Taming the Insecurity of Cellular Emergency Services (9-1-1): From Vulnerabilities to Secure Designs

Min-Yue Chen, Yiwen Hu, Guan-Hua Tu, *Member, IEEE*, Chi-Yu Li, *Senior Member, IEEE*, Sihan Wang, Jingwen Shi, Tian Xie, *Member, IEEE*, Ren-Chieh Hsu, Li Xiao, Chunyi Peng, *Senior Member, IEEE*, Zhaowei Tan, and Songwu Lu, *Fellow, IEEE*

***Abstract*— Cellular networks, vital for delivering emergency services, enable mobile users to dial emergency calls (e.g., 9-1-1 in the U.S.), which are forwarded to public safety answer points (PSAPs). Regulatory requirements allow anonymous user equipment (UE) without a SIM card or valid mobile subscription to access these services. However, supporting emergency services for anonymous UEs introduces different operations, expanding the attack surface of cellular infrastructure. In this study, we explore the insecurity of cellular emergency services, identifying six security vulnerabilities. These vulnerabilities can be exploited for free data service attacks against carriers and data DoS/overcharge and denial of cellular emergency service (DoCES) attacks against mobile users. Experimental validation in networks of three major U.S. carriers and two major Taiwan carriers demonstrates the global impact of our findings. Finally, we propose and prototype standard-compliant remedies to mitigate these vulnerabilities.**

***Index Terms*— Cellular networks, emergency services, 911 (9-1-1), security.**

I. Introduction

EMERGENCY services are a vital lifeline to people in emergency conditions. The globally-deployed cellular networks with ubiquitous coverage have been the most accessible channel to emergency users. To ensure the availability for emergency uses, cellular standards and regulatory authorities have stipulated requirements for the offering of cellular emergency services. Specifically, from the GSM Association (GSMA) standard [2], emergency services must be supported by mobile phones without SIM (Subscriber Identity Module) cards, which are indicated as anonymous user equipments (UEs), and be free of charge for mobile users. The 3GPP standard [3] requires emergency services to be provided with higher priority than other services. In the U.S., FCC [1] stipulates that cellular carriers have to deliver all wireless 911 calls to the public safety answering point (PSAP), which deals with emergency service requests, without respect to call validation results. Thus, cellular emergency services have become highly available and reliable for emergency uses.

The security research of emergency services has attracted much attention recently. Several attacks have been proposed to threaten emergency services, but they mainly focus on distributed denial-of-service (DDoS) attacks [4], [5], [6] against PSAPs (e.g., 911 call centers) rather than the cellular emergency services. Many solutions [7], [8], [9], [10], [11] have been thus introduced to address them. For the cellular emergency services, there have been also some proposed attacks [12], [13], [14] from the literature. Specifically, Lee et al. [12] and Hussain et al. [13] uncover that fabricated emergency alerts can be sent to victim UEs based on the abuse of cellular alert protocols and the hijacking of paging channels, respectively. Hou et al. [14] allow the adversary to not only bypass the victim UE's screen lock to dial any numbers on the emergency panel, but also block phone calls made to a set of numbers in a specific area, by providing the victim UE with a list of fake local emergency numbers via control-plane signaling messages.

The above attacks corresponding to the cellular emergency services mainly target the vulnerabilities on the UE side, but the security of the cellular infrastructure supporting emergency services still remains unexplored. Moreover, the cellular emergency services operate differently from conventional cellular services. Once any conventional designs are applied to the emergency services without careful reviews from a security perspective, security vulnerabilities may arise. Furthermore, allowing anonymous UEs to access the emergency services can increase attack surface of the cellular infrastructure. We are thus motivated to study whether the emergency services introduce any new security threats to mobile ecosystem or not.

Surprisingly, we discover six security vulnerabilities from operational cellular emergency services in the cellular networks of three major U.S. carriers and two Taiwan carriers: (V1) unverifiable emergency IP-CAN (IP Connectivity Access Network) session requests, (V2) inconsistent emergency

Manuscript received 3 April 2023; revised 19 December 2023; accepted 2 March 2024; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor S. M. Kim. Date of publication 26 March 2024; date of current version 20 August 2024. This work was supported in part by the National Science Foundation (NSF) under Grant CNS-2246050, Grant CNS-2246051, and Grant CNS-2321416; and in part by the National Science and Technology Council (NSTC) under Grant 110-2221-E-A49-031-MY3, Grant 112-2628-E-A49-016-MY3, Grant 112-2218-E-A49-021, Grant 112-2634-F-A49-001-MBK, and Grant 112-2218-E-A49-023. *(Min-Yue Chen and Yiwen Hu contributed equally to this work.) (Corresponding author: Guan-Hua Tu.)*

Min-Yue Chen, Yiwen Hu, Guan-Hua Tu, Sihan Wang, Jingwen Shi, Tian Xie, and Li Xiao are with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48823 USA (e-mail: chenmi33@msu.edu; huyiwen3@msu.edu; ghtu@msu.edu; wangsih3@msu.edu; shijingw@msu.edu; xietian1@msu.edu; lxiao@msu.edu).

Chi-Yu Li and Ren-Chieh Hsu are with the Department of Computer Science, National Yang Ming Chiao Tung University, Hsinchu 300093, Taiwan (e-mail: chiyuli@cs.nctu.edu.tw; kenny302.cs11@nycu.edu.tw).

Chunyi Peng is with the Department of Computer Science, Purdue University, West Lafayette, IN 47907 USA (e-mail: chunyi@purdue.edu).

Zhaowei Tan and Songwu Lu are with the Department of Computer Science, University of California at Los Angeles, Los Angeles, CA 90095 USA (e-mail: tan@cs.ucla.edu; slu@cs.ucla.edu).

Digital Object Identifier 10.1109/TNET.2024.3379292

TABLE I

A SUMMARY OF THE IDENTIFIED VULNERABILITIES AND ATTACKS OF OPERATIONAL CELLULAR EMERGENCY SERVICES

Category	Type	Vulnerability / Attack ID	Description	Leveraged vulnerabilities for attacks	Applicabilities								Victims' devices under attacks
					Carriers					Systems			
					US-I	US-II	US-III	TW-I	TW-II	4G	5G NSA	5G SA	
Vulnerabilities	Design defects	V1: Unverifiable emergency IP-CAN session requests (§4.1)	The establishment procedure of the emergency IP-CAN session cannot be protected and its initial request is naturally unverifiable.	-	✓	✗†	✗†	✓	✓	✓	✓σ	✗σ	-
		V2: Inconsistent emergency IP-CAN session support (§4.2)	The inconsistent support of the emergency IP-CAN session between the 3GPP and GSMA standards may fail the establishment.	-	✓	✗‡	✓	✗‡	✓	✓	✓σ	✓σ	
		V3: Improper cross-layer security binding (§4.3)	The network-layer security (i.e., IPSec) is bound to the application-layer security (i.e., SIP registration).	-	✓	✓	✓	✗♯	✗♯	✓	✓σ	✓σ	
		V4: Non-atomic emergency service initialization (§5.1)	UE can only establish an emergency IP-CAN session without doing IMS emergency registration and establishing an emergency session with PSAPs.	-	✓	✓	✓	✓	✓	✓	✓σ	✓σ	
		V5: Improper access control on emergency IP-CAN sessions (§5.2)	The emergency IP-CAN session is not restricted to deliver traffic to the IMS server based on given PCC rules.	-	✓	✓	✓	✓	✓	✓	✓σ	✓σ	
	Operational slips	V6: One-size-fits-all prioritization for emergency IP-CAN sessions (§5.3)	The emergency sessions requested by invalid UE IDs (i.e., IMEIs), which can escape from tracking, are not handled differently from those with valid IDs.	-	✓	✓	✓	✓	✓	✓	✗σ	✗σ	
Proof-of-concept Attacks	Denial of cellular emergency services	A1: UE blocking (§5.4)	Adversary prevents victims from establishing emergency IP-CAN sessions by tampering their requests with the UE capabilities that are not supported by carriers.	V2	✓	✗‡	✓	✗‡	✓	✓	✓σ	✓σ	Verified on all tested smartphones, including Samsung Galaxy S8/S10/S21, Google Pixel 3/5, and iPhone 13; the uncovered vulnerabilities are on the infrastructure side rather than the device side.
		A2: UE detaching(§5.4)	Adversary detaches the victim's emergency IP-CAN session, thereby preventing them from accessing all emergency services.	V1	✓	✗†	✗†	✓	✓	✓	✓σ	✗σ	
		A3: Call cancel (§5.4)	Adversary cancels the victim's emergency call attempt.	V3	✓	✓	✓	✗♯	✗♯	✓	✓σ	✓σ	
		A4: Call drop (§5.4)	Adversary terminates the victim's ongoing emergency call conversation with a PSAP.		✓	✓	✓	✗♯	✗♯	✓	✓σ	✓σ	
	Emergency IP-CAN session hijacking	A5: Free services (§5.4)	Adversary gains free data/voice/text services.	V4, V5, and V6; (V6 is for reducing the attack traceability, which is optional.)	✓	✓	✓	✓	✓	✓	✓σ	✓σ	
		A6: Data DoS/overcharge (§5.4)	Adversary bypasses carriers' firewall protection and injects spams to impose denial of service or excessive data bill on the victim.		✗∗	✓	✓	✗∗	✗∗	✓	✓σ	✓σ	
		A7: Remote scanning (§5.4)	Adversary can remotely scan network services/applications available on the victim's device and launch remote attacks based on reported vulnerabilities.		✗∗	✓	✓	✗∗	✗∗	✓	✓σ	✓σ	

†: US-II and US-III do not follow what 3GPP stipulates but adhere to FCC regulations [1] by accepting duplicate requests to maximize the availability of emergency services.
‡: US-II and TW-I implement the GSMA's emergency service requirements by supporting both IPv4 and IPv6 for emergency IP-CAN sessions, whereas US-I, US-III, and TW-II follow the 3GPP's by supporting IPv4-only or IPv6-only.
♯: There are two requirements for tested COTS phones to validate V3 due to ethical issues, but we cannot find any for TW-I and TW-II: (1) they shall be carrier-certified; (2) they can be customized to intercept IMS signaling messages.
σ: All the vulnerabilities validated in 4G networks, except for V6, can be also applied to 5G NSA networks since they share the same 4G core networks. More discussion is presented in §7.
∗: US-I, TW-I, and TW-II do not support the emergency-to-data-service (E2D) communication.

IP-CAN session support, (V3) improper cross-layer security binding, (V4) non-atomic emergency service initialization, (V5) improper access control on emergency IP-CAN sessions, and (V6) one-size-fits-all prioritization for emergency IP-CAN sessions.

We then develop two proof-of-concept attacks based on them. The first attack is the denial of cellular emergency service (DoCES) developed based on V1, V2, and V3; it allows the adversary to prevent mobile users from accessing cellular emergency services, and only two SDR (Software-defined Radio) platforms servicing as an attack UE and a sniffer are needed. This attack includes four variants, namely UE blocking, UE detaching, call cancel, and call drop. Our study reveals that all the five tested cellular networks are vulnerable to at least one of those four attack variants. The second attack developed based on V4, V5, and V6 includes three variants, namely free data/voice/text service, data DoS/overcharge, and remote scanning. Tables I summarizes the discovered vulnerabilities and their corresponding proof-of-concept attacks. All of them are experimentally confirmed in those five tested carriers, unless explicitly stated otherwise.

In all the experiments, we take a responsible manner that always prevents emergency calls or texts from being sent to PSAPs. To have a fine-grained control over the UE, we use the SDR platform for all the validation and evaluation experiments, except for the validation of V3, which requires Commercial Off-The-Shelf (COTS) phones. However, it is important to note that the vulnerabilities and attacks are not only limited to SDR-based UEs but also COTS UEs. The major reason is that they exist on the infrastructure side instead of the device.

There have been many studies exploring DoS, free service, and data overcharge attacks in cellular networks [13], [15], [16], [17], [18], [19], [20], [21], but the present study differs from them in the major aspect that it targets cellular emergency services, the operation and requirement of which are different from those of non-emergency services examined by those studies. For example, if an emergency device cannot successfully connect to the current serving network, it shall attempt to exploring all the other available cellular networks [22]; detaching an emergency device is based on not only the DETACH REQUEST, but also other criteria (e.g., no tracking area update is observed) [23], so it does not suffer from the DoS attacks based on forged DETACH REQUEST messages [19], [20], [21]. Moreover, the proposed free service and data overcharge attacks are launched by exploiting anonymous devices and free emergency services, and can be stealthier than the prior art. Table II presents a more detailed comparison.

Although we discover vulnerabilities on the infrastructure side, it does not mean that carriers should take the blame. After a careful analysis, we find that all identified vulnerabilities, except for V6, root in design defects of the cellular emergency standards, whereas V6 is an operational slip but exists for all the tested carriers. We further propose countermeasures including not only long-term security designs, which can address the vulnerabilities completely based on their root causes, but also standard-compliant short-term remedies, which mitigate the impact of the vulnerabilities. We finally evaluate the short-term remedies based on an emulation prototype.

II. CELLULAR EMERGENCY SERVICE PRIMER

Network architecture. Figure 1 depicts a 4G/5G network architecture supporting cellular emergency services. The emergency service requests (calls or texts) are initiated by the UE with or without a valid SIM card and finally routed to PSAPs, which are connected to the cellular network through the Internet (IP) or the public switched telephone network (PSTN). Within the cellular network, an emergency service request from the UE in turn traverses radio access network

TABLE II

COMPARISON OF PROPOSED ATTACKS AND PRIOR ART (DOS, FREE SERVICE, AND OVERCHARGE ATTACKS)

Attack	Features	Mirsky *et al.*[4]	Tsiatsikas *et al.*[6]	Tu *et al.*[17]	Yang *et al.*[19]	Bitsikas *et al.*[21]	Wang *et al.*[24]	Peng *et al.*[15]	Peng *et al.*[16]	Li *et al.*[18]	Our work
Denial of Service	DoS Type	Emergency services	Emergency services	Data	Mobile Connectivity	Mobile Connectivity	Voice and Text (IoT)	-	-	Voice	Emergency services
	Victim (Individual/PSAP)	PSAP	PSAP	Individuals	Individuals	Individuals	Individuals	-	-	Individuals	Individuals
	Protocols involved	SIP	SIP	SIP	NAS	NAS	SIP,TCP,NAS	-	-	SIP	NAS,SIP
	Exploiting emergency service specific vulnerabilities?‡	✗	✗	✗	✗	✗	✗	-	-	✗	○
	Need many attack devices?	○	○	✗	✗	✗	✗	-	-	✗	✗
	Shall interact with victim UEs?	✗	✗	○	○	○	○	-	-	○	✗
	Require service subscriptions?	○	○	○	✗	✗	○	-	-	○	✗
	Attack stealthiness	Low	Low	Low	High	High	Low	-	-	Low	High
Free services/Data overcharge	Victim (Individual/Infrastructure)	-	-	-	-	-	-	Individual	Both	Both	Both
	Service priority obtained	-	-	-	-	-	-	Normal	Normal	Higher	Highest
	Require service subscriptions?	-	-	-	-	-	-	○	○	○	✗
	Attack stealthiness	-	-	-	-	-	-	Low	Low	Low	High

‡: 3GPP standards stipulate different requirements (e.g., [22], [25]) for both mobile devices and the infrastructure to ensure the emergency service availability. Hence, traditional DoS attacks may not be applied to emergency service users.

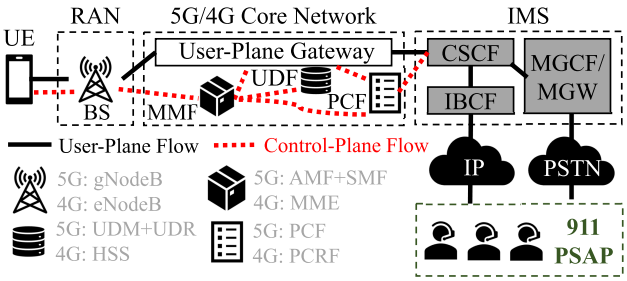


Fig. 1. 5G/4G emergency service architecture.

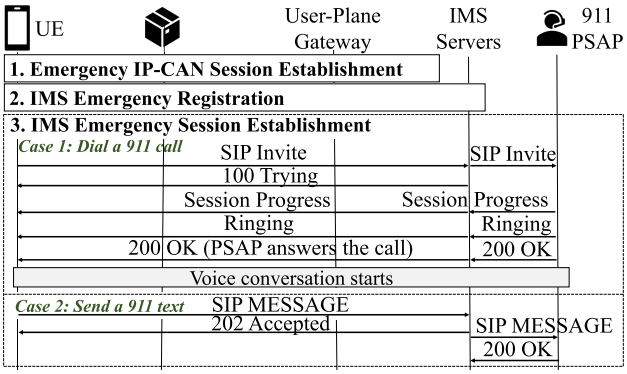


Fig. 2. IMS emergency service flow.

(RAN), core network, and IP Multimedia Subsystem (IMS). Notably, 5G and 4G use distinct network entities for similar network functions; for example, the RAN uses base stations (BSs) to offer radio access; the BS is referred to as gNodeB in 5G and eNodeB in 4G. For simplicity, we intentionally avoid 5G/4G telecom jargons which are shown at the left bottom of Figure 1, but use generic names of network entities throughout this paper.

In the core network, the user-plane gateway (UPG) in the user plane is to route user traffic packets from the UE to the IMS network and eventually to the external network (e.g., PSAPs); it provides the emergency IP connectivity for emergency services with the functionality of UE IP address assignment and IMS server selection. In the control plane, there are three main control functions: (1) Mobility Management Function (MMF) manages radio access, user mobility, authentication, resource reservation, and emergency IP connectivity establishment; (2) User Data Function (UDF) is responsible for storing user and service subscription information; (3) Policy Control Function (PCF) is in charge of generating billing policies, QoS parameters, routing control rules and so on. The PCF also creates policies for the emergency IP connectivity and provisions them to the UPG or the MMF to assist in the control for voice and text emergency services.

The IMS provides emergency voice and text services over IP for UEs. It consists of three key network entities: Call Session Control Function (CSCF, referred to as IMS server hereafter), Media Gateway Control Function/Media Gateway (MGCF/MGW), and Interconnect Border Control Function (IBCF). The IMS server is responsible for IMS service signaling, which runs Session Initiation Protocol (SIP) [26]. The MGCF/MGW is connected to the traditional PSTN, whereas the IBCF is a session border controller which is interconnected to other IP/IMS networks.

IMS emergency service flow. Figure 2 illustrates a service flow for the cellular emergency voice/text service. To establish an emergency session with the PSAP, the emergency UE needs to perform the following three actions. First, *Emergency IP-CAN Session Establishment* allows the UE to obtain the emergency IP connectivity to communicate with the IMS server; an IP-CAN session is identified by the UE's IP address and identity information. Second, *IMS Emergency Registration* [3], [27] has the IMS server and the UE authenticate with each other and enables the UE to register the emergency service. Third, *IMS Emergency Session Establishment* allows an emergency UE to establish an IMS emergency call/text session with the PSAP [3], [27], [28], [29] through the IMS server. The UE sends SIP INVITE and SIP MESSAGE messages to the IMS server for establishing emergency call and text sessions, respectively. Notably, anonymous UEs may be still allowed to access the IMS emergency service without being registered in accordance with local regulatory requirements [30].

III. THREAT MODEL AND METHODOLOGY

Threat model. In this work, the adversary uses an SDR-based UE to attack operational cellular networks and cellular UEs; the SDR-based UE does not have any SIM card installed, but can successfully connect to operational cellular networks. There are two attacks presented in Sections IV-D and V-D, respectively. In the former, the victims are the cellular users who connect to operational emergency services using anonymous UEs. In the latter, the victims are cellular operators and non-emergency cellular users. For these attacks, neither operational cellular networks nor victim UEs are compromised; it is assumed that the adversary adheres to all cryptographic assumptions (e.g., a ciphered message cannot be decrypted without the ciphering key).

Experimental methodology. We validate the presented vulnerabilities and attacks in the operational cellular networks of three U.S. carriers and two Taiwan carriers, which are

denoted as US-I, US-II, US-III, TW-I and TW-II, respectively. Two kinds of emergency UEs are tested in the experiment: (1) SDR-based UEs developed based on the srsRAN [31], which is an open-source 4G/5G software radio suite; and (2) commercial off-the-shelf (COTS) UEs, including Samsung Galaxy S8/S10/S21, Google Pixel 3/5, and Apple iPhone 13. To prevent emergency calls or texts from being accidentally sent to the cellular infrastructure during the experiment, we use the SDR-based UEs with a fine-grained control over network operations to validate vulnerabilities and execute proof-of-concept attacks, but employ the COTS UEs as victim devices in the proposed attacks.

Notably, all the vulnerabilities and attacks are validated in only 4G networks, but they can be also applied to 5G networks; more discussions are given in Section VII. There are two reasons for the limited validation. First, there is no any SDR-based platform that can serve as 5G UE to stably connect to operational 5G networks at the submission of this paper. While the latest srsRAN [31] offers the 5G UE support, it can be challenging to connect its emulated UE to operational 5G networks since it requires to connect the emulated UE and the base station using a physical cable, or to have a precise clock setting synchronized with the target 5G network.

Second, experimenting with COTS UEs on operational 5G networks is currently not feasible due to two issues. First, carriers in most areas support only the 5G NSA (Non-standalone) network [32], where the 5G UE will use VoLTE (Voice over LTE) rather than VoNR (Voice over New Radio) for voice services. This phenomenon is observed on all the tested carriers around our campus. Second, according to 3GPP standards [22], if a UE fails in an emergency call attempt, the 5G UE should automatically make a second attempt in other domains (e.g., circuit-switched (CS) fallback, allowing a UE to switch to 3G and access 3G CS voice services). The second attempt cannot be intercepted when generated by the cellular modem.

Vulnerability characterization. Vulnerabilities discovered in this study are classified into three categories, namely design defect, implementation flaw, and operational slip, based on the following guidelines. First, a design defect can persist even with correct implementation. Second, an implementation flaw is caused by incorrect implementation but with a correct design. Third, an operational slip comes from improper uses/configurations of available options on the infrastructure side but with correct design and implementation. Notably, we examine the designs stipulated by 3GPP and GSMA with stringent standards, since they are strictly followed by all carriers and device vendors. If the current 3GPP/GSMA standards have defects on safeguarding emergency services, all the corresponding carriers and mobile users will suffer from the same security threats, especially that additional non-standard security measures are not commonly observed (see Table I). Thus, we classify flawed or inadequate designs leading to security vulnerabilities as design defects.

Ethical consideration. We understand that some feasibility tests and attack evaluations may be detrimental to cellular network carriers and users. We thus proceed with this preliminary study in a responsible manner. Specifically, there were three approaches adopted in the experiment methodology to avoid adverse effects on the infrastructure and cellular user. First, all transmitted messages strictly adhere to 3GPP standards, including both control-plane signalings and IMS signalings, thereby preventing any abnormal behaviors on the infrastructure side. Their volume was comparable to that of normal cellular users. Second, all the victim devices in the experiments were our own devices, so no benign users were harmed. Third, we not only subscribed to *unlimited service plans* for all the experiment devices, but also minimized the resource consumption in the experiments. Specifically, we used SDR-based UEs with only a single antenna and a maximum transmission rate of only 3 Mbps, so the resource consumed by the experiments is much less than that offered by the unlimited plans. Moreover, all the vulnerability validation and attack experiments were conducted with small-scale tests based on the principle of identifying security issues in cellular emergency services rather than exacerbating damages. Notably, in all the experiments, no emergency calls or text messages were sent to operational IMS servers or PSAPs.

Responsible disclosure. We have reported the identified issues and the proposed solutions to U.S. carriers, as well as 3GPP and GSMA standard organizations, and received positive feedback from most of them. Specifically, two U.S. carriers classified the reported issues as **high-level security concerns**, and one of them offered **a security award** for the disclosure. For the 3GPP, after our disclosure, we had a meeting with the chair and key members of the TSG SA3 working group, which focuses on security and privacy in the 3GPP organization, and were suggested to submit our findings to their next regular SA3 meeting for further discussion. For the GSMA, we reported to its Coordinated Vulnerability Disclosure (CVD) program; currently, we are collaborating with them to validate and address the discovered vulnerabilities. Notably, since the discovered vulnerabilities have not been addressed for the tested carriers, their names are not disclosed in this paper.

IV. Denial of Cellular Emergency Service

For emergency use, UEs shall be always allowed to make emergency calls/texts through a cellular network no matter whether they have valid service subscriptions, according to the FCC 911 regulations [1]. It aims to maximize the availability of cellular emergency services in emergency conditions. It can also work for the UEs with valid subscriptions at the time when they are unable to access the emergency services from their home carrier networks; i.e., they are allowed to connect to other carrier networks for the emergency services. However, we discover that such anonymous emergency service access is not well protected, thereby leading to a potential security threat, DoCES. It is mainly rooted in three vulnerabilities: unverifiable emergency IP-CAN session requests (V1), inconsistent emergency IP-CAN session support (V2), and improper cross-layer security binding (V3). In the following, we first introduce each vulnerability and then present the DoCES attack with several variants.

A. V1: Unverifiable Emerg. IP-CAN Session Request

Since an anonymous UE that attempts to consume the emergency service of a cellular network does not have any security association with the network infrastructure, the establishment

procedure of the emergency IP-CAN session cannot be protected and its initial request is naturally unverifiable. When a duplicate establishment request is maliciously presented to the network, the network cannot differentiate it from the initial request; the impact depends on how the network deals with multiple emergency IP-CAN session requests from the same anonymous UE.

Surprisingly, the 4G and 5G standards take different approaches to handle the duplicate request. The 4G standard (i.e., TS24.301 [25]) stipulates that the MMF shall either reject it with a reason that multiple PDN connections for a given APN are not allowed, or accept it while implicitly detaching the existing established emergency IP-CAN session. On the other hand, the 5G standard (i.e., TS23.501 [33]) specifies that the duplicate request shall be always rejected.

As a result, the adversary may have a chance to prevent anonymous UEs from accessing the emergency services by sending fabricated emergency requests to the network before or after valid requests. Since the requests are not ciphered or integrity-protected, they can be easily fabricated based on the same device ID.

• **Experimental validation.** We validate this vulnerability using two SDR-based UEs: UE1 and UE2; neither of them has a SIM card installed. At the beginning, UE1 performs the establishment procedure of an emergency IP-CAN session with a tested 4G cellular network. Afterwards, UE2 sends the same cellular network a duplicate establishment request with the UE1's device ID, i.e., International Mobile Equipment Identity (IMEI). Once the UE1's emergency IP-CAN session is interrupted by the duplicate request, UE1 can be implicitly detached and then lose the IP connectivity. To detect whether this implicit detachment indeed happens, we make UE1 keep attempting to establish a new TCP connection with an assigned IMS server; the failure of any TCP connection establishment can indicate the connectivity loss.

We conduct this experiment with all the five carriers. The results show that the UE2's duplicate request can successfully interrupt the ongoing emergency IP-CAN session of the UE1 for three carriers, namely US-I, TW-I, and TW-II, but it does not work for the others, i.e., US-II and US-III. These two carriers accept the duplicate request without interrupting the ongoing one. However, it does not come without any reason. They may follow the FCC regulation of maximizing the availability of emergency services [1] that UEs are allowed to access emergency services through a cellular network without call validation. This implementation may pose another security vulnerability that the network resource may be abused by a large number of fabricated emergency IP-CAN session requests.

Note that with this vulnerability, the adversary can implicitly detach the victim UE, and the UE does not receive any notification from the network. This attack may not last for a long time with a single fabricated request; once UEs have certain mechanisms deployed with anomaly detection and recovery for emergency services, or emergency users manually request the services again. To make this attack persistent, the adversary may need to repeatedly generate fabricated requests, but it can still be stealthy with a low attack cost due to two reasons. First, this attack targets nearby emergency users only, rather than common mobile users, who are targeted by other cellular DoS attacks [4], [6], [17], [19]. Flooding the network is thus not needed. Second, in emergency situations, users may not have the opportunity for many attempts to call for help.

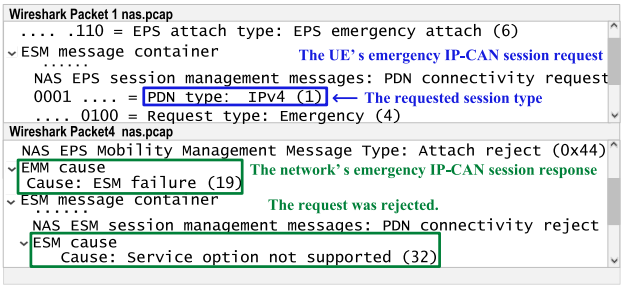


Fig. 3. US-III: the establishment request with IPv4 address type is rejected.

B. V2: Inconsistent Emerg. IP-CAN Session Support

Before establishing an emergency IP-CAN session, the UE and the MMF in the cellular network need to negotiate and then agree with a suite of required service options, including security algorithms, IP-CAN session types (e.g., IPv4 and IPv6), etc. If no consensus can be reached, the establishment can fail. However, the inconsistent support of the emergency IP-CAN session between the 3GPP and GSMA standards may lead to this situation. For example, the GSMA standard [28] requires the UE/MMF to support both IPv4 and IPv6 types of emergency IP-CAN sessions, whereas the 3GPP standard [23], [25] with a looser requirement allows the UE/MMF to support only one of those two types. Such inconsistency may lead to unexpected failures and be furthermore exploited by the adversary to launch UE blocking attacks.

• **Experimental validation.** We validate this vulnerability by using one SDR-based UE without any SIM card. The UE is configured to request the following three session types in turn, IPv4-only, IPv6-only, and IPv4v6, while performing the emergency IP-CAN session establishment for three times in each experiment run. The experiment is run for each of the tested five carriers.

The experimental results yield two findings. First, the UE can successfully establish an emergency IP-CAN session with each of the session types from US-II and TW-I, and obtain both IPv4 and IPv6 addresses when requested; it indicates that these two carriers adhere to the GSMA regulation. Second, the other three carriers, namely US-I, US-III, and TW-II, support only one session type; specifically, they support IPv6, IPv6, and IPv4, respectively. So, they follow the 3GPP regulation. Take US-III as an example. The UE can successfully establish an emergency IP-CAN session with the IPv6 address type, whereas the establishment request is rejected when the IPv4 address type is requested, as shown in Figure 3; notably, US-III supports both IPv4 and IPv6 for non-emergency IP-CAN sessions (e.g., accessing the Internet). The error is an ESM (EPS Session Management) failure with a cause, Service Option Not Supported [25]. The ESM failure is also observed from US-I and TW-II when an unsupported session type is requested, but with different causes, Insufficient Resources [25] and Service Option Not Supported, respectively.

• **Root cause and lessons.** The root cause of the V3 lies in the inconsistent regulations between 3GPP and GSMA;

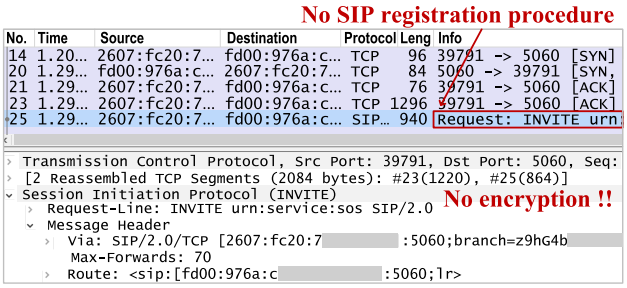


Fig. 4. An unencrypted emergent call message is observed for a COTS phone without any SIMs in the US-III network.

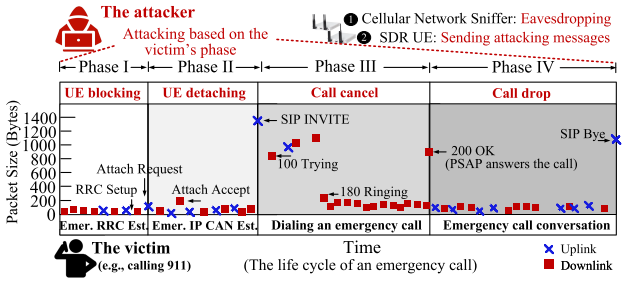


Fig. 5. Four-phase DoCES attack with four attack variants, namely UE blocking, UE detaching, call cancel, and call drop.

the IP-CAN session type may be merely one instance of them. Although the committees of both standards have their own rationalities, such as ensuring service availability for emergency users and complying with regulatory requirements, we believe that a closer collaboration between them is still necessary to develop consistent designs for cellular emergency services. Note that given this vulnerability and the absence of protection on the emergency attach request, the adversary can overshadow the requests sent from COTS UEs while altering their session types to be the ones that are not supported by the network, thereby causing the COTS UEs to be blocked from the emergency service. This exploitation can proceed no matter how each COTS UE sends the emergency request or whether the session types have different priorities.

C. V3: Improper Cross-Layer Security Binding

The UE with valid mobile subscription cannot establish IPSec security associations with the IMS server for the emergency services until it completes the IMS emergency registration [34], since the IPSec ciphering and integrity keys are derived from the registration procedure. It appears that the network-layer security (i.e., IPSec) is bound to the application-layer security (i.e., SIP registration). Therefore, when anonymous UEs are allowed to skip the IMS registration due to no security context shared with the core network, the IPSec security associations with the IMS server cannot be built. It can leave the IMS emergency sessions of anonymous UEs to be unprotected, thereby suffering from attacks.

• **Experimental validation.** We validate this vulnerability by observing whether anonymous UEs indeed have unprotected IMS emergency call sessions. In the experiment, COTS UEs and operational cellular networks are considered. In order to prevent any emergency call signaling messages from being routed to PSAPs, we develop a smartphone application, namely 911-CallBlocker, which discards all the SIP INVITE messages sent from the smartphone to the network infrastructure. After activating the 911-CallBlocker at the tested smartphone without any SIM card (i.e., anonymous UE), we dial 911 while using TCPDump to record all the packets. Notably, we find that the emergency calls of the TW-I/TW-II-certified phones without SIM cards are made based on the 3G CS call technology, instead of the IMS-based one; thus, the 911-CallBlocker cannot prevent them from being routed to PSAPs. To avoid the possible ethical issue, the validation experiment is conducted for only three US carriers.

For all the tested carriers, we obtain the same observations. First, the IMS emergency registration procedure is not performed. Second, the SIP INVITE messages are all sent in plain-text without ciphering protection. Figure 4 shows a representative trace from an anonymous UE connecting to the emergency service of the US-III network. Thus, the critical session information (e.g., call-ID and call tag) can be leaked to the adversary; it can thus allow the adversary to manipulate ongoing emergency call sessions.

• **Root cause and lessons.** The current cross-layer security design that binds the IPSec security association establishment to the IMS registration does not come without any reasons. It is necessary for non-emergency UEs to do the IMS registration; when the registration fails, no IMS services are provided to the UEs. That is, the IPSec is needed only when the registration succeeds; the cross-layer security binding is thus reasonable and can work properly.

However, this security binding should not be directly applied to the cellular emergency services without any modifications. Anonymous emergency UEs can skip the IMS registration but are still allowed to establish IMS emergency sessions. Without the registration, the improper security binding causes the IPSec security association establishment to be skipped. Such design is explicitly stipulated in the 3GPP/GSMA emergency service standards [2], [3], so it can happen in all standard-compliant mobile devices. It thus calls for a security mechanism that is decoupled from the IMS registration while protecting the emergency sessions.

D. Proof-of-Concept Attacks

We exploit the aforementioned three vulnerabilities to execute the DoCES attack against anonymous UEs. It consists of four attack variants, which just cover the entire life cycle of an emergency call, as depicted in Figure 5: (1) *UE Blocking*, which disrupts the establishment of an emergency IP-CAN session; (2) *UE Detaching*, which terminates an established emergency IP-CAN session from a UE; (3) *Call Cancel*, which cancels an emergency call that has not yet been answered by the PSAP; and (4) *Call Drop*, which terminates an emergency call that has been answered by the PSAP. Notably, according to this comprehensive attack covering the major four phases of an emergency call, it can make each emergency UE suffer from at least one of those four attack variants, as summarized in Table I.

Launching this attack requires two device components: (1) a cellular network sniffer, which eavesdrops on the communication of nearby UEs and identifies attackable UEs (i.e., anonymous UEs initiating cellular emergency services), and (2) an SDR-based UE, which sends attack messages to the cellular networks where victim UEs are. Notably, this attack does not require the adversary to deploy rouge cellular infrastructure

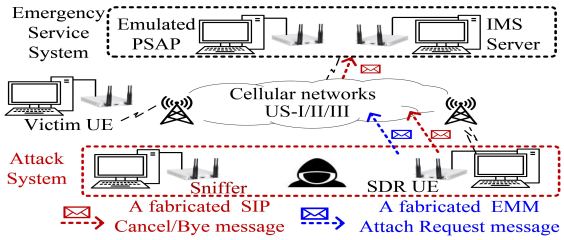


Fig. 6. An emulation testbed for DoCES attack evaluation.

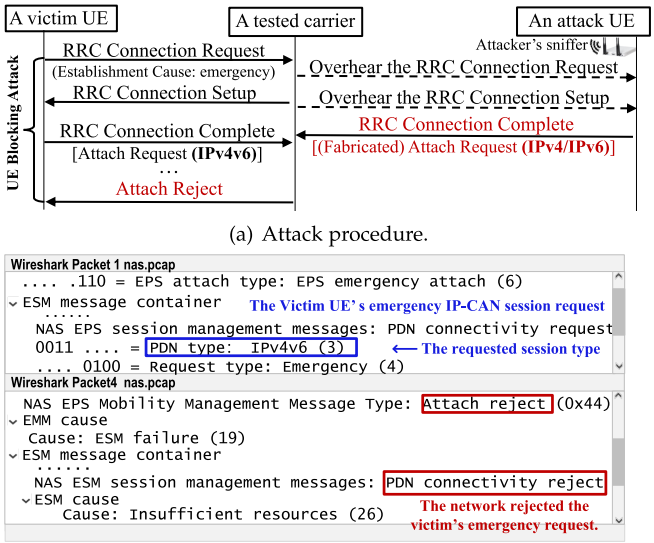
near victims. Moreover, the adversary does not need to be at the scene of victims; instead, the sniffer, together with the attack UE, can be deployed at any location where the victims' communication can be eavesdropped on.

We next present the experimental setting and then elaborate on each attack variant. Note that the following evaluation results demonstrate that the adversary could prevent mobile users from accessing emergency services in certain settings, but these should not be interpreted as common failures of operational cellular systems.

• **Experimental setting.** We evaluate the DoCES attack with four variants on an emulation testbed deployed over the networks of the three U.S. carriers. Using the emulation testbed is to prevent any emergency calls from being sent to PSAPs. Figure 6 shows the testbed with three major parts: (1) the emergency service system, (2) the attack system, and (3) the victim UE. The emergency service system includes an IMS server developed based on the open-source LinPhone VoIP SIP server [35] and an emulated IP-based PSAP; both of these two servers are implemented on SDR-based UEs connecting to the tested cellular network via emergency IP-CAN sessions. The attack system consists of a cellular network sniffer, and an SDR-based attack UE with the LinPhone VoIP SIP client and cellular signal overshadowing functions installed. The cellular network sniffer was developed on top of srsRAN [31] and Ltesniffer [36] for downlink and uplink sniffer functions, respectively. It is also enabled to decode control-plane signaling messages that carry information elements of emergency services, e.g., the establishment cause of "emergency" in the RRC Connection Request message, and the EPS attach type of "emergency attach" in the Attach Request message. The attack UE connects to the tested cellular network with an emergency IP-CAN session. The victim UE is built based on the same SDR-based UE as the one in the attack system.

The emulated IMS server, emulated IP-based PSAP, attack UE, and victim UE were built on top of four SDR-based UEs connected to the tested carrier network with established emergency IP-CAN sessions. Their communications are facilitated through the carrier's emergency-to-emergency (E2E) communication, exploiting the vulnerability V5, allowing two anonymous UEs to communicate directly using established emergency IP-CAN sessions (more details are elaborated in § V-B).

• **Phase 1: UE blocking attack.** We exploit vulnerability V2 to devise the UE blocking attack that can cause the victim UE's emergency IP-CAN session requests to be rejected at the early stage. To launch this attack, the adversary needs to know the unsupported type of the emergency IP-CAN session for the target carrier network, and then overshadows the victim's Attach Request message using a fabricated message that



(a) Attack procedure.

(b) The victim UE's emergency IP-CAN session request with the requested IPv4v6 type is rejected by US-I after a fabricated request with a requested type IPv4 is sent by the attack UE.

Fig. 7. UE blocking attack.

requests an unsupported session type. Figure 7(a) illustrates the procedure of this attack. To establish an emergency IP-CAN session, the victim UE initially sets up a RRC (Radio Resource Control [37]) connection with the infrastructure by sending a message of RRC Connection Request, where the establishment cause is set to "emergency". Such emergency connection message can be identified by the adversary using a cellular network sniffer and then its sender is considered as a potential victim UE.

To launch this attack, the adversary sends the fabricated Attach Request message, especially with a stronger signal than the victim's for overshadowing their message, soon after overhearing the base station's RRC Connection Setup message. Specifically, only two parameters, namely C-RNTI (Cell Radio Network Temporary Identifier) and the assigned uplink channel information, from the RRC Connection Setup message are needed. Notably, no information is needed from the victim UE's genuine Attach Request message, especially for the device ID (i.e., IMEI). The reason is that the Attach Reject message replied by the infrastructure does not include the device ID; it prevents the victim UE from being aware that the attach rejection is caused by the fabricated message with a forged device ID, and then the victim UE accepts it without any warning.

To overshadow the victim's Attach Request message in the uplink direction and avoid accidental interference with other benign users, the adversary monitors the RRC connection messages from nearby UEs to collect their assigned RNTIs (from RRC Connection Setup), then obtains each observed UE's DCI (Downlink Control Information) based on its RNTI by monitoring the Physical Downlink Control Channel (PDCCH), and finally gets the UE's uplink channel assignment information about when and how the Attach Request message will be delivered over the Physical Uplink Shared Channel (PUSCH). Afterwards, for each victim UE, the attack UE can overshadow its Attach Request message with 3dB [19] signal stronger by modifying the transmission gain (`tx_gain`).

We initially evaluate this attack with 10 experiment runs for the UE-I network by making the attack UE send the same Attach Request message as the victim does for the overshadowing. While the victim UE fails to establish an emergency IP-CAN session for all the runs, it is observed that not all the failures are caused by the UE blocking attack but some of them are made by the UE detaching attack, which will be presented in the next section. The reason why the UE blocking attack does not work in some cases is that the fabricated Attach Request message is not sent timely and arrives at the infrastructure later than the genuine one so that the victim UE's message is not successfully overshadowed. Given the same IMEI given in both the genuine and fabricated messages, the delayed fabricated message is seen as a duplicate Attach Request message by the infrastructure. It causes the victim UE to suffer from the UE detaching attack, according to vulnerability V1.

To assess the effectiveness of the UE blocking attack, we further conduct another experiment in the US-I network by configuring a different IMEI in the fabricated Attach Request message. The result shows that 8 out of 30 attack attempts are successful with a success rate of 26.6%; Figure 7(b) shows an example of the successful attack. The low success rate stems from the fact that the fabricated message is not always transmitted promptly. It is because with the present testbed, the sniffer needs to collaborate with the attack UE to execute the attack and this interaction may delay the message delivery. Moreover, it is observed from the experiment that the time delay from receiving the RRC Connection Setup message on the victim UE to starting to send the Attach Request message is 53∼307 ms, whereas that is 69∼291 ms on the adversary. To enhance the attack success rate, the adversary can integrate the sniffer with the attack UE to reduce their coordination time and then expedite the delivery of fabricated messages. We leave this improvement to the future work. Although this attack may fail, the other proposed attacks can cover the failure and still prevent the victim UE from accessing emergency services.

• **Phase 2: UE detaching attack.** We next devise an attack that implicitly detaches emergency UEs based on vulnerability V1. Beyond the validation experiment that generates duplicate establishment requests, the attack requires to monitor control-plane messages, identify potential victim UEs, and obtain their IMEIs using a sniffer at run time.

Figure 8(a) illustrates the attack procedure. While the victim UE nearby the sniffer performs the EMM Attach procedure [25] to establish an emergency IP-CAN session with the cellular network, the sniffer in the attack system can overhear the EMM Attach Accept message, which indicates the finish of the session establishment, from the network. Afterwards, the attack UE can fabricate a duplicate Attach Request message using the victim UE's IMEI. Once the attack succeeds, the network implicitly detaches the victim UE while replying Attach Accept to the attack UE.

Note that although some previous works (e.g., [20]) have shown that a fabricated Detach Request message can be used to launch an attack of UE detachment, it may not be applied to emergency UEs, which have different designs from normal UEs in 3GPP standards due to the important support of emergency services. Specifically, the Detach Request

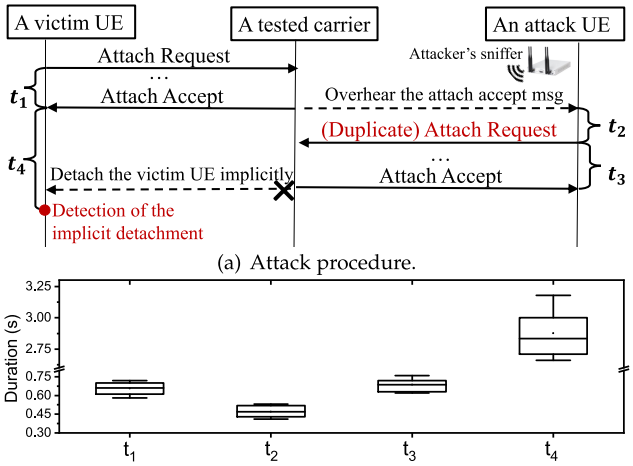


Fig. 8. UE detaching attack.

message cannot be a single criterion to detach emergency UEs, but additional criteria from them need to be considered, e.g., they are still performing periodic tracking area updates or responding to paging [25]. Moreover, if emergency UEs cannot successfully connect to one cellular network, e.g., receiving the Detach Request message, they are required to explore to connect all the other available cellular networks [22]. However, the present attack causes the network to detach emergency UEs without considering additional criteria and is also implicit so that the UEs will not explore more available networks.

We evaluate this attack by conducting the attack procedure for 10 runs in the US-I network. The evaluation result shows that the victim UE can be implicitly detached in all the experiment runs; that is, it does not receive any notification from the network after being detached. Figure 8(b) shows the measured values of the time durations in the attack procedure. It is observed that the attacker can successfully detach the victim UE within 2.66∼3.18 s (i.e., t4) right after the emergency session is established.

• **Phase 3: Call cancel attack.** We then devise an attack that cancels the victim UE's emergency call attempt by exploiting vulnerability V3. In this attack, a fabricated SIP Cancel message is sent to the IMS server as soon as a SIP 100 Trying message sent to the victim is overheard (see Figure 2). After receiving the fabricated message, the IMS cancels the victim UE's call attempt by replying with a message of Request Terminated. Notably, to fabricate a valid SIP Cancel message, the adversary can obtain required session information including Call-ID, tag@From, and branch@Via [26], from the SIP 100 Trying message.

In the evaluation, the victim UE initiates a SIP call to the emulated PSAP; meanwhile, the attack UE launches the call cancel attack. The result shows that the victim UE receives a message of the 487 Request terminated from the IMS server; it indicates that the victim UE's emergency call is successfully canceled. Figure 9 shows a representative trace of this successful attack result in the US-I network; the same results are observed in all the three carriers.

• **Phase 4: Call drop attack.** The attacker can also exploit V3 to launch the call drop attack by sending a forged SIP Bye message after overhearing the SIP 200 OK message.

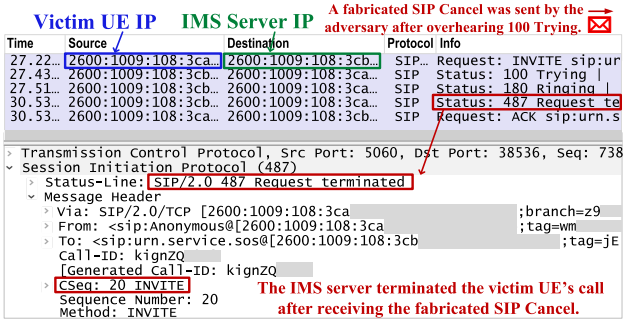


Fig. 9. An emergency call is terminated by a fabricated SIP CANCEL message sent by the adversary.

It can cause an ongoing emergency call of the victim UE to be terminated. The evaluation result shows that this attack can be successfully performed for all the tested carriers.

V. Emergency IP-CAN Session Hijacking

The emergency service request can be issued from anonymous UEs and is free of charge for cellular users due to its emergency purpose [2], [3], [25], [38]. However, we have discovered that no additional security mechanisms are introduced to protect the emergency IP-CAN session. Thus, it could be arbitrarily established and then hijacked to launch various attacks, such as free data/voice/text service and DoS attacks. In the following, we first introduce three discovered vulnerabilities: non-atomic cellular emergency service initialization (V4), improper access control on emergency IP-CAN sessions (V5), and one-size-fits-all prioritization for emergency IP-CAN sessions (V6), and then present three proof-of-concept attacks.

A. V4: Non-Atomic Emergency Service Initialization

The cellular emergency service initialization is triggered right after a user submits an emergency call/text request on the UE. It consists of three actions, as described in Section II. For the timely delivery of an emergency service request, the initialization is expected to have the atomic property where those three steps are executed continuously without being decoupled or being interleaved with other UE actions. Specifically, the UE can only do IMS emergency registration or/and establish an emergency session with a PSAP whenever an emergency IP-CAN session, which is built for the exclusive use, is established. After the initialization, the emergency service request can reach the PSAP.

However, the cellular network infrastructure may not fulfill this property, since no related security mechanisms are stipulated in the 3GPP/GSMA standards [2], [3], [25], [38]. It may allow an adversary to establish an emergency IP-CAN session to abuse while skipping the last two initialization actions. Without the IMS emergency registration or/and session establishment, the IMS server and the PSAP cannot be aware of the abuse. More threateningly, the emergency IP connectivity can be requested by anonymous UEs, so it is challenging to trace back to the adversary.

• **Experimental validation.** We validate this vulnerability by developing an SDR-based UE using the srsRAN [31]. The UE without any SIM card installed is made to perform the emergency IP-CAN session establishment with five carriers, but skip the last two initialization actions and transmit no packets to the infrastructure.

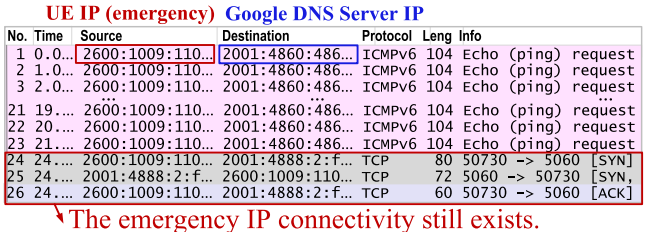


Fig. 10. The UE can keep the emergency IP-CAN session active by periodically sending packets out.

We have two findings. First, the anonymous UE can successfully obtain an IP address for the established emergency IP connectivity from each carrier. Second, the emergency IP connectivity can be interrupted by the infrastructure (i.e., implicit UE detachment), after an inactivity time interval. Based on our experimental results, the inactivity intervals taken by US-I, US-II, US-III, and TW-I are 10s, 5s, 3s, and 30s, respectively, whereas for TW-II, the connectivity can last for longer than 60s without any interruption.

Nevertheless, considering such cases, we discover that the UE can prevent the interruption by sending packets out periodically; moreover, the destination is not necessarily to be the IMS server. As shown in Figure 10, the UE can keep the emergency IP connectivity active by sending ICMP packets to the Google DNS server; notably, no ICMP response packets are received by the UE, but the major purpose that the emergency IP connectivity appears to be in use with those outgoing packets has been achieved.

• **Root cause and lessons.** This vulnerability can be attributed to a design defect that the cellular infrastructure does not enforce the atomicity of the cellular emergency service initialization. This design defect appears when the emergency service migrates from the 2G/3G CS system to the 4G/5G packet-switched (PS) one without a careful security review. In the CS system, the emergency service initialization is completely taken charge of by a single network entity, MSC (Mobile Switch Center [39]), so the atomicity can be easily ensured by the MSC.

However, the emergency service becomes to be IMS-based in the PS system and the initialization is decomposed into two parts, the emergency IP-CAN session establishment and the IMS emergency registration/session establishment, which are managed by the MMF and the IMS server, respectively. Without an additional security mechanism stipulated to protect the emergency service initialization among them, they do not cooperate to ensure the atomicity. Specifically, the MMF can know which UEs obtain the emergency IP connectivity, but have no information about if those UEs continue to proceed with the IMS emergency service operation; on the other hand, the IMS server does not know which UEs have gained the emergency IP connectivity. Thus, it calls for a concerted solution to ensure the atomicity.

B. V5: Improper Access Control

The access control on emergency IP-CAN sessions is fulfilled by the PCF to provision PCC (Policy and Charging Control) rules for MMFs or UPGs [40], [41]. For an IP-CAN session, each PCC rule identifies a set of service flows

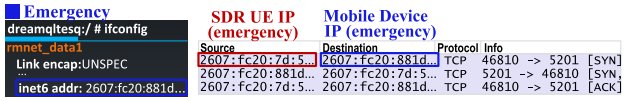


Fig. 11. An SDR-based UE communicates with another UE using their emergency IP-CAN sessions (M2M) in US-III; the former's emergency-service interface is shown in the left figure.

based on the 5-tuple information (i.e., source/destination IP addresses, source/data port numbers, and transport protocol ID) and the corresponding service flows are managed based on an associated policy control setting, including precedence, QoS parameters (e.g., maximum uplink/downlink throughput), gate status (allowed or disallowed), etc. Thus, for the exclusive use of the emergency service, the emergency IP-CAN session should be restricted to deliver traffic to the IMS server based on given PCC rules. However, the cellular network standards [40], [41] do not stipulate such a regulation or give the PCF the information of the IMS server assigned to emergency UEs during their emergency IP-CAN session establishment, so the restriction may be ignored. Without the access control, adversaries may abuse emergency IP-CAN sessions to access the Internet or other cellular devices.

• **Experimental validation.** We conduct an experiment to examine whether the emergency IP-CAN session is restricted to only service flows between the UE and the IMS server. Two types of service flows which do not reach the IMS server are tested for five tested carriers: mobile-to-Internet (M2I) and mobile-to-mobile (M2M), which represent the communication between the UE using the emergency IP-CAN session and Internet hosts, and the communication between that emergency UE and another tested UE, respectively. For the M2M case, we further test three kinds of IP-CAN sessions that may be used by the tested UE: (1) the data-service IP-CAN for Internet access, (2) the IP-CAN of the IMS call signaling, and (3) the emergency IP-CAN. Notably, the UE creates a network interface for each IP-CAN session, e.g., the interface of the emergency IP-CAN session is shown in Figure 11.

In this experiment, we still use the SDR-based UE without SIM card to obtain an emergency IP-CAN session from each tested carrier network. For the M2I case, the UE is tested to communicate with the Google DNS server using the emergency IP-CAN. In the M2M case, two phones are connected to the tested carrier network; one phone with a valid SIM card can obtain two IP-CAN sessions for *data service* and *IMS signaling*, respectively, whereas the other phone without SIM card can obtain an emergency IP-CAN session. Four phone models, including Samsung Galaxy S8/S10/S21 and Google Pixel 3/5, are tested. The SDR-based UE is tested to communicate with those two phones through each of those three different IP-CAN sessions. The tested communication is based on the ICMP echo request/reply and the TCP three-way handshake.

Table III summarizes the result for all the five tested carriers. We have two observations. First, the M2I communication based on the emergency IP-CAN session is forbidden for all the carriers. Second, all the carriers allow the emergency IP-CAN session to have the M2M communication, but the allowable cases vary with carriers. Specifically, the US-III allows the communication for all the three different cases, where the emergency-to-emergency (E2E) communication is shown in Figure 11, whereas US-I permits only the E2E communication; US-II permits two communication types, namely E2E and emergency-to-data-service (E2D); TW-I and TW-II allow E2E and emergency-to-IMS-signaling (E2IMS). In sum, all the tested carriers have improper access control on the emergency IP-CAN session.

TABLE III
ACCESS CONTROL ON EMERGENCY IP-CAN SESSIONS FOR CARRIERS

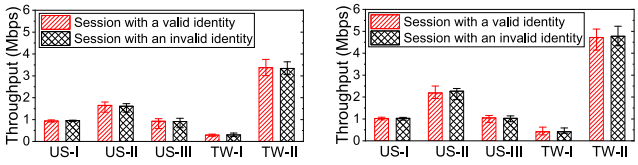
Carriers	Mobile-to-Internet	Mobile-to-Mobile		
		E2E	E2IMS	E2D
US-I	X	O	X	X
US-II	X	O	X	O
US-III	X	O	O	O
TW-I	X	O	O	X
TW-II	X	O	O	X

• **Root cause and lessons.** The root cause of this vulnerability is a lack of an access control mechanism on the emergency IP-CAN session in the standards, so it can be attributed to a design defect. At the first glance, designing the access control mechanism is straightforward, since the only requirement is to install the PCC rules that can restrict the emergency IP-CAN to the IMS server only. Specifically, during the emergency IP-CAN session establishment, the MMF or the UPG should provide the PCF with the IMS server information and then the PCF produces the corresponding PCC rules for the installation.

However, the real situation is much more complex; the IMS server may not be always determined during the emergency IP-CAN establishment. It can be also assigned based on the DNS or DHCP services after the UE obtains the emergency IP-CAN [27]. In this case, the PCC rules cannot be produced and installed until the IMS emergency registration proceeds. According to the 3GPP standard [42], during the registration, the IMS server needs to notify the PCF after receiving the UE's SIP Register message; however, the adversary is allowed to skip the registration and bypass this notification, leading to improper access control for emergency services. Thus, additional security measures are required beyond merely installing PCC rules to safeguard emergency services from attacks.

C. V6: One-size-fits-all Prioritization for Emergency IP-CAN Sessions

To ensure the quality of cellular emergency services, the infrastructure is designed to prioritize emergency IP-CAN sessions according to the 3GPP standard [3]. However, this does not imply that all the requested emergency sessions shall be prioritized indiscriminately; specifically, the emergency sessions requested by invalid UE IDs (i.e., IMEIs), which can escape from tracking, are not handled differently from those with valid IDs. Such the one-size-fits-all prioritization approach may be exploited by the adversary to grab prioritized resource by abusing emergency services with invalid IDs. Notably, a valid IMEI is composed of three parts: (1) Type Allocation Code (TAC), a unique 8-digit code assigned by GSMA to identify the device model and manufacturer; (2) Serial Number (SNR), a 6-digit code assigned by the device manufacturer to identify each equipment within the TAC area; (3) Check Digit (CD), a single digit used to avoid manual transmission errors [43]. The TAC and the SNR form a globally unique ID for being identified.



(a) Uplink Throughput (b) Downlink Throughput

Fig. 12. The 25th/50th/75th percentiles of uplink and downlink throughput on emergency IP-CAN sessions with valid/invalid user identity.

• **Experimental validation.** We validate this vulnerability by checking whether the emergency IP-CAN session requested by an invalid IMEI can be built successfully and then receive the network resource comparable to that requested by a valid IMEI. This experiment consists of three steps. First, we generate an invalid IMEI (i.e., 300000000000000) and confirm its invalidity using many online IMEI checkers [44], [45], including those provided by carriers [46], [47]. Second, an SDR-based UE is employed to establish an emergency IP-CAN session using the generated invalid IMEI and a valid IMEI, respectively. Third, we measure the uplink/downlink throughput of those two different emergency IP-CAN sessions using IPerf with 10 runs each.

Figure 12 shows the throughput statistics for those two kinds of emergency sessions from each of the five tested carriers. We observe that for each carrier, all the emergency IP-CAN sessions have comparable uplink and downlink throughput performance. For instance, in the US-II network, the median uplink/downlink throughput for the emergency IP-CAN sessions with the invalid IMEI is 1.61 Mbps/2.26 Mbps, which is similar to 1.65 Mbps/2.19 Mbps obtained from those with a valid IMEI. These results confirm that the network infrastructure fails to differentiate the priorities of the emergency sessions; no noticeable restrictions are imposed on those with invalid UE IDs.

• **Root cause and lessons.** No resource differentiation on emergency services requested from valid and invalid IMEIs seems reasonable from the regulation perspective, since the FCC mandates that carriers must forward all wireless 911 calls to the PSAP, regardless of call validation results [1]. However, without enforcing the security principle of least privilege, where the resource assigned to potentially malicious UEs with invalid IMEIs should be constrained, this feature becomes a vulnerability from the security perspective. It leaves a larger attack surface for the adversary to abuse the emergency resource. Moreover, the FCC does not prevent carriers from imposing restrictions (e.g., offering voice call services with basic quality) on suspicious or malicious emergency UEs.

D. Proof-of-Concept Attacks

We devise three proof-of-concept attacks, namely free data/voice/text services, data DoS/overcharge, and remote scanning, using the vulnerabilities presented in this section. The cost of these attacks is to have an SDR platform compatible with 4G/5G networks; it serves as an M2I gateway that provides the free services over an emergency IP-CAN session, and an attack UE, for the first and last two attacks, respectively. We next elaborate on the details of each attack.

• **Free data/voice/text service attack.** The adversary can exploit the E2E communication, the delivered data of which are free of charge, to obtain free data/voice/text service.

Fig. 13. Exploiting the E2E communication to enable free data service using a Mobile-to-Internet gateway.

To achieve it, an M2I gateway needs to be deployed to forward data between the UE with an emergency IP-CAN session and the Internet, as shown in Figure 13. At the gateway, the SDR UE connects to the cellular infrastructure using an emergency IP-CAN session and receives/transmits all data to/from the other UEs through the free E2E communication, the Wi-Fi router connects to the Internet, and the computer forwards data between the SDR UE and the router.

We next evaluate the data service over that free-of-charge communication channel for all the three UE carriers. We use IPerf to assess its throughput, jitter, and packet loss rate with 20 runs each. The result shows that the median values of the uplink/downlink throughput range from 0.83 Mbps to 2.17 Mbps, all the jitter values are smaller than 30 ms, and all the packet loss rates are smaller than 1%. Note that the measured throughput is constrained by the SDR-based UE, which supports only a single antenna [48] with the current srsRAN version (20.10), so the adversary may increase the throughput using more advanced UEs.

We further use Google Voice over the free-of-charge channel to have voice and text services at no cost [49]. We assess the voice and text services by considering the call setup time and the text delivery time, respectively. By comparing the attack with a normal case, where the UE with a valid mobile service subscription uses the Google voice, it is seen that they have comparable performance. Specifically, they have the ranges of the call setup time, 0.86s∼3.87s and 0.47s∼2.58s, respectively, whereas those of the text delivery time are 2.39s∼6.27s and 1.87s∼5.46s, respectively.

• **Data DoS/overcharge attack.** The adversary can use the E2D communication to launch a data DoS/overcharge attack against cellular users. The spamming data can be generated from the attack UE's emergency interface at no cost and sent to a victim UE's data interface, thereby consuming the data quota of the victim's data service plan. It can cause the victim UE to suffer from an overcharged bill or the data DoS, where its subscribed data quota is exhausted. In particular, massive cellular IoT devices (e.g., water meters) are more vulnerable to this attack, since they usually have only a small amount of data quota with high unit rates (e.g., $0.99 per MB) in common IoT service plans. The prerequisite of this attack is to obtain the IP addresses of potential victim UEs. To target cellular IoT devices, the adversary can remotely identify their IP addresses [24], whereas s(he) can also attack specific UEs and steal the IP information by installing the malware or launching phishing attacks.

We validate the feasibility of this DoS/overcharge attack for both US-II and US-III, as they are the only two carriers that enable E2D communications among the tested ones. The evaluation involves four distinct victim UEs: Samsung Galaxy S8/S10 and Google Pixel 3/5. Each validation test consists of the following three steps. First, we obtain the latest data usage amount three days after powering off the victim UE. Second, after powering on it, we use the attack UE to send

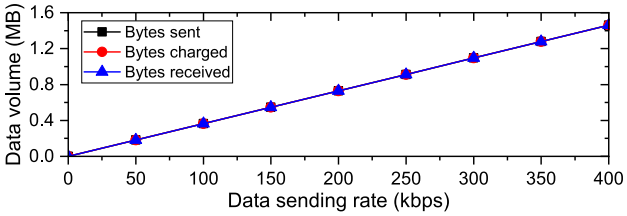


Fig. 14. The volume of spamming data which are sent, received, and charged from data DoS/overcharge attack against a victim in US-III.

spamming data from its emergency interface to the victim UE's data interface. The spamming packets are the UDP datagrams created by the attack UE using a randomly selected UDP destination port number and the victim UE's IP address. The victim UE may reply ICMP Port Unreachable error message to the attack UE. Third, we power off the victim UE and keep it for three days; afterwards, we query the latest data usage amount again.

We show the evaluation result of US-III only, since the attack becomes unavailable for US-II during the evaluation experiment[1]. In the experiment, we vary spamming rates from 50 Kbps to 400 Kbps and for each test, the spamming attack lasts for 30s. Figure 14 shows the volume of spamming data which are sent, received, and charged in the US-III network. It can be seen that the victim is charged for all the spamming data.

• **Remote scanning attack.** The E2D communication also allows the adversary to scan victim UEs remotely for vulnerability discovery while bypassing cellular network firewalls. Specifically, the adversary can send probing packets (e.g., TCP SYN) to various port numbers of the victim UEs, and then determine which ports are open and which services are running at each victim UE based on the responses (e.g., TCP SYN+ACK or ICMP Port Unreachable) corresponding to the probing packets. The collected information of each UE is then used to query the CVE (Common Vulnerabilities and Exposures) database to examine whether the UE has any potential security vulnerabilities.

We validate this attack by using Nmap, which is an open-source utility for network discovery and security auditing, to send the probing packets from the attack UE's emergency interface to the victim UE's data interface. This validation test is conducted in US-II and US-III, both of which allow the E2D communication, with three victim UEs, including Samsung Galaxy S8, Google Pixel 5, and iPhone 13. We discover that to scan 5,000 ports, the attack UE needs to send and receive 322.8 KB and 306.1 KB data, respectively, and it takes around 13s.

VI. Countermeasures

All the discovered vulnerabilities, except for the vulnerability V6, root in design defects of the cellular emergency services stipulated in the 3GPP/GSMA standards. However, addressing them based on their root causes to have a secure design may not be practical in the short term, since the required design changes lie in some core network functions and even security functions of billions of UEs. It cannot be achieved without significant effort or a long time. Therefore, in the following, we first present long-term secure designs that can address the vulnerabilities, together with their expected overhead, and then introduce four short-term, yet low-overhead, remedies that can mitigate those vulnerabilities.

A. Long-Term Security Designs

We present the design change required for those five vulnerabilities rooted in the design defects of cellular emergency service standards below.

• **V1 (unverifiable emergency IP-CAN session requests).** It calls for a device-level authentication mechanism, which can differentiate emergency IP-CAN session requests from different UEs, even when the UEs do not have SIM cards. Notably, this remedy does not aim to prevent anonymous UEs from accessing emergency services but to impose a proper restriction on establishing multiple emergency IP-CAN sessions. It may require each UE to have device credentials (e.g., certificates). However, upgrading each UE to install a carrier-certified certificate is not easy and cannot be done quickly, as it cannot be automated with a software patch due to security concerns.

• **V2 (inconsistent emergency IP-CAN session support).** Resolving such inconsistencies requires collaborative efforts from 3GPP and GSMA to align their specifications for supporting emergency services so that the network carriers and device manufactures can adhere to the same requirement. They need to handle all the inconsistent specifications and design solutions, and then update all the related standard documents including testing specifications.

• **V3 (improper cross-layer security binding).** The cross-layer security binding between the establishment of IPSec security association and the IMS registration shall be decoupled. However, such design change could incur a large overhead, since the general IMS operation for both emergency and non-emergency services needs to be modified; specifically, the derivation of the IPSec security context needs to be removed from the IMS registration procedure.

• **V4 (non-atomic emergency service initialization).** The three steps in the cellular emergency service initialization need to be combined into an atomic operation. Specifically, the request of the emergency IP-CAN establishment piggybacks the requests of both IMS emergency registration and session establishment procedures. Once this combined request arrives at the core network, the corresponding emergency call attempt can reach the IMS server so that the emergency IP-CAN cannot be hijacked without raising awareness from the IMS. However, handling that combined request requires modifications on the MMF, the UPG, and the IMS server, which cannot be done in a short time.

• **V5 (improper access control on emergency IP-CAN sessions).** The MMF or the UPG shall provide the PCF with the IP address of the IMS server assigned to each emergency UE, and the PCF (or firewall) shall then restrict emergency IP-CAN sessions to the IMS server only and may be further strengthened with stateful rules for them. However, the assignment of the IMS server can be done through the DHCP

[1]This attack was successfully validated for US-II in August 2021, but it became unavailable later in December 2021. The observed difference between these two experiment times was that the IP addresses assigned to non-emergency IP-CAN sessions changed from IPv6-based to IPv4-based, whereas those of emergency IP-CAN sessions were still IPv6-based. Such changes in the network configuration/infrastructure could be the reason why the E2D communication became unavailable.

or DNS service, after the establishment of the emergency IP-CAN session [27]; there could still exist a window period when the emergency IP-CAN session is not restricted and may be abused. Thus, the IMS server assignment shall be executed during the emergency IP-CAN session establishment; this proposed design may incur a large overhead due to the required support of multiple core network functions, e.g., MMF, UPG, PCF, and IMS server.

B. Short-Term Remedies

In this section, we propose a suite of standard-compliant remedies, which can reduce attack incentives or mitigate attack damage, instead of fully addressing the vulnerabilities.

• **Restricted resource on duplicate/suspicious emergency IP-CAN session (for V1 and V6).** Simply rejecting each duplicate emergency session request or each emergency session request with an invalid UE ID is seemingly an effective solution to address V1 and V6, respectively, but the duplicate/suspicious ones may be sent by benign UEs in some rare but still possible scenarios. For example, while a user is having an emergency call, the smartphone may be accidentally rebooted due to some unexpected software/hardware errors [50], [51]; this accidental event does not allow the smartphone to perform the detach procedure of the emergency IP-CAN session and the session is not released, so when the user dials an emergency call again after the smartphone reboots, a duplicate emergency session request can be generated. Moreover, benign users may purchase used phones whose IMEIs were modified by previous owners to invalid ones for some reasons. Note that the duplicate requests generated by benign UEs may not be commonly observed, since UEs can usually send out a message of Detach Request to the infrastructure before rebooting or shutting down, but we still need to consider all the possible emergency conditions. The simple-rejection method may hurt the availability of the emergency service for benign UEs. In order to not only defend against the DoCES attack but also keep the service high availability, we propose to accept duplicate/suspicious emergency session requests but restrict their session capability; the existing emergency sessions that are duplicated will be kept.

Specifically, the duplicate/suspicious emergency IP-CAN sessions are restricted to only the access of basic IMS emergency services (e.g., 31 Kbps for voice calls with the basic audio codec [52]), but not allowed to access video calls or voice calls with high audio quality codecs. Even though duplicate/suspicious emergency sessions are established by the adversary, the resources available to be abused are limited, since these duplicate/suspicious emergency sessions are granted only the minimum resource supporting the basic IMS emergency service; the attack incentive can be thus greatly reduced. On the other hand, when the duplicate/suspicious ones are created by benign UEs, they are still available to offer the emergency services.

• **Enabling Alternative Emergency Services Timely (for V2).** In situations where there are inconsistent capabilities between UEs and the 5G/4G infrastructure, an emergency IP-CAN session cannot be established successfully. In such cases, repeated attempts will not solve this problem. We thus propose to use an alternative emergency service, e.g., the circuit-switched (CS)-based emergency service, to resolve this vulnerability. There are two potential implementation options. First, it can be initiated by the UE to transmit a message of "Extended Service Request" with the CS Fallback Indicator [53] to the infrastructure; it can promptly transition the UE to legacy systems, e.g., 3G network, and then initiate the CS-based emergency service. Second, the infrastructure can make the UE connect to other alternative networks by providing it with a 3GPP-stipulated EMM error code, "EPS services not allowed" [25].

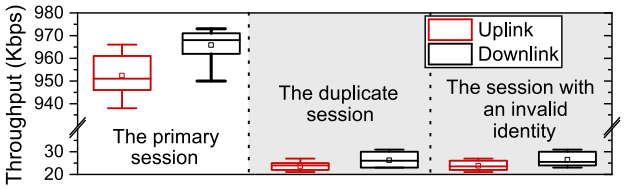
• **Enabling TLS protection over IMS emergency session (for V3).** The vulnerability V3 can be addressed by enabling the ciphering and integrity protection over IMS emergency sessions. However, emergency UEs may not have credentials to do IMS emergency service registration and then establish IPSec security associations with their IMS servers. We then propose a standard-compliant method that an emergency UE establishes a TLS session with its IMS server using only the server's certificate prior to the IMS emergency service registration [34]. The TLS session can protect the IMS signaling messages with ciphering and integrity, thereby preventing fabricated SIP messages. Notably, this approach does not require significant support from carriers, since it was originally stipulated by the cellular network standards [34] to be used as an optional security mechanism to improve the security of IMS service access.

• **Delay authorization of emergency IP-CAN session (for V4 and V5).** To address vulnerabilities V4 and V5, we propose to delay authorization of each emergency IP-CAN session. The initial IP-CAN session obtained from the emergency IP-CAN session establishment for a UE is deemed as a temporarily-authorized session, the availability of which is only authorized for a short time period (e.g., 3 s); moreover, the bandwidth of this temporarily-authorized session is also limited to a small value (e.g., 31 Kbps). Its permanent authorization is delayed until the IMS server assigned to the UE receives SIP messages from the UE, and then determined by the IMS server. If no anomaly happens, the IMS server authorizes the session permanently by instructing the PCF to remove the session's time constraint and install proper PCC rules to restrict the IP-CAN session to the IMS server only. With this mechanism, even though the adversary may abuse the IP-CAN session during the initial, temporarily-authorized time period, their incentive can be largely decreased by that short abuse time. Notably, not all UPGs understand the IMS-related messages, so the permanent authorization of the emergency IP-CAN session cannot be done at the UPG during its establishment procedure.

C. Prototype and Evaluation

We prototype and evaluate the above four standard-compliant remedies. To emulate the cellular emergency service architecture, we use srsRAN (v20.1) [31], Open IMS Core [54], and LinPhone Voice client [35] to serve as the 4G LTE infrastructure, the IMS core with an IMS server, and the Voice over IMS app, respectively.

• **Restricted resource on duplicate/suspicious emergency IP-CAN sessions.** We upgrade srsRAN to support the emergency IP-CAN session establishment and modify the PCF to limit the maximum throughput of duplicate emergency



(a) Restricted resource on duplicate/suspicious emergency sessions.

Time	Protocol	Info
0.000...	NAS...	Attach request, PDN connectivity request
0.634...	NAS...	Attach reject (ESM failure), PDN connectivity reject
3.020...	NAS...	Attach request, PDN connectivity request
3.479...	NAS...	Attach reject (ESM failure), PDN connectivity reject
5.719...	NAS...	Attach request, PDN connectivity request
6.246...	NAS...	Attach reject (EPS services not allowed) PDN connec

(b) Guide emergency UEs to enable alternative services timely.

LinPhone client OpenIMS server

No.	Source	Destination	Protocol	Length	Info
4	192.168.200.130	192.168.200.131	TLS...	585	Client Hello
6	192.168.200.131	192.168.200.130	TLS...	814	Server Hello, Certi
8	192.168.200.130	192.168.200.131	TLS...	194	Client Key Exchange
9	192.168.200.131	192.168.200.130	TLS...	310	New Session Ticket,
					SIP Invite 100 Trying
61	192.168.200.130	192.168.200.131	TLS...	1447	Application Data
66	192.168.200.131	192.168.200.130	TLS...	396	Application Data

(c) TLS-protected IMS emergency sessions.

Fig. 15. Short-term remedy evaluation for (1) restricted resource on duplicate/suspicious emergency IP-CAN sessions, (2) enabling CS fallback switches, (3) enabling TLS-protected IMS emergency sessions.

IP-CAN sessions and the ones with invalid user identities to 31 Kbps. In the experiment, three types of emergency IP-CAN sessions are evaluated, namely the primary (first) session, the secondary (duplicate) session, and the session with an invalid IMEI, on the testbed in terms of throughput performance. Figure 15(a) plots the throughput result obtained from 10 experiment runs. It is observed that the maximum throughputs of the secondary and invalid-IMEI emergency IP-CAN sessions are limited to 31 Kbps, whereas that of the primary one is as high as 973 Kbps. Together with the proposed delay authorization method, this remedy can largely decrease adversaries' incentives.

• **Enabling Alternative Emergency Services Timely.** We modify the emergency IP-CAN session establishment procedure in srsRAN. Specifically, when a UE attempts to establish an emergency IP-CAN session and its requested service option is not supported by the network, the network rejects the request with the EMM error cause of the ESM failure for the first two attempts. The ESM failure is to notify the UE that there is a failure in the emergency session management and it needs to change the requested service option. However, if the UE insists on using the option that is not supported by the network, on the third attempt, the network rejects the emergency UE's request with the EMM cause of the EPS services not allowed and then guides the UE to switch to a 2G/3G network for accessing CS-based emergency services, as shown in Figure 15(b). This can prevent the UE blocking attacks, where attackers exploit unsupported service options and cause the victim's emergency IP-CAN session establishment to fail.

• **Enabling TLS protection over IMS emergency session.** We enable the TLS support on the OpenIMS server and LinPhone Voice client. As illustrated in Figure 15(c), all the SIP messages of the emergency call establishment are protected by the established TLS session between the client and the server. It can thus prevent the DoCES attack, which relies on the SIP messages sent in plaintext.

Time	Protocol	Info
18.287...	S1AP/NAS...	InitialContextSetupRequest, Attach accept,
18.327...	S1AP	UECapabilityInfoIndication, UECapabilityIn
18.532...	S1AP	InitialContextSetupResponse
18.533...	S1AP/NAS...	UplinkNASTransport, Attach complete, Activ
18.533...	S1AP/NAS...	DownlinkNASTransport, EMM information
21.287...	S1AP	UEContextReleaseCommand
21.287...	S1AP	UEContextReleaseComplete

The UE was implicitly detached by the MME in about 3 seconds.

Fig. 16. UE is implicitly detached by MME when no valid IMS emergency session is established within 3 seconds.

• **Delay authorization of emergency IP-CAN session.** We modify the PCF server to restrict the access of the emergency IP-CAN sessions with specified PCC rules at the UPG. For the delay authorization mechanism, a 3 s timer is set for each emergency IP-CAN session right after it is established. By default, after 3 s, it will be terminated by the UPG and its PCC rules will be removed; the Delete Bearer Request message [55] is sent to the MMF for the termination. For normal emergency service requests, the IMS server can receive a valid SIP INVITE message for the emergency IP-CAN session within that 3 s; then, it will authorize the emergency IP-CAN session by sending the AAR (Authentication Authorization Request) message [42] to the PCF through the standardized Rx interface [42].

We evaluate this remedy for the UE in three tested scenarios: (1) transmitting nothing to the infrastructure, (2) transmitting an invalid SIP INVITE message with a non-emergency phone number to the IMS server, and (3) transmitting a valid SIP INVITE message using urn:service:sos as the recipient's number to the IMS server. As shown in Figure 16, the UE will be implicitly detached by the infrastructure if no valid SIP INVITE message is received within 3 s after its emergency IP-CAN session is established. The result shows that the adversary cannot keep the emergency IP-CAN session being alive for a long time without a valid IMS emergency session.

VII. Discussion

Launching attacks from COTS UEs? Some attacks (e.g., data DoS/spamming/free attacks) can be launched from COTS UEs, but they need to be finished within a short time period, because the UEs can be switched to the legacy 3G network, where the attacks are not allowed, after they fail to communicate with the IMS emergency server.

Similar to attacks exploiting unprotected communication? It seems that the anonymous UE, which lacks security context to protect communication, is similar to an identified scenario with unprotected communication in commercial networks due to design and implementation flaws [20]. However, they differ in two major aspects. First, not all the proposed attacks rely on the anonymous UE's unprotected communication; for example, the attacks of free services (A5), Data DoS/overcharge (A6), and remote scanning (A7) do not. Second, disabling the cipher suite may not be common, as it is not mandated by the 3GPP or GSMA standard, resulting in limited impact. In contrast, our proposed DoCES attacks (A1∼A4) root in design defects from the 3GPP/GSMA standards so that they can be applied to all the 3GPP networks unless additional non-3GPP security defenses are deployed.

Vulnerabilities/attacks applied to 5G networks? Most discovered vulnerabilities and attacks can be applied to 5G networks. There are two types of 5G networks: 5G NSA and 5G SA (Standalone). The 5G NSA simply deploys 5G base stations but reuses the 4G core network. With this network

type, all the vulnerabilities which root in 3GPP design defects and are validated in 4G networks can still exist, including V1-V5. The 5G SA uses both 5G base stations and the 5G core network. After analyzing the 3GPP/GSMA standards [3], [27], [33], [38], [41], [56], we find that all the vulnerabilities and attacks can still exist in 5G SA networks, except for V1 and V6; V1 stems from a 4G-specific design defect, whereas V6, an operational slip, may not occur in 5G networks. The root causes of the other vulnerabilities are confirmed to still exist in the 5G SA networks.

VIII. Related Work

We classify the related work of the emergency service security into non-cellular and cellular categories.

Non-cellular Emergency Service Security. Several studies have been proposed to examine the security of non-cellular emergency services. Specifically, Goebel et al. [57] presented the vulnerabilities of the 9-1-1 call system from the perspectives of confidentiality, integrity, and availability. Aschenbruck et al. [5] discussed a VoIP-based DDoS attack, where multiple devices with VoIP software generate a massive amount of calls to overload PSAPs. Tsiatsikas et al. [6] proposed a DDoS attack using a PSAP-unsupported codec to compel expensive real-time codec conversion. Fuchs et al. [8] developed an adapted intrusion detection architecture against the DoS attacks where many faked VoIP-based emergency calls are generated. Seth et al. [58] designed a Wi-Fi based emergency service framework that enables mobile devices to contact the PSAP securely.

Cellular Emergency Service Security. The security issues of the cellular emergency service have attracted much attention in recent years. They can be classified into three categories. The first category of the studies is to launch or defend against the DDoS attack on the PSAP or the IMS emergency service server. Specifically, Mirsky et al. [4] showed that the adversary can jeopardize the statewide and nationwide PSAPs by generating random UE identities (e.g., IMEIs). Jung et al. [7] presented a CAPTCHA-based DDoS defense system that can protect the PSAP from DDoS attacks generated by compromised UEs (bots). Onofrei et al. [9] developed an adaptive firewall pinholing mechanism that can mitigate DDoS attacks against the server of the IMS emergency service.

The second category is to examine the security issue that fabricated emergency/presidential alerts can be sent to UEs. Lee et al. [12] demonstrated that fabricated emergency alerts can be sent to UEs successfully. Hussain et al. [13] discovered that the adversary can hijack legitimate paging channels to send fabricated paging messages with emergency alerts to victim UEs successfully. Bitsikas et al. [21] investigated the security of 5G public warning system (PWS) and demonstrated attacks that can spoof, suppress, or bar the warning messages sent to the victim UEs.

The last category is to exploit the cellular emergency service or resources to attack UEs or carriers. Hou et al. [14] developed two attacks based on the emergency service: UE screen lock bypassing and call service DoS. The first attack allows the adversary to dial any number on the emergency panel of the victim's UE and the call can be routed to the number owner, whereas the second attack can block phone calls made to a set of any numbers in a specific area.

The present study belongs to the last category; however, it differs from the above study from two major aspects as follows. First, the explored vulnerabilities and attacks are different; this study mainly presents the free data service, data DoS/overcharge, and DoCES attacks. Second, the adversary in the above study requires deploying a malicious eNodeB and let victim UEs connect to the eNodeB, whereas only SDR-based UE without SIMs is needed in this work.

Notably, while some prior works [4], [5], [6] also aim to disrupt emergency services, they differ from the DoCES attack in terms of feasibility and impact. Those attacks focus on flooding PSAPs with SIP messages by relying on numerous attack devices to occupy network resources; they incur high costs, and can be detected and mitigated easily [7], [8], [9]. In contrast, our DoCES attack targets individual mobile users using fewer resources and is stealthier.

IX. Conclusion

Cellular networks offer mobile users with ubiquitous emergency services. For emergency uses, anonymous UEs are usually allowed to access cellular emergency services, according to regulatory authority requirements. However, such emergency support increases the attack surface of cellular networks. It leads us to discover six security vulnerabilities and exploit them to develop several attacks including free data service, data DoS, and DoCES. All of the vulnerabilities root in either cellular design defects or commonly observed operational slips, which happen because some conventional non-emergency functions and services are directly applied to the emergency service operation without being carefully reviewed from security aspects. We have experimentally validated the vulnerabilities and attacks with three representative U.S carriers and two major Taiwan carriers, and shown that both carriers and mobile users may suffer from the attacks. We finally propose short-term remedies and evaluate their feasibility, but the ultimate solution still requires a concerted effort from the standard community, carriers, and device vendors.

Acknowledgment

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors only and do not necessarily reflect those of the NSF and NSTC.

References

[1] Code of Federal Regulations, *FCC 911 Regulations: 47 CFR Part 9: 911 Requirements*, document FCC 911, 2021.

[2] GSMA, *Emergency Communication (Version 1.0)*, document NG.119, Jul. 2021.

[3] *IP Multimedia Subsystem (IMS) Emergency Sessions (Release 17)*, document TS 23.167, 3GPP, Sep. 2021.

[4] Y. Mirsky and M. Guri, "DDoS attacks on 9-1-1 emergency services," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 6, pp. 2767–2786, Nov. 2021.

[5] N. Aschenbruck, M. Frank, and P. Martini, "Present and future challenges concerning DoS-attacks against PSAPs in VoIP networks," in *Proc. 4th IEEE Int. Workshop Inf. Assurance (IWIA)*, 2006, pp. 103–108.

[6] Z. Tsiatsikas, G. Kambourakis, and D. Geneiatakis, "At your service 24/7 or not? Denial of service on ESInet systems," in *Proc. TrustBus*, 2021, pp. 35–49.

[7] S. W. Jung, "CAPTCHA-based DDoS defense system of call centers against zombie smart-phone," *Int. J. Secur. Appl.*, vol. 6, no. 3, pp. 29–36, 2012.

[8] C. Fuchs, N. Aschenbruck, F. Leder, and P. Martini, "Detecting VoIP based DoS attacks at the public safety answering point," in *Proc. ACM Symp. Inf., Comput. Commun. Secur.*, Mar. 2008, pp. 148–155.

[9] A. Ancuta Onofrei, Y. Rebahi, and T. Magedanz, "Preventing distributed denial-of-service attacks on the IMS emergency services support through adaptive firewall pinholing," *Int. J. Next-Generation Netw.*, vol. 2, no. 1, pp. 1–17, Mar. 2010.

[10] H. Tschofenig, H. Schulzrinne, M. Shanmugam, and A. Newton, "Protecting first-level responder resources in an IP-based emergency services architecture," in *Proc. IEEE Int. Perform., Comput., Commun. Conf.*, Apr. 2007, pp. 626–631.

[11] B. Kumar Subudhi et al., "Performance testing for VoIP emergency services: A case study of the EMYNOS platform and a reflection on potential blockchain utilisation for NG112 emergency communication," *J. Ubiquitous Syst. Pervasive Netw.*, vol. 12, no. 1, pp. 1–8, Nov. 2019.

[12] G. Lee et al., "This is your president speaking: Spoofing alerts in 4G LTE networks," in *Proc. 17th Annu. Int. Conf. Mobile Syst., Appl., Services*, Jun. 2019, pp. 404–416.

[13] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A systematic approach for adversarial testing of 4G LTE," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2018.

[14] K. Hou, Y. Li, Y. Yu, Y. Chen, and H. Zhou, "Discovering emergency call pitfalls for cellular networks with formal methods," in *Proc. 19th Annu. Int. Conf. Mobile Syst., Appl., Services*, Jun. 2021, pp. 296–309.

[15] C. Peng, C.-Y. Li, G.-H. Tu, S. Lu, and L. Zhang, "Mobile data charging: New attacks and countermeasures," in *Proc. ACM Conf. Comput. Commun. Secur.*, Oct. 2012, pp. 195–204.

[16] C. Peng, C.-Y. Li, H. Wang, G.-H. Tu, and S. Lu, "Real threats to your data bills: Security loopholes and defenses in mobile data charging," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 727–738.

[17] G.-H. Tu, C.-Y. Li, C. Peng, and S. Lu, "How voice call technology poses security threats in 4G LTE networks," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 442–450.

[18] C.-Y. Li et al., "Insecurity of voice solution VoLTE in LTE mobile networks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2015, pp. 316–327.

[19] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on LTE," in *Proc. USENIX Security*, 2019, pp. 55–72.

[20] H. Kim, J. Lee, E. Lee, and Y. Kim, "Touching the untouchables: Dynamic security analysis of the LTE control plane," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1153–1168.

[21] E. Bitsikas and C. Pöpper, "You have been warned: Abusing 5G's warning and emergency systems," in *Proc. 38th Annu. Comput. Secur. Appl. Conf.*, Dec. 2022, pp. 561–575.

[22] *Service Aspects; Service Principles (Release 17)*, document TS 22.101, 3GPP, Jun. 2023.

[23] *General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 17)*, document TS 23.401, 3GPP, Dec. 2021.

[24] S. Wang et al., "Insecurity of operational cellular IoT service: New vulnerabilities, attacks, and countermeasures," in *Proc. 27th Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2021, pp. 437–450.

[25] *Non-Access-Stratum (NAS) Protocol for Evolved Packet System (EPS); Stage 3 (Release 17)*, document 3GPP, 3GPP, Dec. 2021.

[26] J. Rosenberg et al., *SIP: Session Initiation Protocol*, document RFC 3261, Jun. 2002.

[27] *IP Multimedia Subsystem (IMS); Stage 2 (Release 17)*, document TS 23.228, 3GPP, Dec. 2021.

[28] *IMS Profile for Voice and SMS (Version 15.0)*, document IR.92, GSMA, May 2020.

[29] *SMS Evolution (Version 2.0)*, document NG.111, GSMA, Nov. 2020.

[30] *IP Multimedia Call Control Protocol Based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 17)*, document TS 24.229, 3GPP, Sep. 2021.

[31] srsRAN. (2022). *Get the srsRAN Software and Documentation*. [Online]. Available: https://docs.srsran.com/en/latest/index.html

[32] *5G Implementation Guidelines*, GSMA, London, U.K., Jul. 2019.

[33] *System Architecture for the 5G System (5GS) (Release 17)*, document TS 23.501, 3GPP, Dec. 2021.

[34] *Access Security for IP-based Services (Release 17)*, document TS 33.203, 3GPP, Dec. 2021.

[35] Linphone. (2020). *For Smartphones, Tablets and Desktop Platforms*. [Online]. Available: https://www.linphone.org/

[36] T. D. Hoang et al., "LTESniffer: An open-source LTE downlink/uplink eavesdropper," in *Proc. 16th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, May 2023, pp. 43–48.

[37] *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification (Release 17)*, document TS 36.331, 3GPP, Apr. 2022.

[38] *Non-Access-Stratum (NAS) Protocol for 5G System (5GS); Stage 3 (Release 17)*, document TS 24.501, 3GPP, Dec. 2021.

[39] *Universal Mobile Telecommunications System (UMTS); Network Architecture (Release 5)*, document TS 23.002, 3GPP, Sep. 2003.

[40] *Policy and Charging Control (PCC); Reference Points (Release 17)*, document TS 29.212, 3GPP, Sep. 2021.

[41] *Policy and Charging Control Framework for the 5G System (5GS); Stage 2 (Release 17)*, document TS 23.503, 3GPP, Dec. 2021.

[42] *Rx Interface and Rx/Gx Signalling Flows (Release 6)*, document TS 29.211, 3GPP, Jun. 2007.

[43] *Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, Addressing and Identification*, document TS 23.003, 3GPP, Sep. 2022.

[44] IMEI.INFO. (2023). *Check IMEI Number to Get to Know Your Phone Better.* [Online]. Available: https://www.imei.info/

[45] IMEIcheck.com. (2023). *IMEI Number Check*. [Online]. Available: https://imeicheck.com/imei-check

[46] Imeipro.info. (2023). *Free U.S. Cell Phone IMEI Checker*. [Online]. Available: https://www.imeipro.info/att-imei-check.html

[47] Verizon. (2023). *Tell Us About Your Device*. [Online]. Available: https://www.verizon.com/sales/byod/devicedetails/imei.html

[48] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Layer Procedures (Release 17)*, document TS 36.213, 3GPP, Jan. 2022.

[49] G. Voice. (2022). *Google Voice Calling Rates*. [Online]. Available: https://voice.google.com/rates

[50] Harvey. (2022). *How to Fix a Galaxy S9 That Reboots on Its Own During Calls*. [Online]. Available: https://thedroidguy.com/how-to-fix-a-galaxy-s9-that-reboots-on-its-own-during-calls-1091448

[51] Androidcentral. (2015). *Shutting and Rebooting Down During Calls*. [Online]. Available: https://forums.androidcentral.com/moto-x/575325-shutting-rebooting-down-during-calls.html

[52] *IP Multimedia Subsystem (IMS); Multimedia Telephony; Media Handling and Interaction (Release 17)*, document TS 26.114, 3GPP, Dec. 2021.

[53] *Circuit Switched (CS) Fallback in Evolved Packet System (EPS); Stage 2 (Release 17)*, document TS 23.272, 3GPP, Sep. 2021.

[54] OpenIMSCore.org. (2008). *Welcome to Open IMS Core's Homepage*. [Online]. Available: http://openimscore.sourceforge.net/

[55] *3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control Plane (GTPv2-C); Stage 3 (Release 17)*, document TS 29.274, 3GPP, Dec. 2021.

[56] *5G; Procedures for the 5G System (5GS)(Release 17)*, document TS 23.502, 3GPP, Dec. 2021.

[57] M. Goebel, C. Dameff, and J. Tully, "Hacking 9-1-1: Infrastructure vulnerabilities and attack vectors," *J. Med. Internet Res.*, vol. 21, no. 7, Jul. 2019, Art. no. e14383.

[58] M. Seth, S. K. Kasera, and R. P. Ricci, "Emergency service in Wi-Fi networks without access point association," in *Proc. 1st Int. Conf. Wireless Technol. Humanitarian Relief*, Dec. 2011, pp. 411–419.