IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) | 978-1-6654-9427-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/INFOCOMWKSHPS57453.2023.10225884

Remote Detection of 4G/5G UEs Vulnerable to Stealthy Call DoS

Man-Hsin Chen*, Chiung-I Wu*, Yin-Chi Li*, Chi-Yu Li*, Guan-Hua Tu+
*College of Computer Science, National Yang Ming Chiao Tung University
+College of Computer Science and Engineering, Michigan State University
{shin.owo.cs10, jejewcccc.cs10, eesss.cs11, chiyuli}@nycu.edu.tw, ghtu@msu.edu

***Abstract*—Nowadays, all the 4G/5G voice solutions are offered by the IMS (IP Multimedia Subsystem) system. They include 4G VoLTE (Voice over LTE) and 5G VoNR (Voice over New Radio), as well as a non-3GPP access solution, VoWiFi (Voice over WiFi). Since VoWiFi is implemented on mobile OS, instead of the modem with hardware security for VoLTE and VoNR, it can be a vulnerability of the IMS system and may further impair other IMS-based services. It has been exposed that due to vulnerable VoWiFi sessions, several IMS vulnerabilities are discovered and the smartphones with IMS-based call services may suffer from a stealthy call DoS attack, where the smartphones cannot make or receive any calls and no ringtone or messages are appeared on them during the attack. In this paper, we develop a detector that can remotely and concurrently detect such DoS attack for multiple UEs (User Equipments). It consists of three major components: session hijacking, SIP fabrication, and call detection. We demonstrate its effectiveness in the operational networks of two carriers from different countries by considering three different phone models with VoLTE and VoWiFi call services.**

***Index Terms*—4G, 5G, mobile network, security, call DoS**

I. Introduction

The cellular voice solution has evolved to IMS (IP Multimedia Subsystem) call services over IP since the 4G cellular network. With 3GPP access networks, they include VoLTE (Voice over LTE) and VoNR (Voice over New Radio) for 4G and 5G networks, respectively; VoWiFi (Voice over WiFi) is introduced for non-3GPP access networks (i.e., WiFi) to cover the areas with poor 3GPP access signals, and has been supported since the 4G. A GSMA report [1] shows that there are up to 3.9 billion VoLTE subscribers worldwide in 2022, and moreover, it is expected that VoNR will be commercialized at a larger scale from 2025. Thus, the IMS call services will be used popularly and their security is of vital importance.

However, the VoWiFi technology can be a vulnerability of the IMS call system, since it is implemented at the mobile OS without hardware security from the modem, which is used for VoLTE and VoNR. Given a phone with root privilege, its VoWiFi session connecting to the core network can be hijacked for malicious users to send fabricated messages to the IMS system. It causes the stealthy call DoS (Denial of Service) attack to be developed against the phones with IMS call services, since the call state machine at the callee UE (User Equipment) may get stuck when a malicious caller manipulates the transmission of fabricated messages [2]. Specifically, the caller in the normal case can initiate a call with the callee by exchanging SIP (Session Initiation Protocol) messages as shown in the upper layer of Figure 1; in the abnormal case as shown in the lower layer, when an attacker hijacks a VoWiFi session and initiates a call without replying `PRACK` (Provisional Response Acknowledgement) to the callee, the callee as the victim will keep retransmitting the message, `183 Session Progress`, for a period of time and then suffer from call DoS, which prevents the victim from making or receiving any calls, during this period. Notably, this DoS attack is silent without causing any ringtone or message to appear on the victim UE.

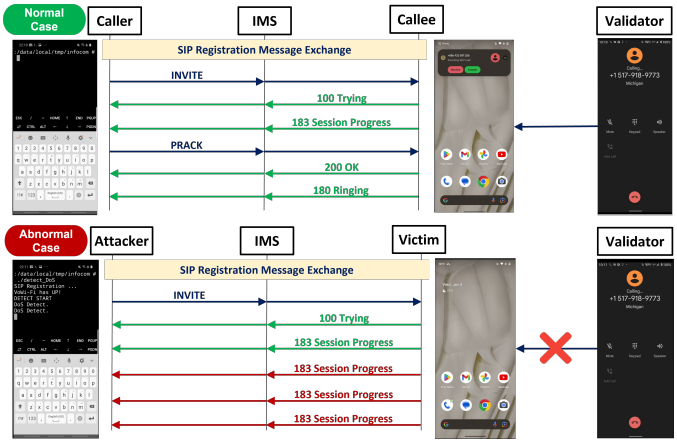

Fig. 1: Stealthy call DoS attack.

In this work, we develop a detector that can remotely and concurrently detect multiple 4G/5G UEs vulnerable to the call DoS attack. It requires only phone numbers from the detected phones, but needs to be implemented on rooted smartphones with the VoWiFi service so that the VoWiFi session can be hijacked for the detection. We demonstrate its effectiveness by remotely detecting three different phone models and using VoLTE/VoWiFi services in operational networks of two carriers, where one in Asia and the other in U.S. During the detection, validator phones are used to test the detected UEs and confirm that the detection result is correct.

In the following, we elaborate on the implementation of the detector and demonstration scenarios.

978-1-6654-9427-4/23/$31.00 ©2023 IEEE

II. Detector of Stealthy Call DoS

The detector identifies the vulnerability that causes the call DoS based on the observation of retransmitted `Session Progress` messages, as shown in the lower layer of Figure 1. To achieve this, it hijacks the VoWiFi session, fabricates SIP messages, and makes ghost calls, which represent call attempts without getting the callee's attention (e.g., no ringtone), by using three developed modules, session hijacking, SIP fabrication, and call detection, respectively, as shown in Figure 2. Moreover, for the latter two modules, multiple call instances are created to detect multiple UEs at a time; each instance interacts with one UE. We elaborate on each module below; more details about the vulnerability and attack can be found in [2].

Session hijacking module. It allows the detector to send valid packets of the VoWiFi session to the IMS system without compromising the VoWiFi app. Since the VoWiFi session is protected by IPsec (Internet Protocol Security), its hijacking requires all the used IPsec parameters, including IPsec version, IPsec transport mode, security algorithm, and security keys. All these parameters can be obtained from the security association database (SAD) in Android. Moreover, this module keeps track of sequence numbers for IPsec and TCP sessions, which carry SIP messages. They are then used to generate IPsec/TCP packets; notably, carriers may have different IPsec implementations, so this module needs to be tuned for each carrier.

SIP fabrication module. It fabricates valid SIP messages (e.g., `SIP INVITE` and `CANCEL`), which are carried by the IPsec/TCP packets, so that the IMS system can accept them. For the fabrication, this module is given the format and required parameters of each SIP message type which is used by the IMS call services. Some SIP parameters (e.g., IMS IP address) can be obtained from the SIP registration messages, whereas some related to each call session can be assigned arbitrarily but need to be consistent within a call session and with specified formats.

Call detection module. Given a list of phone numbers, the module sends a ghost call to each of them. The ghost call is made by sending an `INVITE` message to the callee without replying `PRACK`. When observing retransmitted `Session Progress` messages from a phone number, we identify its device as vulnerable to the call DoS attack. Multiple ghost calls can be made concurrently to detect multiple UEs at a time; notably, their SIP messages can be differentiated based on the call session ID. Whenever the detection result of a phone number is obtained, the module sends `SIP CANCEL` to cancel the detection call.

III. Demonstration

We demonstrate the call DoS detector in the operational networks of two carriers: one is in Asia and the other is in U.S. The detector is deployed at a rooted smartphone, Samsung Galaxy S8, with the VoWiFi service. Figure 2 shows the demonstration scenario for both carriers. The detector remotely and concurrently detects two smartphones; in the meantime,

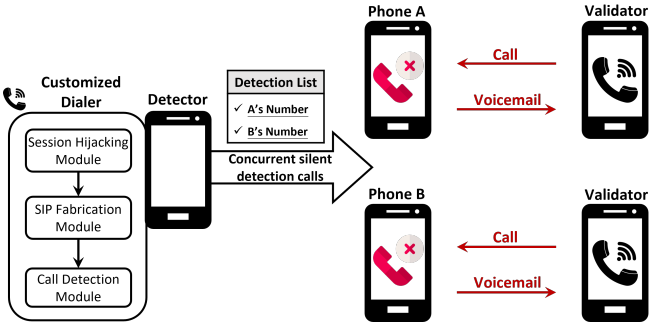

Fig. 2: Remote detection of 4G/5G UEs vulnerable to stealthy call DoS.

one validator smartphone makes a call to each detected smartphone and observes whether the call attempt succeeds or fails with a voice mail message. When a smartphone is detected as vulnerable to the call DoS attack, the validator's call should fail, since the detection call can also make the target smartphone suffer from the call DoS during the detection period. The demonstration video is shown at [3].

The demonstration consists of three steps. First, the validator phones check whether the call services of two testees, which are detected UEs, operate normally by making them normal calls. Two testees can successfully receive the calls with ringtone. Second, the detector starts to run with three major tasks: (1) hijacking its VoWiFi session; (2) making two concurrent DoS detection calls; (3) detecting whether the testees are vulnerable. Third, while the testees are under the detection (or stealthy DoS calls), the validators check whether they are call DoS; that is, the validators receive voicemail messages and the testee does not receive any call or ringtone.

There are two parts in the demonstration video. In the first part, the U.S. carrier is considered and the testees' call services are with VoWiFi; the smartphones for the testees are Google pixel 7 and Samsung Galaxy S21. The detection result shows that these two smartphones with VoWiFi can suffer from the stealthy call DoS. In the second part, the Asia carrier is tested and the call services of the testees are VoLTE; the smartphones used for them are Google pixel 7 and Sony Xperia 10 III. The same result is also observed for these two smartphones.

We note two things. First, the videos of the cases that some smartphones are detected to be immune to the DoS attack are omitted. Second, for clear demonstration, the demonstration video shows the concurrent detection with only 2 smartphones, but it can support up to 5 smartphones.

References

[1] E. Kolta, *4G-5G Subscribers March 2022*. GSMA Intelligence, 2022.
[2] Y.-H. Lu, C.-Y. Li, Y.-Y. Li, S. H.-Y. Hsiao, T. Xie, G.-H. Tu, and W.-X. Chen, "Ghost Calls from Operational 4G Call Systems: IMS Vulnerability, Call DoS Attack, and Countermeasure," in *ACM MobiCom*, Sydney, Australia, Oct. 2020.
[3] "Demo video," 2023. [Online]. Available: https://youtu.be/M9hURobiRRk