Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling

Jaejong Baek
Arizona State University
jbaek7@asu.edu

Sukwha Kyung
Arizona State University
skyung1@asu.edu

Haehyun Cho
Arizona State University
haehyun@asu.edu

Ziming Zhao
Rochester Institute of Technology
zhao@mail.rit.edu

Yan Shoshitaishvili
Arizona State University
yans@asu.edu

Adam Doupé
Arizona State University
doupe@asu.edu

Gail-Joon Ahn
Arizona State University
Samsung Research
gahn@asu.edu
gailjoon.ahn@samsung.com

ABSTRACT

Wi-Fi Calling, which is used to make and receive calls over the Wi-Fi network, has been widely adopted and deployed to extend the coverage and increase the capacity in weak signal areas by moving traffic from LTE to Wi-Fi networks. However, the security of Wi-Fi Calling mechanism has not been fully analyzed, and Wi-Fi Calling may inherently have greater security risks than conventional LTE calling. To provide secure connections with confidentiality and integrity, Wi-Fi Calling leverages the IETF protocols IKEv2 and IPSec.

In this paper, we analyze the security of Wi-Fi Calling specifications and discover several vulnerabilities that allow an adversary to track the location of users and perform DoS attacks. By setting up a rogue access point in live testbed environment, we observe that user devices can leak the International Mobile Subscriber Identity (IMSI), despite it being encrypted. The leaked information can be further exploited for tracking user locations. We also discuss how these protocols are vulnerable to several denial of service attacks.

To protect user privacy and services against these attacks, we propose practical countermeasures. We also present trade-off considerations that pose challenges for us to apply countermeasures to mitigate the existing vulnerabilities. Additionally, we propose to introduce corresponding amendments for future specifications of protocols to address these trade-offs.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**;

KEYWORDS

Wi-Fi Calling, Privacy, IMSI, DoS, Impersonation Attack, IPSec

ACM Reference Format:
Jaejong Baek, Sukwha Kyung, Haehyun Cho, Ziming Zhao, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn. 2018. Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling. In *2018 Annual Computer Security Applications Conference (ACSAC '18), December 3–7, 2018, San Juan, PR, USA.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3274694.3274753

ACSAC '18, December 3–7, 2018, San Juan, PR, USA

ACM ISBN 978-1-4503-6569-7/18/12…$15.00
https://doi.org/10.1145/3274694.3274753

1 INTRODUCTION

The evolution of mobile communication systems has heavily focused on supporting various forms of data. However, voice continues to exist as a core element of the mobile network operators (MNOs) business model [13]. The critical success factor for voice is wide coverage and sufficient capacity so that users do not experience dropped calls, black spots, or awkward hand-offs across networks. In this context, the Wi-Fi Calling, or Voice over Wi-Fi (VoWi-Fi), has been proposed as a solution to extend the coverage and improve the capacity in low signal areas by moving traffic between Long-Term Evolution (LTE) and Wi-Fi connections. Instead of using the carrier's mobile network, Wi-Fi Calling can make voice calls via a Wi-Fi network with regular phone numbers and does not require any additional applications, such as Skype [1] or WhatsApp [2].

Recently, most MNOs are integrating their VoLTE (Voice over LTE) services with Wi-Fi Calling to offload voice services in areas where their licensed spectrum coverage is limited [22]. When it comes to major MNOs in the U.S., every T-Mobile phone offers Wi-Fi Calling as a built-in feature. For Sprint, it is available on both iPhone (iOS 9.1 or higher) and Android variants. Similarly, AT&T offers Wi-Fi Calling for 23 models, and Verizon has 33 models in its Wi-Fi lineup. Republic Wireless and Google Project Fi also support Wi-Fi Calling feature on their phones as well [11]. It is projected that 90% of the major 62 MNOs in the world will deploy Wi-Fi Calling by 2020 [27].

[1] https://www.skype.com/
[2] https://www.whatsapp.com/

To maintain and enhance the security in Wi-Fi Calling, two Internet Engineering Task Force (IETF) protocols — Internet Key Exchange (IKEv2) and IP Security (IPSec) — are used for network traffic [1]. There is a general belief that those protocols provide strong privacy and availability guarantees to mobile subscribers, even when used in an unprotected Wi-Fi network. However, it is critical to scrutinize what potential attacks and vulnerabilities can be found in the current Wi-Fi Calling systems.

Also, albeit the MNOs continue to expand Wi-Fi Calling services for its effectiveness, most of the recent research has focused on analysis of the LTE security and the privacy. O'Hanlon et al. [24] and Chalakkal el al. [10] proposed the International Mobile Subscriber Identity (IMSI) privacy threat in Wi-Fi Calling. However, they did not analyze possible denial-of-service (DoS) attacks in Wi-Fi Calling environment, and omitted the detail implementation procedure of the threat. In addition, those works did not evaluate the proposed threat against the MNOs and devices.

In this paper, we analyze Wi-Fi Calling related protocol specifications with an empirical approach and identify several vulnerabilities based on the analysis results. Subsequently, we show that it is possible to exchange forged and manipulated packets successfully with the sender and receiver without any identity validation process. By building a rogue AP equipped with an IPSec server in live testbed Wi-Fi networks, we confirm that user devices can leak the IMSI, which can cause critical privacy problems, such as tracking user locations. Moreover, we find those protocols can be vulnerable to several DoS attacks. All of the vulnerabilities we found stem from the lack of mutual authentication mechanism in the security negotiation phase.

With regards to defense mechanisms, we propose several practical countermeasures to protect user's privacy and usability against IMSI leaking and DoS attacks. We also discuss trade-off considerations on the security of Wi-Fi Calling including why those vulnerabilities exist.

The contributions of this paper are summarized as follows.

- **Empirical analysis of the Wi-Fi Calling specifications:** We analyze Wi-Fi Calling protocol specifications and uncover several vulnerabilities experimentally. We classify these attacks into two different categories: IMSI privacy attacks and Denial of Service (DoS) attacks. In the IMSI privacy attack, we describe the feasibility of the server impersonation attack using the lack of mutual authentication. In the DoS attack, we demonstrate how three different messages can force a user equipment (UE) into a vulnerable state, leading to DoS attacks.
- **Implementation and Evaluation of Attacks:** We design and implement the IMSI privacy attack and DoS attack that can be deployed on a laptop with a Wi-Fi interface and confirm their effectiveness using low-cost devices. We demonstrate that these attacks can be easily built and operated using readily available tools. We describe our experiments and procedures that are based on commercially available hardware and software. We also evaluate the attacks using commercially available smartphones in real (lab-controlled) networks.

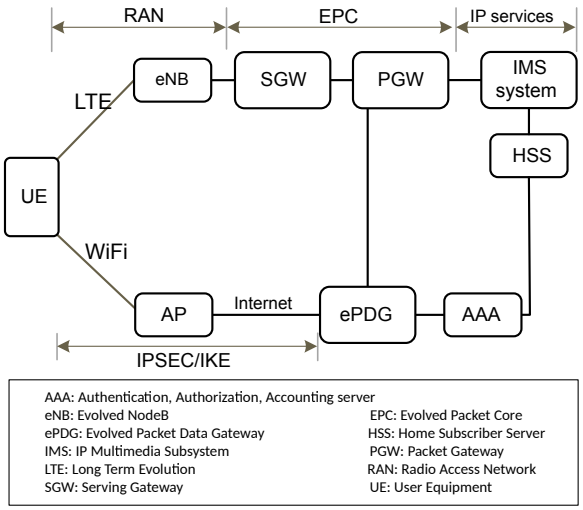

Figure 1: Wi-Fi Calling Architecture.

- **Security Analysis:** We discuss the underlying reasons for the vulnerabilities, along with trade-offs between security/privacy and other criteria such as usability, deployment cost, and recommended fixes.

The remainder of this paper is organized as follows. In Section 2, we provide an overview of the Wi-Fi Calling technologies. In Section 3, we analyze the possible threats and attack in Wi-Fi Calling. Then, we present our attack scenarios and explain how we implement our attacks in Section 4 and 5 for IMSI privacy and DoS attack respectively. We also discuss the impact and applicability of the attacks in those section. Based on the analysis, we propose the countermeasures in Section 6. We discuss the trade-offs between usability and deployment issues in Section 7. Section 8, we compare our approach with other related works. Finally, we conclude our work in Section 9.

2 WI-FI CALLING

We briefly describe the Wi-Fi Calling architecture as well as security mechanisms for understanding the vulnerabilities and attacks we propose in this work.

2.1 Wi-Fi Calling Architecture

The Wi-Fi Calling feature evolved based on the LTE architecture. We consider a simplified architecture: we skip other details of the architecture that are not relevant from the point of view of understanding our attacks. Figure 1 depicts this simplified architecture which contains three main components: User Equipment (UE), Radio Access Network (RAN), and Evolved Packet Core (EPC) 3GPP specification. The three components are described below.

User Equipment (UE). UE refers to the actual communication device, such as smartphones, tablets, and any devices equipped with Wi-Fi and cellular interfaces. A UE stores the International Mobile Subscriber Identity (IMSI) in a Subscriber Identity Module (SIM) card [6]. The IMSI is a globally unique

15 digit identifier of a subscriber consisting of the mobile country code (MCC, 3 digits), the mobile network code (MNC, 2 or 3 digits), and the mobile subscriber identification number (MSIN, 10 digits). When the UE joins to the network for the first time, the IMSI is used for authenticating a subscriber by the network with Home Subscriber Server (HSS) which has a user database for performing authentication.

Radio Access Network (RAN). RAN consists of an AP to manage the radio signals with the UE and facilitates communication between the UE and EPC. The protocols, specifications, and functions of the AP are the same as the generic IEEE 802.11-based APs used in homes, offices, and public places.

Evolved Packet Core (EPC). EPC is a core network framework for providing voice and data services on an LTE network [1]. It consists of several elements as defined in 3GPP TS 23.002 [3]. However, we describe only the Evolved Packet Data Gateway (ePDG), which is newly introduced in the LTE architecture to support Wi-Fi Calling. The ePDG acts as the gateway between the public Internet and EPC. ePDG is responsible for authenticating to UEs when they connect to the network involving security association (IKEv2/IPsec-based setting up integrity and encryption for signaling) [4].

2.2 Wi-Fi Calling Handshakes

In Wi-Fi Calling, a UE and an ePDG must perform message handshakes in two phases to establish an IPSec tunnel for secure communication. Figure 2(a) briefly shows the IPSec two-step handshake process: IKE security negotiation between UE (initiator) and the ePDG (responder) [18]. IKE is used for performing mutual authentication and establishing and maintaining Security Associations (SAs). A security association (SA) is a set of policy and key(s) used to protect information used by the negotiating peers.

The first phase of the Wi-Fi Calling handshake is illustrated in Figure 2(b) in detail:

(1) A UE sends the `IKE_SA_INIT_REQ` message to ePDG with cryptographic materials (Diffie-Hellman (D-H) and nonce values) for creating the IKE Security Association (SA).
(2) ePDG checks security parameters delivered from the UE and sends the `IKE_SA_INIT_RES` including cryptographic materials to the UE. At this point, each party can generate the key materials for all of the proceeding messages.
(3) After the `IKE_SA_INIT` exchange messages, the payloads of the `IKE_AUTH_REQ`, which contains the identity (IMSI) of the UE, are encrypted and integrity protected using SK_e (encryption) and SK_a (authentication or integrity protection) derived from the Diffie-Hellman (D-H) value to protect the IKE SA.
(4) Once the UE transmits message, `IKE_AUTH_RES`, correspondingly the ePDG validates the identity of the UE and sets up an SA for the first AH or ESP child SA with message.

3 SECURITY IN WI-FI CALLING

The security of Wi-Fi Calling mechanism inherently has the same risks as the conventional WI-FI network. Here, we briefly overview possible threats and attacks under the Wi-Fi network based on 3GPP Technical Specification 33.234 [1]. Furthermore, we demonstrate

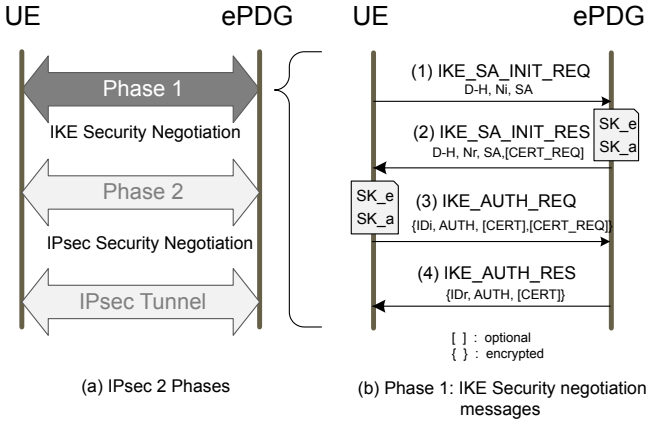

Figure 2: Wi-Fi Calling Handshaking Phases.

specific attacks which should be taken into consideration carefully when deploying security mechanisms for Wi-Fi Calling. Table 1 summarizes all possible threats and attacks in Wi-Fi network, which also identifies what attacks are specific to Wi-Fi Calling from the others. Regarding the Wi-Fi Calling specific threats and attacks, we discovered two vulnerabilities: (1) the lack of mutual authentication and (2) unprotected message exchanges in handshaking. By exploiting these vulnerabilities, we can carry out the IMSI privacy attack and the DoS attack using deauthentication frames against UEs.

3.1 Privacy of Users

The privacy data in mobile networks includes users' personal information, such as the IMSI that can be used to identify a specific user. Also, the privacy data includes information of a user's service subscription and physical location at a given time. If an attacker obtains the privacy data such as the IMSI, the attacker can track where and when the user has accessed Wi-Fi services.

IMSI privacy attacks for tracking the user location in mobile communications are commonly known problems. The IMSI catcher [31], called Stingray, is an active radio attack device in 3GPP networks that impersonate a base station to force disclosure of the subscriber's IMSI [20, 23, 29, 30, 33]. The device can collect user data from all phones within coverage and listen to the calls. Stingray has been used primarily by government monitoring agencies for law enforcement purposes to track and locate suspects [12]. If an attacker can get the IMSI of a user, the attacker can also find the actual phone number through paid web services [14].

In addition, an attacker can intercept, manipulate, and analyze the messages containing private user data transferred during the handshake (authentication) phase of Wi-Fi Calling. As shown in (3) and (4) of Figure 2(b), the cryptographic certificates are not an essential requirement but it can be optionally used for protecting the IMSI. This weak specification makes a server impersonation attack, which reveals the IMSI, possible, even when the IMSI it is encrypted. An attacker can set up his own IPSec server to impersonate the ePDG server, which would be capable of participating in the IMSI authentication process. Consequently, the attacker can acquire users' IMSI information.

Table 1: Possible Threats and Attacks in Wi-Fi Network.

	UE	AP	Specific to Wi-Fi Call
Victim (threats)	malware, identity theft, (D)DoS, eavesdropping, MitM	DoS, eavesdropping, MitM	identy theft, eavesdropping, DoS
Attacker (attacks)	impersonation (rogue UE), spoofing, eavesdropping, DoS	impersonation (rogue AP), spoofing, eavesdropping, DoS	impersonation, spoofing, MitM

Furthermore, IMSI leakages by a server impersonation attack can cause more serious privacy problems. For instance, if an attacker could acquire other additional information, such as the UE's hardware MAC address, he can track the victim more efficiently even without the IMSI. In this way, attackers are able to track people and record their movements, hence violating users' privacy.

3.2 Availability of Services

In Wi-Fi networks, first, an attacker can attempt to bypass the access control and authentication mechanisms to obtain the service for free. In other words, an attacker can impersonate a legitimate user to have free access to Wi-Fi services and the victim gets charged instead. Second, an attacker can transmit malicious messages to interfere with the Wi-Fi services because anyone can access the Wi-Fi link layer without any permission. Lastly, if correct mutual authentication is not deployed between two communicating parties, the attacker can perform eavesdropping or man-in-the-middle attacks by setting up a rogue access point, which relays messages between them.

3.3 Attacks Originating From Victim's UE and Attacker's AP

Malware residing in the UE can steal the credentials stored on SIM card of victim's UE. A UE infected by malware can also be used to perform Distributed DoS (DDoS) attacks simultaneously against a target. Also, it is possible to interfere with the victim's UE to make it connect to different APs.

An attacker can leverage a rogue AP masqueraded as a legitimate AP or UE using IP/MAC address spoofing. Once a victim's UE connects to the rogue AP (due to various reasons including weak LTE signal, Wi-Fi auto-connection option turned on, or deliberate connection by the victim), an attacker can easily eavesdrop on the traffic between a user and an AP. The attacker can also act as a Man-in-the-Middle during the authentication procedure and impersonate servers in the network such as a DNS or a DHCP server.

Moreover, the attacker can also perform DoS attacks against UEs and legitimate APs easily sending attack packets to them. The messages an attacker can forge or manipulate the following packets to cause DoS as listed below:

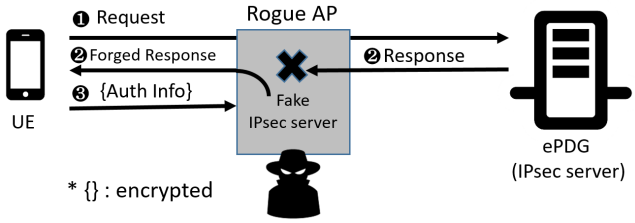

Figure 3: The Design of IMSI Privacy Attack.

(1) DNS response packet: When the target UE attempts to connect to an ePDG, it first looks for an ePDG by broadcasting DNS query. The attacker can compromise availability of LTE service on the target UE by forging DNS response packets containing IP address of the ePDG. In this way, the target UE cannot connect to LTE and is forced to connect to Wi-Fi AP. From this point, the attacker can perform server impersonation attack by introducing a rogue AP.

(2) `IKE_SA_INIT` message: Since the attacker can eavesdrop the `IKE_SA_INIT` packets during the SA negotiation, the attacker can easily impersonate a legitimate user or ePDG. Thus, attacker's capability to sniff those `IKE_SA_INIT` messages provides a base for server impersonation attack to the adversary.

(3) Deauthentication frame: In LTE network, a session can be closed upon receiving deauthentication frame from either serving gateway or UE. The attacker uses forged deauthentication frame to disconnect the target UE from the current network. This attack is called detach attack in LTE [15]. Similarly, deauthentication frame can be used to drop on-going Wi-Fi call of the victim by simply sending it to either the target UE or the AP to which the victim is connected to. In addition, the attacker can send the deauthentication frame to detach the victim from a legitimate AP and force him to connect to a rogue AP.

Please refer to Section 5 for details on how those messages are used in actual attacks.

4 IMSI PRIVACY ATTACK

In this section, we present how the UE's IMSI can be revealed by using server (ePDG) impersonation attack. To this end, we first describe the attack scenario and discuss its impacts. As shown in Figure 3, we design the attack using a rogue AP and a fake IPSec server.

4.1 Attack Scenario

The IMSI privacy attack scenario starts with sniffing Wi-Fi channel and monitoring the ongoing Wi-Fi Calling communication caused by target UEs. The procedural steps to execute the privacy attacks using the server impersonation technique are described as follows and in Figure 4:

(1) The attacker places the rogue AP equipped with the fake IPSec server within Wi-Fi coverage of the victim UE. After the victim connects to the rogue AP through messages ① and

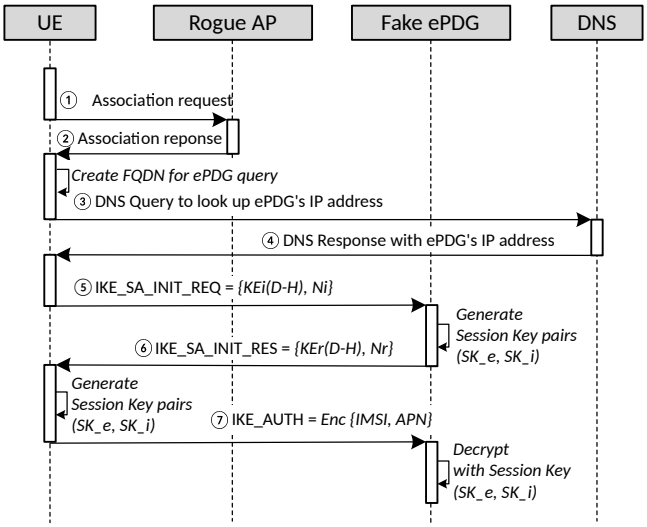

Figure 4: Sequence diagram showing the attack steps.

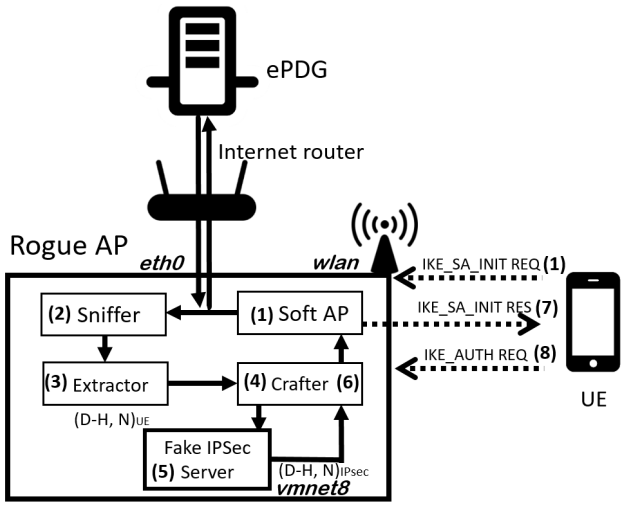

Figure 5: Rogue AP Components and Attack Flows.

②, the attacker can capture and manipulate all the packets of the victim's UE.

(2) The attacker takes advantage of the UE's ePDG lookup response packet ③ to obtain the IP address and port number of the ePDG. The attacker can then deceive the UE as if the rogue AP were an ePDG server.

(3) When the attacker captures the `IKE_SA_INIT_REQ` packet ⑤ transmitted by the UE, the attacker relays it to the fake IPSec server. The fake IPSec server generates the Session Keys (SK_e: encryption, SK_a: authentication) with the UE's D-H and N, then responds to the UE with its own D-H and N ⑥.

(4) The UE generates the session key with D-H and N in the response packets, and then sends the `IKE_AUTH_REQ` packet ⑦ to the rogue AP by encrypting the payload including the IMSI with the ready-made session key.

(5) The attacker intercepts this encrypted packet, decrypts it with the session keys generated in the previous step, and obtains the IMSI and APN.

With this procedure, the encrypted `IKE_AUTH_REQ` packet can be decrypted with the session keys generated by the fake IPSec server. The session keys used to decrypt the packet are extracted during the security association process in the fake IPSec server. With these keys and cryptography information negotiated in security association, we leverage IKEv2 decryption table to obtain decrypted payloads, which have IMSI, APN, etc.

4.2 Attack Setup

To execute the attack, the adversary must lie in the coverage of the target network. To sniff the wireless channel of a target UE, we created a softAP on a Linux laptop (Intel i5 processor and Kali 2017-12-04) and configure the Wi-Fi interface card to use monitor mode (or promiscuous mode). We also utilized the *libpcap*-based live packet capturing of Wireshark [3] and the sniff APIs of Scapy module [28]. Scapy is a packet manipulation tool for computer networks, written in Python. It can forge or decode packets, send them on the wire, capture them, and match requests and replies.

We implement a rogue AP equipped with IPSec server to perform the attacks against UE's registered with a live LTE network. In particular, we integrated the IPSec server to the rogue AP to impersonate the ePDG's behavior. The process of building a rogue AP is described below.

Building rogue AP. To successfully deploy a rogue AP, we utilize a laptop running Kali Linux with a Wi-Fi interface which is capable of working in a monitor mode. The five components that comprise the rogue AP are shown in Figure 5 along with their respective capabilities.

(1) *SoftAP*: Access Point module using *hostapd*, *dnsmasq*, and *iptables* which enables the laptop to function as an AP.

(2) *Sniffer*: Capturing module using Scapy APIs to capture the packets.

(3) *Extractor*: Extracting module using Scapy APIs to extract the payload value for crafting fake packets.

(4) *Crafter*: Crafting module using Scapy APIs to masquerade it as a legitimate packet in the network.

(5) *Fake IPSec server*: Impersonated ePDG server module using *Strong Swan* to handshake with a UE instead of the real ePDG server.

Implementation. Among the five components, *Sniffer*, *Extractor* and *Crafter* functionalities are implemented with Scapy module functions. Algorithm 1 describes pseudo code used for manipulating packets with Scapy, and the components numbers in the comments and interface names such as *"wlan, eth0, vmnet8"* are referenced in Figure 5. The command *sniff()* captures packets at designated

[3] https://www.wireshark.org/

Algorithm 1: Pseudo code for packet manipulation

input : A set of packets captured on wlan, eth0, vmnet8, P
output: A set of manipulated packets, R

```
while P do
    #2 Sniffer component
    P1 = sniff(wlan,sip=UE,dip=ePDG,udp,dp=500)
    P2 = sniff(eth0,sip=ePDG,dip=UE,udp,sp=500)
    P3 = sniff(vmnet8,sip=IPsec,udp,sport=500)
    P = P1 + P2 + P3
    if P = ISAKMP {
        if P = IKE INIT {
            #3 Extractor component
            E1 = rdpcap(P1(isakmp payload))
            E2 = rdpcap(P2(dip, dp))
            #4 Crafter component
            E=isakmp(head, payload(E1))
            send(IP(UE, Fake IPsec)/UDP(dp=500)/E)
        if P = IKE AUTH {
            #6 Crafter component
            E3 = rdpcap(P3(d − h, n))
            R=isakmp(head, payload(E3))
            send(IP(ePDG ← E2, UE)/UDP(dp ← E2)/R)
```

network interfaces with a filter including source/destination IP address and port number. *rdpcap()* reads a pcap file and return a packet list. *isakmp()* crafts Internet security association key management protocol (ISAKMP) packets used in IKE handshakes. *send()* sends packets at layer 3. *IP()* and *UDP()* make IP and UDP packet with the source/destination IP and port. The operator "/"means concatenating packets between each layer.

4.3 Results of Attacks

To identify devices and MNOs vulnerable to this attack, we test 4 major MNOs in the U.S. (T-Mobile, Sprint, AT&T, Verizon) and their particular 10 devices (Samsung Galaxy-Note-4/5, Samsung Galaxy-5/6 and iPhone 6/6s/7/8+). Through the experiments, we confirmed that these devices are affected by our attacks to obtain the subscriber's IMSI and Access Point Name (APN) as shown in Figure 6. In summary, as shown in Table 2, a successful attack would expose additional privacy information such as an ePDG IP address, Security association (SA) messages, etc.

In particular, we found that the certificates (CERT) are not used in all MNO's devices to protect the IMSI exchange. Certificate payloads should be included in an exchange if certificates are available to the sender. To verify, we crafted and sent the certificate request packet to the UEs. However, all UEs respond to the request without certificates. According to the standards, deploying certificates in the IKE exchange is not an essential requirement but an optional requirement [18]. Because of this weak specification, an attacker can set up the rogue AP and send the forged packets to the victim UE without the ePDG server authentication in the UE. In addition, the attacker could decrypt the encrypted packet with self-generated session keys.

```
Exchange type: IKE_AUTH (35)
Payload: Encrypted and Authenticated (46)
  Initialization Vector: 94c8d09f9948e4eb0890bca2ba0c1299 (16 bytes)
  Encrypted Data (336 bytes) <AES-CBC-256 [RFC3602]>
  Decrypted Data (336 bytes)
    Contained Data (323 bytes)
      Payload: Identification - Initiator (35)
        ID type: ID_RFC822_ADDR (3)
        Identification Data: 0310260xxxxxxxxx@xxx.mnc260.mcc310.XXXXX   <- IMSI
      Payload: Certificate Request (38)
        Certificate Type: X.509 Certificate - Signature (4)
        Certificate Authority Data: 88eef7b9d185ac98b94b493764f589eb92
      Payload: Identification - Responder (36)
        ID type: KEY_ID (11)
        Identification Data:
          ID_KEY_ID: xxxxx   <- APN
      Payload: Security Association (33)
      Payload: Traffic Selector - Initiator (44) # 1
      Payload: Traffic Selector - Responder (45) # 1
      Payload: Notify (41) - HTTP_CERT_LOOKUP_SUPPORTED
      Payload: Notify (41) - EAP_ONLY_AUTHENTICATION
      Payload: Notify (41) - INITIAL_CONTACT
      Payload: Notify (41) - ESP_TFC_PADDING_NOT_SUPPORTED
      Payload: Notify (41) - NON_FIRST_FRAGMENTS_ALSO
```

Figure 6: Decrypted packet sample (T-Mobile).

Table 2: Test Results of IMSI privacy attacks.

	T-Mobile	Sprint	AT&T	Verizon
e-PDG address	Exposed	Exposed	Exposed	Exposed
Crypto (IKEv2)	AES256 SHA1 MODP1024	AES128 SHA1 MODP1024	AES256 SHA256 MODP2048	AES256 SHA1 MODP1024
IMSI identity	Exposed	Exposed	Exposed	Exposed
CERT	Unused	Unused	Unused	Unused

4.4 Impact and Applicability

The IMSI privacy attack exploits the lack of mutual authentication between UEs and ePDG servers using a rogue AP's impersonation of the real server. Our rogue AP does not relay any messages to the real server. Hence, this is not a MitM attack which relays all messages to the real source and destination. The handshaking instance between a UE and a fake ePDG (rogue AP) server implicitly ends after message (7) in Figure 4 due to the authentication failure.

We integrated all the functions into one Linux based laptop, so this attack demands that the attacker be placed in the same physical area of the target UE. However, depending on the attacker's ability, this attack can be performed remotely by installing many fake ePDG servers in target area.

Potentially, the exposed IMSI can be used to lookup the user's mobile number [14] using a paid web service. In addition, it is possible to track the victim's location even if the SIM card is transferred to a different device. These location privacy risks have gradually permeated in our lives during Internet of Things (IoT) era.

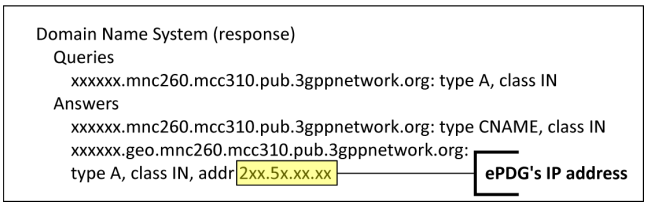

Figure 7: ePDG's IP address exposure (T-Mobile).

5 DOS ATTACKS

The purpose of DoS attack is to impair the availability of services provided to legitimate clients and subscribers. From our security analysis of Wi-Fi Calling, we derived three types of DoS attacks. The attacks are aimed at preventing the UE's access to Wi-Fi networks. First, we describe the attack scenarios to attack Wi-Fi Calling functionality by using the three messages in Wi-Fi Calling specification. Then, we discuss the impact on subscribers and operator services level respectively.

5.1 Attack Scenarios

ePDG discovery. The ePDG discovery procedure, also known as ePDG look-up, is a necessary mechanism for the connection of an UE with the LTE network. In this attack, we exploit the DNS lookup packet generated as part of this procedure [5]. In response to the DNS query, the response packet contains the static IP address of the UE's ePDG in local network. Figure 7 shows the captured DNS lookup packet as observed during ePDG discovery procedure. We can manipulate the ePDG's static IP address of the UE or drop the packet. This misbehavior leads to an unsuccessful session establishment. We tested all four major MNOs in the United States which comply with the standards, and we verified that all of these vulnerabilities exist in their systems. In our attack, the rogue AP sets up this address in *iptables* utility to filter the packets from ePDG and forward some packets to the attacker for issuing fake handshakes. (i.e.:*# iptables -A FORWARD -i eth0 -s 2xx.5x.x.x/16 -j DROP*)

IKE_SA_INIT message. During the handshake procedure, the UE sends a list of its capabilities to the network in an "IKE_SA_INIT" message. In particular, these capabilities include supported security algorithm features (e.g., AES256, SHA1, MODEP1024) [1]. However, that capability list is sent to the server without any protection. Thus the cipher suites can be forged easily and sent to the server by an attacker. If the security association fails due to the inappropriate cipher suites, the server refuses the connection attempts.

Deauthentication frame. This attack is known as the detach attack in LTE [15] and can be performed by a deauthentication attack in the Wi-Fi network. In aspects of Wi-Fi Calling, we send deauthentication frames at the link layer for dropping the ongoing calls without any alerts. Furthermore, this attack can be utilized to force an UE to attach to the rogue AP by sending deauthentication frames to the current UE's AP.

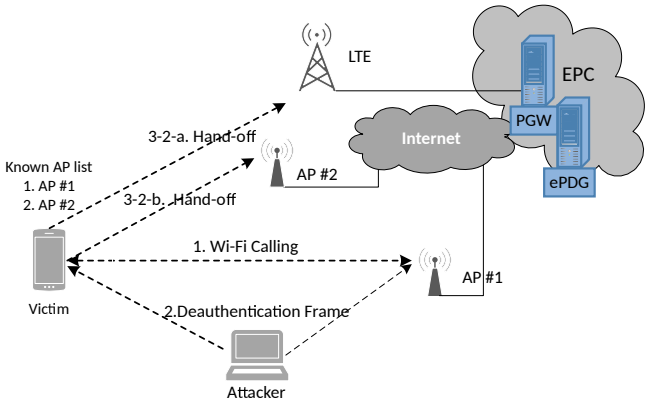

Figure 8: DoS attack environment.

5.2 Attack Setup

We performed and evaluated the deauthentication frame attack since it is the most practical DoS attack among the possible DoS attack scenarios.

Figure 8 depicts the experimental setup. We assume that (1) victim's UE is enabled to connect to known Wi-Fi AP automatically, (2) the victim and attacker are staying within range of the Wi-Fi network where the call started, and (3) the victim is talking on the Wi-Fi Calling mode.

First, the attacker identifies the target AP #1 and its attached device (victim) by radio scanning. Then, the attacker sends deauthentication frames continuously to AP #1 and victim.

If the victim gets attacks while using Wi-Fi Calling, two cases can occur, as shown in Table 3: First, the call is dropped immediately without any alerts. Second, due to the Voice Call Continuity (VCC) feature, it hand-offs the call to the LTE or to the AP #2 seamlessly. VCC specification is defined in TS23.206 by 3GPP to hand-off the call from the LTE to a known Wi-Fi AP, or vice versa, without dropping the call. Currently, the specification of IMS Service Continuity replaced VCC [7].

5.3 Results of Attacks

Through the experimental results as shown in Table 3, we confirmed that DoS attack could drop on-going calls in Wi-Fi Calling mode. The average call dropping rate over 20 attempts per device is approximately 26.25%. The experiments was performed in an area where the LTE signal is strong enough to support the hand-off from Wi-Fi to LTE.

The results may vary depending on the specific environment. For instance, the call indeed dropped if there is no LTE signal and known APs. Although it is not yet possible to guarantee a DoS attack due to the VCC function, future attacks could leverage more techniques than Wi-Fi Calling.

5.4 Impact and Applicability

Compared with the LTE DoS attacks described in [19], our deauthentication frame attack executes against UEs instead of networks so that UEs either can experience unexpected call drops or cannot connect to the legitimate Wi-Fi Calling networks. As the results

Table 3: Experimental Results of DoS attacks.

Devices	Call Drop	Hand-off		Total (Drop rate)
		AP	LTE	
Galaxy Note 5 (T-Mobile)	7	5	8	20 (35%)
iPhone 6 (Sprint)	4	6	10	20 (20%)
Galaxy Note 4 (AT&T)	8	4	8	20 (40%)
iPhone 8+ (Verizon)	2	5	13	20 (10%)

show, even in the environment with strong LTE signal, we could successfully cause call drops through the attack. Also, the results show that there is no visible impact of our attack in case of the call hand-off from Wi-Fi to LTE but the attack could interrupt an user from making a Wi-Fi call. Therefore, even if the call drop would not occur by the deauthentication frame attack, the attack can cause irregular situations to operators and users by forcing the hand-off. For operators, Wi-Fi Calling cannot obtain the expecting efficiency to offload data usage from LTE data networks. Simultaneously, the users cannot satisfy the needs of seamless call services in a low signal area.

6 COUNTERMEASURES

6.1 IMSI Privacy Attack Countermeasures

We provide countermeasures to identified attacks in this work from the perspective of operators and users. Operators include the mobile hardware and software manufacturers.

6.1.1 Operators and Vendors. (a) The optimal way to protect the IMSI in the packet is to utilize the public key infrastructure in the IKE_AUTH exchange process. Messages from the ePDG could be signed by using a public key digital signature mechanism. UEs would be able to verify these messages. This method could prevent UEs from fake handshaking.
(b) It is important to note that there are no means of authenticating the fake ePDG. To address this problem, mobile service providers must ensure that the hidden seed values (i.e., the ePGD's unique value: MAC address, etc.) are used to verify the ePDG. Those values also must not be created by and not open to the third party. That is, if this hidden seed is involved in generating a hash or nonce used for session key generation, we can validate the ePDG with the pre-shared secret keying value.
(c) Regarding enabling/disabling Wi-Fi Calling, the hand-off policy between LTE and Wi-Fi Calling should be determined not by the user's action (i.e., deauthentication frame coming from the user side) but by the quality of the signal and the security of APs. Currently, the hand-off policy between Wi-Fi Calling and LTE of the most vulnerable UEs is based on the user's action. However, we found out that some iPhones with iOS 11.3 on T-Mobile use the cellular preference policy, which activates calling hand-off only when signal strength is very low [26].

6.1.2 Users. We believe that the most important requirement from the user side is to disable the automatic connect option so that the UE is not forced to connect to the rogue AP. In particular, ISPs such as COX supports free hotspot service to their customers through automatic connections with affiliated APs [17]. As a result, UEs easily and automatically connect to known networks by relying on in-built Wi-Fi connection mechanisms. Therefore, users must intervene directly to avoid connecting to the rogue APs.

6.2 DoS Countermeasures

6.2.1 Operator and Vendors. During the ePDG selection procedure, the security protocols should protect the integrity of the ePDG IP address. To this end, the ePDG must add an authentication vector that can prove itself. As we mentioned in Section 6.1.1, the public key infrastructure can prevent the attacker from masquerading as a legitimate server.

Alternately, a rogue AP detection and prevention mechanism can be applied to WLANs to prevent DoS attacks. For instance, by installing wireless intrusion prevention systems (WIDS) in the target area, or by using applications to detect rogue APs, we can monitor the data in the radio signal (RSSI, MAC, IP, etc.) and detect the fake or suspicious devices in the network.

6.2.2 User. Users can utilize fake AP detection and mobile apps desired to avoid fake APs [16][34] on their devices to assist in attaching to appropriate APs. Also, when the LTE signal is strong enough to make a call, users could disable the Wi-Fi Calling and automatic connection function, especially in suspicious environments. This method, however, impacts the usability of the service as it requires the user's continuous intervention. To mitigate this inconvenience, the procedure to monitor LTE signal strength and automatically disable WiFi-Calling can be included in the operating systems supported by the UE's manufactures.

7 DISCUSSION

In this section, we look into trade-offs between security and usability, then discuss how they impact subscribers. Further, we examine deployment issues, cost, and complexity of various protection features.

7.1 Trade-off Between Security and Usability

If a user disables the automatic connection in the device setting of the UE, the user may need to confirm or re-enter the account information whenever a connection to the Wi-Fi AP is attempted. This procedure can be cumbersome in an environment where Wi-Fi APs frequently change as new connections are made. However, it is a preemptive way to protect the device from the malicious AP's luring.

Many UEs tend to switch to Wi-Fi Calling mode immediately when the user enables the option. However, it is a better idea to let the device decide when to switch to bypass the attacker's capturing time patterns. As we mentioned in Sections 6.1.2 and 6.2.2, the method to lure UE exploits this feature of automatic connection.

Table 4: Trade-offs considerations against countermeasures.

Countermeasures	Security	Usability	Efficiency	Cost
Public Key	●	●	◐	○
Shared secret	●	●	●	◐
Auto connect off	●	○	●	◐
Hand-off Policy	◐	○	◐	◐
WIDS	◐	●	●	○

○: Worst ◐: Medium ●: Best

7.2 Trade-off Between Security and Deployment

Changing any standardized protocol generally involves high cost (propagating changes throughout the mobile communication ecosystem and inducing all users to update each device on the network). As we mentioned in Sections 6.1.1 and 6.2.1, to protect IMSI privacy attack and DoS attacks, carriers may introduce a public key digital signature mechanism and physically install WIDS in the area, shielding UEs from malicious attacks. However, it is always necessary for MNOs to weigh budget and costs against the need to achieve maximum security objectives.

Table 4 summarizes the trade-offs for security, usability, efficiency, and cost for each countermeasure. We evaluate each countermeasure using the criteria mentioned in Sections 7.1 and 7.2. Each countermeasure is evaluated as either the best to the criteria (denoted as ●), may the medium to the criteria (denoted as ◐), or the worst to the criteria (denoted as ○). The deployment of "Public Key Infrastructure" and "WIDS" leads to more complexity and the high-cost burden in the MNOs network. Especially in case of public key infrastructure, the additional processing and increased messages can impact the latency of the connections. Regrading usability, "Auto connection disabling" and "Hand-off policy" modification enables to cause the interruption in seamless service of Wi-Fi Calling. As a result, we recommend that "Shard secret" described in Section 6.1.1 is the best countermeasure to address the vulnerabilities by considering trade-offs.

In summary, as shown in Table 5, we summarized all attacks and vulnerabilities we discovered in the Wi-Fi Calling that lead to security threats that violate the security properties of mobile subscribers. We also classified each vulnerability by its type of reason and arranged the countermeasures with the trade-offs to consider.

8 RELATED WORK

Regarding mobile network's security issues, users' privacy and availability problems of mobile networks have been researched. Shaik et al. [29] discovered an LTE device could leak its location using cell-tower signal strength information, which can be requested by a base station without authentication. They also designed attacks to deny LTE services to a target device by preventing its access to LTE networks and limiting the connection to 2G/3G networks using commercial devices. Kune et al. [21] demonstrated possible location test attacks that include circumventing the temporary identifier designed to protect the identity of the end user. Arapinis et al. [8] discovered the vulnerabilities to trace and identify mobile telephony subscribers in 3G telephony systems using formal methods. Mjolsnes et al. [23] introduced a simple way to catch IMSI and perform DoS attack using a rogue base station. In summary, most research has focused on privacy and DoS attacks by insecure implementations of the network component or signaling denial-of-service attacks. Also note that those works are only concerned with mobile networks, not Wi-Fi Calling.

With respect to Wi-Fi Calling, the first vulnerabilities introduced by Beekman et al. [9] in 2013. They discovered several vulnerabilities regarding TLS certificate validation against T-Mobile; these vulnerabilities allow eavesdropping on voice communications and modification of text by MitM attacks. To discover the vulnerabilities they leveraged the open source code of Android IMS (IP Multimedia Subsystem) stack provided by T-Mobile for developers to access various IMS-services, such as sessions and messaging [32]. However, the current edition of the WiFi-Calling specification no longer utilizes that mechanism, and it is virtually impossible to analyze server-side IMS stack source code (which is no longer open source). Therefore, we cannot directly adopt this approach to analyze in the same way.

There are two research articles regarding vulnerabilities in the current Wi-Fi Calling specification. O'Hanlon et al. [24] showed that a malicious user could obtain a user's IMSI and track over Wi-Fi due to the lack of sufficient privacy protection measures by pre-configured device profiles. Although they mentioned they could acquire an IMSI through the Wi-Fi Calling's IKE handshaking process, they did not provide any specific methods and results. In contrast, our study demonstrates in detail the procedure of attacks and countermeasures not only on IMSI privacy issues but also on DoS attack issues in the Wi-Fi Calling services.

Chalakkal el al. [10] described that sniffing VoLTE (voice over LTE) and Wi-Fi Calling interfaces can obtain the IMSI and private IPs of IMS by extracting IPSec keys from IP Multimedia Services Identity Module [2]. They also introduced injection attacks in Session Initiation Protocol (SIP) headers that enable location manipulation and side channel attacks. They obtained the keys by directly sniffing the mobile phone's network interface using SIMtrack [25]. Accordingly, this approach forces the attackers to tap the device physically, so that it is not feasible to be executed in the real environment. Differentiating from these work, our work focuses on analyzing network packets in transit and extracting the key material using a fake IPSec server.

9 CONCLUSION

In Wi-Fi Calling, the weak requirements in the standard specification regarding certifications allows the lack of mutual authentication during the handshake phases of the security association. By exploiting the vulnerabilities, we can set up a rogue AP that emulates a legitimate server and obtain target UE's IMSI and APN successfully. Those information can be abused to track user locations by malicious stakeholders. We also demonstrated the feasibility of DoS attacks for Wi-Fi Calling by spoofing the packets

Table 5: Wi-Fi Calling Attacks, Vulnerability and Countermeasures.

Attack		Security Property	Vulnerability		
			Type	Countermeasure	Trade-offs
Privacy	IMSI privacy	Confidentiality, Integrity	Incomplete specification Security architecture	Public key, Shared secret, Hand-offs policy	Security vs. Deployment Security vs. Usability
DoS	ePDG discovery	Availability, Confidentiality	Specification flaw	Shared secret, WIDS	Security vs. Deployment
	IKE_SA_INIT	Availability, Integrity	Specification flaw	Public key, WIDS	Security vs. Deployment
	Deauthentication	Availability	Specification flaw	WIDS	Security vs. Deployment, Security vs. Usability

exchanged in Wi-Fi Calling and modifying the payload. Some of the payloads are considered as critical parts of services, such as an address of the ePDG server and cipher suites. Notably, the call could be dropped suddenly without any alerts even if the UE has the voice call continuity function for seamless hand-offs.

To protect user privacy and availability against these attacks, we present practical countermeasures with the trade-off among security, deployment, and usability. As a result, the subsequent changes based on our works can be introduced in future specifications to reinforce the security. Regarding practicality, our attacks can be implemented and executed through readily available hardware at low cost.

ACKNOWLEDGMENT

Many thanks to the anonymous referees for their valuable and helpful comments. We would also like to give special thanks to Gerard Pinto who inspired us to make this work successful.

This material is based upon work supported in part by Samsung Research, Samsung Electronics, the Center for Cybersecurity and Digital Forensics at Arizona State University, the National Science Foundation (NSF 1651661), the Defense Advanced Research Projects Agency (DARPA HR001118C0060), and the Global Research Laboratory Program through the National Research Foundation of Korea funded by the Ministry of Science and ICT under Grant NRF-2014K1A1A2043029.

Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of United States Government or any agency thereof.

REFERENCES

[1] 3GPP. 2002. 3G Security; Wireless Local Area Network (WLAN) Interworking Security. *TS33.234* (2002). Latest release: 14.0.0 (2017-03-27). [Online]. Available: http://www.3gpp.org/DynaReport/33234.htm.

[2] 3GPP. 2002. Characteristics of the IP Multimedia Services Identity Module (ISIM) application. *TS31.103* (2002). Latest release: 15.2.0 (2018-04-03). [Online]. Available: http://www.3gpp.org/DynaReport/311034.htm.

[3] 3GPP. 2015. 3GPP. Network Architecture ; Specification 3GPP TS 23.002 version 12.7.0 Release 12. *TS33.002* (2015). Latest release: 15.0.0 (2018-03-27). [Online]. Available: http://www.3gpp.org/DynaReport/23002.htm.

[4] 3GPP. 2015. 3GPP System Architecture Evolution (SAE); Security architecture. *TS33.401* (2015). Latest release: 15.3.0 (2018-03-27). [Online]. Available: http://www.3gpp.org/DynaReport/33401.htm.

[5] 3GPP. 2015. Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3. *TS24.302* (2015). Latest release: 15.1.0 (2017-12-28). [Online]. Available: http://www.3gpp.org/DynaReport/24302.htm.

[6] 3GPP. 2015. Characteristics of the Universal Subscriber Identity Module (USIM) application. *TS31.102* (2015). Latest release: 15.0.0 (2018-04-03). [Online]. Available: http://www.3gpp.org/DynaReport/31102.htm.

[7] 3GPP. 2015. P Multimedia Subsystem (IMS) Service Continuity; Stage 2. *TS23.237* (2015). Latest release: 15.1.0 (2017-12-22). [Online]. Available: http://www.3gpp.org/DynaReport/23237.htm.

[8] Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. 2012. New privacy issues in mobile telephony: fix and verification. In *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS)*. ACM, 205–216.

[9] Jethro Beekman and Christopher Thompson. 2013. Man-in-the-middle attack on T-Mobile Wi-Fi Calling. *Electrical Engineering and Computer Sciences University of California at Berkeley, http://www. eecs. berkeley. edu/Pubs/TechRpts/2013/EECS-2013-18.html* (2013).

[10] Sreepriya Chalakkal, H Schmidt, and S Park. 2017. Practical Attacks on VoLTE and VoWIFI. *ERNW Enno Rey Netzwerke, Tech. Rep* (2017).

[11] CNET. 2017. Everything you need to know about Wi-Fi Calling. https://www.cnet.com/news/what-you-need-to-know-about-Wi-FiCalling/ [Online; accessed 13-September-2018].

[12] The Economist. 2016. The StingRay's tale. https://www.economist.com/united-states/2016/01/30/the-stingrays-tale [Online; accessed 13-September-2018].

[13] Caroline Gabriel. 2016. Wi-Fi Calling and the ePDG: The continuing importance of voice in the carrier model. *Rethink Technology Research* (January 2016).

[14] HLR Lookup, Enterprise HLR Lookup Portal and API. 2018. https://www.hlr-lookups.com/ [Online; accessed 13-September-2018].

[15] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. *Network and Distributed Systems Security (NDSS) Symposium* (2018).

[16] Hotspot ID. 2018. https://www.hotspotid.com/ [Online; accessed 13-September-2018].

[17] COX Inc. 2018. https://www.cox.com/aboutus/wifi-hotspot-map.html [Online; accessed 13-September-2018].

[18] Internet Engineering Task Force (IETF). 2014. Internet Key Exchange Protocol Version 2 (IKEv2). *RFC7296* (October 2014). [Online; accessed 13-September-2018]. Available: https://tools.ietf.org/html/rfc7296.

[19] Roger Piqueras Jover. 2013. Security attacks against the availability of LTE mobility networks: Overview and research directions. In *Wireless Personal Multimedia*

Communications (WPMC), 2013 16th International Symposium on. IEEE, 1–9.

[20] Roger Piqueras Jover. 2016. LTE security, protocol exploits and location tracking experimentation with low-cost software radio. *arXiv preprint arXiv:1607.05171* (2016).

[21] Denis Foo Kune, John Koelndorfer, Nicholas Hopper, and Yongdae Kim. 2012. Location leaks on the GSM air interface. *ISOC NDSS (Feb 2012)* (2012).

[22] Market Insights Reports. 2017. The VoLTE Ecosystem: 2016-2030 Opportunities, Challenges, Strategies Forecasts. (2017). Latest release: 15.1.0 (2017-12-28). [Online]. Available: https://www.marketinsightsreports.com/reports/091915323/the-volte-voice-over-lte-ecosystem-2016-2030-opportunities-challenges-strategies-forecasts/.

[23] Stig F Mjølsnes and Ruxandra F Olimid. 2017. Easy 4G/LTE IMSI Catchers for Non-Programmers. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*. Springer, 235–246.

[24] O'Hanlon, Piers and Borgaonkar, Ravishankar and Hirschi, Lucca. 2017. Mobile subscriber WiFi privacy. In *IEEE Security and Privacy Workshops (SPW)*.

[25] OSMOCOM. 2018. Osmocom SIMtrack. https://osmocom.org/projects/simtrack/wiki/SIMtrack/ [Online; accessed 13-September-2018].

[26] PiunikaWeb. 2018. iOS 11.3 nasty surprise. http://piunikaweb.com/2018/04/03/ios-11-3-nasty-surprise-t-mobile-prioritises-cellular-over-wifi-calling/ [Online; accessed 13-September-2018].

[27] Rethink Technology Research. 2016. - Mobile network ownership, MVNOs and NWaaS Wholesale, sharing and NWaaS 2015-2020. (2016).

[28] SECDEV. 2018. Scapy. https://scapy.net/ [Online; accessed 13-September-2018].

[29] Altaf Shaik, Ravishankar Borgaonkar, N Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2015. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. *arXiv preprint arXiv:1510.07563* (2015).

[30] Altaf Shaik, Ravishankar Borgaonkar, Jean-Pierre Seifert, N. Asokan, and Valtteri Niemi. 2016. Practical Attacks Against Privacy and Availability in 4G/LTE. In *Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS)*. http://www.internetsociety.org/events/ndss-symposium-2016

[31] Daehyun Strobel. 2007. IMSI catcher. *Chair for Communication Security, Ruhr-Universität Bochum* 14 (2007).

[32] T-Mobile and Movial. 2016. The IMS Open Source Project For Android. https://www.openhub.net/p/ims-android [Online; accessed 13-September-2018].

[33] Fabian van den Broek, Roel Verdult, and Joeri de Ruiter. 2015. Defeating IMSI catchers. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*. ACM, 340–351.

[34] VREM. 2018. VREM Software Development. https://vremsoftwaredevelopment.github.io/WiFiAnalyzer/ [Online; accessed 13-September-2018].