Ghost Calls from Operational 4G Call Systems: IMS Vulnerability, Call DoS Attack, and Countermeasure

Yu-Han Lu, Chi-Yu Li, Yao-Yu Li, Sandy Hsin-Yu Hsiao
Department of Computer Science
College of Computer Science
National Chiao Tung University
Hsinchu, Taiwan

Tian Xie, Guan-Hua Tu
Department of Computer Science and Engineering
Michigan State University
East Lansing, Michigan, USA

Wei-Xun Chen
Department of Computer Science
College of Computer Science
National Chiao Tung University
Hsinchu, Taiwan

ABSTRACT

IMS (IP Multimedia Subsystem) is an essential framework for providing 4G/5G multimedia services. It has been deployed worldwide to support two call services: VoLTE (Voice over LTE) and VoWi-Fi (Voice over Wi-Fi). VoWi-Fi enables telephony calls over the Wi-Fi network to complement VoLTE. In this work, we uncover that the VoWi-Fi signaling session can be hijacked to maliciously manipulate the IMS call operation. An adversary can easily make ghost calls to launch a stealthy call DoS (Denial of Service) attack against specific cellular users. Only phone numbers, but not any malware or network information, are required from the victims. This sophisticated attack harnesses a design defect of the IMS call state machine, but not simply flooding or a crash trigger. To stealthily detect attackable phones at run time, we exploit a vulnerability of the 4G network infrastructure, call information leakage, which we explore using machine learning. We validate these vulnerabilities in operational 4G networks of 4 top-tier carriers across Asia and North America countries with 7 phone brands. Our result shows that the call DoS attack can prevent the victims from receiving incoming calls up to 99.0% time without user awareness. We finally propose and evaluate recommended solutions.

CCS CONCEPTS

• **Networks → Mobile and wireless security**; *Application layer protocols*; • **Security and privacy → Denial-of-service attacks**.

1 INTRODUCTION

IMS (IP Multimedia Subsystem) is the designated core system for call services in the 4G/5G era. It has offered two call services: VoLTE (Voice over LTE) and VoWi-Fi (Voice over Wi-Fi). VoLTE is an essential voice solution for the 4G LTE network, to supersede the legacy 2G/3G call services. VoWi-Fi complements VoLTE for the areas with poor cellular signals by enabling telephony calls over the Wi-Fi network. An Ericsson report [17] shows that the number of their subscriptions is projected to reach 6 billion in 2024 for around 90 percent of combined 4G and 5G subscriptions. Undoubtedly, the IMS system will play a decisive role for future call services.

VoWi-Fi extends the reach of the IMS call service, yet with a larger attack surface than conventional voice solutions. Its software-based framework is barely hardened by existing hardware-based security from the telecom modem. It may suffer, when an adversary gets full control over the phone OS (e.g., root access). As VoWi-Fi still follows the same security principle as VoLTE, we are interested in whether VoWi-Fi may imperil the IMS ecosystem. Once it can be breached, the IMS may be exposed to security threats.

In this work, we first discover a vulnerability of VoWi-Fi, *no app-level data-origin authentication*; threateningly, it allows the adversary to arbitrarily manipulate the IMS call operation. Such vulnerability lies in the fact that the standard design treats the device as one entity of security associations in the Internet protocol security (IPSec) protection over IMS services. Its security principle is to keep security parameters inside the phone, but not the IMS app that runs VoWi-Fi. Once the phone is compromised, they can be easily leaked. This vulnerability leads us to disclose that hijacking the VoWi-Fi signaling session is possible, and it allows the adversary to interact with the IMS system on a per-message basis.

We further identify two IMS vulnerabilities based on the hijacking: *no prohibition of concurrent call attempts* and *abusing reliability of provisional responses*. They root in an operational flaw from carriers and a design defect of the standard, respectively. By exploiting them, the adversary can make ghosts calls to launch a stealthy call DoS (Denial of Service) attack against specific cellular users. Only phone numbers, but not any malware or network information, are required from the victims. We conduct experimental validation in operational 4G networks of 4 top-tier carriers across Asia and North America countries with 7 phone brands. Note that we take a responsible manner that prevents carriers and cellular users from being hurt in all the tests. We neither try to overwhelm the IMS system by flooding data traffic, nor attempt to crash it using malformed signaling messages. We always use our own phones as the victims.

However, this attack works for only VoLTE and VoWi-Fi users in the same carrier network as the adversary. Given a target phone number, the phone may have only the 3G call service, temporarily handover from 4G to 3G, or belong to another different carrier. In these states, the phone may play ringtone under the attack, thereby making its user aware. We thus introduce a stealthy detection method that can remotely detect attackable phones at run time. We leverage machine learning (ML) to explore signaling message features available for the runtime detection and then integrate the feature-based detection into the attack. Our attack evaluation

MobiCom '20, September 21–25, 2020, London, United Kingdom
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-7085-1/20/09…$15.00
https://doi.org/10.1145/3372224.3380885

shows that the victims can suffer from call DoS up to 99.0% time under the attack without awareness. We finally propose a suite of recommended solutions and confirm their effectiveness based on a prototype. This paper makes four contributions as follows.

- We identify three vulnerabilities from VoWi-Fi and the IMS system. They can be exploited to hijack the VoWi-Fi signaling session and maliciously manipulate the IMS call operation. We validate them experimentally and analyze root causes.
- We devise a stealthy call DoS attack by exploiting the vulnerabilities. It is further advanced to an adaptive multi-layer DoS attack that maximizes call DoS durations.
- We apply ML into exploring a vulnerability of the 4G network infrastructure, call information leakage, which enables remote detection of a phone's call technology and state. It can assist in stealthily detecting attackable phones at run time.
- We validate the vulnerabilities and assess attack impact in operational 4G networks. We confirm them as general threats by covering 4 top-tier carriers across Asia and North America countries with 7 phone brands in our experiments.

The rest of the paper is organized as follows. Section 2 presents the attack surface and model. In Section 3, we disclose vulnerabilities of VoWi-Fi and IMS call technologies. We propose a stealthy call DoS attack and advance it with ML in Sections 4 and 5, respectively. We present solution, discussion, and related work in Sections 6, 7, and 8, respectively. Section 9 concludes the paper.

2 VOWI-FI: NEW ATTACK SURFACE

2.1 VoWi-Fi Primer

VoWi-Fi is a cellular voice service that enables cellular calls over Wi-Fi networks. Its service flow differs from conventional cellular voice solutions, VoLTE and circuit-switched (CS) call services. Figure 1 shows the 4G LTE network architecture with VoWi-Fi support. The UE (User Equipment) consumes the VoWi-Fi service by connecting to the core network through the Wi-Fi AP and the Internet, but has the conventional ones through the LTE base station. Their traffic flows reach the core network at the ePDG (evolved Packet Data Gateway) and the S-GW (Serving Gateway), respectively. The ePDG enables the untrusted non-3GPP access from the Internet. It authenticates the UE through the authentication server and then establishes an IPSec tunnel to the UE for the untrusted access [6, 12]. In the core network, the P-GW (Packet Data Network Gateway) forwards the VoWi-Fi traffic between the ePDG and the IMS core.

VoWi-Fi is a VoIP (Voice over IP) service supported by the IMS core [8] and protected by the security manner of the untrusted non-3GPP access, i.e., the IPSec tunnel between the UE and the ePDG. It uses SIP (Session Initiation Protocol) as its signaling protocol but with some 3GPP-specific modifications [24, 29]. It requires an IMS app installed at the UE. To start the VoWi-Fi, the app does registration and mutual authentication, which is based on the IMS Authentication and Key Agreement [5, 11] protocol, with the IMS core. This registration procedure derives IPSec ESP (Encapsulating Security Payload) [30] security associations between the IMS app and core. The IPSec integrity protection over the SIP signaling is mandatory, but the confidentiality is optional [11].

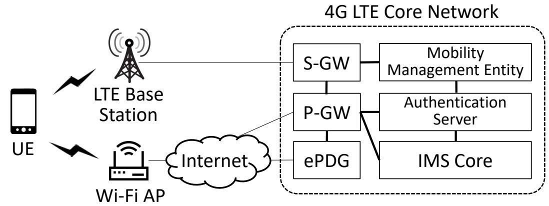


Figure 1: 4G LTE network architecture with VoWi-Fi.

2.2 Exposure of IMS Potential Vulnerabilities

VoWi-Fi has a larger attack surface than conventional cellular voice solutions. It keeps service operation and security functions in the software including the IMS app and mobile OS, but the conventional ones hide full (e.g., CS-based) or part of them (e.g., VoLTE [31, 33]) within the hardware modem. Its software framework may create more exploitable vulnerabilities. Specifically, the adversary can easily learn service operation from collected packet traces [54], and may steal security parameters from the software or the delivery path from the SIM card to the IMS app (e.g., extracting security keys with a sniffer, SIMTrace [18]). Such vulnerabilities may allow the adversary to directly interact with the IMS core.

It is threatening that VoWi-Fi may cause the IMS potential vulnerabilities, which were hidden by conventional IMS-based services, to be exposed. Once the adversary can gain fine-grained interaction with the IMS on the exchange of signaling messages, any design defects of its call flow procedure or state machine may be exploited to launch attacks. Such exploitation is not possible by abusing conventional telephony APIs, which support only coarse-grained call operation. We look into this security threat using VoWi-Fi and seek to answer the following three questions.

- Can the hijacking of the VoWi-Fi signaling session be completely prevented by its mandatory IPSec integrity protection and the IPSec tunnel of its non-3GPP access?
- Does the IMS restrict the IMS app to normal call operation? If not, the adversary may be allowed to make any call attempts arbitrarily or ghost calls by manipulating the delivery of SIP messages, given the hijacked signaling session.
- Does the IMS prevent intentional faults or malicious actions in the call procedure from a compromised app? If not, the adversary may generate them to obstruct call services.

Unfortunately, we discover that the answers to these questions are all *no*. We elaborate on the details and experimentally validate them in the next section. Note that the 5G voice solution, VoNR (Voice over New Radio), is also an IMS-based service, so the potential vulnerabilities can threaten upcoming 5G networks.

2.3 Attack Model and Methodology

Victims are mobile users with VoLTE or VoWi-Fi services. The attacker requires only commodity smartphones without any remote access to victim devices or any malware on them. Attack phones have to carry SIM cards with VoWi-Fi services, as well as be rooted for full programmability and system data access. Although getting smartphones rooted becomes increasingly difficult, it is not completely prohibited and we have rooted smartphones from six phone brands. Moreover, only one or few attack phones are required for the attack. To maximize attack impact, the attacker can give attack phones strong Wi-Fi signal strength and no interference by controlling their Wi-Fi environments. In all cases, carrier networks are not controlled by the attacker and have no compromised facilities.

We conduct experiments in the networks of four carriers: two from one country in North America and the other two from another country in Asia. The former two carriers, denoted as NA-I and NA-II, together take more than 52.4% market share of the country, whereas the latter two, denoted as AS-I and AS-II, take about 42.9% in the Asia country. We consider all the experiments for Carriers NA-I and AS-I, but only validate vulnerabilities for the others. We use 8 phone models as the attack phones with Android versions from 5.1.1 to 9.0.0: Samsung S5/S6/S8, Google Pixel XL, hTC U11, Sony Xperia XA2, Essential PH-1, and Asus Zenfone 4. Since carriers have different phone models available to the VoWi-Fi service, our attack phone models vary with them. For security concerns, we do not disclose specific combinations of the phone models and carriers in each experiment. We avoid encouraging people to launch attacks using the available combinations. The victim phones include 15 different models with Android/iOS systems from 7 brands: Samsung, Essential, Google Pixel, Asus, Apple, hTC, and Sony.

Responsible methodology. We conduct this study in a responsible manner that prevents carriers and cellular users from being hurt in all tests. For the carriers, we neither try to overwhelm the cellular infrastructure or the IMS core by flooding data traffic, nor attempt to crash the IMS using malformed SIP messages. Instead, we interact with the IMS using valid SIP messages under its constraints (e.g., the limit of concurrent call attempts). Our focus is to validate its vulnerabilities, but not attack it or cause any damages. Moreover, we always use our own phones as the victim phones. Although we focus on only attacks against phone devices, we believe more powerful attacks against the IMS core are possible to be launched successfully based on the exposed vulnerabilities.

3 MALICIOUS MANIPULATION OF IMS CALL SERVICE OPERATION

We uncover that the VoWi-Fi signaling session can be hijacked to maliciously manipulate the IMS call operation. Given the security mechanisms stipulated in the standard, the session hijacking is not completely forbidden due to no app-level data-origin authentication (V1). It can be used to further expose two vulnerabilities of the IMS system: no prohibition of concurrent call attempts (V2) and abusing reliability of provisional responses (V3).

3.1 Hijack VoWi-Fi Signaling Session

The VoWi-Fi signaling session between the IMS app and core is protected by two levels of security mechanisms according to the standard [6, 7, 11, 12]. Figure 2 shows the security architecture and its current practice. At the first level, an IPSec tunnel shall be built between the Wi-Fi interface and the ePDG for the untrusted access over non-3GPP networks [6]. When the packets are sent via the IMS virtual interface (VIF), they are encapsulated into the IPSec tunnel and then delivered to the core network via the Wi-Fi interface. At the second level, the VoWi-Fi signaling session shall be protected by the IPSec transport mode with the ESP protocol, which is built between the IMS VIF and core, in terms of integrity protection [7].

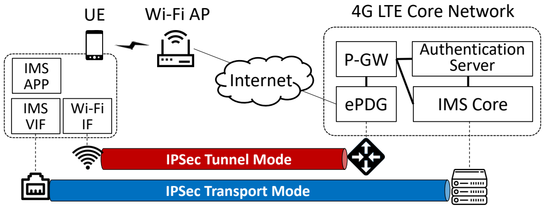
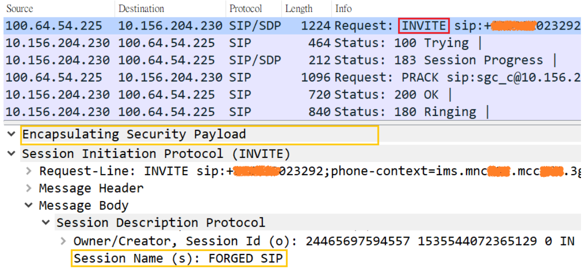


Figure 2: Two levels of IPSec protection over the VoWi-Fi signaling session between the IMS app and core.



```
Source          Destination     Protocol  Length Info
100.64.54.225   10.156.204.230  SIP/SDP    1224 Request: INVITE sip:+[redacted]023292
10.156.204.230  100.64.54.225   SIP         464 Status: 100 Trying |
10.156.204.230  100.64.54.225   SIP/SDP     212 Status: 183 Session Progress |
100.64.54.225   10.156.204.230  SIP        1096 Request: PRACK sip:sgc_c@10.156.2
10.156.204.230  100.64.54.225   SIP         720 Status: 200 OK |
10.156.204.230  100.64.54.225   SIP         840 Status: 180 Ringing |
v Encapsulating Security Payload
v Session Initiation Protocol (INVITE)
  > Request-Line: INVITE sip:+[redacted]023292;phone-context=ims.mnc[redacted].mcc[redacted].3
  > Message Header
  v Message Body
    v Session Description Protocol
      > Owner/Creator, Session Id (o): 24465697594557 1535544072365129 0 IN
        Session Name (s): FORGED SIP
```

Figure 3: A VoWi-Fi call is successfully made by the forged INVITE and PRACK messages in the AS-I network.

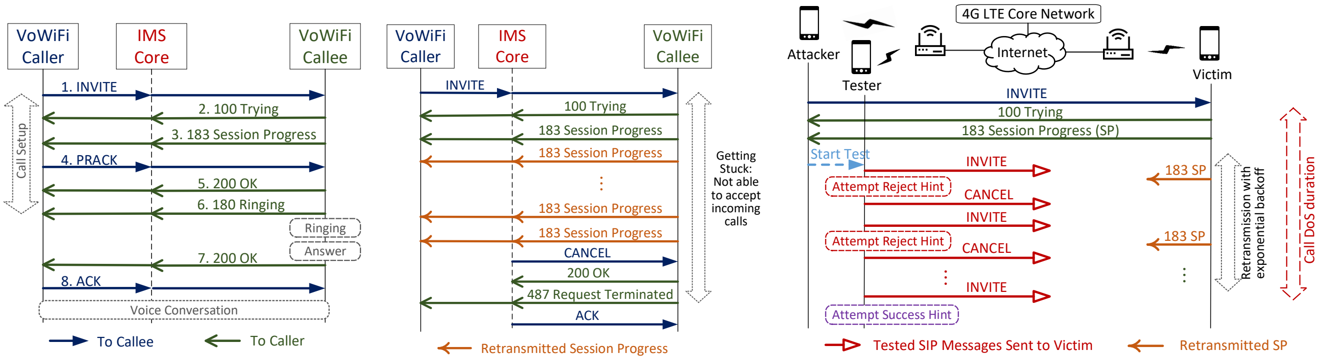
Such two-level security protection can defend against most outside attacks from non-3GPP networks, though there are still some threats with limited impact (e.g., call inference [58] and man-in-the-middle [13] attacks). However, it may not be immune to inside threats at the UE. When the UE is not trusted and a malicious app gains its root access, the app may be able to hijack the VoWi-Fi signaling session.

3.1.1 *V1: No App-level Data-origin Authentication.*

We discover that there is no app-level data-origin authentication for the VoWi-Fi signaling session; that is, its access is not restricted to only the IMS app. When the IMS app relies on the system to carry out the IPSec transport, we can fetch the parameters of its IPSec security associations from the system and then use them to fabricate valid SIP messages [54]. Besides, other two major steps are needed for the session hijacking. First, we should track the sequence number of the IPSec session at run time, which are required in the ESP payload, as well as follow its TCP sequence number. Second, we should apply the default ESP padding algorithm [30] and then generate authentication data using the specified hash algorithm and keys. Note that the `HMAC-SHA-1-96` algorithm [35] is used by the carriers.

Experimental validation. We discover that Carriers NA-I and AS-I indeed adopt the IPSec transport mode over VoWi-Fi signaling sessions. We can observe that the initial `REGISTER` message sent by the IMS app includes its capable security methods in the `Security-Client` field, such as the supported IPSec version `ipsec-3gpp`, the protocol `esp`, and the mode `transport`. However, the other two carriers do not enable this mandatory feature and leave the signaling sessions unprotected.

We next validate that the VoWi-Fi session hijacking is permitted by using fabricated SIP messages to successfully make a VoWi-Fi call. Figure 3 shows the fabricated `INVITE` message where we set



(a) VoWi-Fi call setup procedure.

(b) VoWi-Fi callee gets stuck.

(c) Gauging call DoS duration caused by an INVITE message.

Figure 4: The VoWi-Fi call setup procedure versus the abuse scenario where the callee gets stuck without receiving PRACK.

the Session Name to be FORGED SIP and its subsequent SIP messages. The responses including the Trying and Session Progress messages from the IMS show that the forged INVITE is considered to be valid. To make the call successful, we send back another forged PRACK (Provisional Response ACKnowledgement) message. Afterwards, the OK and Ringing messages are received and the callee starts to ring. As for Carriers NA-II and AS-II, which do not have that IPSec protection, we can easily hijack their VoWi-Fi sessions.

Variance. Some combinations of phone models and carriers are not susceptible to this vulnerability but may still suffer. The difficulty of exploiting this vulnerability depends on two major factors: the IPSec transport protection on the VoWi-Fi signaling and its device implementation. Carriers and phone vendors respectively take charge of them. There are three main cases from low to high degrees of difficulty in the exploitation. First, the IPSec transport is not enabled by Carriers NA-II and AS-II, so the VoWi-Fi sessions of their supported phones that we have can be easily hijacked. Second, the IPSec is supported by Carriers NA-I and AS-I, but some phone models support its implementation by relying on the system. Their sessions can be hijacked as shown above. Third, some phone models do not rely on the system for the IPSec implementation, so the IPSec parameters cannot be easily obtained. It is more challenging for the exploitation but still possible. The adversary can use the SIM card sniffer to capture the IPSec parameters [18] from the communication between the IMS app and the ISIM (IP Multimedia Services Identity Module) module on the SIM card.

Root cause and lesson. This vulnerability can be attributed to a *design defect* that the standard stipulates only device-level IPSec protection. It works for the conventional voice solutions, VoLTE and 3G CS-based voice, since they hide full or partial signaling operation in the device modem and it is protected by the hardware-based security. However, the VoWi-Fi signaling operation is handled by the software. Its security parameters have to be passed to the mobile OS so that they can be easily stolen. Given this inherent weakness of VoWi-Fi, the standard does not strengthen its security mechanism and should take the blame. It calls for an app-level data-origin authentication from the IMS system.

On the other hand, it can be also attributed to an *operational flaw* by considering that Carriers NA-II and AS-II do not even enable that mandatory IPSec protection. The possible reason is that the signaling messages have been protected by the first-level IPSec tunnel, so it is sufficient to defend against outside network threats. Apparently, they ignore the threats coming from inside the phone.

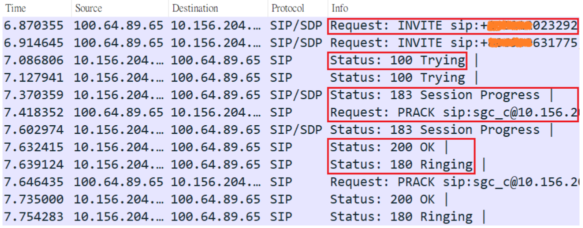
3.2 Manipulate IMS Call Service Operation

The IMS call service relies on the SIP signaling for the call control. As shown in Figure 4(a), the IMS core mediates the delivery of the SIP messages between the caller and the callee in the VoWi-Fi call setup procedure. All messages except the PRACK and its 200 OK response are similar to those of conventional VoIP calls. The PRACK is introduced to provide end-to-end reliability for provisional responses (e.g., Session Progress) [41], which provide information on the progress of request processing. The reliability is essential for the IMS to provide carrier-grade voice services.

Once the SIP signaling session is hijacked, the adversary can interact with the IMS core on a per-message basis. By carefully examining the call operation in practice, we discover two potential vulnerabilities in the following.

3.2.1 V2: No Prohibition of Concurrent Call Attempts. The caller is allowed to make successive calls to speak over a call while holding the other(s), or have a conference call [4], but concurrent call attempts are prohibited by the system's GUI and call API. In the conference call service, the caller can have concurrent call sessions, but needs to make them one by one and add each callee that has answered to the conference call. Seemingly, only one call attempt is permitted to be made at a time; however, it may not be the case. The prohibition may be fulfilled only at the end device but not at the IMS. Once the prohibition based on the system's GUI and call API can be bypassed by using V1, it may be possible to generate concurrent call attempts successfully. To this end, the adversary can send out multiple INVITE messages simultaneously and handle their session states individually.

Experimental validation. We validate this vulnerability by initializing two concurrent call attempts from a caller towards two different callees and properly handling their subsequent SIP messages at the caller. Both of the call attempts indeed take effect. We can hear the callees' ringtones simultaneously and observe the SIP messages of those two concurrent calls at the caller in Figure 5. The messages enclosed by rectangles belong to one call attempt,



```
Time      Source        Destination   Protocol Info
6.870355  100.64.89.65  10.156.204.…  SIP/SDP  Request: INVITE sip:+[redacted]023292
6.914645  100.64.89.65  10.156.204.…  SIP/SDP  Request: INVITE sip:+[redacted]631775
7.086806  10.156.204.…  100.64.89.65  SIP      Status: 100 Trying |
7.127941  10.156.204.…  100.64.89.65  SIP      Status: 100 Trying |
7.370359  10.156.204.…  100.64.89.65  SIP/SDP  Status: 183 Session Progress |
7.418352  100.64.89.65  10.156.204.…  SIP      Request: PRACK sip:sgc_c@10.156.2
7.602974  10.156.204.…  100.64.89.65  SIP/SDP  Status: 183 Session Progress |
7.632415  10.156.204.…  100.64.89.65  SIP      Status: 200 OK |
7.639124  10.156.204.…  100.64.89.65  SIP      Status: 180 Ringing |
7.646435  100.64.89.65  10.156.204.…  SIP      Request: PRACK sip:sgc_c@10.156.2
7.735000  10.156.204.…  100.64.89.65  SIP      Status: 200 OK |
7.754283  10.156.204.…  100.64.89.65  SIP      Status: 180 Ringing |
```

Figure 5: Two concurrent call attempts that successfully make two separate calls from a caller in the AS-I network.

Carrier	Max number of concurrent call attempts	Provisional response	Failure status
NA-I	3	Yes	603 Decline
NA-II	3	Yes	403 Forbidden
AS-I	5	Yes	606 Not Acceptable
AS-II	1	No	N/A

Table 1: Maximum number of concurrent call attempts.

whereas the others are from the other call attempt. These two call attempts are made to different call numbers, and both callees report the status `Ringing` at the end.

Variance. We test the maximum number of concurrent call attempts from a caller to different callees by varying the call attempt number and observing the response associated with each attempt. Table 1 shows that the carriers differ in the maximum number and the response message of the case that an `INVITE` message is not accepted. All the carriers except AS-II reply to the unaccepted `INVITE` with a provisional response including a failure status. One interesting observation is that the caller can initiate multiple valid call attempts, which are determined based on a non-failure status, towards a single callee. We further observe that the maximum number of concurrent call attempts for the single callee case is the same as that for the multi-callee case.

Root cause and lesson. This vulnerability lies in an *operational flaw* from carriers. They may enable concurrent call sessions to support conference calls or other services and also set number limits of the call sessions. It causes concurrent call attempts to be permitted at the IMS, since the acceptance of a valid call attempt (i.e., `INVITE`) leads to the initialization of a call session. Such allowable operation is not used in practice and even is prohibited by the device system's call API, but gives a chance to be abused by the adversary. To prevent it, the IMS needs to differentiate call attempts from established call sessions and then set different limits on them.

3.2.2 V3: Abusing Reliability of Provisional Responses. The establishment of an IMS call may fail in the absence of sufficient resource, and meanwhile the callee user may have been alerted. To eliminate this annoying case where an invalid call causes the phone to ring, a mechanism called precondition [16] is introduced to enable resource reservation during the call setup [7]. It relies on a SIP provisional response (e.g., `Session Progress`); moreover, a reliability mechanism that acknowledges the response should be supported to confirm the reservation. The precondition mechanism is not widely used in the Internet VoIP applications, but the 3GPP standard suggests its support for the IMS call service [7], in order to maintain the carrier-grade call quality.

To enable the precondition mechanism, the caller sets an option-tag `precondition` in the `INVITE` message's `Supported` header field, together with another option-tag `100rel`, which indicates the reliability. As shown in Figure 4(a), the callee replies to the `INVITE` with a provisional response, `Session Progress`. In the response, the callee confirms a set of service requirements (e.g., port and session parameters) that are specified in the `INVITE` SDP (Session Description Protocol), as well as sets the `precondition` option-tag. Meanwhile, it starts to do resource reservation based on the requirements and waits for a reliable alerting indication (i.e., the `PRACK` message) to alert the user. After receiving the `Session Progress`, the caller also reserves resource at its side and acknowledges it with the `PRACK`. After receiving the `PRACK`, the callee starts to ring.

However, the reliability mechanism of the provisional response may be abused, since it can get the callee stuck in the *proceeding* state of a call session [42]. In this state, the callee is not able to accept other incoming calls. It cannot leave it until the `PRACK` message, which acknowledges the `Session Progress`, is received or the session is canceled. For the reliability, the callee retransmits the `Session Progress` with an exponential backoff timer. When the retransmission times reach a maximum number, the IMS cancels the session by sending a `CANCEL` message to the callee. The maximum number and the initial retransmission timeout are carrier-specific.

The caller can abuse this mechanism to prevent the callee from receiving incoming calls without awareness of the callee user. As shown in Figure 4(b), the caller sends the `INVITE` to the callee without answering `PRACK`, thereby keeping it in the proceeding state. The callee does not ring without the `PRACK`. Although being stuck can sustain for only a short time period, it can be exploited as a building block to launch a long-time call DoS attack on the callee.

Experimental validation. We validate this vulnerability using three phones: an attacker, a tester, and a victim. We control the attacker and the tester to send SIP messages. As shown in Figure 4(c), the attacker sends the victim an `INVITE` message without answering `PRACK`, and then the victim keeps retransmitting `Session Progress` messages. We seek to gauge the DoS duration caused by the single `INVITE`. We let the tester continue to send `INVITE` messages to the victim. By considering the last failed `INVITE`, we observe that the DoS durations are at least 14.5 s and 32.4 s for Carriers NA-I and AS-I, respectively. The callees from these two carriers respectively send 4 and 5 `Session Progress` messages to the attacker with the exponential backoff mechanism. Each of them finally receives a `CANCEL` message from the IMS core. We observe similar results from the other two carriers.

Note that there are two important findings. First, this vulnerability also exists at the VoLTE callee for all those carriers and test phones. It is because VoLTE is also supported by the IMS core with the similar call operation. Second, the callee is prohibited to make any outgoing call during the DoS duration. When we use the GUI to dial a call at the callee, the GUI gets stuck at the dialing page until the DoS duration ends. This negative impact happens for most test phones and is vendor-specific.

Variance. We discover two other variances in the phone's IMS app implementation. First, some phone models do not enable the precondition mechanism by default, but we can force them to suffer. In this case, the callee sends a Ringing message directly in response to the INVITE and then plays ringtone. Since the Ringing is also a provisional response, we can request its reliability by specifying an 100rel option-tag in the Require header field of the INVITE. It causes the callee to wait for a PRACK message before playing ringtone. Second, a phone model does not follow the reliability mechanism though it is enabled. It starts to play ringtone right after sending out the Session Progress without waiting for the PRACK. The DoS attack can get the phone stuck at the call GUI, but its owner is alerted. On the other hand, the phone can suffer from the annoying case prevented by the reliability mechanism.

Root cause and lesson. The root cause is a *design defect* that the standard does not prevent negative impact from the reliability mechanism. It is reasonable to enable such mechanism due to two reasons. First, the cellular resource is costly compared with the Internet. Second, the essential call service has to be carrier-grade for the cellular network, so it is not acceptable for an invalid call to make the phone ring. When adopting this feature, the 3GPP standard [7] does not carefully review it in terms of security. This security vulnerability has not been disclosed in the IETF standard [16].

4 GHOST CALLS: STEALTHY CALL DOS

We propose a stealthy call DoS attack against telephony users by generating ghost calls based on the vulnerabilities. Given only the victim's phone number, it can prevent the victim phone from receiving incoming calls or making outgoing calls. It is stealthy without causing the device to ring or getting the victim's attention. We finally introduce other attack variances.

4.1 Stealthy Call DoS Attack

We devise this attack by using V3 as a building block. It works for only phones that are using VoWi-Fi or VoLTE and subscribe to the same carrier as the attack phone. Without knowing the status of target phones, the attacker needs to detect whether they are attackable. They may handover between 3G/4G networks or use the 3G call service, so the detection shall be done at run time. We here assume that the target phones are always attackable and will introduce an ML-assisted stealthy detection approach in Section 5.

The reason why this attack can work only when two call ends belong to the same carrier is that current IMS systems from different carriers do not communicate with each other directly based on the SIP protocol. Instead, the communication relies on the traditional PSTN (Public Switched Telephone Network) network. Even when two call ends from different carriers both use VoWi-Fi/VoLTE, their call setup involves translations between the SIP and PSTN protocols. It prevents the attacker from manipulating the victim's call state machine. Although the 3GPP standard [8] provides two communication options, an SIP proxy and an SIP/PSTN translation gateway, most carriers are currently taking the second option by inheriting the legacy PSTN system.

Static DoS attack. We develop an attack app on the attack phone. It can initiate a call DoS duration on the victim phone by sending it an INVITE message without acknowledging any provisional responses. It can keep repeating this process to continue the call DoS for a long-duration attack. Once receiving the CANCEL from the IMS, the attack app can start next DoS phase by sending another INVITE message. The upper part of Figure 6 shows this attack process.

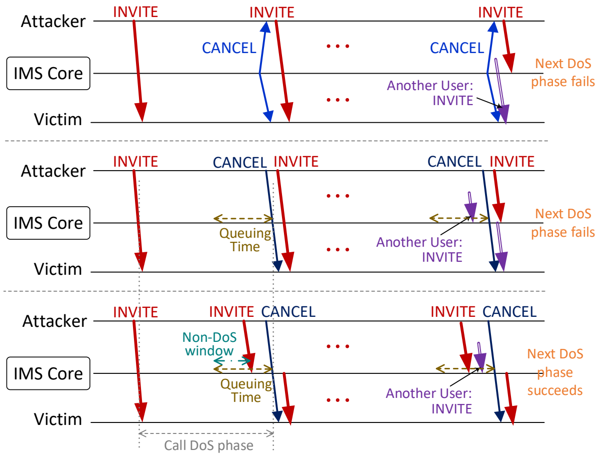


Figure 6: Stealthy call DoS attack scenarios.

Prioritized Mark	NA-I	NA-II	AS-I	AS-II
DSCP (Value)	CS6 (48)	CS4 (32)	AF31 (26)	AF41 (34)
802.11e AC	AC_VO	AC_VO	AC_VI	AC_VI

Table 2: DSCP and 802.11e AC parameters used for VoWi-Fi traffic vary with carriers.

However, there exists a non-DoS window period between the adjacent call DoS phases, so another normal call's INVITE may sneak into this period and cause the next DoS phase to fail. In order to shorten the non-DoS window, we enable the attack phone to actively cancel the current DoS phase so that the INVITE of the next DoS phase can arrive right after the CANCEL, as shown in the middle of Figure 6. Furthermore, we discover that another non-victim phone's INVITE that is sent before the attack phone sends out CANCEL can still successfully arrive at the victim and thus hinder the next attack INVITE from being forwarded by the IMS core. This validation is done by letting the attack phone ask the non-victim phone to send out the INVITE before canceling the current call session. It implies that the IMS core queues INVITE messages for a while before denying them. This phenomenon is observed from all the four carriers.

Given the INVITE queuing at the IMS core, only the first INVITE arriving within the queuing period prior to the CANCEL arrival is considered to be valid and accepted. Its following ones will not be accepted, as shown in the lower part of Figure 6. For the success of the next DoS phase, the attack INVITE has to be the first one to arrive within that queuing period. The non-DoS window becomes the time interval between the start time of the queuing and the arrival of the attack INVITE. In order to make this non-DoS window as short as possible, we seek to maximize an *attack interval* that is between the sending times of the INVITE and CANCEL messages at the attacker, given that the INVITE is accepted.

Static attack interval. We next determine the maximum of valid attack intervals that can always start new DoS phases. They may vary with network conditions of Wi-Fi networks, the Internet,

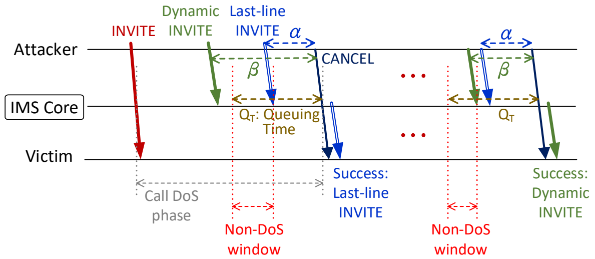


Figure 7: The adaptive multi-layer DoS attack.

and cellular networks, since varying wireless channel and network congestion can affect arrival times of the SIP messages. However, we discover that carriers prioritize VoWi-Fi traffic to ensure its low-latency delivery and the service quality. They utilize DSCP (Differentiated Services Code Point) in IP networks and the 802.11e high-priority AC (Access Category) in Wi-Fi networks. Table 2 shows the DSCP/AC parameters used by those four carriers. Such low-latency delivery can minimize the impact of those network dynamics on the message arrival times and the valid attack intervals.

We conduct experiments to gauge the maximum of the valid attack intervals for Carriers AS-I and NA-I. We vary attack intervals from 0 ms to 600 ms at every 10 ms, each of which has 20 runs, and gauge each interval's success ratio. We observe that the maximum values of the attack intervals with 100% success (i.e., valid attack intervals) for those two carriers are 100 ms and 50 ms, respectively; the minimum ones of those with all failures are 490 ms and 290 ms. We further validate that the maximum valid intervals can work in various cases. We vary the victim's location to consider four cases of the Wi-Fi signal strength: -40~-49 dBm, -50~-59 dBm, -60~-69 dBm, and -70~-79 dBm. We also examine different Internet conditions by considering three test times: morning, afternoon, and night. With 20 runs in each of these 12 combination cases, we confirm that those two intervals 100 ms and 50 ms can always make the DoS attack succeed for Carriers AS-I and NA-I, respectively. We note two important things. First, the attack phone is always given strong Wi-Fi signal strength in the attack model, so we do not consider its signal strength with different cases. Second, when a VoWi-Fi phone's Wi-Fi signal strength is smaller than -80 dBm, its voice service is usually switched to 3G or VoLTE.

Although the maximum valid attack interval may vary with carriers, victim locations, or other factors, the attacker can stealthily probe it before and during an attack. We observe that whether an INVITE message is accepted can be judged based on its subsequent response message (e.g., Session Progress) without causing ringtone on the victim phone. Specifically, given an accepted INVITE, the Session Name field of the SDP in the response message contains the string QC VOIP for both Carriers NA-I and AS-I. It becomes "-" and Xmserver respectively for a failed INVITE. Moreover, the attacker can ensure successful attacks by conservatively choosing smaller attack intervals that just increase the non-DoS window.

4.2 Adaptive Multi-layer DoS Attack

We thus design an adaptive multi-layer DoS attack to tackle the dynamics of valid attack intervals. It dynamically approaches the maximum of valid attack intervals over time by exploiting two INVITE messages. It uses the first INVITE to approach the maximum interval and it is sent at dynamic times. Its delivery times are adjusted according to consecutive success or failure trials. Since the first INVITE may fail, the second INVITE is used as the last line of the attack to ensure that the next DoS phase can be successfully launched. The attack interval of the last-line INVITE can be chosen as the one that always succeeds in various cases.

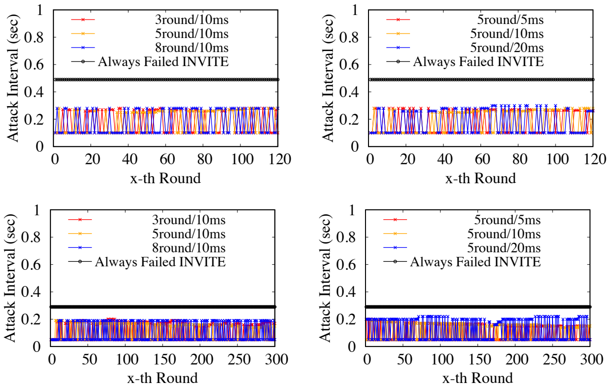


Figure 8: Attack intervals of valid INVITE messages in adaptive call DoS attacks (Upper: AS-I; lower: NA-I).

Figure 7 illustrates the adaptive multi-layer DoS attack. The first INVITE initiates the first call DoS phase. The attacker sends out this session's CANCEL after a specified DoS duration. Before the CANCEL, two INVITE messages for the next DoS phase are sent. The dynamic one is sent first based on a dynamic attack interval β; the last-line one is then sent at a fixed interval α. We can adapt β at the granularity a ms based on b consecutive rounds of successes and failures. In this case, the last-line INVITE succeeds but the dynamic one fails, so the non-DoS window at the IMS is the interval between the start time of the queuing and the arrival of the last-line one. In the latter case, where the dynamic one succeeds and the last-line one is invalid, the non-DoS window becomes shorter. Note that this adaptive attack requires three concurrent call attempts (i.e., three outgoing uncanceled INVITE), which include the INVITE of current DoS phase, and the next phase's dynamic and last-line ones.

We note two important things for this adaptive attack. First, the attacker is allowed to collect statistics and then adjust β accordingly by identifying the status of INVITE messages stealthily. Second, the total number of dynamic and last-line INVITE messages can be more than two, but is constrained by the maximum number of concurrent call attempts. Although Carrier AS-II does not support this adaptive attack, the static call DoS attack is still applicable.

4.3 Attack Prototype and Evaluation

We implement the adaptive DoS attack on our attack phones and evaluate its DoS time with an one-hour attack. Since we are not able to know the exact DoS time at the IMS core, we estimate its lower bound as follows. We use another test phone to send the victim an INVITE at the time when it certainly fails. According to the experiment in Section 4.1, the times can be chosen as 490 ms and 290 ms before the attacker's CANCEL for Carriers AS-I and NA-I, respectively. The interval between the sending time of this invalid

INVITE and that of the valid INVITE from the attack phone can be considered as the upper bound of the non-DoS window, which can give the DoS time's lower bound. For the fixed and initial dynamic intervals (α, β), we set them to be (100 ms, 280 ms) and (50 ms, 200 ms), respectively. We set the call attack period, which is the interval between two adjacent CANCEL messages, to be 30 s and 12 s, respectively, based on the DoS durations caused by an INVITE. For the one-hour attack, the attacker requires 120 rounds of the period in Carrier AS-I's network but needs 300 rounds in Carrier NA-I's.

Figure 8 shows the attack intervals of valid INVITE messages (dynamic or last-line) in an one-hour attack, where we vary a and b. Carriers AS-I and NA-I respectively have 0.17-0.19 s and 0.10-0.12 s attack intervals in average. It shows that different parameter values make negligible effect on the result. By considering the always-failure case, we can get upper bounds of the aggregate non-DoS windows, 1.00% and 1.59% time, respectively. We compare the adaptive attack with the static one where only the last-line INVITE message is sent. With the static attack's upper bounds 1.30% and 2.00% time, the adaptive attack can perform better with 23.08% and 20.50% gains on the lengths of aggregate non-DoS durations. In other words, it can cause victim phones to suffer from the call DoS for at least 99.00% (AS-I) and 98.41% (NA-I) time. Note that the victim phones never ring during the experiment.

Multi-victim attack. We devise this attack based on the requirement of only one call attempt at a time. The attack phone sends out a new INVITE only after the existing call session is canceled. The phone can launch this simple attack against multiple victims concurrently, but the maximum number of victims depends on the maximum allowable number of concurrent call attempts, e.g., 5 and 3 victims for Carriers AS-I and NA-I respectively. Table 3 summarizes the DoS times in various attack cases.

4.4 Other Attack Variances

DoS attacks on multi-line telephony systems. The targets of this attack include customer call services of the enterprise and emergency call systems of the public sector. They rely on multi-line telephony systems to serve multiple customer calls simultaneously. The number of available telephony lines/representatives is limited, so the adversary may launch DoS attacks by generating ghost calls to exhaust them based on V2. Such call floods can cause customers to stand in long lines and possibly hang up their calls.

Social engineering attacks: large-scale missed calls. The adversary may generate missed calls on a large number of potential victims for social engineering attacks by exploiting V2. The missed calls can lure the victims to call back, and then the adversary charges a ton by minute or achieves other purposes.

Conventional SIP attacks. The adversary can launch conventional SIP attacks against the IMS system by exploiting V1, since the SIP messages sent by the adversary are considered valid and processed by the IMS. There are three possible SIP attacks [22, 42]. First, the SIP flooding attacks including INVITE and REGISTER flooding may deplete resources in the IMS and prevent it from handling new calls. Second, malformed SIP messages may cause the IMS to crash or get stuck. Third, the call ID spoofing can be exploited to impose phone harassment on cellular users.

Attack mode Number of victims	Adaptive 1	Static 1	Multi-victim 2	Multi-victim 4
AS-I (one attacker)	99.00%	98.70%	97.38%	96.80%
NA-I (one attacker)	98.41%	98.00%	93.60%	N/A

Table 3: DoS times in percentage of one hour for various attack cases. Multi-victim attack results are in average.

5 ML-ASSISTED CALL DOS ATTACK

In the call DoS attack, the attacker needs to remotely detect attackable phones that are using VoWi-Fi or VoLTE in the same carrier network. We use an ML approach to identify SIP message features that the attacker can use for the remote detection. The attacker does this ML-based identification for each interested carrier based on collected call SIP traces before launching attacks, and runs detection based on the identified features during attacks. The remote detection not only needs to be stealthy without causing target phones to ring, but also supports real-time operation during attacks. It should allow the attack app to detect when a victim phone under an attack has switched from VoWi-Fi/VoLTE to the 3G call service, and then stop the attack immediately.

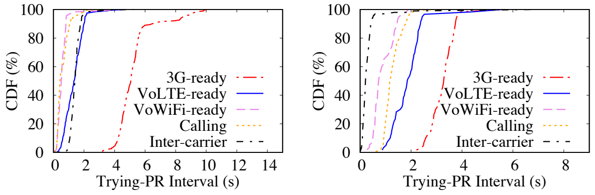
The attack app needs to know the result of each attack INVITE so that it can take corresponding actions. The result depends on the target device's call state at the INVITE arrival. There are three call states: idle, calling, and talking. They respectively represent no proceeding of call setup or talking, proceeding with a call setup, and talking in a call. The attack INVITE succeeds (i.e., it is accepted) in both idle and talking states, but fails in the calling state. Thus, the attack app should detect the target phone's call technology and state at run time.

To be stealthy, the attack app is only allowed to rely on the initial SIP messages that arrive at the attack phone before the PRACK delivery. We observe that the content of the SIP messages can vary with carriers and phone models. Given a carrier, we aim to identify a set of features that can be used to classify call technologies and states at the callee. Moreover, it has to be independent of various phone models and can be applied to all the phones in the same carrier network, since the adversary does not know the victim's phone model.

However, it can be very labor-intensive to manually extract the classification features from the SIP traces of various phones for each carrier, since the SIP messages contain a lot of information and their content may also vary with phones. Specifically, they contain many fields, each of which has various values, and there are variances in the message flow and the message interval. It thus calls for an ML-based classification method, which can be applied to all the carriers and automatically identify the classification features for each given carrier.

5.1 ML-based Call Information Leakage

In this section, we discover that the attack app can cause a remote phone to leak its call technology and state using a silent call. We first collect traces of the initial SIP messages in various cases and categorize them. We further apply the SVM (Support-Vector Machine) method [21] into the category classification, by leveraging its kernel trick [37] to perform a non-linear classification for a



(a) Carrier AS-I.

(b) Carrier NA-I.

Figure 9: The Trying-PR intervals vary with call technologies and states.

Carrier AS-I				
Actual / Predicted	VoWiFi/VoLTE-ready	3G-ready	Calling	Inter-carrier
VoWiFi/VoLTE-ready	100%	0%	0%	0%
3G-ready	0%	100%	0%	0%
VoWiFi/VoLTE/3G-calling	0%	0%	100%	0%
Inter-carrier	0%	0%	0%	100%

Carrier NA-I				
Actual / Predicted	VoWiFi/VoLTE-ready	3G-ready	Calling	Inter-carrier
VoWiFi/VoLTE-ready	100%	0%	0%	0%
3G-ready	0%	95.8%	4.2%	0%
VoWiFi/VoLTE/3G-calling	0%	0%	98.6%	1.4%
Inter-carrier	0%	0%	1.4%	98.6%

Table 4: Confusion matrix of the call classification.

high-dimensional feature space. We finally summarize the findings of the call information leakage.

Trace collection. We consider three call technologies including 3G, VoLTE, and VoWi-Fi, as well as their three possible call states: idle, calling, and talking. By covering intra-carrier and inter-carrier calls with different combinations of caller/callee phones and carriers, we collect traces of the SIP messages from more than 5,000 call attempts. There are totally 10 different phone models with 7 brands and 4 carriers. For each combination, the traces of 10 call attempts are collected. We develop a semi-automatic tool for the trace collection. Given a callee setting including the call technology and the carrier, the tool can automatically go through three states with 10 call attempts each while collecting the initial SIP messages.

Categorization. Our goal is to detect attackable phones and get results of attack INVITE messages at the attack app. It is unnecessary to clearly differentiate all the 18 different combinations of call technologies (3G/VoWi-Fi/VoLTE), call states (idle/calling/talking), and carrier cases (intra-carrier/inter-carrier). We group two sets of the combinations without affecting the needs of our goal achievement. First, we group all the inter-carrier cases, where the call DoS attack is not applicable, into only one category "inter-carrier". Second, we group the idle and talking states, both of which allow the INVITE to succeed, for each technology into a single category "ready". The callee in these two states treats new call attempts as incoming calls without difference. After the grouping, only 7 categories remain: 3G-ready, 3G-calling, VoWiFi-ready, VoWiFi-calling, VoLTE-ready, VoLTE-calling, and inter-carrier.

Methodology. We consider 14 features in the SVM feature space. We extract 10 features from the SIP message content and empirically define the other 4 features. The former features include P-Early-Media, Allow, Session_Name, Bandwidth, etc. They are mainly carried by the non-100 SIP messages, which include Session Progress and Ringing. The other 4 features include Trying-PR interval, Message_Flow, etc. Especially, the Trying-PR interval indicates the interval between the arrival time of the Trying and that of its subsequent provisional response (Session Progress or Ringing) at the caller. The rationale is that the Trying is always immediately returned by the IMS, but the delivery of the provisional response can be triggered by different entities, e.g., the IMS itself, the SIP/PSTN translation gateway, and the inter-carrier gateway. It may thus result in different values for call technologies.

We convert the string values of the features into numerical values to form an input vector, whereas the output is the index of those defined 7 categories. We use the one-hot encoding [25] and the feature hashing [56] to handle different types of string values. We focus on the analysis of Carriers AS-I and NA-I with 2400 and 1600 traces, respectively. We use 60% data for the training and the other 40% data for the testing. Note that similar findings can be also observed from the small set of the other two carriers' traces.

Findings. We first summarize several common findings from both of the carriers and then discuss them individually.

- VoWiFi-ready and VoLTE-ready cases cannot be clearly differentiated. Since both of them belong to attackable cases, we group them together in the result.
- The three calling cases with different technologies cannot be separated, so we also group them into one category. Note that the calling state is very short, so the call technology can be detected after it ends.
- The combined case of VoWiFi-ready and VoLTE-ready can be distinguished from that of the calling ones.
- The 3G-ready case results in much larger Trying-PR values than the other cases, as shown in Figure 9.

Table 4 shows the classification results of Carriers AS-I and NA-I. They have different dominant features that can give the highest classification accuracy. For Carrier AS-I, all the four categories can be clearly differentiated. There are 8 2-feature sets which can give 100% accuracy. For example, one of them contains Session_Name and Message_Flow features, the combination of which gives different string values to those four categories. Note that these feature sets do not contain the Trying-PR feature, which has overlaps on different categories as shown in Figure 9(a). However, it is still needed for the stealthy detection that differentiates the 3G-ready case from the others (see Section 5.2).

For Carrier NA-I, a 2-feature set including Allow and Trying-PR can give the highest accuracy. Most data of the four categories can be separated, but there are few exceptions. Specifically, 4.17% 3G-ready, 1.39% calling, and 1.39% inter-carrier data are mistakenly classified into calling, inter-carrier, and calling cases, respectively. It can be attributed to the Trying-PR feature. As shown in Figure 9(b), they have some small overlaps. Note that although the overlap portion between the VoLTE-ready and 3G-ready cases is not small, they can still be differentiated based on the Allow feature.

Note that we can avoid those few exceptions in real detection for Carrier NA-I by making judgement based on multiple trials. The inter-carrier, calling, and 3G-ready cases respectively have 97% data in [0.01, 0.57], 98% data in [0.61, 2.06], and 100% data in [2.21, 5.64], in terms of the Trying-PR. Assume that each case has the probability ρ to happen in a given range. We set a threshold

Phase	AS-I		NA-I	
	Action	Classification	Action	Classification
I	Single call: stop right after receiving SP	Check SN and MF	Multi-call: stop right after receiving SP	Check Allow and Interval (inter-carrier: [0.01, 0.57])
II	Single call: stop at 3.0 s after receiving Trying	No non-100 provisional resp: 3G-ready; Otherwise, check SN and MF	Multi-call: stop at 2.2 s after receiving Trying	Check Allow in a non-100 provisional resp if any; otherwise, 3G-ready after n calls

Table 5: Two-phase stealthy detection methods of phone status for Carriers AS-I and NA-I.

θ to exclude the possibility of one case. At the nth detection trials with m times not in the range, the case should be excluded when $(1-\rho)^m \rho^{n-m} < \theta$.

Trying-PR interval. We have three main findings regarding the Trying-PR interval. First, the inter-carrier cases usually have very short intervals. Together with the observation that the callee never rings when a call session is canceled right after its provisional response is received, we can infer that the caller is notified before the inter-carrier callee is reached. Second, the VoLTE/VoWiFi-ready and calling cases both have relatively shorter intervals. In the former case, it can be attributed to fast SIP message forwarding between the caller and the callee. In the latter case, the IMS answers the provisional response on behalf of the phones in the calling state. Third, the 3G-ready cases usually result in the longest intervals, since the SIP/PSTN translation is needed.

5.2 Stealthy Detection of Phone Status

We next devise a method that can stealthily detect a target phone's status based on the call information leakage. The detection runs at the caller by sending an INVITE to the target phone and observing its response. To be stealthy, we have to prevent the phone from playing ringtone during the detection. The absence of PRACK in V3 does not suppress the ringtone in the inter-carrier and 3G-ready cases, but we can use other methods to achieve it. The inter-carrier callee does not ring when the caller cancels its call attempt right after the provisional response arrives. For the 3G-ready callee, the caller can cancel its call attempt before receiving the provisional response, since the long Trying-PR interval allows the caller to differentiate it from the other cases. We thus consider two phases in the detection: (1) inter-carrier determination; (2) call status classification, which detects one of the other three intra-carrier cases. The attacker can use the first phase to exclude inter-carrier phones from attack targets, and employ the second phase to detect the victim phone's status at run time during the attack. We summarize the two-phase stealthy detection method for Carriers AS-I and NA-I in Table 5[1]. Note that although the inter-carrier determination can also be done through the online carrier lookup service [1], it cannot be automatic due to anti-bot protection.

Evaluation. We evaluate the stealthy detection for both of the carriers using our developed app. In each run, the app sends an INVITE to a target phone and then detects the phone's status at run time. We consider 7 scenarios: 3G-ready/calling, VoWiFi-ready/calling, VoLTE-ready/calling, and inter-carrier. For each carrier, we generate 25 runs for first 6 scenarios each and 25 runs for other four different carriers each in the inter-carrier case. In each run, we collect the app's detection output and the given scenario. For both Carriers AS-I and NA-I, our result shows that the app can accurately classify all these tests into four categories with 50, 25, 75, and 100 runs, respectively: VoWiFi/VoLTE-ready, 3G-ready, calling, and inter-carrier.

Impact from network conditions. Among the SVM features, only the Trying-PR interval can be affected by network conditions. Their dynamics may lead to large variance of the interval, thereby hurting the classification accuracy in some cases. However, the prioritized delivery of the VoWi-Fi traffic, which relies on DSCP and 802.11e AC as described in Section 4.1, can minimize the impact. The Trying-PR interval is mainly used to differentiate 3G-ready from the other cases for Carrier AS-I, as well as discriminate between 3G-ready, inter-carrier, and the others for Carrier NA-I. We conduct experiments to examine whether the variance of the Trying-PR interval in various network conditions can be handled by the stealthy detection method. We consider only the VoWi-Fi case, since network conditions have little impact on the other cases, which have guaranteed services within the 3G/4G networks. For each carrier, we gauge the Trying-PR interval by varying the Wi-Fi signal strength at the target phone and considering three test times (i.e., morning, afternoon, and night). As described in Section 4.1, there are totally 12 combination cases. The result shows that all the intervals fall in the ranges [0.18, 1.98] and [0.79, 1.45] for AS-I and NA-I, respectively. Therefore, the two-phase stealthy detection methods shown in Table 5 can work for all these intervals.

5.3 Apply Stealthy Detection into Call DoS

The adversary can apply the two-phase detection into launching the stealthy call DoS attack against a set of valid phone numbers. Given cellular accounts from Carriers AS-I and NA-I, the adversary first uses the first-phase detection to identify which phone numbers belong to each of these two carriers. For each phone number of these two carriers, the adversary can launch a detection-enabled attack by applying the second-phase detection. There are two modes, attack and probing, for each potential victim. In the attack mode, the attack app launches the call DoS attack against the victim while detecting its status. It does not stop the attack until the victim's status becomes 3G-ready. With the 3G-ready victim, it switches to the probing mode that periodically probes the victim's status. Whenever the victim switches back to VoLTE or VoWi-Fi, it returns to the attack mode. Note that the calling states do not trigger the mode switch, since the call technology cannot be determined.

We integrate the second-phase detection into the call DoS attack. For Carrier AS-I, the detection can be done by a single call attempt, so we enable it for each attack INVITE. Specifically, we cancel each attack INVITE which does not have any non-100 provisional response within 3.0 s after Trying. The cancellation represents that the victim phone is detected to be in the 3G-ready status. For Carrier NA-I, the detection relies on multiple call attempts. In each call DoS phase, the attack app uses three INVITE messages for the

[1] In the action field, an INVITE is sent for each call, and the stop is done by sending CANCEL. Interval, SP, SN, and MF stand for Trying-PR interval, Session Progress, Session_Name, and Message_Flow, respectively.

Attack mode (detection-enabled) Number of victims	Adaptive 1	Multi-victim 2	Multi-victim 4
AS-I (one attacker)	98.86%	97.20%	95.80%
NA-I (one attacker)	98.20%	92.00%	N/A

Table 6: The DoS times in percentage of one hour for various detection-enabled attacks.

detection. In the adaptive attack, there are two kinds of attack INVITE messages: dynamic and last-line. To avoid impeding the attack operation, we send another INVITE specific for the detection before the dynamic one. This INVITE should be sent so early that it can be canceled successfully before the delivery of the last-line one (here, 3 s earlier than the last-line), since the maximum number of concurrent INVITE messages is 3. In this detection-enabled attack, we cancel each INVITE which does not have any non-100 provisional response within 2.2 s after Trying. When none of those three INVITE messages have the provisional response, the victim phone is considered to be in the 3G-ready status.

Evaluation. Table 6 shows the DoS times of various detection-enabled attacks. Specifically, the adaptive, detection-enabled attack can still achieve DoS with 98.86% and 98.20% time for Carriers AS-I and NA-I, respectively. Enabling the detection in those attacks has small overhead with only up to 1.60% decrease of the DoS times.

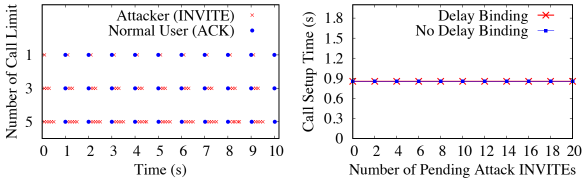
6 SOLUTION

In this section, we propose a suite of solution methods to address the vulnerabilities, as well as prototype and evaluate them. They are standard compliant and easily applied into phone devices and networks. It can make carriers and vendors have strong incentives to use them. Note that a long-term solution is still required, but it needs a concerted effort from carriers, network/phone vendors, and the cellular standard community based on their practical concerns.

App-level data-origin authentication. This component ensures the entity that exchanges SIP messages with the IMS to be a legitimate IMS app (V1). Such data-origin authentication can be achieved based on current IPSec transport-mode security, which is mandatory and stipulated in the standard [11], but the entity of the IPSec security associations at the end device shall be the IMS app. To prevent the IMS session hijacking, the IMS keys used by the IPSec shall not be leaked outside the IMS app and the SIM card.

It requires two security measures. First, the IMS app shall embed the IPSec implementation without relying on the mobile OS so that it can keep the IMS keys safe inside itself. Second, the IMS app shall be authenticated by the SIM card and securely obtain the IMS keys, which are generated by the SIM card's ISIM module. Based on the authentication, the app can build security associations with the SIM card to secure delivery of the IMS keys. It can prevent the adversary from extracting them with an SIM card sniffer. Note that we assume the SIM card is the trusted hardware, so the IMS app can still be authenticated given the compromised or rooted OS.

Call limit decoupling. We propose to decouple the limit number of established call sessions from that of call attempts for each phone device. By the phone design and usage practice, only one call attempt can be made at a time from a phone, though keeping concurrent sessions with established calls is allowed. The IMS core should consider them differently, instead of treating them as the same to cause V2. Carriers can keep the same limit on the number of concurrent call sessions, but restrict that of the call attempt made by each phone to be one.



(a) Effectiveness.

(b) Call setup overhead.

Figure 10: Evaluation of the call limit decoupling and the delay call binding.

Delay call binding. We propose a delay call binding mechanism to address V3. It delays the call binding to the arrival of the PRACK instead of the INVITE. Even though many attack INVITE messages may arrive at the callee, it can bind the call to the earliest one which returns the PRACK and start to play ringtone. Such mechanism can prevent the callee from getting stuck with a specific INVITE. Both the callee and the IMS core consider the sessions without the PRACK as pending ones. When seeing an INVITE without any pending sessions, they reserve resource for a call but do not bind it to the INVITE. The callee follows the same call setup procedure to serve it. Afterwards, no new resources are allocated for further INVITE messages. Whenever a PRACK message is returned, both the callee and the IMS core bind the call resource to its corresponding session and dismiss the other pending sessions. The call resource for the callee will be released once no pending sessions exist.

Note that this mechanism does not conflict with the purpose of the PRACK, which confirms the caller's resource reservation and prevents annoying ringtone caused by an invalid call. Although the binding of the call resource is delayed at the callee side, the call resources at two ends have been confirmed for establishing a valid call after the callee receives the PRACK.

6.1 Prototype and Evaluation

We prototype the call limit decoupling and delay call binding methods, which can already mitigate the call DoS attack, as well as evaluate their effectiveness.

Prototype. We use Open IMS Core [2] and Twinkle 1.10.2 [3] as the IMS core and app, respectively. Both of them run on computers with the elementary OS 0.4.1. In the IMS app, we implement the precondition mechanism and its reliability function. For the delay call binding, we make modification only to the IMS app, since the IMS core by default forwards all the INVITE messages to the app without thwarting the delay binding. At the IMS core, we separate the call limit to two states in the management of call dialogs, which are maintained for active call sessions.

Evaluation. We first examine the effectiveness of the prototype. We vary the number limit of call attempts for each phone, but keep that of established calls being 5. Each test takes 10 seconds. In each test, we emulate three phone devices: an attacker, a victim, and a normal user. The attack phone periodically sends an INVITE to the victim every 100 ms without returning PRACK. The normal user makes a call to the victim every 1 s, and hangs up the call immediately right after it is established. Figure 10(a) shows the arrival times of the attack INVITE messages at the victim, and those of the ACK messages acknowledging call acceptance from the normal user. It is observed that the number of the attack INVITE messages is constrained by the call limit. Although there are pending sessions of those messages ahead, the normal user can still make a call to the victim successfully in every second according to the delay call binding. After the successful call binding, the states of the pending attack sessions are discarded. This is why the victim can receive new attack INVITE messages at the beginning of every second.

We next gauge the overhead of the delay call binding in terms of call setup time. We vary the number of pending INVITE messages, which are from multiple attackers, before a normal call is established between the normal user and the victim, and get the average setup time over five runs in each test. We emulate the round trip time (RTT) between them by using the minimum RTT value observed from the carriers. Figure 10(b) shows the result of the cases with and without delay binding. The overhead of the delay binding is observed to be negligible.

7 DISCUSSION

Fingerprints of IMS systems. We can use different responses from IMS systems (e.g., the failure messages in Table 1) as fingerprints to identify them and protect end devices against their vulnerabilities. When a list of potential vulnerabilities is built for each IMS system, each phone can identify its system vulnerabilities based on the fingerprints and then take corresponding precautions.

Flooding-based brute force attack. The adversary may take a brute force attack that floods the IMS system with INVITE or CANCEL messages. We expect that most of the messages may be considered invalid or dropped due to two security manners. First, the maximum number of concurrent call attempts can limit the number of active INVITE. Second, the carrier may deploy rate-limit or message-limit security function against the flooding.

8 RELATED WORK

Cellular network security. Cellular network security has been an active research area. Its studies can be classified into the following three categories, in addition to the IMS-related ones. First, several studies focus on security issues of cellular-specific network protocols and operation, such as LTE access network with rogue base stations [49], layer-two protocols [9, 43], misconfiguration [19], temporary identifier relocation [10] , charging functions [28], and GSM encryption [36]. Second, some research works investigate security threats caused by Internet technologies and malicious traffic in the cellular network. The topics include middleboxes [27, 55], malicious Internet traffic [32, 53], and botnets [52]. Third, many of them examine security issues of 3G services including CS-based call [59], SMS (Short Messaging Service) [15, 23, 26, 34, 36, 38, 40, 45, 51], and MMS (Multimedia Messaging Service) [39]. Different from them, this work focuses on the IMS security.

IMS security. There have been several studies on the security issues of IMS services including IMS-based SMS [54], VoLTE [31, 33], and VoWi-Fi [13, 14, 18, 58]. The SMS study [54] shows the feasibility of IMS-based SMS spoofing and its potential threats. The VoLTE studies [31, 33] investigate possible resource abuse of VoLTE bearers in the 4G networks, but do not explore vulnerabilities of the IMS call system. Among the VoWi-Fi works, one [14] is to launch a man-in-the-middle attack over VoWi-Fi, another [18] shows how to steal IPSec keys used for VoLTE and VoWi-Fi using an SIM sniffer, and the others [13, 58] disclose user privacy and launch DoS attacks by intercepting VoWi-Fi packets en route to/from the Internet. The attack models in these prior VoWi-Fi studies assume that the adversary can intercept the victim phone's VoWi-Fi packets by being located at the same local area network as the victim. In this work, the proposed attack does not have such attack limitation; the adversary can use a VoWi-Fi phone to remotely attack the victim phone in another different Wi-Fi network.

SIP and VoIP security. There have been some security considerations related to the SIP protocol [20, 22, 42, 44, 50, 57]. They include eavesdropping, session hijacking, impersonation, message tampering, and DoS attacks. Most of them happen because of no protection of authentication, confidentiality, or/and integrity. However, the IMS SIP session is protected by two-layer IPSec security including all those three protection functions. We uncover new vulnerabilities of the IMS call service; moreover, we exploit them to launch DoS attacks, rather than simply doing traditional SIP flooding attacks. For the VoIP security, there are several VoIP detection systems of flooding [47], intrusion [48], and DoS attacks [46], but they do not cover the vulnerabilities exposed by this work.

9 CONCLUSION

Carriers have deployed the IMS system since launching VoLTE. Its vulnerability was hardly exposed, because its access from the phone device was protected by the hardware-based security. However, VoWi-Fi removes this security barrier attributed to its inherent design. In this work, we examine not only the vulnerability of VoWi-Fi but also the security implications of IMS. We show that the VoWi-Fi signaling session can be hijacked to maliciously manipulate IMS call operation. By exploiting the IMS vulnerability, the adversary can make ghost calls to launch a stealthy call DoS attack against cellular users with only their phone numbers. We further advance it to an ML-assisted Call DoS Attack that can detect attackable phones at run time without getting attention from unattackable ones. All these security threats are global, since our experiments cover 4 top-tier carriers across 2 countries with 7 phone brands. They call for immediate attentions from global carriers, device vendors, and the cellular standard community.

ACKNOWLEDGMENTS

We greatly appreciate our anonymous shepherd and reviewers for their constructive comments. This work is supported in part by the Ministry of Science and Technology, Taiwan, under Grants 106-2628-E-009-003-MY3 and 108-2218-E-009-045, and the National Science Foundation under Grants CNS-1814551 and CNS-1815636. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors only and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] 2019. Free Carrier Lookup Service. https://freecarrierlookup.com/

[2] 2019. Open IMS Core: an Open Source Implementation of IMS Call Session Control Functions. https://www.openimscore.com

[3] 2019. Twinkle: a Softphone for VoIP and Instant Messaging Communications using the SIP Protocol. https://mfnboer.home.xs4all.nl/twinkle

[4] 2019. Verizon Conference Calling Services. https://www.verizonwireless.com/support/calling-services/conference-calling/

[5] 3GPP. 2018. *3G Security; Access Security for IP-based Services (Release 15).* 3GPP Standard TS33.203 V15.1.0.

[6] 3GPP. 2018. *3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (Release 15).* 3GPP Standard TS33.402 V15.1.0.

[7] 3GPP. 2018. *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 16).* 3GPP Standard TS24.229 V16.0.0.

[8] 3GPP. 2019. *IP Multimedia Subsystem (IMS); Stage 2 (Release 15).* 3GPP Standard TS23.228 V15.4.0.

[9] Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. 2012. New Privacy Issues in Mobile Technology: Fix and Verification. In *Proceeding ACM Conference on Computer and Communications Security (CCS).* Raleigh, NC, USA.

[10] Myrto Arapinis, Loretta Ilaria Mancini, Eike Ritter, and Mark Ryan. 2014. Privacy through Pseudonymity in Mobile Telephony Systems. In *Proceeding IEEE The Network and Distributed System Security Symposium (NDSS).* San Diego, CA, USA.

[11] GSM Association. 2017. *IMS Profile for Voice and SMS.* GSMA Official Document IR.92 (Version 11.0).

[12] GSM Association. 2017. *IMS Profile for Voice, Video and SMS over Untrusted Wi-Fi Access.* GSMA Official Document IR.51 (Version 5.0).

[13] Jaejong Baek, Sukwha Kyung, Haehyun Cho, Ziming Zhao, Yan Shoshitaishvili, Adam Doupe, and Gail-Joon Ahn. 2018. Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling. In *Proceeding ACM Annual Computer Security Applications Conference (ACSAC).* San Juan, PR, USA.

[14] Jethro G. Beekman and Christopher Thompson. 2013. Breaking Cell Phone Authentication: Vulnerabilities in AKA, IMS and Android. In *Proceeding USENIX Workshop on Offensive Technologies (WOOT).* Washington, D.C., USA.

[15] Abhijit Bose, Xin Hu, Kang G. Shin, and Taejoo Park. 2008. Behavioral Detection of Malware on Mobile Handsets. In *Proceeding ACM International Conference on Mobile Systems, Applications, and Services (MobiSys).* Breckenridge, CO, USA.

[16] G. Camarillo, W. Marshall, and J. Rosenberg. 2002. *Integration of Resource Management and Session Initiation Protocol (SIP).* IETF RFC 3312.

[17] Patrik Cerwall. 2018. *Ericsson Mobility Report.* Ericsson.

[18] Sreepriya Chalakkal. 2017. How Secure Are Your VoLTE And VoWiFi Calls?. In *DeepSec In-Depth Security Conference Europe (IDSC).* Vienna, Austria.

[19] Merlin Chlosta, David Rupprecht, Thorsten Holz, and Christina Pöpper. 2019. LTE Security Disabled - Misconfiguration in Commercial Networks. In *Proceeding ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec).* Miami, FL, USA.

[20] Mark Collier. 2005. Basic Vulnerability Issues for SIP Security. (2005).

[21] Corinna Cortes and Vladimir Vapnik. 1995. Support-Vector Networks. *Machine Learning* 20, 3 (1995), 273–297.

[22] Fadi El-moussa, Parmindher Mudhar, and Andy Jones. 2010. Overview of SIP attacks and countermeasures. In *Information Security and Digital Forensics LNICST.* Heidelberg:Springer, 82–91.

[23] William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. 2005. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceeding ACM Conference on Computer and Communications Security (CCS).* Alexandria, VA, USA.

[24] M. Garcia-Martin. 2005. *Input 3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP).* IETF RFC 4083.

[25] David Harris and Sarah Harris. 2012. *Digital Design and Computer Architecture, 2nd Edition.* Morgan Kaufmann.

[26] Rongyu He, Guolei Zhao, Chaowen Chang, Hui Xie, Xi Qin, and Zheng Qin. 2009. A PK-SIM Card Based End-to-end Security Framework for SMS. *Computer Standards & Interfaces* 31, 4 (2009), 629–641.

[27] Hyunwook Hong, Hyunwoo Choi, Dongkwan Kim, Hongil Kim, Byeongdo Hong, Jiseong Noh, and Yongdae Kim. 2017. When Cellular Networks Met IPv6: Security Problems of Middleboxes in IPv6 Cellular Networks. In *Proceeding IEEE European Symposium on Security and Privacy (EuroS&P).* Paris, France.

[28] Hyunwook Hong, Hongil Kim, Byeongdo Hong, Dongkwan Kim, Hyunwoo Choi, Eunkyu Lee, and Yongdae Kim. 2016. Pay as You Want: Bypassing Charging System in Operational Cellular Networks. In *World Conference on Information Security Applications (WISA).* Jeju Island, South Korea.

[29] R. Jesske, K. Drage, and C. Holmberg. 2014. *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP.* IETF RFC 7315.

[30] S. Kent. 2005. *IP Encapsulating Security Payload (ESP).* IETF RFC 4303.

[31] Hongil Kim, Dongkwan Kim, Minhee Kwon, Hyungseok Han, Yeongjin Jang, Dongsu Han, Taesoo Kim, and Yongdae Kim. 2015. Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations. In *Proceeding ACM Conference on Computer and Communications Security (CCS).* Denver, CO, USA.

[32] Charles Lever, Manos Antonakakis, Brad Reaves, Patrick Traynor, and Wenke Lee. 2013. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. In *Proceeding IEEE The Network and Distributed System Security Symposium (NDSS).* San Diego, CA, USA.

[33] Chi-Yu Li, Guan-Hua Tu, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu, and Xinbing Wang. 2015. Insecurity of Voice Solution VoLTE in LTE Mobile Networks. In *Proceeding ACM Conference on Computer and Communications Security (CCS).* Denver, CO, USA.

[34] Johnny Li-Chang Lo, Judith Bishop, and J.H.P. Eloff. 2008. SMSSec: An End-to-end Protocol for Secure SMS. *Computer & Security* 27, 5 (2008).

[35] C. Madson and R. Glenn. 1998. *The Use of HMAC-SHA-1-96 within ESP and AH.* IETF RFC 2404.

[36] Ulrike Meyer and Susanne Wetzel. 2004. On the Impact of GSM Encryption and Man-in-the-middle Attacks on the Security of Interoperating GSM/UMTS Networks. In *Proceeding IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC).* Barcelona, Spain.

[37] Mehryar Mohri, Afshin Rostamizadeh, and Ameet Talwalkar. 2012. *Foundations of Machine Learning.* The MIT Press, Chapter 5, 89–120.

[38] Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin, and Jean-Pierre Seifert. 2013. SMS-Based One-Time Passwords: Attacks and Defense. In *Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).* Berlin, Germany.

[39] Radmilo Racic, Denys Ma, and Hao Chen. 2006. Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery. In *Proceeding IEEE Securecomm and Workshops.* Baltimore, MD, USA.

[40] Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin R.B. Butler. 2016. Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *Proceeding IEEE Symposium on Security and Privacy (S&P).* San Jose, CA, USA.

[41] J. Rosenberg and H. Schulzrinne. 2002. *Reliability of Provisional Responses in the Session Initiation Protocol (SIP).* IETF RFC 3262.

[42] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. 2002. *SIP: Session Initiation Protocol.* IETF RFC 3261.

[43] David Rupprecht, Katharina Kohls, Christina Pöpper, and Thorsten Holz. 2019. Breaking LTE on Layer Two. In *Proceeding IEEE Symposium on Security and Privacy (S&P).* Oakland, CA, USA.

[44] Samer El Sawda and Pascal Urien. 2006. SIP Security Attacks and Solutions: A state-of-the-art review. In *Proceeding IEEE International Conference on Information and Communication Technologies (ICT).* Damascus, Syria.

[45] Neetesh Saxena and Narendra S. Chaudhari. 2014. EasySMS: A Protocol for End-to-End Secure Transmission of SMS. *IEEE Transactions on Information Forensics and Security* 9, 7 (2014), 1157–1168.

[46] Hemant Sengar, Haining Wang, Duminda Wijesekera, and Sushil Jajodia. 2006. Fast Detection of Denial-of-Service Attacks on IP Telephony. In *Proceeding IEEE International Workshop on Quality of Service.* New Haven, CT, USA.

[47] Hemant Sengar, Haining Wang, Duminda Wijesekera, and Sushil Jajodia. 2008. Detecting VoIP Floods Using the Hellinger Distance. *IEEE Transactions on Parallel and Distributed Systems* 19, 6 (2008), 794–805.

[48] Hemant Sengar, Duminda Wijesekera, Haining Wang, and Sushil Jajodia. 2006. VoIP Intrusion Detection Through Interacting Protocol State Machines. In *Proceeding IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).* Philadelphia, PA, USA.

[49] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2016. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. In *Proceeding IEEE The Network and Distributed System Security Symposium (NDSS).* San Diego, CA, USA.

[50] Dorgham Sisalem, Jiri Kuthan, and Sven Ehlert. 2006. Denial of Service Attacks Targeting a SIP VoIP Infrastructure: Attack Scenarios and Prevention Mechanisms. *IEEE Network* 20, 5 (2006), 26–31.

[51] Patrick Traynor, William Enck, Patrick McDaniel, and Thoman La Porta. 2009. Mitigating Attacks on Open Functionality in SMS-capable Cellular Networks. *IEEE/ACM Transactions on Networking* 17, 1 (2009), 40–53.

[52] Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, and Thomas La Porta. 2009. On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In *Proceeding ACM Conference on Computer and Communications Security (CCS).* Chicago, IL, USA.

[53] Patrick Traynor, Patrick McDaniel, and Thomas La Porta. 2007. On Attack Causality in Internet-Connected Cellular Networks. In *Proceeding USENIX Conference on Security (SEC).* Boston, MA, USA.

[54] Guan-Hua Tu, Chi-Yu Li, Chunyi Peng, Yuanjie Li, and Songwu Lu. 2016. New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks. In *Proceeding ACM Conference on Computer and Communications Security (CCS).* Vienna, Austria.

[55] Zhaoguang Wang, Zhiyun Qian, Qiang Xu, Zhouqing Mao, and Ming Zhang. 2011. An Untold Story of Middleboxes in Cellular Networks. In *Proceeding ACM SIGCOMM.* Toronto, Ontario, Canada.

[56] Kilian Weinberger, Anirban Dasgupta, John Langford, Alex Smola, and Josh Attenberg. 2009. Feature Hashing for Large Scale Multitask Learning. In *Proceeding of International Conference on Machine Learning (ICML)*. Montreal, Canada.

[57] Warodom Werapun, Anas Abou El Kalam, Béatrice Paillassa, and Julien Fasson. 2009. Solution Analysis for SIP Security Threats. In *Proceeding IEEE International Conference on Multimedia Computing and Systems (ICMCS)*. Ouarzazate, Morocco.

[58] Tian Xie, Guan-Hua Tu, Chi-Yu Li, Chunyi Peng, Jiawei Li, and Mi Zhang. 2018. The Dark Side of Operational Wi-Fi Calling Services. In *Proceeding IEEE Conference on Communications and Network Security (CNS)*. Beijing, China.

[59] Yuwei Zheng, Lin Huang, Haoqi Shan, Jun Li, Qing Yang, and Wenyuan Xu. 2017. Ghost Telephonist Impersonates You: Vulnerability in 4G LTE CS Fallback. In *Proceeding IEEE Conference on Communications and Network Security (CNS)*. Las Vegas, NV, USA.