




Research Article

5G mobile networks: reviewing security control correctness for mischievous activity

Eric Yocam¹ · Amjad Gawanmeh²  · Ahmad Alomari³ · Wathiq Mansoor²

Received: 1 May 2022 / Accepted: 4 October 2022

Published online: 17 October 2022

© The Author(s) 2022 

Abstract

A mobile telecommunications network has arguably become a vital part of today's critical communications infrastructure underpinning society's interconnectedness. A mobile telecommunications network can be considered a critical communications infrastructure that has been built upon a complex set of network technologies. However, the migration in recent years from pre-5G to 5G network technologies has presented the mobile telecommunications network operators with not only several security-related challenges but also potential unfortunate risk exposure. A new approach called Control-Risk-Correctness (CRC) addresses the need for evaluating a complex mix of network technology and the associated trade-offs between security and risk. CRC simplifies the analysis by examining the mobile telecommunications network from the perspective of security control effectiveness and risk treatments. This article outlines the application of CRC when assessing a mobile telecommunication network and highlights direct risk mitigation treatments in an aim to increase security control effectiveness and decrease risk exposure. CRC usefulness will assist in the evaluation of existing networks and safeguarding new networks over the coming years.

Article highlights

- Propose Control-Risk-Correctness (CRC) method for mobile telecommunications networks.
- Use CRC for simplified risk analysis in mobile networks and apply it on various trust boundaries.
- Identify elevated risk rating for trust boundaries.

Keywords Fake cell tower · Threat modeling · Risk control correctness · Simplified risk rating

1 Introduction

Mobile wireless networks have always been prone to several security challenges. Starting with the first generation, cell phones and communication channels were easy targets for several security attacks, such as illegal cloning and masquerading. In the second generation, net types of attacks such as message spamming were very common,

particularly for marketing and broadcasting false information. With the evolvement of 3G, several Internet-based attacks were migrated to wireless networks. Eventually, when 4G dominated the market, the increased mobile traffic as well the emergence of several new types of services, such as live streaming and interactive gaming, posed several new security and privacy challenges [1].

✉ Amjad Gawanmeh, amjad.gawanmeh@ieee.org; Eric Yocam, eric.yocam@trojans.dsu.edu; Ahmad Alomari, ahmad.alomari.1@ens.etsmtl.ca; Wathiq Mansoor, wmansoor@ud.ac.ae | ¹Department of Computer and Cyber Sciences, The Beacom College, Dakota State University, Madison, SD, USA. ²Electrical Engineering Department, College of Engineering and IT, University of Dubai, Dubai, UAE. ³Department of Software Engineering and Information Technology, Ecole de Technologie Supérieure (ETS), Montreal, Canada.



Among all the threats, the fake cell tower is a very common security vulnerability that existed in all network generations that support data communications [2]. It is also known by many other names, including stingray, International Mobile Subscriber Identity (IMSI) catcher, cell site simulator, man-in-the-middle base station, fake base station, and false base station.

The fake cell tower threat has existed since the second-generation cellular network (2G) as well as continued to persist with the evolution of mobile networks. The use of a fake cell tower by an adversary has led to mischievous activity that can compromise the security control correctness of a U.S. Carrier's mobile network. There are many known threats and vulnerabilities with existing 2G radios found within mobile devices and mobile network equipment used within mobile network ecosystems around the world [3].

Even with the existing 3G/4G, remnants of legacy 2G radios and infrastructure equipment exist within U.S. Carrier's mobile network. Many of these might be inherited into the more recent 5G advanced technology as well. Though many U.S. Carriers have shut down (or begun to move away from) legacy 2G within mobile network ecosystems, user devices (or user equipment) still have 2G radio capabilities that are more than willing to attach to a fake cell tower. Along with the legacy 2G, the adversary can pursue mischievous activities with various attacks, including (1) downgrade attacks (from 3G/4G/5G), (2) denial of service attacks, and (3) exposure to device/identity tracking attacks used by adversaries [4]. To address mischievous activity, using performance indicators or signatures can increase security control correctness and conversely decreases the potential of risk exposure through risk mitigation [5]. Correspondingly, this work will use the identification, classification, predictions, and prevention signatures to address the adversary's ability to pursue mischievous activities with various attacks.

There have been several research works conducted on 5G security control. The work in [6] presented a review of new security risks as well as challenges faced by new infrastructures. The authors proposed a risk prevention and control model for monitoring and warning. An agile security risk-aware edge server mechanism for 5G was discussed in [7]. In addition, several 5G security risks have been exposed and discussed in recent literature [8]. For instance, Hypervisors, which are commonly used in 5G infrastructure [9], have common vulnerabilities exposure [10, 11]. The work in [12] presented an overview of the 5G new security requirements compared to 4G, and then defined possible threats using the STRIDE [13] threat classification model, which is based on Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service and Elevation of privileges

(STRIDE). Authors used the model to estimate the likelihood and impact of several threat scenarios. In addition, there are several recent surveys that discussed the importance of security and risk analysis in 5G network [14–16]. Other recent interesting works addressed some security concerns in 5G serve based architecture [17], handover [18], air interfaces [19], security metrics [20], and Intrusion Detection Systems [21].

In this paper, a novel approach for control risk correctness in 5G networks is proposed. The objective of the method is to evaluate the trade-offs between security and risk in 5G network based on several control correctness measure. The proposed method simplifies the analysis by examining the mobile telecommunications network from the perspective of security control effectiveness and risk treatments. In addition, the work identifies how the proposed method can be deployed during the assessment of a mobile telecommunication network. Finally, the proposed architecture can also outline the direct risk mitigation treatments in an aim to increase security control effectiveness and decrease risk exposure. A comparison with existing risk evaluation methods and proposed risk evaluation method is provided as well as contributions highlighted within this paper.

The rest of this paper is organized as follows. The second section presents background on 5G mobile networks security requirements. The third section explains the risk measurement concept in 5G and pre-5G networks. Forth section presents pre-5G signature-based processing. The fifth section introduces the 5G security control correctness method. The following section presents the risk rating methodology. Finally, the conclusion section ends the paper.

2 Background

In this section, we discuss the background information necessary to understand the paper. First, we introduce the meaning of control risk correctness and why is it necessary in 5G era. Next, we introduce the trust boundaries concept. In the following subsection, threat modeling in the context of 5G risk assessment is explained. Threat attack vectors are discussed.

2.1 Control-risk-correctness

A combination of defining trust boundaries, applying threat modeling, and performing a novel approach called Control-Risk-Correctness simplifies the analysis, especially when evaluating the security control correctness for mischievous activity occurring within the 5G mobile network ecosystem. The intuition behind the

conceptual relationship with the Control-Risk-Correctness approach is that an inverse relationship between control correctness “correctness” level and risk level may exist, whereby the higher the control correctness “correctness” level, the lower the risk level.

The Control-Risk-Correctness methodology was used to simplify the analysis performed and translate findings into suggested risk remediation recommendations necessary to treat elevated risk. The use of this methodology frames trust boundaries identifies security controls, evaluates threats with threat modeling, translates potential risks, and compares risk level trade-offs with the security control correctness (see Fig. 1).

2.2 Trust boundaries

The user’s device trust boundary consists of firmware, baseband processor, operating processes, and antenna. The subscriber identity trust boundary consists of the human user, operating system processes, and universal integrated circuit card (UICC). The air interface consists of the antenna. The core network consists of a cell tower, base station, gateway, signaling system number 7 (SS7) interface, diameter interface, and web application APIs for storage signal processing. The U.S. Carrier’s mobile network business trust boundary consists of the U.S. Carrier’s mobile network business applications (e.g., metering, billing) used in conjunction with the U.S. Carrier’s mobile network ecosystem [22].

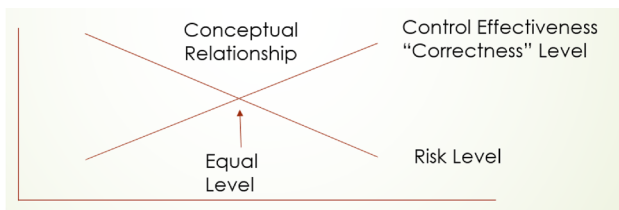


Fig. 1 Control-risk-correctness

2.3 Threat modeling and trust boundaries

Threat modeling is a valuable means to identify, categorize, and prioritize threats in order to evaluate threats representing these threats in terms of simplified risk ratings [23]. The STRIDE threat model is adopted in this work among many available threat models. The acronym STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The use of the STRIDE threat model classifies threats [24].

The trust boundaries (previously mentioned) are used along with the STRIDE threat modeling. The trust boundaries include user device (or user equipment), subscriber identity, air interface, core mobile network, and U.S. Carrier’s mobile network business. The STRIDE threat model identifies threat categories within each of these trust boundaries to assist in structuring the threat analysis applied to a U.S. Carrier’s mobile network ecosystem.

STRIDE classifications align with the Open System Interconnection (OSI) security architecture defined in ITU Telecommunication Standardization Sector (ITU-T) X.800 standard [25]. The STRIDE threat category relates to a security service within the OSI security architecture. Spoofing threat relates to authentication service. Tampering threat relates to integrity service. Repudiation threat relates to non-repudiation service. Information disclosure threat relates to confidentiality service. Denial of service threat relates to availability service. Elevation of a privilege threat relates to authorization service.

2.4 Threat attack vectors

The threat attack vectors include signal jamming downgrade, emergency 911 denial of service, spoofed wireless emergency alerts, SS7/Diameter, and device/identity tracking as shown in Table 1. First, the signal jamming downgrade attack forces the user’s device to downgrade from 5G/4G/3G to 2G taking advantage of existing 2G security and control weaknesses that allow call and data interception [26]. Second, the emergency 911 denial of service attack floods the mobile connection by sending unauthenticated ‘attach reject’ messages that render the emergency 911 inaccessible. Third, the spoofed WEA message enables an adversary (or attacker) to prevent emergency calls

Table 1 Threat attack VECTORS

Threat attack type	Threat attack vector
Signal jamming downgrade attack	Potential for call and data interception
E911 denial of service attack	Sending unauthenticated attach reject messages
Spoofed WEA message	Preventing emergency calls
Signaling System No. 7 (SS7)/diameter attack	Sending unauthenticated attach reject messages
Device/identify tracking	Successfully correlation of a device and an individual

from occurring. Forth, the SS7/Diameter interface attack is another type of denial-of-service attack that sends unauthenticated attach reject messages to render the SS7/Diameter interfaces unavailable. Finally, the device/identity tracking attack can allow an adversary to successfully correlate (and associate) a particular user's device with a subscriber, thereby breaching the subscriber's geolocation privacy [27].

3 Risk measurement in 5G and pre-5G

This section presents security analysis for identification, classification, prediction, and protection that enables a cell tower to be declared as legitimate versus a non-legitimate or fake cell tower. Likewise, the detection of a potential fake cell tower indicator type can be divided into two risk types, including cell tower misconfigurations and inconsistencies in control messages, as illustrated in Table 2.

In addition, the two risk types can have both impact and likelihood ratings associated with each of them to characterize the amount of risk present. The level of risk mitigation includes (1) full ability for risk mitigation, (2) partial ability for risk mitigation, and (3) minimal ability for risk mitigation. A simplified risk rating represents the level of mitigation necessary to address the risk present.

5G networks are complex systems. However, a risk measurement approach can be considered when determining the risk associated with 5G that is, the approach based on the Information Security Risk Management (ISO/IEC 27005) international standard. This standard outlines the process for conducting an information security risk assessment in accordance with the ISO 27001 requirements. The 5G risk can be measured using the ISO/IEC 27005 and demonstrated through a series of steps. For example, the first step is to identify a specific 5G risk

scenario (e.g., disruption of base station's functionalities in a limited area) and outline a detailed description of the risk scenario (e.g., an antenna stops working or an attack has affected solely the hardware of a given base station and the neighboring base stations are not affected). The second step is to determine one or more technical outcomes of the risk scenario (e.g., misconfiguration of 5G security features at the base station). The third step is to evaluate and assign a risk category (e.g., availability), likelihood rating (e.g., certainly may happen) and consequence rating (e.g., moderate). The final step is to evaluate and assign a risk level rating (e.g., high) [28].

3.1 Risk lifecycle

A risk management lifecycle consists of (1) identifying risks, (2) mitigating risks, (3) pursuing risk plans, and (4) monitoring risks. In the mitigating phase of the risk management lifecycle, there are risk mitigation options that can be performed to address residual risk, including accept, avoid, limit, plan, research, and transfer. A risk management framework becomes useful when determining the appropriate risk mitigation option for addressing risk [29]. Each threat scenario has been analyzed to determine the appropriate risk mitigation option given the trade-offs between risk tolerance and control risk correctness. For example, by leveraging the protect function found within a risk management framework, the risk mitigation option may limit or contain any further impact from a potential cyberattack on existing controls by redesigning and implementing more effective controls.

3.2 Potential loss or damage

A risk is any potential loss or damage that results from a threat exploited vulnerability found within a security

Table 2 Risk types and fake cell tower indicators

Risk type	Indicator types
Cell tower misconfigurations	Carrier wrong frequency, 911 services disabled, Encryption not set, Neighbor list empty, Not listing Absolute Radio-frequency Channel Number (ARFCN) for CO, Wrong frequency for location, Wrong cell ID for location, Cell site parameters
Control message inconsistencies	Location Area Code (LAC), Rolling LAC not on LAC boundaries, Neighbor list, Random-access Channel (RACH) control parameters, Cell channel description, Network color codes, Cell channel options, Cell site not used at location, MS-TXPWR-MAX-CCH Parameter set very high, RXLEV_ACCESS_MIN Parameter set very low, control msg. padding, description fields indicating the wrong version of 3GPP support

control. A control weakness (or low correctness level) can lead to more potential threat attack vectors. An adversary can take advantage of an attack vector within a mobile network ecosystem. An adversary can take advantage of potential threat attack vectors, including signal jamming downgrade attack, emergency 911 denial of service attack, spoofed wireless emergency alerts attack (WEA), SS7/Diameter attack, and device/identity tracking attack. 5G has introduced several security enhancements over pre-5G or legacy (e.g., 2G/3G/4G) mobile networks, but despite these security enhancements, 5G networks will still be a target where the adversary can take advantage of threat attack vectors [30, 31].

3.3 SS7 and diameter interfaces

An adversary will find two notable interfaces, SS7, and diameter, within a U.S. Carrier's mobile network ecosystem. The SS7 interface is an international standard used between public switched telephone networks (PSTN) and digital signaling network to exchange communication information among mobile networks among the U.S. Carrier's mobile networks as well as international mobile networks. The diameter interface is used to authenticate, authorize, and provide accurate mobile network billing information for real-time internet protocol (IP) mobile network communication used among U.S. Carrier's mobile networks.

An adversary can use a combination of modified mobile network equipment and gained technical knowledge in order to infiltrate the mobile network ecosystem. The modified mobile network equipment may take the form as any one of the following: fake SS7 interface, fake diameter interface, fake cell tower and signal jammer.

3.4 Fake cell tower

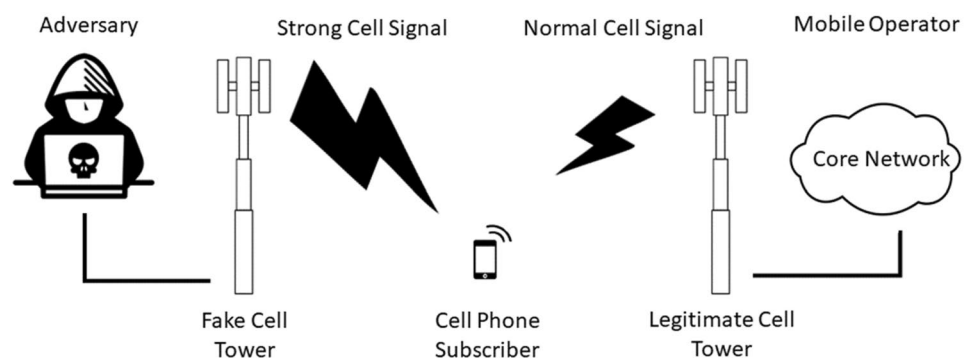
A connection between user's device and a fake cell tower consists of five steps that enable mischievous activities

by the adversary. First, the adversary mimics a U.S. Carrier's mobile network configurations with the adversary's fake cell tower. Second, the user's device sees the adversary's fake cell tower emitting the strongest signal. Third, the adversary's fake cell tower accepts the user's device (or can target a particular user's device). Forth, the user's device registers with the adversary's fake cell tower. Finally, the adversary's fake cell tower intercepts all out-bound calls and data services between the user's device and the adversary's fake cell tower. In this sequence of steps, the adversary's fake cell tower will not be able to capture inbound calls and data services since there is no roaming agreement in place with the adversary's fake cell tower and a U.S. Carrier's mobile network.

An adversary's fake cell tower can significantly impact customer's trust and U.S. carrier's reputation in the mobile telecommunications industry [32]. To perform security control correctness analysis for a particular mobile network ecosystem, it is divided into five trust boundaries, namely, user's device, subscriber identity, air interface, core mobile network, and U.S. carrier's business. A simplified representation with trust boundaries is useful when applying a threat modeling technique to determine potential threats and risks within a particular trust boundary. Figure 2 below shows the position of the fake cell tower within the network architecture.

There are messages as part of the broadcast system information messages in cellular networks, such as master information block (MIB) and system information block (SIB), which can be useful for establishing a fake base station when combined with pre-signing [33]. A fake base station enables an attacker to conduct man-in-the-middle attacks, replay attacks, down-grade attacks, and denial-of-service attacks [34]. However, 5G specification has no provision for broadcast message authentication. 3GPP has proposed various solutions to the fake base station in their technical report 33.809 [35]. Presently, 5G devices are still susceptible to attacks due to the lack of authentication of the initial broadcast messages.

Fig. 2 Fake cell tower



3.5 System information blocks

A system information block, or SIB, provides valuable information about user devices (or user equipment) and cell towers including (1) cell tower information, (2) cell re-selection, and (3) inter-frequency and inter-ratio access technology (RAT) cell selections. The indicator types (see Table 2) are of interest when detecting a fake cell tower. Several inherit signatures (or fingerprints) can be identified across various SIBs including SIB type 1, 2, 3, 4 and 13 [36].

For example, SIB type 1 provides information pertaining to cell access related to parameters and scheduling of other SIBs. SIB type 2 provides information pertaining to common and shared channel configuration; random access channel (RACH) related configuration is present. SIB type 3 provides information pertaining to parameters required for intra-frequency, inter-frequency, and I-RAT cell re-selections. SIB type 4 provides information pertaining to intra-frequency neighboring cells (e.g., E-UTRA). SIB type 13 provides information pertaining to acquiring the multimedia broadcast multicast services (MBMS) control information associated with one or more multimedia broadcast multicast services single frequency network (MBSFN) areas.

4 Pre-5G signature-based processing

The process consists of identification, classification, prediction, and prevention. First, identifying an indicator type provides a clue that represents a signature (or fingerprint) candidate that can be used to detect a fake cell tower as part of a threat scenario (as previously mentioned). The threat scenario manifests into a simplified risk rating that can be used for the mitigation of risk. A signature

candidate consists of the relationship among the three different types, including indicator, data, and SIB. Second, the classification of the signature candidates is necessary for establishing correlations across multiple SIBs (e.g., type 1, 2, 3, 4, and 13). Table 3 shows signature candidates classifications based on indicator type, data type, and SIB.

The information found within each of the SIBs can be used for the detection of a fake cell tower over time. Likewise, classification such as cell tower inconsistencies in configuration or suspicious activity enables prediction of a potential fake cell tower where the most likely signature candidates can be further investigated to determine applicable risk mitigation. Third, the prediction of an adversary (or attacker) can be achieved through the correlation of the signature candidates based on information contained across multiple SIBs (e.g., types 1, 2, 3, 4, and 13). Table 4 shows the second part of signature candidates' classifications based on indicator type, data type, and SIB.

The successful prediction of a fake cell tower enables action and the mitigation of risk. The use of identification, classification and prediction of a fake cell tower enables prevention of a fake cell tower to take place. Finally, the prevention of an adversary (or attacker) using a fake cell tower within a threat scenario is of paramount importance to safeguard a mobile network. Likewise, the prevention is not a point in time but a continual process of strengthening the security control correctness and mitigation of risk.

For example, in pre-5G the detection of a fake cell tower requires identification of likely signature candidates. The signature candidates enable a correlation to take place using the information contained across multiple SIBs (e.g., type 1, 2, 3, 4 and 13) for each of the threat scenarios. Once a fake cell tower has been successfully detected, the prevention of a future fake cell tower can be achieved.

Table 3 Signature candidates

Indicator type	Data type	SIB type
Wrong frequency for carrier	GPS LAT, GPS LONG, ARFCN	1
911 services disabled	Is cell on-line but not operational	1, 2, 3, 4
Neighbor list empty	GPS LAT, GPS LONG, neighbor list	2
Not listing absolute radio-frequency channel number (ARFCN) for C0	GPS, LAT, GPS, LONG, captured SI-1 Block	1
Wrong frequency for location	GPS LAT, GPS LONG, ARFCN	1
Wrong cell ID for location	GPS LAT, GPS LONG, CELLID	3
Location area code (LAC) inconsistent	GPS LAT, GPS LONG, LAC	3
Rolling LAC not on LAC boundaries	GPS LAT, GPS LONG, LAC	3
Neighbor list inconsistent	GPS LAT, GPS LONG, neighbor list	2
Random-access channel (RACH) control parameters inconsistent	GPS, LAT, GPS, LONG, captured SI-2 Block	1, 2, 3, 4
Cell channel description inconsistent	GPS, LAT, GPS, LONG, captured SI-3 Block	3
Cell channel options inconsistent	GPS, LAT, GPS, LONG, captured SI-3 Block	3

Table 4 Signature candidates continued

Indicator type	Data type	SIB type
Cell site not used at location	GPS LAT, GPS LONG, CELLID	3
Cell selection parameters inconsistent	GPS, LAT, GPS, LONG, captured SI-3 Block	3
MS-TXPWR-MAX-CCH parameter set very high	GPS, LAT, GPS, LONG, captured SI-3 Block	3
RXLEV_ACCESS_MIN parameter set very low	GPS, LAT, GPS, LONG, captured SI-3 Block	3
Inconsistencies in control msg. padding	GPS LAT, GPS LONG, captured SI-1, SI-2, SI-3, SI-4 and/or SI-13 message	1, 3, 4, 13
Inconsistencies in description fields indicating wrong ver. of 3GPP support	GPS LAT, GPS LONG, captured SI-1, SI-2, SI-3, SI-4 and/or SI-13 message	1, 2, 3, 4, 13

However, the protection mechanisms would need to be implemented on the user device (or user equipment) and network equipment across the U.S. carrier's mobile s. That is, a software application would need to be developed for user devices (or user equipment) that would detect anomalies represented by the signature candidates. With permission from the subscriber, mobile network information would be collected and shared with the carrier for further correlation analysis of the signature candidates. The result from the analysis assists the carrier in strengthening security controls. The security controls requirements and/or changes in existing requirements can then be submitted to the 3GPP and GSMA standards bodies where mobile network equipment manufacturers (e.g., Ericsson, Nokia, Samsung, and Cisco) can transform the requirements into functional capabilities.

Another example, in 5G there are several security enhancements including (1) unified authentication framework and access-agnostic authentication, (2) primary authentication by the carrier and additional secondary authentication to an external data network, (3) increased home U.S. carrier's mobile network control, (4) enhanced

subscriber privacy, and (5) user plan integrity protection in Radio Access Network, Service Based Architecture and interconnect security [37]. Likewise, these 5G protections mitigate many of the risks found within existing carriers' pre-5G mobile networks. However, many of the 5G protections are optional for carriers to configure so there is no guarantee that carriers will consistently implement 5G protections across the carriers' entire mobile network. Table 5 below lists the symbols and abbreviations used throughout the paper.

5 Security control correctness

The security control correctness (as defined by NIST SP 800-137) represents the measure of correctness of control implementation in accordance with risk tolerance. For example, the security preference is utilizing a security by design best practice pattern for significant control correctness. That is, the preferred control correctness results from a high certainty of correctness associated with the control implementation and an acceptable risk tolerance.

Table 5 List of abbreviations

Symbol/Abbreviation	Meaning
AMF	Access and mobility management function
ARFCN	Absolute radio-frequency channel number
AUSF	Authentication server function
IMSI	International mobile subscriber identity
PSAP	Public safety answering point
PSTN	Public switched telephone networks
SIB	System information block
SIM	Subscriber identity module
SS7	Signaling system number 7
STRIDE	Spoofing identity, tampering with data, repudiation threats, information disclosure, denial of service and elevation of privileges
SUCI	Subscription concealed identifier
SUPI	Subscription permanent identified
UDM	Unified data management

In contrast, a less than preferred control correctness would require a significant amount of risk remediation necessary to increase the control correctness to bring up the level of control implementation correctness to a level that is back within acceptable risk tolerance. A simplified risk rating using threat modeling enables a thoughtful discussion about the trade-offs between security control correctness and acceptable risk tolerance. Figure 3 shows the proposed control correctness architecture.

5.1 User device control correctness

A review of the user device (or user equipment) control correctness suggests that the protection of the international mobile subscriber identity (IMSI) is not sufficient in pre-5G. As part of the user device registration process, the subscriber identity module (SIM) containing the IMSI is used during authentication to register with the user device with a legitimate U.S. Carrier’s mobile network. The fake cell tower can target exposed IMSIs to attach while rejecting others. The exposed IMSI can be captured and allow an adversary (or attacker) to perform main-in-the-middle and

eavesdropping attacks. In pre-5G, the detection of fake cell towers stems from identification of a candidate signatures found through a correlation of information found across multiple system information blocks (e.g., SIBs type 1, 2, 3, 4 and 13) (see Table 6). In 5G, the IMSI is encrypted. However, there is no guarantee that the U.S. Carrier’s mobile network will consistently implement this 5G protection across the entire U.S. Carrier’s mobile network.

5.2 Subscriber identity control correctness

A review of the subscriber identity control correctness includes subscriber privacy protections. The user device (or user equipment) is expected to authenticate to the mobile network but is not required for the mobile networks to authenticate to devices. This allows a fake cell tower to impersonate a legitimate base station and capture an unsuspecting subscriber’s IMSI. Likewise, a fake cell tower can force a user device to use no encryption during calls or use easily breakable encryption, allowing eavesdropping by the adversary (or attacker).

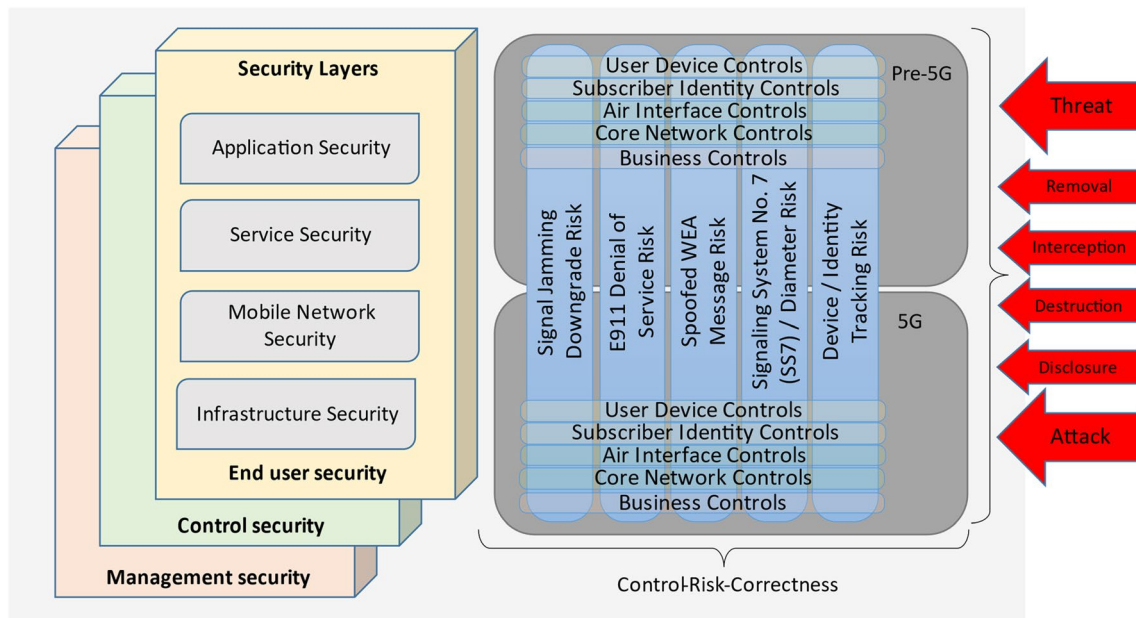


Fig. 3 Proposed control risk correctness architecture

Table 6 User device correctness

Network technology	Mischievous activity	Protection
Pre-5G	Fake cell tower can target exposed IMSI	Identification of signatures
5G	Fake cell tower can target exposed IMSI	IMSI is encrypted but depends on U.S. Carrier implementation

In pre-5G, the detection of fake cell towers stems from the identification of candidate signatures that can be found by correlation across multiple system information blocks (e.g., SIBs type 1, 2, 3, 4 and 13). In contrast to pre-5G, 5G subscription permanent identifier (SUPI), and subscription concealed identifier (SUCI) are introduced as potential mitigation to the exposure of the IMSI as demonstrated in Table 7. The SUPI is encrypted using the U.S. Carrier's mobile network public key, which allows the user device to authenticate and connect to the U.S. Carrier's mobile network. However, more sophisticated adversaries or attackers may be able to force user devices to communicate in non-5G mode and minimize the control correctness of the 5G mitigation. Table 7 shows mischievous activities difference in 5G networks over previous generations and protection mechanisms used, indicating how 5G imposed a major shift in the paradigm of protection policies.

5.3 Air interface control correctness

A review of the air interface control correctness includes the same protections found within the radio access network for 2G, 3G and 4G. The primary challenge is with fake cell towers that enable (1) targeting IMSIs during the user device's initial attach procedure to a fake cell tower and (2) paging attacks using the IMSI paging feature of a fake cell tower. The obtained information about IMSIs may be used for various types of attacks. In pre-5G, detecting fake cell towers stems from the identification of a signature found by correlation across multiple system information blocks (e.g., SIBs type 1, 2, 3, 4 and 13). In 5G, the data and signaling transmitted and received at the radio layer are expected to be appropriately encrypted and integrity protected at higher layers whenever possible (see Table 8). However, there is no guarantee that the carrier

will consistently implement these 5G protections across the U.S. carrier's entire network (as previously mentioned).

5.4 Core network control correctness

A review of the core network control correctness identifies the U.S. carrier's mobile network functions do establish the necessary protection to thwart an adversary (or attacker) from mischievous action. These core mobile network functions include access and mobility management function (AMF), authentication server function (AUSF), and Unified data management (UDM). The AMF provides authentication, authorization, and mobility management services to the user device (or user equipment). The AUSF stores data for authentication of the user device, and the UDM stores the UE subscription data. A launch of both user plane and signaling plane attacks on core mobile network functions can lead to a significant degradation or event that makes critical services unavailable for a legitimate subscriber with a user device (or user equipment). Even in 5G, an attack against these core mobile network functions can result in reduced availability of services or even mobile network outages [38] (see Table 9).

In addition, there are potential network slicing, network function virtualization, software-defined networking, interworking, and roaming threats that remain possible with 5G protections [14, 39]. These threats are interesting and worth pursuing; however, they are beyond the scope of topics covered within this paper and will be considered further in future work.

5.5 Business control correctness

A review of the U.S. carrier's business control correctness used in conjunction with the U.S. carrier's mobile network includes potential user privacy compromises with tracking

Table 7 Subscriber identity control correctness

Network technology	Mischievous activity	Protection
Pre-5G	Fake cell tower can target exposed IMSI	Identification of signatures
5G	Fake cell tower can target exposed IMSI	Encrypted SUPI and concealed SUCI but depends on U.S. Carrier implementation

Table 8 Air interference control correctness

Network technology	Mischievous activity	Protection
Pre-5G	Fake cell tower can target exposed IMSI paging	Identification of signatures
5G	Fake cell tower can target exposed IMSI	Encryption at radio layer and higher layer integrity protections but depends on U.S. Carrier implementation

Table 9 Core network control correctness

Network technology	Mischievous activity	Protection
Pre-5G	Downgrade or reduced availability of critical network resources or outage	Various levels of protections based on the network technology
5G	Downgrade or reduced availability of critical network resources or outage	Trusted internal interfaces, service-based architecture, and interconnected security but depends on U.S. Carrier implementation

and location detection of a user device (or user equipment) that can lead to significant damages and losses to both carriers and subscribers. Depending on how the carrier uses location data as part of data aggregation and monetization services to provide user device data to third parties for further service enrichment by the carrier. In 5G, the exposure of user permanent identifier (e.g., SUPI) may enable unauthorized tracking of user device movements and activities, as shown in Table 10.

6 Simplified risk ratings

The resultant simplified risk rating can be derived from the association among the following: threat type, threat scenario, and STRIDE threat classification. The risk mitigation depends on a combination of simplified risk rating and security services that aligns with each of the STRIDE threat classifications.

The risk calculation used for the simplified risk rating incorporates the same impact and likelihood calculation found in the NIST Special Publication 800-30. The risks were given impact and likelihood to calculate risk and apply a simplified risk rating. The simplified risk ratings include (1) full mitigation (or detection) represents Low, (2) partial mitigation (or detection) represents Medium, and (3) minimal mitigation or detection represents Elevated. The simplified risk rating was stated as Low (Normal) when there was high impact and low likelihood. A simplified risk rating was stated as Elevated when high impact and medium likelihood. A straightforward equation is

used to evaluate risk at a scale from 1 to 100 as follows: $\text{risk} = \text{impact} * \text{Likelihood}$. Since the impact is considered severe for all types of risk, it is set for the default value of 100%. Hence, the calculated risk is directly proportional to the likelihood. For example, the user device trust boundary risk rating is calculated for signal jamming by estimating the likelihood of that risk at 0.5, which results in a risk value 50, for which the risk is considered elevated. On the other hand, for the core network, it is estimated to be 0.1, and hence the calculated risk is 10, which is considered low or normal.

The resulting simplified risks ratings suggest that the user device (or user equipment), subscriber identity, and air interface are three out of the five trust boundaries of most interest and focus of the threat modeling analysis for each of the threat scenarios. These trust boundaries of interest include user device (or user equipment), subscriber identity, and air interface with elevated simplified risk ratings for all the threat scenarios. In contrast, the core mobile network and U.S. Carrier’s mobile network business trust boundaries have low (normal) simplified risk ratings for all the threat scenarios and are not considered to need additional detailed analysis. Table 11 shows the overall simplified risk rating analysis.

6.1 Signal jamming downgrade risk mitigation

The user device (or user equipment) connection to a fake cell tower in a signal jamming downgrade attack threat scenario consists of seven steps. First, the adversary (or attacker) jams the U.S. Carrier’s mobile network (possible

Table 10 Business control correctness

Network technology	Mischievous activity	Protection
Pre-5G	Fake cell tower can target user privacy compromise with tracking and location detection	Identification of signatures
5G	Fake cell tower can target user privacy compromise with tracking and location detection	Encrypted SUPI and concealed SUCI but depends on U.S. Carrier implementation

Table 11 Over simplified risk rating

Trust boundary	Threat scenarios				
	Signal jamming downgrade	E911 denial of service	Spoofed WEA message	SS7/diameter attack	Device/identify tracking
User device	Elevated	Elevated	Elevated	Elevated	Elevated
Subscriber identity	Elevated	Elevated	Elevated	Elevated	Elevated
Air interface	Elevated	Elevated	Elevated	Elevated	Elevated
Core network	Low (normal)	Low (normal)	Low (normal)	Low (normal)	Low (normal)
Business	Low (normal)	Low (normal)	Low (normal)	Low (normal)	Low (normal)

multiple channels). Second, the adversary (or attacker) mimics the U.S. Carrier's mobile network on an open frequency. Third, the user device sees the adversary (or attacker) network as the U.S. Carrier's mobile network that is too noisy. Forth, the adversary (or attacker) accepts all user devices or only a targeted device. Fifth, the user devices hand over with a fake mobile network. Sixth, the adversary (or attacker) intercepts outbound calls and data. Finally, the inbound calls are not possible as there is no roaming agreement in place.

In this case, the threat scenario represents the potential for call and data interception. The associated STRIDE threat is information disclosure (e.g., privacy breach or data leak) of the security controls related to confidentiality security service. The confidentiality security service provides protection of data from unauthorized disclosure. The elevated simplified risk rating for the user device, subscriber identity, and air interface trust boundaries can be explained for the signal jamming downgrade threat scenario in the context of pre-5G and 5G technologies.

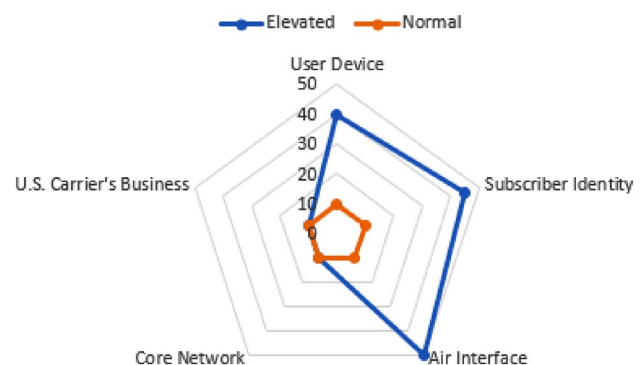
First, the user device pre-5G risk relates to an exposed IMSI can be detected through an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the IMSI can be encrypted to mitigate exposed IMSI. Still, this capability is optional for the U.S. Carrier mobile network to implement, thus maintaining the same simplified risk rating found in pre-5G.

Second, the subscriber identity pre-5G risk is like the user device pre-5G risk that relates to an identified signature found by correlation across multiple system information blocks, and hence can be used by the adversary (or attacker), which may result in an elevated simplified risk rating with high impact and medium likelihood. While the SUCI and SUPI mitigate risk in 5G, more sophisticated adversaries (or attackers) may force user devices to communicate in non-5G mode. Hence, the simplified risk rating is the same as found in pre-5G.

Finally, the air interface pre-5G risk is like the user device and subscriber identity pre-5G risk that relates to

an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the data and signaling transmitted and received at the radio layer are expected to be appropriately encrypted and integrity protected at higher layers and thereby mitigate the risk. However, this capability is optional for the U.S. Carrier mobile network to implement, thus maintaining the same simplified risk rating found in pre-5G.

A suggested signal jamming risk mitigation combines fake cell tower detection for pre-5G and consistent implementation of 5G protections across the U.S. Carrier's mobile network. The user device (or user equipment), subscriber identity and air interface trust boundaries have simplified risk rating of elevated. The core mobile network and U.S. Carrier's mobile network business trust boundaries have a simplified risk rating of low (normal). Figure 4 shows how signal jamming can influence different trust boundaries based on the calculated risk rating. For instance, both core network and carrier's business will have normal risk rating because of this type of threat. On the other hand, user device, subscriber identity, and air inference will have elevated risk rates, as illustrated in the blue line.

**Fig. 4** Signal jamming downgrade risk rating

6.2 911 Denial of service risk mitigation

The user device (or user equipment) connection to a fake cell tower in an emergency 911 denial of service attack threat scenario consists of four steps. First, the adversary (or attacker) mimics the U.S. Carrier’s mobile network and broadcasts support for emergency 911 but is not connected to the public-safety answering point (PSAP). Second, the user device sees the adversary (or attacker) mobile network with a strong signal and attempts to hand over. Third, the adversary (or attacker) accepts all devices (or only targeted user devices). Finally, the adversary (or attacker) does not route emergency 911 calls to PSAP, and the user device stays connected trying to connect to emergency 911 PSAP.

In this case, this threat scenario represents the potential for sending unauthenticated ‘attach reject’ messages. This type of STRIDE threat is associated with the denial of service. Security controls are normally related to the availability security service, ensuring that a resource is accessible and usable. The elevated simplified risk rating for user device, subscriber identity and air interface trust boundaries can be explained for the emergency 911 denial of service attack threat scenario in the context of pre-5G and 5G technologies.

First, the user device pre-5G risk relates to an exposed IMSI can be detected through an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the IMSI can be encrypted to mitigate exposed IMSI, but this capability is optional for the U.S. Carrier’s mobile network to implement, thus maintaining the same simplified risk rating found in pre-5G.

Second, the subscriber identity pre-5G risk is like the user device pre-5G risk that relates to an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the SUCI and SUPI can mitigate risk; however, more sophisticated adversaries (or attackers) may force user devices to communicate in non-5G mode, so the simplified risk rating is the same as found in pre-5G.

Finally, the air interface pre-5G risk is like the user device and subscriber identity pre-5G risk that relates to an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the data and signaling transmitted and received at the radio layer are expected to be appropriately encrypted and integrity protected at higher layers and thereby mitigate the

risk. However, this capability is optional for the carrier to implement, thus maintaining the same simplified risk rating found in pre-5G.

A suggested emergency 911 denial of service risk mitigation combines fake cell tower detection for pre-5G and consistent implementation of 5G protections across the U.S. carrier’s mobile network. As illustrated in Fig. 5, the user device, subscriber identity, and air interface trust boundaries have a simplified risk rating of elevated. The core mobile network and U.S. carrier’s business trust boundaries have a simplified risk rating of low (normal).

6.3 Spoofed WEA message risk mitigation

The user device (or user equipment) connection to a fake cell tower in a spoofed WEA messages attack threat scenario consists of five steps. First, the adversary (or attacker) mimics the U.S. Carrier’s mobile network. Second, the user device sees the adversary (or attacker) mobile network with a strong signal. Third, the adversary (or attacker) accepts all user devices (or only targeted user devices). Forth, the user device hands over to the fake mobile network. Finally, the adversary (or attacker) injects WEA messages to the user devices (e.g., amber alerts, emergency broadcasts messages or presidential alerts).

In this case, this threat scenario represents the potential for preventing emergency calls. The associated STRIDE threat is the denial of service. Security controls are directly related to the availability security service, assuring that a resource is accessible and usable. The elevated simplified risk rating for user device, subscriber identity, and air interface trust boundaries can be explained for the spoofed WEA message threat scenario in the context of pre-5G and 5G technologies.

First, the user device pre-5G risk relates to an exposed IMSI can be detected through an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that

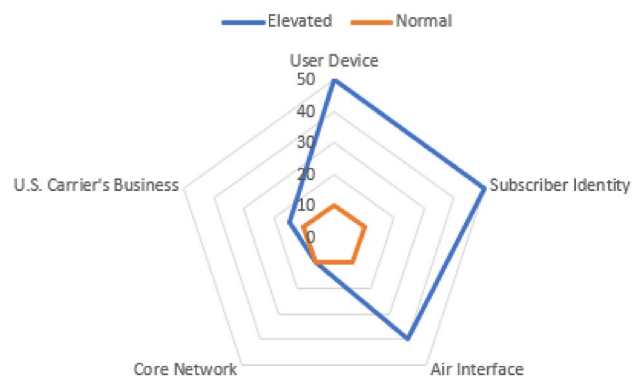


Fig. 5 E911 DOS risk rating

results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the IMSI can be encrypted to mitigate exposed IMSI, but this capability is optional for the U.S. Carrier's mobile network to implement, thus maintaining the same simplified risk rating found in pre-5G.

Second, the subscriber identity pre-5G risk is like the user device pre-5G risk that relates to an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the SUCI and SUPI can mitigate risk; however, more sophisticated adversaries (or attackers) may be able to force user devices to communicate in non-5G mode, so the simplified risk rating is the same as found in pre-5G.

Finally, the air interface pre-5G risk is like the user device and subscriber identity pre-5G risk that relates to an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the data and signaling transmitted and received at the radio layer are expected to be appropriately encrypted and integrity protected at higher layers and thereby mitigate the risk. However, this capability is optional for the U.S. Carrier's mobile network to implement, thus maintaining the same simplified risk rating found in pre-5G.

A suggested spoofed WEA message risk mitigation combines fake cell tower detection for pre-5G and consistent implementation of 5G protections across the U.S. Carrier's mobile network. Figure 6 shows that the user device, subscriber identity, and air interface trust boundaries have a simplified risk rating of elevated. The core mobile network and U.S. Carrier's mobile network business trust boundaries have simplified risk ratings of low (normal).

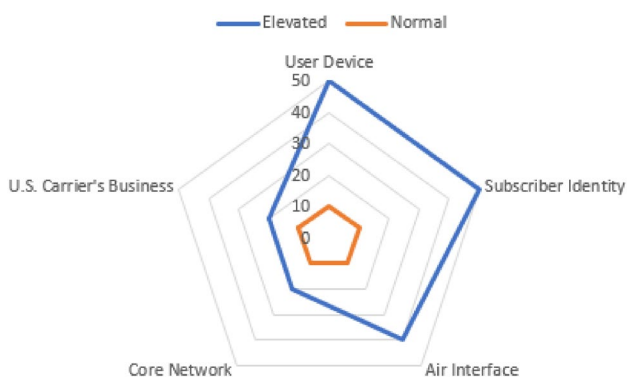


Fig. 6 Spoofed WEA message risk rating

6.4 SS7/diameter risk mitigation

The user device (or user equipment) connection to a fake cell tower in an SS7/ diameter attack threat scenario consists of five steps. First, the adversary (or attacker) mimics the U.S. Carrier's mobile network for both 2G and 4G networks. Second, the user device registers with the Fake 2G network. Third, the adversary (or attacker) sends relevant SS7 or diameter messages to home mobile network. Forth, the subscriber roams to the fake U.S. Carrier's mobile network. Finally, the inbound calls are routed over SS7 or DIAMETER to the fake tower intercepting all calls and data to/from the user device.

In this case, this threat scenario represents the potential for sending unauthenticated 'attach reject' messages. The associated STRIDE threat is the denial of service. The security controls are related to the availability security service, assuring that a resource is accessible and usable. The elevated simplified risk rating for the user device, subscriber identity, and air interface trust boundaries can be explained for the SS7/Diameter threat scenario in the context of pre-5G and 5G technologies.

A suggested SS7/Diameter attack risk mitigation combines fake cell tower detection for pre-5G and consistent implementation of 5G protections across the U.S. Carrier's mobile network. Figure 7 shows that the user device, subscriber identity and air interface trust boundaries have simplified risk rating of elevated. The core mobile network and U.S. Carrier's mobile network Business Control Correctness trust boundaries have a simplified risk rating of low (normal).

6.5 Device/identity tracking risk mitigation

The user device (or user equipment) connection to a fake cell tower in a device/identity tracking attack threat scenario consists of five steps. First, the adversary (or attacker) mimics the U.S. Carrier's mobile network. Second, the user device sees the adversary (or attacker) mobile network

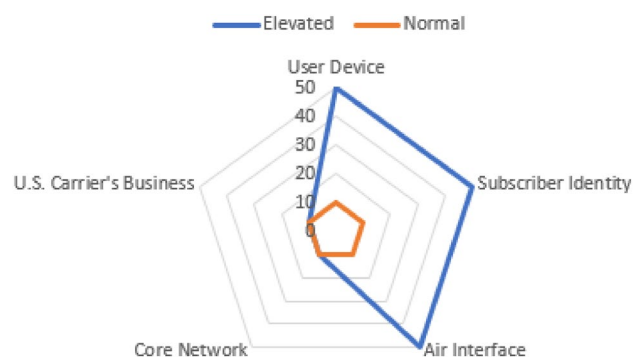


Fig. 7 SS7/diameter risk rating

with a strong signal. Third, the adversary (or attacker) sends a radio resource control (RRC) connection reconfiguration command, which contains the cell identifiers (IDs) of at least three neighboring cell towers and their connection frequencies to the user device. Forth, the user device sends a response to the message that contains the signal strengths of the previously specified cell towers. Finally, the user device location can be calculated using a technique called trilateration. Trilateration involves calculating the intersection of the radius from the three cell towers, given the reported signal strength from each of the cell towers. Alternatively, newer user devices will report the user devices exact GPS coordinates and therefore, no trilateration calculations are necessary.

In this case, the threat scenario represents the potential for successful correlation of a device and an individual. Hence, the associated STRIDE threat is information disclosure (privacy breach or data leak). The security controls related to confidentiality security service. Therefore, the elevated simplified risk rating for user device, subscriber identity and air interface trust boundaries can be explained for the device/identity tracking threat scenario in the context of pre-5G and 5G technologies.

First, the user device pre-5G risk relates to an exposed IMSI can be detected through an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the IMSI can be encrypted to mitigate exposed IMSI; however, this capability is optional for the U.S. Carrier's mobile network to implement, thus, maintaining the same simplified risk rating found in pre-5G.

Second, the subscriber identity pre-5G risk is like the user device pre-5G risk that relates to an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the SUCI and SUPI mitigate the risk; however, more sophisticated adversaries (or attackers) may be able to force user devices to communicate in non-5G mode so the simplified risk rating is the same as found in pre-5G.

Finally, the air interface pre-5G risk is like the user device and subscriber identity pre-5G risk that relates to an identified signature found by correlation across multiple system information blocks and used by the adversary (or attacker) that results in an elevated simplified risk rating with high impact and medium likelihood. In 5G, the data and signaling transmitted and received at the radio layer are expected to be appropriately encrypted and integrity protected at higher layers and thereby mitigate the risk. However, this capability is optional for the U.S. Carrier's

mobile network to implement, thus maintaining the same simplified risk rating found in pre-5G.

A suggested device/identity risk mitigation combines fake cell tower detection for pre-5G and consistent implementation of 5G protections across the U.S. Carrier's mobile network. The user device, subscriber identity and air interface trust boundaries have simplified risk rating of elevated. The core mobile network and U.S. Carrier's mobile network business trust boundaries have simplified risk ratings of low (normal) (see Fig. 8).

There is agreement among security professionals that increasing security and reducing risk exposure in 5G and future versions of telecommunication technology will continue to be a challenging and highly demanding. An important first step towards increasing security and reducing risk exposure is reviewing and evaluating risks in these networks. Risk assessment provides the necessary tools to manage and plan where and how to best apply available resources to mitigate risk. The contribution of this article is to highlight a reviewing process for several risk factors, providing a simplified risk review, and evaluating existing risk methods intended to support the risk assessment process as well as to reason comparatively about existing risks. This translates into the proposed risk evaluation process can be used to determine the relative riskiness of a particular threat with regard to various trust boundaries as demonstrated previously in Table 10.

A pre-5G cell site simulator can be configured for capturing the MIB and SIB information for a fake base station. The equipment may vary depending on the approach taken but in general, the simulator includes a core network in a box (e.g., YateBTS, antenna, software defined radio (e.g., fake cell site), test mobile system (TEMS) phone, device under test (e.g., victim phone), custom radio sensor, GPS simulator, and signal attenuator. Another type of pre-5G simulator configuration may consist of the equipment including a GSM modem, antenna, raspberry Pi, GPS simulator, device under test (e.g., victim phone, and hot-spot device [27]. In contrast, a 5G cell site simulator can be

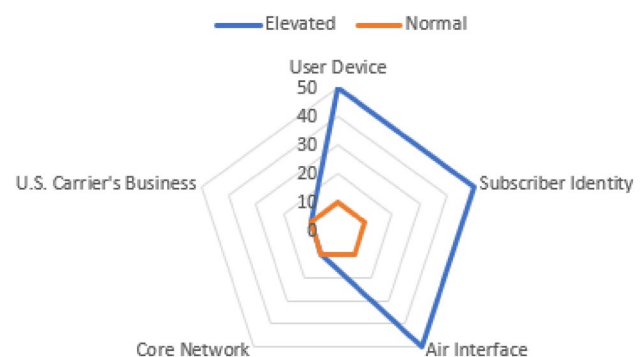


Fig. 8 Device/identity tracking risk rating

Table 12 Comparison with existing risk evaluation methods

Reference	Threat scenarios	Pre-5G	5G	Risk evaluation limitations
[28]	Signal jamming downgrade (bidding down) E911 denial of service Spoofed WEA message Signaling System No. 7 (SS7)/diameter attack Device/identify tracking	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	No simplified risk rating No trust boundaries Correlated risks
[41]	E911 denial of service	✓	✓	Did not address several threats No trust boundaries
[42]	Signal jamming downgrade (bidding down) E911 denial of service Device/identify tracking	✓ ✓ ✓	✓ ✓ ✓	No simplified risk rating Did not address few threats No trust boundaries Correlated risks
[43]	Signal jamming downgrade (bidding down)		✓	Did not address several threats No trust boundaries
[26]	Signal jamming downgrade (bidding down) E911 denial of service Device/identify tracking	✓ ✓ ✓		No simplified risk rating Did not address few threats No trust boundaries Correlated risks
This work	Signal jamming downgrade (bidding down) E911 denial of service Spoofed WEA message Signaling System No. 7 (SS7)/diameter attack Device/identify tracking	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	Correlated risks Interleaved trust boundaries

configured for capturing the MIB and SIB information for a fake base station. The CTIA industry council has recently established a 5G security testbed (<https://5gsecuritytestbed.com/use-cases-and-architecture/>) with a specific 5G use case to test the protection against international mobile subscriber identity (IMSI) catchers or rogue base stations used by cyber criminals. The 5G security test bed simulator configuration includes a radio access network (RAN), core network, user equipment, measurement toolset, and monitoring equipment [40].

A set of empirical research articles describe similar threat scenarios, risks, and risk evaluation approaches the proposed risk evaluation outlined in this article for pre-5G and 5G. Table 12 below summarizes a comparison with existing risk evaluation methods and how the proposed risk evaluation approach is different.

7 Conclusions

The threats present in a mobile network can lead to the use of fake cell towers (or fake cell towers) by adversaries (or attackers) to compromise the confidentiality, integrity, and availability of the pre-5G and 5G technologies that make up a U.S. Carrier's mobile network. A novel methodology called Control-Risk-Correctness was used to form the basis for simplifying the analysis when making recommendations pertaining to risk remediation necessary in the treatment of elevated risk. The result of the analysis identified that user device, subscriber identity, and air

interface are three out of the five trust boundaries of most interest with elevated risk ratings. These findings suggest that for the current security control trade-offs between pre-5G and 5G mobile network technologies identified of most interest with elevated risk ratings include user device, subscriber identity, and air interface. Risk mitigation, which is necessary for the treatment of each of elevated risk ratings, was provided to increase the control correctness level and decrease the associated risk level.

As future work, we intend to pursue an enhanced model for control-risk-correctness combined with an implementation of the risk assessment method. 5G addresses many pre-5G threats with built-in controls such as mutual authentication and enhanced subscriber identity protection as safeguards. However, options remain for the U.S. Carriers to choose whether to implement or not implement certain security capabilities as part of the 5G build-out. Hence, the elevated risk remains a possibility in situations where pre-5G and 5G co-exist. Further investigation deemed necessary into new threat scenarios where the usefulness of the control-risk-correctness model and associated implementation of the risk assessment method provides ample opportunity to be applied to mitigate and remediate man-in-the-middle attacks, as well as the development of a set of recommendations for best practices used by practitioners in the communications industry.

In addition, there are several other risk assessment challenges that arise when combining 5G with other paradigms. For instance, caching in 5G networks may raise several concerns related to performance and risk

analysis [44, 45]. In addition, Fault-Resilience is one of the prominent challenges that arise when using 5G in the context of industrial Software Defined Networks [44]. Finally, there are potential threats to investigate when applying several paradigms with 5G, such as network slicing, network function virtualization, software-defined networking, interworking, and roaming.

Acknowledgements Special thanks to Dr. Yong Wang at Dakota State University for his valuable comments and feedback.

Funding Financial interests: Authors Eric Yocam, Amjad Gawanmeh, Ahmad Alomari, and Wathiq Mansoor declare they have no financial interests. The authors have no relevant financial or non-financial interests to disclose.

Data availability Authors will be providing any data required about the study.

Declarations

Conflict of interest The authors declares that they have no conflict of interest.

Research involving human and/or animal participants This article does not contain any studies with human participants or animals performed by any of the authors.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Ahmad I, Kumar T, Liyanage M, Okwuibe J, Ylianttila M, Gurtov A (2018) Overview of 5G security challenges and solutions. *IEEE Commun Stand Mag* 2(1):36–43
2. Rosenblum A (2014) Mysterious phony cell towers could be intercepting your calls. *Popular Science*. Available at <https://www.popsoci.com/>
3. Dabrowski A, Petzl G, Weippl E (2016) The messenger shoots back: network operator based IMSI catcher detection. In: International symposium on research in attacks, intrusions, and defenses. Springer, Cham, pp 279–302
4. Dabrowski A, Pianta N, Klepp T, Mulazzani M, Weippl E (2014) IMSI-catch me if you can: IMSI-catcher-catchers. In: Proceedings of the 30th annual computer security applications conference. ACM, pp 246–255
5. Koscher K, Ney P (2019) Seaglass application. Electronic Frontier Foundation. <https://github.com/seaglass-project/seaglass-app>
6. Zhu L, Ma Z, Huang H, Yan M (2021) Research on security risk prevention and control of new infrastructure. *J Phys Conf Ser* 1856(1):012034
7. Carvalho GHS, Woungang I, Anpalagan A, Traore I (2020) When agile security meets 5G. *IEEE Access* 8:166212–166225
8. Khan JA, Chowdhury MM (2021) Security analysis of 5G network. In: 2021 IEEE international conference on electro information technology (EIT). IEEE, pp 001–006
9. Liyanage M, Ahmad I, Abro AB, Gurtov A, Ylianttila M (2018) A comprehensive guide to 5G security. Wiley, Hoboken
10. Ranaweera P, Jurcut A, Liyanage M (2021) MEC-enabled 5G use cases: a survey on security vulnerabilities and countermeasures. *ACM Comput Surv* 54(9):1–37
11. Rogalski M (2021) Security assessment of suppliers of telecommunications infrastructure for the provision of services in 5G technology. *Comput Law Secur Rev* 41:105556
12. Gerrit H, William L, Dimitri PD, Alain M, Jérôme B, Vincent L (2021) 5G system security analysis. arXiv preprint. <https://arxiv.org/abs/2108.08700>
13. Shostack A (2022) The threats to our products. Microsoft SDL Blog. Microsoft. Available at: <https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/>. Accessed 10 Jan 2022
14. Hasneen J, Sadique KM (2022) A survey on 5G architecture and security scopes in SDN and NFV. In: Applied information processing systems. Springer, Singapore, pp 447–460
15. Dutta A, Hammad E (2020) 5G security challenges and opportunities: a system approach. In: 2020 IEEE 3rd 5G world forum (5GWF). IEEE, pp 109–114
16. Madi T, Alameddine HA, Pourzandi M, Boukhtouta A (2021) NFV security survey in 5G networks: a three-dimensional threat taxonomy. *Comput Netw* 197:108288
17. Køien GM (2021) On threats to the 5G service based architecture. *Wirel Pers Commun*. <https://doi.org/10.1007/s11277-021-08200-0>
18. Zhao D, Yan Z, Wang M, Zhang P, Song B (2021) Is 5G handover secure and private? A survey. *IEEE Internet Things J* 8(16):12855–12879
19. Yu C, Chen S, Wang F, Wei Z (2021) Improving 4G/5G air interface security: a survey of existing attacks on different LTE layers. *Comput Netw* 201:108532
20. Zhao L, Oshman MS, Zhang M, Moghaddam FF, Chander S, Pourzandi M (2021) Towards 5G-ready security metrics. In: ICC 2021-IEEE international conference on communications. IEEE, pp 1–6
21. Derhab A, Aldweesh A, Emam AZ, Khan FA (2020) Intrusion detection system for internet of things based on temporal convolution neural network and efficient feature engineering. *Wirel Commun Mob Comput*. <https://doi.org/10.1155/2020/6689134>
22. How IMSI-Catchers Exploit Cell Networks (2019) Electronic Frontier Foundation. <https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks>
23. Scandariato R, Wuyts K, Joosen W (2015) A descriptive study of microsoft threat modeling technique. *Requir Eng* 20(2):163–180
24. Shostack A (2014) Threat modeling: designing for security. Wiley, Hoboken, pp 61–78
25. CCITT (1991) ITU-T Rec. X.800 (03/91) Security architecture for Open Systems Interconnection for CCITT applications. ITU-T Rec. X.800. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.800-199103-1!!PDF-E&type=items
26. Zhenhua L, Weiwei W, Christo W, Jian C, Chen Q, Taeho J, Lan Z, Kebin L, Xiangyang L, Yunhao L (2017) FBS-radar: uncovering fake base stations at scale in the wild. <https://doi.org/10.14722/ndss.2017.23098>. <https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/fbs-radar-uncovering-fake-base-stations-scale-wild/>

27. Ney P, Smith I, Cadamuro G, Kohno T (2017) SeaGlass: enabling city-wide IMSI-catcher detection. *Proc Priv Enhanc Technol* 2017:39–56
28. Batalla JM, Andrukiewicz E, Gomez GP, Sapiecha P, Mavroustakis C, Mastorakis G, Zurek J, Imran M (2020) Security risk assessment for 5G networks: national perspective. *IEEE Wirel Commun* 27(4):16–22. <https://doi.org/10.1109/MWC.001.1900524>
29. Van Den Broek F, Verdult R, de Ruiter J (2015) Defeating IMSI catchers. In: *Proceedings of the 22Nd ACM SIGSAC conference on computer and communications security*. ACM, pp 340–351
30. 5G Americas – 5G security white paper (2019) <https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper-07-26-19-FINAL.pdf>
31. Chochliouros IP, Spiliopoulou AS, Kostopoulos A, Kourtis M-A, Lazaridis PI, Zaharis ZD, Prasad NR (2021) Security threat analysis of the 5G ESSENCE platform. *Wirel Pers Commun* 120(3):2409–2426
32. Barrett M (2018) Framework for improving critical infrastructure cybersecurity. NIST. <https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11>
33. Gao H, Zhang Y, Wan T, Zhang J, Duan H (2021) On evaluating delegated digital signing of broadcasting messages in 5G. In: *2021 IEEE global communications conference (GLOBECOM)*. pp 1–7. <https://doi.org/10.1109/GLOBECOM46510.2021.9685173>
34. Hussain SR, Echeverria M, Singla A, Chowdhury O, Bertino E (2019) WiSec '19: proceedings of the 12th conference on security and privacy in wireless and mobile networks. pp 1–11. <https://doi.org/10.1145/3317549.3323402>
35. "3GPP, Specification number TR 33.809 version 0.16.0, Study on 5G security enhancements against false base stations." Available at <https://portal.3gpp.org/>
36. Universal Mobile s Systems (UMTS); Radio Resource Control (RRC); Protocol specification (3GPP TS 25.331 version 13.2.0 Release 13) (2016) ETSI. https://www.etsi.org/deliver/etsi_ts/125300_125399/125331/13.02.00_60/ts_125331v130200p.pdf
37. Report on Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation (2020) Communication Security, Reliability, and Interoperability Council VII. <https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii>
38. Park S, Shaik A, Borgaonkar R, Martin A, Seifert J (2017) White-stingray: evaluating {IMSI} catchers detection applications. In: *11th USENIX workshop on offensive technologies (WOOT 17)*. <https://www.usenix.org/conference/woot17/workshop-program/presentation/park>
39. Olimid RF, Nencioni G (2020) 5G network slicing: a security overview. *IEEE Access* 8:99999–100009
40. CTIA. 5G Security Test Bed. Use cases and architecture. <https://5gsecuritytestbed.com/use-cases-and-architecture/>
41. Hussain SR, Echeverria M, Chowdhury O, Li N, Bertino E (2019) Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. <https://doi.org/10.14722/ndss.2019.23442>.
42. Singla A, Behnia R, Hussain SR, Yavuz A, Bertino E (2021) Look before you leap: secure connection bootstrapping for 5g networks to defend against fake base-stations. In: *Proceedings of the 2021 ACM Asia conference on computer and communications security, ser. ASIA CCS '21*. Association for Computing Machinery, New York, pp 501–515. <https://doi.org/10.1145/3433210.3453082>
43. Orlando D, Palamà I, Bartoletti S, Bianchi G, Melazzi NB (2021) Design and experimental assessment of detection schemes for air interface attacks in adverse scenarios. *IEEE Wirel Commun Lett* 10(9):1989–1993. <https://doi.org/10.1109/LWC.2021.3089636>
44. Ahmad F, Ahmad A, Hussain I, Uthansakul P, Khan S (2020) Cooperation based proactive caching in multi-tier cellular networks. *Appl Sci* 10(18):6145
45. Askar S (2021) SDN based 5G VANET: a review. <https://ideas.repec.org/a/aif/journal/v5y2021i6p131-147.html>, Available at SSRN: <https://ssrn.com/abstract=3963000>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.