Yiwen Hu, Min-Yue Chen, Guan-Hua Tu *Michigan State University, MI*
Chi-Yu Li *National Yang Ming Chiao Tung University, Hsinchu, Taiwan*
Sihan Wang, Jingwen Shi, Tian Xie, Li Xiao *Michigan State University, MI*
Chunyi Peng *Purdue University, West Lafayette, IN* **Zhaowei Tan, Songwu Lu** *UCLA, CA*

Editors: Nicholas D. Lane and Xia Zhou

UNVEILING THE INSECURITY OF OPERATIONAL CELLULAR EMERGENCY SERVICES (911): Vulnerabilities, Attacks, and Countermeasures

Illustration, istockphoto.com

Excerpted from "Uncovering insecure designs of cellular emergency services (911)," from *MobiCom '22: Proceedings of the 28th Annual International Conference on Mobile Computing And Networking Conference* with permission. https://dl.acm.org/doi/abs/10.1145/3495243.3560534 ©ACM 2022

The cellular network offers a ubiquitous emergency call service with its pervasive coverage. In the United States, it can be consumed by dialing 911 for cellular users, and the emergency call is forwarded to the public safety answer point (PSAP), which handles emergency service requests. According to regulatory authority requirements [1,2,3] for cellular emergency services, anonymous user equipment (UE) is allowed to access them without a SIM (Subscriber Identity Module) card, a valid mobile subscription, or a roaming agreement with the visited cellular network. Such support of the cellular emergency services requires different operations from conventional cellular services, thereby increasing the attack surface of the cellular infrastructure.

The security research of the cellular emergency services has attracted much attention recently. Some of the proposed studies mainly focus on distributed denial-of-service (DDoS) attacks [4,5,6] against the PSAP. The other related studies introduce attacks against the cellular emergency services by targeting the vulnerabilities on the UE [7,8,9]. However, the security of the cellular infrastructure supporting the emergency services remains unexplored. We thus study whether it can introduce any new security threats to mobile ecosystem.

Surprisingly, our study shows that the U.S. cellular emergency services are not only deniable from a denial of cellular emergency service (DoCES) attack, but also abusable from several attack variants, including free services, data DoS/overcharge, and remote scanning. These two attacks are rooted in four security vulnerabilities discovered from the cellular emergency services in the cellular networks of three major American carriers: (V1) unverifiable emergency IP-CAN (IP Connectivity Access Network) session requests, (V2) improper cross-layer security binding, (V3) non-atomic cellular emergency service initialization, and (V4) improper access control on emergency IP-CAN sessions. At the first glance, carriers should take the blame, since necessary security mechanisms are not deployed. However, after a careful analysis, we find that all

the identified vulnerabilities are rooted in design defects of the cellular emergency standards, which span multiple protocols and network functions, so carriers cannot address them without significant effort.

This work makes three key contributions: (1) we identify four vulnerabilities from cellular emergency service standards, as well as validate them experimentally and analyze root causes; (2) we devise two proof-of-concept attacks with three variants each by exploiting the identified vulnerabilities and assess their real-world impact with three major American cellular carriers; and (3) we propose a suite of recommended solutions for addressing all of the identified vulnerabilities. Notably, we validate the presented vulnerabilities and attacks in the operational cellular networks of three American carriers, denoted as OP-I, OP-II, and OP-III, with two kinds of emergency UEs, COTS smartphones and software-defined radio (SDR) platforms. All the experiments are conducted in a responsible manner with ethical consideration, so any emergency calls/text messages are prevented from being sent to operational cellular networks or PSAPs.

CELLULAR EMERGENCY SERVICE PRIMER

Figure 1 depicts a 5G/4G network architecture with the service flow for emergency voice/text services. An emergency service request from the UE traverses radio access network (RAN), core network, IP Multimedia Subsystem (IMS), and the 911 PSAP. Specifically, the RAN uses the base station (BS) to offer radio access. In the core network, the user-plane gateway (UPG) routes user traffic packets from the UE to the IMS network. Mobility Management Function (MMF) manages user mobility, authentication, and resource reservation. User Data Function (UDF) stores user and service subscription information. Policy Control Function (PCF) generates billing policies, QoS parameters, routing control rules, etc. In the IMS, Call Session Control Function (CSCF, referred to as IMS server hereafter) is responsible for IMS service signaling, which runs Session Initiation Protocol (SIP). Interconnect Border Control Function (IBCF) is a session border controller that is interconnected to other IP/IMS networks. To establish an emergency session with the PSAP, the emergency UE needs to perform three actions: (1) *Emergency IP-CAN Session Establishment* allows the UE to obtain the emergency IP connectivity to communicate with the IMS server; (2) *IMS Emergency Registration* has the IMS server and the UE authenticate with each other and enables the UE to register the emergency service; and (3) *IMS Emergency Session Establishment* allows the UE to establish an IMS emergency call/text session with the PSAP.

DENIABLE CELLULAR EMERGENCY SERVICE

Anonymous UEs can access the cellular emergency services of any U.S. cellular networks, according to the FCC 911 requirements [3]. The goal of this anonymous access is to maximize the availability of emergency services through cellular networks in emergency conditions. However, we discover that such anonymous emergency service access is not well protected. In the following, we present two identified vulnerabilities and the corresponding DoCES attack.

V1: Unverifiable Emergency IP-CAN Session Requests

Since an anonymous UE does not have any security association with the cellular 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. Given that the duplicate request is either rejected, or accepted while implicitly detaching the existing one, according to the standards [11,12], the adversary may have a chance to prevent anonymous benign UEs from accessing the emergency services by sending fabricated emergency requests to the network. In particular, the unprotected requests can be easily fabricated based on the captured device IDs. This vulnerability has been experimentally validated on the three carriers with two UEs. Specifically, one UE's duplicate request can successfully interrupt the other UE's ongoing emergency IP-CAN session in the OP-I network, but it does not work in the networks of OP-II and OP-III.

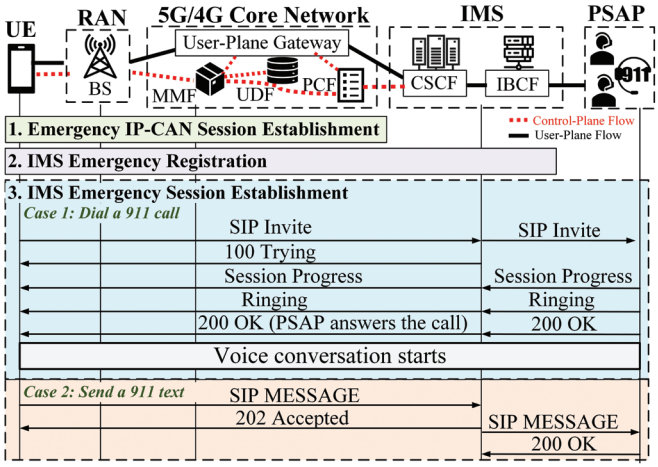


FIGURE 1. 5G/4G network architecture with the service flow for emergency voice/text services.

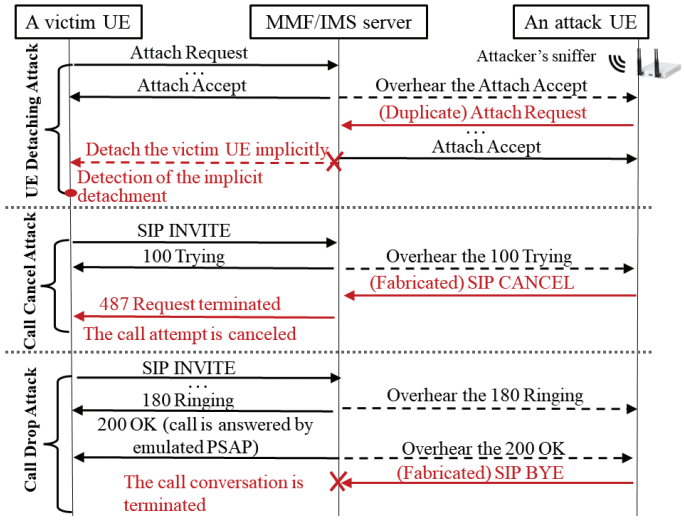
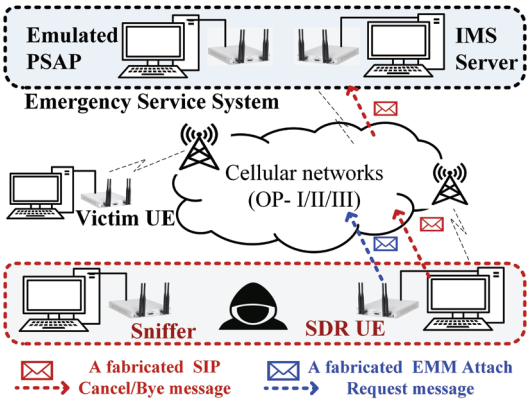
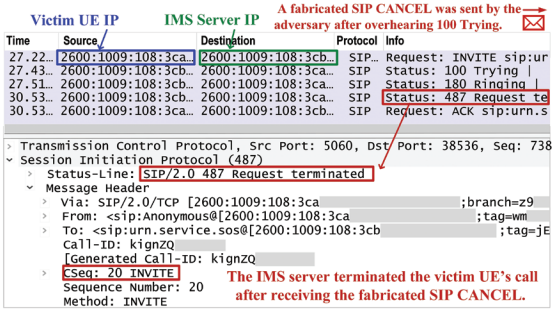


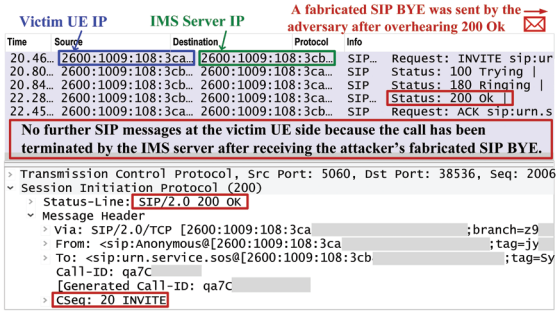
FIGURE 2. Three DoCES attack variants.



(a) DoCES attack evaluation testbed



(b) SIP packet trace collected during the call cancel attack



(c) SIP packet trace collected during the call drop attack

FIGURE 3. DoCSE attack evaluation.

V2: Improper Cross-layer Security Binding

A subscribed UE cannot establish IPsec security associations with the IMS server for the emergency services until it completes the IMS emergency registration, 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. This vulnerability has also been validated on the three carriers with an anonymous UE, which is a COTS smartphone. It is observed that for all the carriers, the IMS emergency registration is not performed, and thus the call SIP messages are all sent in plain text without any security protection.

DoCES Attack

We exploit the above two vulnerabilities to launch the DoCES attack against anonymous UEs. This attack contains three attack variants, as shown in Figure 2: (1) UE detaching attack, caused by a fabricated, duplicate Attach Request message, (2) call cancel, and (3) call drop attacks, based on fabricated SIP CANCEL and BYE messages, respectively.

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 attack UE, which sends attack messages to the cellular networks where victim UEs are. We build an emulation testbed over the networks of the three carriers with two device components, an emulated PSAP, and an emulated IMS server, as shown in Figure 3a; the underlying communications are based on the emergency IP-CAN sessions of the operational networks. The experimental result shows that the UE attaching attack only works in OP-I, whereas the other two attacks are feasible for all the three carriers. Specifically, these three attacks lead to implicit detaching, call cancellation (see Figure 3b), and call termination (see Figure 3c), respectively, at the victim UE.

ABUSABLE CELLULAR EMERGENCY SERVICE

The emergency IP-CAN session is established whenever a cellular emergency service is requested. Particularly, the emergency service request can be issued from anonymous UEs and be free of charge for cellular users due to its emergency purpose [3]. It can be thus more vulnerable than other non-emergency services. However, we discover that no additional security mechanisms are introduced to protect the emergency IP-CAN session. In the following, we first introduce two identified vulnerabilities and then present the corresponding attacks.

V3: Non-Atomic Cellular Emergency Service Initialization

The cellular emergency service initialization consists of three actions, as illustrated in Figure 1. 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. However, no related security mechanisms are stipulated in the 3GPP/GSMA standards. It may allow an adversary to establish an emergency IP-CAN session to abuse while skipping the last two initialization actions. The skip can prevent the IMS server and the PSAP from being aware of the abuse. More threateningly, the emergency IP connectivity can be requested by anonymous UEs. This vulnerability has been experimentally validated for the three carriers; that is, an anonymous UE can successfully obtain an IP address by performing only the emergency IP-CAN session establishment and then keep the IP connectivity for a long time to transmit data.

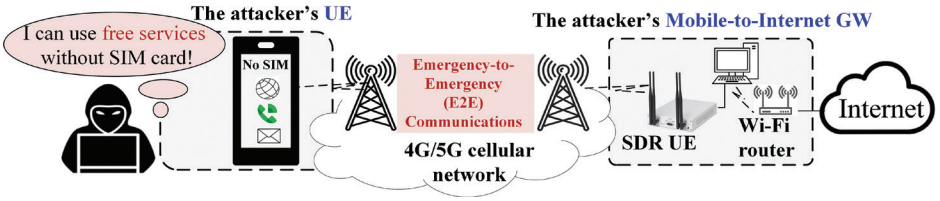
V4: Improper Access Control on Emergency IP-CAN Sessions

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. For the exclusive use of the emergency service, the emergency IP-CAN sessions should be restricted to deliver traffic to the IMS server by installing the corresponding PCC rules. However, the cellular network standards do not stipulate such a regulation. The reason is that those PCC rules cannot be produced during the emergency IP-CAN session establishment when the IMS server is determined based on the DNS or DHCP service after the session establishment. Based on our validation experiments, it is observed that for all the three carriers, the emergency IP-CAN session is not restricted to only the communication between the UE and the IMS server. It allows an anonymous UE to communicate with another UE through the latter's three types of IP-CAN sessions: data, IMS signaling, and emergency services. These three communication types work for all the three carriers, except the first two types for OP-I and the second type for OP-II.

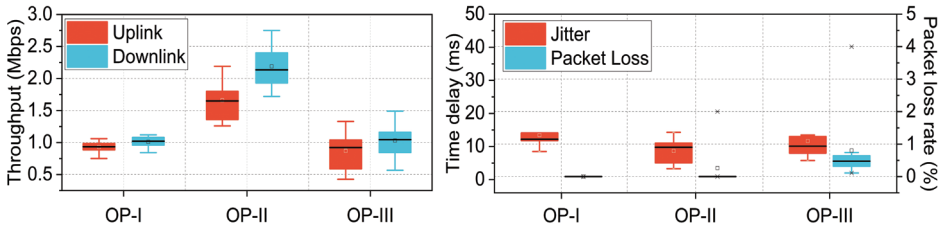
Emergency IP-CAN Session Hijacking Attack

We devise three proof-of-concept attacks, namely free data/voice/text services, data DoS/overcharge, and remote scanning, using V3 and V4. In the first attack, the adversary can exploit the emergency IP-CAN session, the delivered data of which are free of charge, to obtain free services. In the second attack, data spamming can be generated from the attack UE's emergency interface at no cost and sent to a victim UE's data interface, thereby causing DoS or overcharge at the victim UE. In the third attack, the emergency IP-CAN session can be also exploited to scan the data interface of the victim UE remotely for vulnerability discovery while bypassing cellular network firewalls.

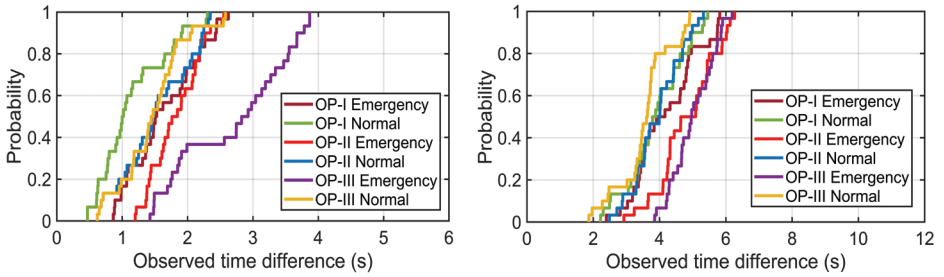
Here, we present only the experiments of the free data service attack while skipping the others due to limited space (see details in [10]). To achieve the attack, a Mobile-to-Internet gateway needs to be deployed to forward data between the UE with an emergency IP-CAN session and the Internet, as shown in Figure 4a. We evaluate



(a) Exploiting the emergency IP-CAN session to enable free data service using a Mobile-to-Internet gateway



(b) The min/med/max and 25th/75th percentiles of throughput, jitter, and packet loss rate



(c) Call setup time

(d) Text delivery time

FIGURE 4. Free service attack evaluation.

the data service over that free-of-charge communication channel in all the three carrier networks in terms of throughput, jitter, and packet loss rate. As shown in Figure 4b, the median throughput values 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, so it can be increased with more advanced UEs. In terms of the call setup and text delivery times, the experiments show that this attack can offer comparable performance to normal cases, as shown in Figures 4c and d.

COUNTERMEASURES

We next propose recommended solutions for addressing the identified vulnerabilities. V1: it calls for a device-level authentication mechanism (e.g., using device certificates), which can make differences on emergency IP-CAN session requests from different UEs, even when the UEs do not have SIM cards. V2: the cross-layer security binding between the establishment of IPsec security association and the IMS registration shall be decoupled; specifically, the derivation of the IPsec security context needs to be removed from the IMS registration procedure. V3: 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 session establishment can piggyback the requests of both IMS emergency registration and session establishment procedures. V4: the IMS server assignment shall be executed during the emergency IP-CAN session establishment; moreover, the MMF or the UPG shall provide the PCF with the IMS IP address assigned to each emergency UE so that the PCF can install a proper access control rule that can restrict the emergency IP-CAN session to the IMS server only.

Notably, these required design changes lie in some core network functions and even security functions of billions of UEs, so they cannot be achieved without significant time and effort. Therefore, we also propose a suite

of short-term, yet low-overhead, remedies that can mitigate those vulnerabilities shortly (see details in [10]).

CONCLUSION

Cellular networks offer mobile users 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 four security vulnerabilities and exploit them to develop several threatening attacks. All of the vulnerabilities are rooted in cellular design defects; the reason is that conventional non-emergency functions and services are directly applied to the emergency service operation without being carefully reviewed from the security aspect. We have experimentally validated the vulnerabilities and attacks with three major American carriers, and shown that both carriers and mobile users may suffer from the attacks. We finally propose recommended solutions for addressing the identified vulnerabilities, but their deployment still requires a concerted effort from the standard community, carriers, and device vendors. ■

Yiwen Hu received her bachelor's degree in Computer Science from Zhejiang University in 2018. Currently, she is a PhD student in Computer Science and Engineering at Michigan State University. Her research interests include mobile networks and systems, network security, cellular/Wi-Fi IoT, and blockchain technologies.

Min-Yue Chen is a PhD student in Computer Science and Engineering Department at Michigan State University. His research focuses on wireless networking, mobile systems, and network security. His recent works focus on the security of 5G/4G cellular networks, discovering critical security vulnerabilities and recommending mitigation solutions.

Guan-Hua Tu received his PhD in computer science from UCLA, LA, in 2015. He is currently an assistant professor in the Computer Science and Engineering Department at Michigan State University. His research interests are in the broad areas of security, IoT, mobile systems, and wireless networking, with a recent focus on innovating 5G/4G mobile network architecture/protocol/technologies, cellular/Wi-Fi IoT, secure cloud computing/services, and blockchain technologies.

Chi-Yu Li received his PhD in computer science from the University of California, Los Angeles (UCLA) in 2015. He is currently an associate professor in the Department of Computer Science at National Yang Ming Chiao Tung University, Hsinchu, Taiwan. His research interests include wireless networking, mobile networks and systems, and network security.

Sihan Wang received his bachelor's degree in Computer Science and Engineering from Northeastern University, China, in 2016. Currently, he is working toward his PhD in Computer Science and Engineering at Michigan State University. His research focuses on mobile IoT, mobile systems, mobile service security, and network security.

Jingwen Shi is currently a PhD student in the Department of Computer Science and Engineering at Michigan State University. She received her master's degree from the University of Chinese Academy of Sciences and her bachelor's degree from Hunan University. She is broadly interested in Networks Security, Cloud Computing, and AI for Distributed Systems.

Tian Xie received his bachelor's degree with honor in Electrical and Computer Engineering from Michigan State University in 2016. Currently, he is working toward the PhD in Computer Science and Engineering at Michigan State University. His research focuses on mobile networks, mobile systems, mobile IoT, and network security.

Li Xiao received her BS and MS in computer science from the Northwestern Polytechnic University, China, and her PhD in computer science from the College of William and Mary, Virginia. She is a professor of computer science and engineering at Michigan State University. Her research interests are in the areas of distributed and networking systems, overlay systems and applications, and wireless networks.

Chunyi Peng received her PhD in Computer Science from UCLA in 2013. She is currently an associate professor at the Department of Computer Science, Purdue University, West Lafayette, IN. Her current research interests are in the broad areas of mobile networking, system and security, with a recent focus on renovating 5G access technologies for demanding apps (performance and reliability), AI for networks, 5G/IoT security, mobile edge computing (mainly for drones and robots).

Zhaowei Tan received his PhD in Computer Science from UCLA, LA. He is currently studying as a post doc scholar. He is broadly interested in systems and security, especially building fast, resilient, and secure systems for emerging applications (IoT, AR/VR, AI, etc.).

Songwu Lu is currently a professor of computer science UCLA, LA. His research interests include mobile networking and systems, cloud computing, and network security.

REFERENCES

[1] GSMA. Official Document NG.119 -Emergency Communication (Version 1.0), July 2021. https://www.gsma.com/newsroom/wp-content/uploads//NG.119-v1.0-3.pdf.

[2] 3GPP. TS 23.167: IP Multimedia Subsystem (IMS) emergency sessions (Release 17), Sept. 2021. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=799

[3] Federal Communications Commission. FCC 911 Regulations: 47 CFR Part 9: 911 Requirements, 2021. https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-9.

[4] Nils Aschenbruck, Matthias Frank, and Peter Martini. Present and future challenges concerning DoS-attacks against PSAPs in VoIP networks. 2006. *Fourth IEEE International Workshop on Information Assurance (IWIA'06).*

[5] Yisroel Mirsky, and Mordechai Guri. DDoS Attacks on 9-1-1 Emergency Services. 2020. *IEEE Transactions on Dependable and Secure Computing 18*, No. 6, 2767-2786.

[6] Ziziz Tsiatsikas, Georgios Kambourakis, and Dimitrios Geneiatakis. 2021. At your service 24/7 or not? Denial of service on ESInet systems. *International Conference on Trust and Privacy in Digital Business*, Springer, Cham, 35-49.

[7] Kaiyu Hou, You Li, Yinbo Yu, Yan Chen, and Hai Zhou. Discovering emergency call pitfalls for cellular networks with formal methods. 2021. *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, 296-309.

[8] Syed Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTE Inspector: A systematic approach for adversarial testing of 4G LTE. *Network and Distributed Systems Security (NDSS) Symposium 2018*.

[9] Gyuhong Lee, Jihoon Lee, Jinsung Lee, Youngbin Im, Max Hollingsworth, Eric Wustrow, Dirk Grunwald, and Sangtae Ha. 2019. This is your president speaking: Spoofing alerts in 4G LTE networks. *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, 404-416.

[10] Yiwen Hu, Min-Yue Chen, Guan-Hua Tu, Chi-Yu Li, Sihan Wang, Jingwen Shi, Tian Xie et al. Uncovering insecure designs of cellular emergency services (911). 2022. *Proceedings of the 28th Annual International Conference on Mobile Computing and Networking*, 703-715.

[11] 3GPP. TS 24.301: Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS), Dec. 2021. https://portal.3gpp.org/desktopmodules/Specifications/ SpecificationDetails.aspx?specificationId=1072.

[12] 3GPP. TS 23.501: System architecture for the 5G System (5GS) (Release 17), Dec. 2021. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144.