication system specifications in March 2018, setting the foundations for the 5th generation of mobile communications (5G). With groundbreaking upgrades at the radio layer, the New Radio (NR) standard implements an advanced physical layer that supports millimeter wave communications and antenna arrays for massive multiple-input, multiple-output (MIMO) antenna systems [1]. In parallel, the 5G core network (5GC) has been redesigned for enhanced flexibility and service versatility. The goal of 5G networks is to provide ubiquitous, high-speed, and low-latency connectivity for enhanced mobile broadband, massive machine type communication and real-time control. 5G will enable the tactile Internet, untethered augmented and virtual reality, smart and connected vehicles and new types of connectivity [2], [3].

As with its preceding generations–2G, 3G and the 4G Long Term Evolution (LTE)–, security is of capital importance for 5G networks and services. Cellular communication networks provide connectivity to billions of civilians worldwide. They are also the connectivity cornerstone for current and emerging critical infrastructure, supporting the smart grid, first responder units, and advanced military operations [4]. The advent of 5G will enable new verticals in the civilian, industrial and mission-critical domains [3].

Motivated by the inherent security weaknesses of legacy 2G networks, such as the lack of mutual authentication between the network and the user equipment (UE), security has been one of the key design considerations for mobile communications starting with 3G. LTE implements strong encryption and integrity protection algorithms, backed by a mutual authentication using symmetric keys that are securely stored in the Universal Subscriber Identification Module (USIM) and the operator's Home Subscriber Server (HSS) [5]. Nevertheless, a series of vulnerabilities inherent to the LTE protocol still exist and have been identified by researchers over the last few years. For example, a substantial number of pre-authentication messages are sent in the clear, which can be exploited to launch Denial of Service (DoS) attacks and obtain location information of mobile subscribers [6]–[8].

The first release of the LTE specifications, 3GPP Release 8, was published in 2007. The main security vulnerabilities were not identified and reported in open literature until much later though. One of the reasons for this was the lack of available and affordable tools for LTE security research.

The associate editor coordinating the review of this manuscript and approving it for publication was Mugen Peng.

LTE open-source software libraries running on personal computers and using commercial off-the-shelf software-defined radio (SDR) peripherals did not reach a sufficient level of maturity until recent years. Once they became available, a wave of excellent security research in the area of LTE mobile communications emerged and identified numerous protocol vulnerabilities [6], [8]–[11].

As in LTE, security is a key consideration and core aspect for the definition and specification of 5G systems. Since the inception of the communication protocols for 5G Systems (5G-S), there has been a substantial effort in addressing known LTE protocol exploits with particular focus on preventing International Mobile Subscriber Identifier (IMSI) catchers or Stingrays [12]. As a result, 5G introduces the Subscription Permanent Identifier (SUPI), as replacement of the IMSI, and a Public Key Infrastructure (PKI), which allows the encryption of the SUPI into the Subscription Concealed Identifier (SUCI) [13].

Preventing protocol exploits that leverage pre-authentication messages was also a key security design goal for 5G [14]. Nevertheless, and despite the efforts to design a secure architecture, a number of insecure protocol edge cases still exists. Moreover, there is no clear solution yet to prevent the implicit trust of pre-authentication messages, which can be exploited by an adversary to both deny the service to subscribers as well as intercept sensitive user information [8].

If the PKI architecture that is used to conceal the SUPI is also intended to prevent other pre-authentication message-based protocol exploits, full security against such exploits can only be achieved if all USIMs in all mobile devices had the public keys of all operators in the world. In addition, all operators would need to keep the corresponding private keys well secured. Not only is such key management and rotation unfeasible and, as of Release 15, left outside the 3GPP specifications, but political and operator disagreements would most likely result in the lack of global adoption. Insecure protocol implementation and exploitation of pre-authentication messages could be the consequences.

This paper provides a wide-angle analysis of the 5G radio access network (RAN) security architecture and procedures and its potential deployment challenges as a result of the proposed 5G security framework. Specifically, this paper provides a general security analysis of the security specifications described in 3GPP TS 33.501 [13]. The underlying requirements and assumptions for 5G security are identified and analyzed holistically, with specific focus on global adoption and the resulting consequences. The objective of this paper is not to provide a comprehensive analysis of the security of 5G network layers and elements, but rather to assess the critical challenges of the current 5G security specifications with an outlook at future network deployments. Analyzing the security of specific 5G technologies and system architectures, such as the Cloud-RAN, is out of the scope of this paper.

The remainder of this paper is organized as follows. Section II provides an overview of the 5G security architecture and components, setting the context for Section III, which discusses the main 5G security requirements and procedures of the 3GPP Release 15 specifications. Section IV provides a holistic analysis of the deployment challenges of the proposed 5G security framework, highlighting the potential risk of protocol exploits and sensitive information leaks. The 5G security framework is then analyzed in terms of the known LTE protocol exploits in Section V. Section VI summarizes our findings and proposes research directions to address the identified security vulnerabilities.

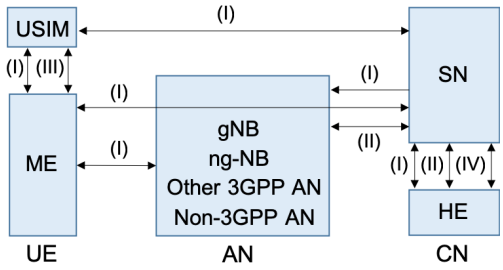

FIGURE 1. 5G security architecture.

II. OVERVIEW OF THE 5G SECURITY ARCHITECTURE

The 5G security architecture spans across the UE, radio access network, core network and application [13]. The architecture is correspondingly organized into an application stratum, a serving stratum, and a transport stratum. Figure 1 shows a simplified diagram of the serving stratum and the transport stratum. Different security features are defined across the network and end user components, which combined create a secure system design:

- Network access security (I): A set of features and mechanisms that enable a UE to authenticate and securely access network services. UEs therefore exchange protocol messages through the access network with the serving network (SN) and leverage the PKI, where keys are stored in the USIM and the home environment (HE).
- Network domain security (II): A set of features and mechanisms that enable network nodes to securely exchange control plane and user plane data within 3GPP networks and across networks.
- User domain security (III): A set of features and mechanisms at the UE that secure the access to mobile equipment and mobile services. It establishes hardware security mechanisms to prevent the mobile terminals and USIMs from being altered.
- Service-Based Architecture (SBA) domain security (IV): A set of network features and mechanisms for network element registration, discovery and authorization, as well as for protecting the service-based interfaces. It allows new 5GC functions, which may be implemented as virtual network functions, to be securely integrated. It also enables secure roaming, which involves the SN as well as the home network (HN)/HE.

- Visibility and configurability of security (not shown in Fig. 1): A set of features and mechanisms that allow informing users whether a security feature is in operation. It can also be used to configure security features. The 3GPP security specifications for 5G formally establish optional security features and degrees of freedom for secure network implementation and operation. This means that 5G users will likely encounter different security context.

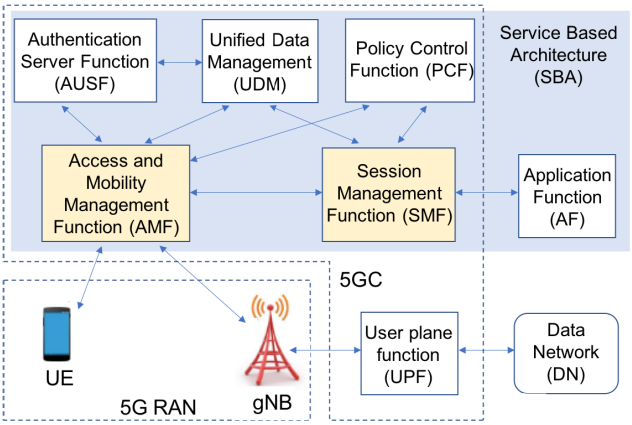

FIGURE 2. Simplified 5G reference network architecture.

The 5G specifications define a number of network functions and their interfaces, enabling the data flow between the 5G RAN, 5GC, and external networks. Figure 2 illustrates the simplified 5G reference network architecture. The network functions and security features specify a flexible, yet secure design for developing 5G mobile communication systems.

III. 5G SECURITY REQUIREMENTS AND PROCEDURES

The 5G security framework defines a series of security requirements, features and procedures [13], which we summarize in continuation. Table 1 captures the core security requirements and the corresponding procedures for the 5G RAN. This table highlights, in italics, some of the requirements and procedures that can lead to security vulnerabilities. These vulnerabilities and their potential implications are analyzed in subsequent sections.

A. KEY FRAMEWORK

The 5G security procedures leverage a hierarchical key derivation, distribution, and management framework. Keys are stored in a number of network entities. The long term key K is stored by the Authentication Credential Repository and Processing Function (ARPF) of the Unified Data Management (UDM) layer and the USIM holds the user corresponding copy of that symmetric key. All other keys are derived from it. The key generation and distribution is detailed in [13].

B. AUTHENTICATION AND HOME CONTROL

3GPP establishes the Extensible Authentication Protocol for Authentication and Key Agreement (EAP-AKA) and 5G AKA as the authentication methods that must be supported by the UEs and the network and are used for mutual authentication and subsequent service security and encryption procedures. A 5G UE sends the SUCI in its registration requests to initiate the authentication process using the method it selects. 5G AKA enhances the AKA protocol of 4G LTE [5] by providing the HN with proof of successful authentication of the UE from the visited network.

C. SECURITY CONTEXTS

The 5G security specifications define a number of security contexts for different scenarios: a single 5G SN, across multiple SNs, and between 5G and 4G networks. When a UE is registered with two SNs, both networks must independently maintain and use a separate security context. When the UE is registered to two SNs in the same public land mobile network (PLMN), 3GPP and non-3GPP, the UE establishes two independent Non-Access Stratum (NAS) plane connections with those networks, but uses a common NAS security context consisting of a single set of keys and security algorithms.

D. STATE TRANSITION AND MOBILITY

Procedures for maintaining or disregarding a security context during state transition and handover are also defined, to some extent, in [13]. The specifications state that it is up to the operator's policy how to configure the selection of handover types. This decision is a function of the operator's security requirements, thus leaving the security during handovers as an opt-in feature instead of enforcing it through the standard. As a consequence, an operator could potentially implement an insecure handover procedure.

E. NON-ACCESS STRATUM

Cryptographic separation and replay protection of two active NAS connections is supported through a common NAS security context, which has parameters that are specific to each NAS connection. NAS uses 128-bit ciphering algorithms for integrity and confidentiality protection. However note that null encryption and null integrity protection are both supported. Moreover, if the UE has no NAS security context, the initial NAS message is sent in the clear and contains the subscription identifier and UE security capabilities, among others.

F. RADIO RESOURCE CONTROL

The Radio Resource Control (RRC) integrity and confidentiality protection is provided by the packet data convergence protocol (PDCP) layer between the UE and gNB and no layers below PDCP shall be integrity protected. Replay protection is to be activated when integrity protection is activated, except when the null integrity protection is selected. RRC integrity checks are performed both at the UE and the gNB. In the case where a failed integrity check is detected after the start of the integrity protection, the corresponding message are to be discarded.

G. USER PLANE

The Session Management Function (SMF) provides the user plane security policy for a protocol data unit (PDU) session to

TABLE 1. 5G RAN security requirements and procedures (security domain association according to Fig. 1).

Scope	Security requirements	Procedures
General (I)	• Mitigation of bidding down attacks. • Mutual authentication. • UE, access and serving network authorization. • *Allowance for unauthenticated emergency services.*	Authentication procedures using EAP-AKA and 5G AKA authentication methods.
UE and gNB (I)	• User and signaling data confidentiality protection through cyphering. *gNB triggered, considering UE security capabilities and SN's list of security capabilities. Null encryption supported. Confidentiality protection optional to use.* • User and signaling data integrity and replay protection. gNB triggered, *considering UE security capabilities and SN's list of security capabilities. Null integrity protection supported. Integrity protection of user data optional to use.* RRC and NAS signaling protection mandatory, *but exceptions exists, including unauthenticated emergency sessions.*	Key derivation, distribution and agreements from a key hierarchy, supporting 128 bit key and 256 bit key encryption. For every key in a network entity, there is a corresponding key in the UE, with the root key stored in the USIM.
UE (III)	• Secure storage and processing of subscription credentials using a tamper resistant secure hardware component. • Subscriber privacy through use of temporary and concealed subscriber identities (5G-GUTI and SUCI). • *If provisioned by the home operator, the USIM shall store the HN public key used for concealing the SUPI.*	*Null-scheme supported and shall be used when public key not provisioned by HN, which controls subscriber privacy and the provisioning and updating of keys.*
gNB (I), (II)	• Authorized setup and configuration by O&M through certificates, the use of which is optional. • Key management, *optional for the 5G PKI-based architecture*. • Secure environments for keys, user plane and control plane data storage and processing.	*Authentication and key derivation may be initiated by the network as often as the operator decides when an active NAS connection exists.*

the gNB during the PDU session establishment. If user plane integrity protection is not activated for data radio bearers (DRBs), the gNB and the UE will not integrity protect the traffic of such DRB. If user plane ciphering is not activated for DRBs, the gNB and the UE will not cipher the traffic of such DRBs. The local SMF can override the confidentiality option in the user plane security policy received from the SMF of the HN.

H. SUBSCRIPTION ID PRIVACY

The SUCI is the concealed version of the 5G permanent subscription identifier SUPI. The SUCI is transmitted over the air to prevent exposing the user identity in the clear. It is constructed from the SUPI using the operator's public key and a probabilistic asymmetric encryption method to prevent identity tracking. However, the SUPI null protection scheme is used for unauthenticated emergency sessions, when so configured by the HN, or when the operator public key has not been provisioned.

The 5G specifications also define a temporary identifier, the 5G Globally Unique Temporary Identifier (5G-GUTI), to minimize the exposure of the SUPI or SUCI. The 5G-GUTI is to be reassigned based on UE triggers, but it is left to the network implementation to determine the rate of such reassignment.

IV. POTENTIAL VULNERABILITIES OF 5G–SECURITY CHALLENGES AND OPPORTUNITIES

As introduced in Sections II and III, 5G mobile networks implement a security architecture similar to that of LTE systems, with a small differences in how trust and security are established. Pre-5G communication systems base all security functions on symmetric keys that are securely stored both in the USIM and the HSS. Based on the shared secret key k_s, an LTE UE can authenticate the network and the network can authenticate the UE. The encryption and integrity protecting keys are derived from k_s [5]. This symmetric key security architecture results in the inability of a communication endpoint, the UE, to verify the authenticity and validity of any message that is exchanged *prior to* the *NAS Attach* cryptographic handshake. The need for pre-authentication messages to be sent in the clear is widely acknowledged as the root cause of many known LTE protocol exploits [7], [8], [15].

For any communication protocol, including 5G, independently of how strong a security architecture is and how

TABLE 2. Summary of 5G security and implementation challenges of 3GPP Release 15.

Security/ implementation challenge	Root cause	Impact
PKI infrastructure	Considered out of scope of the 3GPP specifications	Implementation specific, potential for not being implemented
Key management (rotation, over-the-air provisioning, etc.)	Considered out of scope of the 3GPP specifications	Implementation specific, potential for not being implemented
Global cooperation	Security against pre-authentication message exploits guaranteed only if USIM contains a public key for every operator worldwide	With just one operator or country being non compliant, system security and user privacy can be compromised through rogue base stations and spoofed pre-authentication messages
Support for NULL encryption and NULL integrity	Requirements from standards stake holders and lawful interception working group	Potential for bidding down attacks and rogue base stations, especially if no public key provisioned for the operator

sophisticated its cryptographic algorithms are, it only takes one single edge case or insecure function to defeat the entire system. For example, although in LTE the IMSI should only be sent in the clear the very first time a mobile phone is switched on, there is a number of legitimate and explicitly defined use cases in which the network can request that the UE identifies itself using its IMSI. Clear guidance through standardization and its enforcement are therefore required and are the basis for global compliance. Security functions and procedures that are left out of the scope of the protocol specifications can result in insecure edge cases. Therefore, critical security features and mechanisms cannot be optional and all operators need to opt-in for implementing these and implement them rigorously.

A. PRE-AUTHENTICATION MESSAGE EXPLOITS

The goal of the 5G security architecture is to tackle the challenge of pre-authentication messages and other protocol exploits [14]. By introducing the concept of operator public keys, 5G systems provide the tools for establishing a root of trust between the end user and the mobile operator under the umbrella of the 5G PKI. Leveraging the public keys burned into USIMs, operators can securely receive encrypted messages from the UEs as well as sign messages with their corresponding secret key to be validated by the UEs.

This PKI is the method that is proposed to protect against Stingrays. However, there is no clear solution in the specifications on how to achieve such level of security against all protocol exploits leveraging 5G pre-authentication messages. The specifications fall short of a comprehensive PKI architecture that leverages digital certificates and a Certificate Authority (CA) to tackle the 5G security challenge. Moreover, although SUPI catching is substantially more challenging than IMSI catching, there is still a number of valid protocol edge cases in which the SUPI is transmitted in the clear [13]. Therefore, a rogue 5G base station could potentially trick a UE into disclosing its SUPI.

It is worth noting that there is no method to prevent a rogue base station from instructing a UE to disclose its SUPI leveraging a spoofed pre-authentication message. But, the SUPI would be transmitted encrypted in the form of the SUCI. Similarly, no security method protects a UE from implicitly trusting pre-authentication messages.

In order to avoid pre-authentication message exploits using the current 5G PKI proposal, global compliance would be necessary. That is, in order to verify the validity of all pre-authentication messages in all connectivity scenarios, including roaming, each UE would require a cryptographic root of trust for any network it may connect to. This is so because network originating messages, such as *AttachReject* and *TAU-Reject*, known for their LTE protocol exploits [7], [8], could originate from the visiting network.

A potential solution against 5G pre-authentication message exploits would also require loading the public key of every operator in every country, without exception, into all USIMs. It is anticipated that some countries will ban the public keys from certain other countries or operators, something that has been observed before [16].

In general, protocol exploits like the ones disclosed in [8], [11], and [17] are, as of Release 15, Version 1.0.0, still possible in 5G.

B. OTHER SECURITY CHALLENGES

The proposed security architecture and procedures are considered fundamental for securing emerging 5G mobile networks. Increased home control, for example, is considered useful for preventing certain types of frauds. The proposed 5G security framework supports implementing such procedures, but they are considered beyond the scope of the specifications: *the actions taken by the home network to link authentication confirmation (or the lack thereof) to subsequent procedures are subject to operator policy and are not standardized* [13].

Our initial analysis already highlights a number of remaining security weaknesses that need to be addressed. Table 2 identifies the core 5G security challenges, their root causes and potential impacts. The 3GPP specifications leave out most implementation details that are critical for security, such as the key management of operator public keys residing in the subscribers' USIMs, the structure of certificates and how or whether keys are ever rotated [13]. It is left in the hands of the industry to figure those details out.

Prior experience has shown that rapid roll out and affordable service delivery require simple protocol solutions, which oftentimes compromise security [18]. In addition, lawful interception requirements mandate continuing support for null encryption and null integrity protection, which results in insecure modes of communication and protocol edge cases.

In addition to the aforementioned issues, researchers are already finding weaknesses in the cryptographic operations defined in [13]. Basin *et al.* [19] use formal verification tools to analyze the 5G AKA algorithms and demonstrate that the protocol fails in meeting several security goals, which are explicitly required. The same study shows that the 5G protocol lacks other critical security properties. Other analyses [20]–[22] derive similar conclusions and describe potential downgrade attacks against 5G networks.

C. PKI-BASED ARCHITECTURE ALTERNATIVE

The move towards a PKI-based architecture in 5G is a step in the right direction. PKI systems provide a wider flexibility for sophisticated security solutions that could potentially tackle the challenge of pre-authentication messages, among others. However, such a critical element of the 5G system architecture should not be left outside of the specifications.

Global agreement and adoption of a large scale PKI architecture is necessary for fully addressing the security challenges in 5G in the long term. However, instead of basing the system on public keys burned into the USIM, an improved architecture would include a global 5G Certificate
Authority (CA). The CA would act as the root of trust to authenticate messages and communication peers using digital certificates [23]. Embracing such an authority would provide a more flexible architecture. The corresponding certificate revocation and management challenges have already been addressed and the solutions vetted by the secure Internet implementation community [24].

Similar proposals about the potential of PKI-based architectures applied to mobile communication systems have been discussed for over a decade now [25]. It is also an important element of the European 5G Infrastructure Public Private Partnership (5G PPP) [26].

V. IMPACT OF LTE PROTOCOL EXPLOITS ON 5G

The LTE security architecture was designed to address the challenges of previous generations. The first generation of mobile networks (1G) lacked support for encryption and this was one of the main drivers for introducing 2G digital mobile communications. Legacy 2G networks do not support mutual authentication and use an encryption algorithm that is outdated [27]. LTE implements specific functionalities to guarantee the confidentiality and authenticity of mobile networks and messages, using much stronger cryptographic algorithms and explicit mutual authentication between the UE and the eNodeB. This makes 4G LTE inherently more secure than prior generations, yet still vulnerable to certain exploits.

A. LTE PROTOCOL EXPLOITS

The existence of LTE protocol vulnerabilities has been known for some time, although these have not been publicly discussed until recently. The openness of the standard, the large community of researchers, and the broad availability of SDRs, software libraries and open-source implementations of both the eNodeB and the UE protocol stacks have enabled a number of important LTE security analyses [6], [10], [11], [29], [30]. Despite the stronger cryptographic algorithms and mutual authentication, UEs and eNodeBs exchange a substantial amount of pre-authentication messages that can be exploited to launch DoS attacks [7], [15], [31], catch IMSIs [32] or downgrade the connection to an insecure GSM link [8], [11]. Researchers also found new privacy and location leaks in LTE [17].

The LTE specifications have a number of vulnerable protocol edge cases that, despite being rarely executed, are still supported by the standard. For example, although it is very unlikely that a UE would ever transmit an *Attach Request* message using its IMSI as the identifier, the protocol describes specific scenarios in which this would occur. For example, during network recovery after the core network lost the UE's temporary identifier. In this case, the network can trigger the mobile device to retransmit the *Attach Request* message with its IMSI in the clear [33].

In a nutshell, most active LTE protocol exploits occur because of a combination of the protocol supporting insecure edge cases and the implicit trust of pre-authentication messages [7]. The first two columns of Table 3 summarize some of the most relevant LTE protocol exploits that have been identified in open literature.

B. IMPACT ON 5G NETWORKS

Most of the known LTE protocol security vulnerabilities were studied and dissected by the security working group of 3GPP [14] with the aim of defining a secure 5G standard. As a result of that study, specific security goals for 5G mobile networks were set to address the problems of IMSI catchers, pre-authentication messages and location leaks. Device and user tracking by leveraging the Radio Network Temporary Identifier (RNTI) [17] was, on the other hand, disregarded in the 3GPP study because RNTIs are claimed to be short lived identifiers that cannot be leveraged for privacy leaks. Recent research, however, confirmed that the RNTI can be used to track subscribers [6].

As discussed in this paper, despite being highly sophisticated and robust against many adversarial attacks, the 5G security framework still includes a number of edge cases that facilitate bypassing all security functions. In particular, most of the demonstrated LTE protocol exploits are not fully addressed and are still a potential threat, as outlined in the third column of Table 3.

TABLE 3. Major LTE protocol exploits and their impact on 5G.

LTE protocol exploit	Threat	Impact on 5G
IMSI catching	Privacy threat, location leaks, SS7 leaks, etc. [7], [8], [11], [28]	Potential for IMSI/SUPI catching in some protocol edge cases, such as when an operator does not implement optional security features or when an unauthenticated emergency call is maliciously triggered.
Attach/ Tracking Area Update (TAU) request	DoS [7], [8], [11]	DoS of 5G mobile devices exploiting pre-authentication messages with rogue base station broadcasting a valid Mobile Country and Network Code (MCC-MNC) combination for network with no public key provisioned in the USIM.
Silent downgrade to GSM	Man in the middle attacks, phone call and SMS snooping [7], [8], [11]	Silent downgrade to GSM exploiting pre-authentication messages with rogue base station broadcasting an MCC-MNC of a network with no public key provisioned in the USIM.
Location tracking with RNTI	Location leaks, traffic estimation, service estimation [6]	Potential device location traffic and traffic profiling
Insufficient protection of DNS traffic at layer 2	DNS hijacking over LTE [6]	Man in the middle attacks, credential stealing, remote malware deployment.

Above findings put pressure on 5G. Unlike in the case of LTE, where most security research and resulting protocol weaknesses were identified after the protocol was defined, implemented and globally deployed, the security research community is moving fast with 5G. Weaknesses in the 5G specifications are being identified as the specifications are released [19].

Note that most deployed LTE networks still rely on many early 3GPP Release 8 or 9 features. This underlines that once deployed, after years of standardization, certification and testing, major network upgrades can take considerable time to be widely implemented. Since security cannot be considered as an add-on feature, the advantage of providing early awareness of potential security issues is that these can be pragmatically analyzed, fixed, and the specifications revised during the initial roll outs and before mass commercial deployments of networks, UEs, and services. It is of critical importance that the lessons learned from LTE are applied now to design a 5G system architecture that is fully resilient to protocol exploits. Any potential 5G security problem should therefore be addressed in the current Release 15 and not be pushed off to future releases.

VI. CONCLUSIONS

Wireless communication security has always been of critical importance and will be more so as technology evolves towards 5G. Traditionally used mostly for non-critical voice communication, many of the current and emerging data and control communication systems that leverage cellular access networks have stringent requirements in terms of integrity and privacy of user data. Applications include tactical communication, first responder ad-hoc networks, and mission-critical Internet of Things.

This paper provides the first holistic analysis of the first release of the 5G security specifications [13]. Our study highlights a number of potential insecure protocol edge cases and limitations that result from infeasible requirements or assumptions. Despite clearly targeting to address the known security vulnerabilities of LTE networks, the 5G specifications are, as of Release 15, Version 1.0.0, still vulnerable to the same types of LTE adversarial attacks that leverage pre-authentication messages.

Global adoption and enforcement of a robust security framework is necessary to avoid having to support insecure operational modes and rely on implicit trust of pre-authentication messages. It is therefore critical to ensure that no insecure edge cases are supported by the 5G standard. In particular, null authentication, null encryption, downgrade attacks, exploitation of pre-authentication messages, and SUPI catching shall not be facilitated in any mode of 5G network operation. The success of such a security framework should not be subject to implicit assumptions or implementation options neither.

While the 5G security architecture made a substantial leap in the right direction with the proposed PKI architecture, security research and development is still necessary to fully address the known and new security vulnerabilities of next generation mobile communication systems. Standardization bodies, researchers, regulators, and industry all need to work together to accomplish a securer architecture, design, development and deployment of emerging and future mobile communication and control systems. Global cooperation and collaboration, led by the standardization bodies, is necessary to define and implement the required system architecture and CA that would provide the foundation for secure 5G systems.

Security research should also pivot towards new technologies being discussed in the context of 5G. For example, the security of the 5G RAN and the variety of proposed architectures are important fundamental elements of 5G networks that should be designed with security in mind from ground up.

REFERENCES

[1] A. L. Swindlehurst, E. Ayanoglu, P. Heydari, and F. Capolino, "Millimeter-wave massive MIMO: The next wireless revolution?" *IEEE Commun. Mag.*, vol. 52, no. 9, pp. 56–62, Sep. 2014.

[2] "DOCOMO 5G white paper, 5G radio access: Requirements, concept and technologies," NTT DOCOMO, Tokyo, Japan, White Paper, Jul. 2014.
[3] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 74–80, Feb. 2014.
[4] A. Thompson. (2012). Army Examines Feasibility of Integrating 4G LTE With Tactical Network. The Official Homepage of the United States Army. [Online]. Available: http://goo.gl/F60YNA
[5] *Technical Specification Group Services and System Aspects*, document 3GPP TS 33.401, V14.5.0, System Architecture Evolution-Security Architecture, Jan. 2018
[6] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking LTE on layer two," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019.
[7] R. P. Jover and V. Marojevic, "Security and protocol exploit analysis of the 5G specifications," *CoRR*, vol. abs/1809.06925, 2018. [Online]. Available: http://arxiv.org/abs/1809.06925
[8] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *Proc. 23rd Annu. Netw. Distrib. System Security Symp. (NDSS)*, 2016.
[9] R. P. Jover. (May 2016). *The Impact of Open Source on Mobile Security Research*. [Online]. Available: https://goo.gl/hi4ukn
[10] R. M. Rao, S. Ha, V. Marojevic, and J. H. Reed, "LTE PHY layer vulnerability analysis and testing using open-source SDR tools," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Baltimore, MD, USA, Oct. 2017, pp. 744–749. doi: 10.1109/MILCOM.2017.8170787.
[11] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A systematic approach for adversarial testing of 4G LTE," in *Proc. Symp. Netw. Distrib. Syst. Secur. (NDSS)*, Feb. 2018, pp. 18–21.
[12] D. Strobel, "IMSI catcher," in *Chair for Communication Security*. Bochum, Germany: Ruhr-Univ. Bochum, 2007, p. 14.
[13] *Security Architecture and Procedures for 5G System*, document 3GPP TS 33.501, V1.0.0, Technical Specification Group Services and System Aspects, Mar. 2018.
[14] *Study on the Security Aspects of the Next Generation System (Release 14)*, document 3GPP TR 33.899 V1.3.0, Aug. 2017.
[15] M. Labib, V. Marojevic, J. H. Reed, and A. I. Zaghloul, "Enhancing the robustness of LTE systems: Analysis and evolution of the cell selection process," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 208–215, Feb. 2017.
[16] (May 2018). *Pentagon Orders Stores on Military Bases to Remove Huawei, ZTE Phones The Wall Street Journal*. [Online]. Available: https://goo.gl/ciySYB
[17] R. P. Jover, "LTE security and protocol exploits," Shmoocon, Tech. Rep., Jan. 2016.
[18] M. Labib, V. Marojevic, J. H. Reed, and A. I. Zaghloul, "Extending LTE into the unlicensed spectrum: Technical analysis of the proposed variants," *IEEE Commun. Standards Mag.*, vol. 1, no. 4, pp. 31–39, Dec. 2017. doi: 10.1109/MCOMSTD.2017.1700040.
[19] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler. (Jun. 2018). "A formal analysis of 5G authentication." [Online]. Available: https://arxiv.org/abs/1806.10360
[20] M. Dehnel-Wild and C. Cremers, "Security vulnerability in 5G-AKA draft," Dept. Comput. Sci., Univ. Oxford, Oxford, U.K., Tech. Rep, 2018.
[21] A. Koutsos. (2018). "The 5G-AKA authentication protocol privacy." [Online]. Available: https://arxiv.org/abs/1811.06922
[22] M. Khan, P. Ginzboorg, K. Järvinen, and V. Niemi. (2018). "Defeating the downgrade attack on identity privacy in 5G." [Online]. Available: https://arxiv.org/abs/1811.02293
[23] R. Housley, W. Ford, W. Polk, and D. Solo, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, document RFC 2459, 1998.
[24] A. Freier, P. Karlton, and P. Kocher, *The Secure Sockets Layer (SSL) Protocol Version 3.0*, document RFC 6101, 2011.
[25] G. Kambourakis, A. Rouskas, and S. Gritzalis, "Performance evaluation of public key-based authentication in future mobile communication systems," *EURASIP J. Wireless Commun. Netw.*, vol. 2004, no. 1, pp. 184–197, Aug. 2004. doi: 10.1155/S1687147204403016.
[26] P. Bisson and J. Waryet, "5GPPP phase 1 security landscape," 5GPP, Eur. Commission Eur. ICT Industry (ICT Manuf., Telecommun. Oper., Service Providers, SMEs Res. Inst.), White Paper, 2017.
[27] K. Nohl and S. Munaut, "Wideband GSM sniffing," in *Proc. 27th Chaos Commun. Congr.*, Dec. 2010. [Online]. Available: http://goo.gl/wT5tz
[28] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J. P. Seifert, "LTE and IMSI catcher myths," in *Proc. BlackHat Eur.*, 2015.
[29] V. Marojevic, R. M. Rao, S. Ha, and J. Reed, "Performance analysis of a mission-critical portable LTE system in targeted RF interference," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Toronto, ON, Canada, Sep. 2017, pp. 1–6. doi: 10.1109/VTCFall.2017.8288187.
[30] M. Labib, V. Marojevic, J. H. Reed, and A. I. Zaghloul, "How to enhance the immunity of LTE systems against RF spoofing," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Kauai, HI, USA, Feb. 2016, pp. 1–5.
[31] M. Labib, V. Marojevic, and J. H. Reed, "Analyzing and enhancing the resilience of LTE/LTE-A systems to RF spoofing," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Tokyo, Japan, Oct. 2015, pp. 315–320.
[32] K. Norrman, M. Näslund, and E. Dubrova, "Protecting imsi and user privacy in 5G networks," in *Proc. 9th EAI Int. Conf. Mobile Multimedia Commun.*, 2016, pp. 159–166.
[33] *Non-Access-Stratum (NAS) Protocol for Evolved Packet System (EPS)—Stage 3*, document 3GPP TS 24.301, V9.11.0, UMTS-LTE, 2013.

ROGER PIQUERAS JOVER (M'05–SM'17) received the Dipl.Ing. degree from the Polytechnic University of Catalunya, Barcelona, Spain, the master's degree in electrical and computer engineering from the University of California at Irvine, and the Master's/M.Phil. degree and EBD (Everything But Dissertation) in electrical engineering from Columbia University.

He spent five years at the AT&T Security Research Center, where he led the efforts on wireless and LTE mobile network security, receiving numerous awards for his work. He is currently a Senior Security Architect with the CTO Security Architecture Team, Bloomberg LP, where he is a Technical Leader in mobile security architecture and strategy, corporate network security architecture, wireless security analysis and design, and data science applied to network anomaly detection. He has been actively involved in the field of wireless and mobile network security for the last ten years, and he was one of the first researchers to identify and analyze LTE protocol exploits back, in 2015. As a Subject Matter Expert in the security of LTE/5G mobile networks and wireless short-range networks, he is a Technology Adviser and a Leader on these areas for academia, industry, and government. In his spare time, he is actively involved in identifying, implementing, and proposing solutions to rogue base stations and protocol exploits against LTE and 5G cellular networks and security research in other wireless technologies, such as Bluetooth, LoRa, 802.11, and ZigBee. He holds over 20 patents in mobile/wireless security, anomaly detection, and fraud detection. He has co-authored manuscripts and presented at numerous top security conferences and journals. His research interests are in the areas of mobile and wireless network security and machine learning applied to intrusion detection.

VUK MAROJEVIC (SM'18) received the M.S. degree in electrical engineering from the University of Hannover, Germany, and the Ph.D. degree in electrical engineering from UPC. He was with the Wireless @ Virginia Tech, since 2013, where he developed various cognitive radio and LTE testbeds and conducted several wireless protocol measurement campaigns. He led Virginia Tech's LTE vulnerability analysis research and proposed several ways to harden LTE. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Mississippi State University. His pioneering work on LTE control channel spoofing was picked up by industry and made it into 3GPP Release 13. His research interests are in software-defined radio, spectrum sharing, 4G/5G cellular technology, and resource management with application to public safety and mission-critical networks and unmanned aircraft systems.