The Dark Side of Operational Wi-Fi Calling Services

Tian Xie\textsuperscript{1}, Guan-Hua Tu\textsuperscript{1}, Chi-Yu Li\textsuperscript{2}, Chunyi Peng, Mi Zhang\textsuperscript{1}

\textsuperscript{1}Michigan State University
\textsuperscript{2}National Chiao Tung University
\textsuperscript{3}Purdue University
Wi-Fi Calling Services

• Wi-Fi Calling services empower mobile users to access voice and text services over Wi-Fi instead of cellular networks.

• All of four U.S. major operators have launched Wi-Fi calling services since 2016 – Verizon, AT&T, T-Mobile, and Sprint.

• By 2020, Wi-Fi calling services will take 53% of mobile IP voice service usage including VoLTE (26%) and others (21%).
Wi-Fi Calling Services Primer

• Specifically, they are **SIP-based** voice and text services, however, they are using a 3GPP-modified version.
  • Developed on top of 3GPP **IMS** (IP Multimedia Subsystem)
    • Operators use IMS to provide users with IP-based services such as VoIP
  • It uses **the same infrastructure** for VoLTE (Voice over LTE) users.

• Radio Access Network (RAN)
  • **Wi-Fi Access Point (Wi-Fi Calling)**
  • eNodeB (VoLTE)

• LTE Core Network (CN)
  • **ePDG (Evolved Packet Data Gateway, Wi-Fi calling)**
  • PDN-GW (Public Data Network Gateway)
  • AAA (Authentication, Authorization, and Accounting)
  • IMS (IP Multimedia Subsystem)
Wi-Fi Calling Security Mechanisms

• Using well-examined 3GPP Authentication and Key Agreement (AKA) and SIM-based security adopted by VoLTE – symmetric cryptography.

• All Wi-Fi calling signaling and voice/text packets are delivered through IPsec (Internet Protocol Security) – ciphering and integrity protection.

How Does It Go Wrong?
Finding 1: Wi-Fi calling devices will activate Wi-Fi calling services over an insecure Wi-Fi network.
Vulnerability: Wi-Fi calling devices do not exclude insecure Wi-Fi networks – (design defect of standards)

• Vulnerability – **Wi-Fi calling standards don’t exclude insecure Wi-Fi**
  • Two Wi-Fi access point selection modes do not consider security factors yet!!
  • Manual (use a prioritized list)
  • Automated (ANDSF, Access network discovery and selection function)

• Validation:
  • Deploy an insecure Wi-Fi network using a Wi-Fi router which is vulnerable to ARP spoofing attack – **foundation of a variety of MITM attacks**
    • I.e., victim’s WIFI packets will be intercepted and delivered to adversaries
  • We test whether the Wi-Fi calling devices keep connecting to the above Wi-Fi router

All tested Wi-Fi calling devices connected to the insecure Wi-Fi router!!!
Finding 2: Wi-Fi calling **devices** do not employ security defense against the common Wi-Fi ARP spoofing attacks.
Vulnerability: Wi-Fi calling devices do not defend against ARP spoofing attacks –(implementation issue of devices)

- Vulnerability - Wi-Fi calling devices always accept **ARP Reply** message
  - **All packets sent by Wi-Fi calling devices can be redirected to adversaries**

- Validation
  - We use EtterCap to send ARP reply message to Wi-Fi calling devices.

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>465</td>
<td>56.316883</td>
<td>192.168.2.5</td>
<td>208.54.16.4</td>
<td>ESP</td>
<td>176</td>
<td>ESP (SPI=0x0855c9c8)</td>
</tr>
<tr>
<td>468</td>
<td>56.337334</td>
<td>192.168.2.5</td>
<td>208.54.16.4</td>
<td>ESP</td>
<td>176</td>
<td>ESP (SPI=0x0855c9c8)</td>
</tr>
</tbody>
</table>

**Adversaries can capture all Wi-Fi packets sent by the victim**
Finding 3: Wi-Fi calling devices and infrastructure indeed deploy extra security mechanisms for malicious Wi-Fi attacks, however, it is not enough.
A system-switch mechanism for Wi-Fi Calling Service DoS Attacks

• With the aforementioned two findings, adversaries can launch Wi-Fi Calling service DoS attacks
  • Discarding all intercepted Wi-Fi signaling and voice/text packets

• System-switch (Wi-Fi-> Cellular)
  • **If an user fails to dial a Wi-Fi voice call**, the mobile device will switch to use cellular-network-based voice services.
  • **If Wi-Fi calling service operators cannot route an incoming call to users by Wi-Fi calling**, the operators will switch it to use cellular-network-based one.

For users, they are free of voice/text DoS attacks.
Vulnerability: Service continuity is not revised accordingly – (design defect of standards)

- Service continuity can **seamlessly** switch an ongoing Wi-Fi calling call to back to cellular-network-based voice call
- However, it is only **triggered** while the **quality of Wi-Fi radio signals is bad**

What if Wi-Fi radio quality is good but Wi-Fi calling service quality is poor?

- We start dropping all Wi-Fi calling packets after the call conversation is started (Wi-Fi radio quality is good)

The system-switch security mechanism is bypassed!!
No cellular-based voice call is initiated.
Finding 4: **Wi-Fi calling service operators** do not take extra security mechanisms to protect the *encrypted* Wi-Fi calling packets
Vulnerability: The Wi-Fi calling traffic is vulnerable to side-channel attacks – (operational slip of operator)

- Vulnerability - Wi-Fi calling is the **only service** that is carried by the IPSec channel between the mobile device and ePDG.
  - Adversaries may infer various Wi-Fi calling events such as dialing calls, receiving calls, etc.
- Validation
  - Apply C4.5 to analyze IPSec traffic patterns
  - We are able to infer six Wi-Fi calling events
    - Evt I: Activating Wi-Fi calling service
    - Evt II: Receiving an incoming call
    - Evt III: Dialing an outgoing call
    - Evt IV: Sending a text
    - Evt V: Receiving a text
    - Evt VI: Deactivating Wi-Fi calling service
Two Proof-of-concept Attacks
Attack 1: User privacy leakage

- The **call statistics** has been proven effective to infer user privacy including **personality**[1], **mood**[2], **malicious behaviors**[3], etc.

- Devising WiCA (Wi-Fi Calling Analyzer) to infer a Wi-Fi calling user’s call statistics
  - Who initiates the call (an incoming call or an outgoing call)
  - Who hangs up the call first (caller or callee)
  - Ringing time (how long the callee answers the call)
  - Call conversation time

Infer call statistics@WiCA

• WiCA’s finite state machine

  • Record the number of **Uplink** and **Downlink** packets transmitted every 2 seconds
  • Classify them into three categories by packet size:
    • **Small** (<200 bytes), **Medium** (200-800 bytes), **Large** (>800 bytes)

• Our observations on **small packets**

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Identified Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num_UL_CSmall</td>
<td>Num_DL_CSmall</td>
</tr>
<tr>
<td>=0</td>
<td>&gt;10</td>
</tr>
<tr>
<td>&gt;10</td>
<td>&gt;10</td>
</tr>
<tr>
<td>=0</td>
<td>=0</td>
</tr>
</tbody>
</table>
Ringing time inference

• We observe that Wi-Fi calling service servers will keep sending small packets to both of caller and callee after SIP RINGING message is sent by the callee.

Packet arrivals for the event ‘receiving a call with a ringtone’ (callee perspective).

No uplink small packets after callee’s phone is ringed

Small downlink packets can be used to detect Ringing

Packets sent by Wi-Fi calling server

Packets sent by the callee
Conversation time inference

• We observe small packets on the uplink and downlink during the call conversation.

Packet arrivals for ‘Talking’ (callee perspective).
Call initiation and termination inference

• Relying on the directions and patterns of large packets

  • E.g., if the ringing or talking event is detected and the first large packet (SIP INVITE) is sent by the monitored Wi-Fi user => It is an outgoing call

  • E.g., if the talking and not-talking events are detected and the last large packet (200 OK) is sent by the Wi-Fi server => the monitored Wi-Fi user terminates call first
Performance of WiCA

• Who initiates, Who ends call first : 100% accurate
• Ringing time and conversation time
  • Maximum error is less than 0.8 seconds.

<table>
<thead>
<tr>
<th>Time</th>
<th>T-Mobile</th>
<th>AT&amp;T</th>
<th>Verizon</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean</td>
<td>Std</td>
<td>Mean</td>
</tr>
<tr>
<td>Ringing</td>
<td>0.16s</td>
<td>0.11s</td>
<td>0.34s</td>
</tr>
<tr>
<td>Conversation</td>
<td>0.17s</td>
<td>0.07s</td>
<td>0.67s</td>
</tr>
</tbody>
</table>
Another application of WiCA

• By face recognition, it is not difficult to identify who you are.

• How about their IP addresses if they are using free public WiFi?

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>440</td>
<td>56.276919</td>
<td>208.54.16.4</td>
<td>192.168.2.5</td>
<td>ESP</td>
<td>176</td>
<td>ESP (SPI=0xbb21253b)</td>
</tr>
<tr>
<td>441</td>
<td>56.266969</td>
<td>208.54.16.4</td>
<td>192.168.2.5</td>
<td>ESP</td>
<td>176</td>
<td>ESP (SPI=0xbb21253b)</td>
</tr>
<tr>
<td>465</td>
<td>56.316883</td>
<td>192.168.2.5</td>
<td>208.54.16.4</td>
<td>ESP</td>
<td>176</td>
<td>ESP (SPI=0x855e9c8)</td>
</tr>
<tr>
<td>468</td>
<td>56.337334</td>
<td>192.168.2.5</td>
<td>208.54.16.4</td>
<td>ESP</td>
<td>176</td>
<td>ESP (SPI=0x855e9c8)</td>
</tr>
<tr>
<td>469</td>
<td>56.347763</td>
<td>208.54.16.4</td>
<td>192.168.2.5</td>
<td>ESP</td>
<td>176</td>
<td>ESP (SPI=0xbb21253b)</td>
</tr>
<tr>
<td>470</td>
<td>56.348012</td>
<td>208.54.16.4</td>
<td>192.168.2.5</td>
<td>ESP</td>
<td>176</td>
<td>ESP (SPI=0xbb21253b)</td>
</tr>
</tbody>
</table>
WiCA with visual recognition system

• With the mature visual recognition system, WiCA’s call statistics can help to identify both of user identities and their IP addresses.

• The ways people are surfing and talking on phones are different.

We know which of IP addresses is to initiate Wi-Fi calling call and its call statistics.
Attack 2: Telephony harassment or denial of voice service attack (THDoS)

- We devise a telephony harassment or denial of voice service attack against Wi-Fi calling users.
  - It can bypass the security defenses deployed on Wi-Fi calling devices and the infrastructure.
  - The attack is based on the manipulation of the delivery of Wi-Fi calling signaling and voice packets for an ongoing call.
  - It contains several variants.
Results of Discarding Wi-Fi Signaling and Voice packets

<table>
<thead>
<tr>
<th>No.</th>
<th>Dropped Packets</th>
<th>Sender</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>INVITE</td>
<td>Caller</td>
<td>Caller initiates a cellular-based call.</td>
</tr>
<tr>
<td>2</td>
<td>100 Trying</td>
<td>Server</td>
<td>No effect.</td>
</tr>
<tr>
<td>3</td>
<td>183 Session</td>
<td>Callee</td>
<td>Two outgoing calls arrive at callee.</td>
</tr>
<tr>
<td>4</td>
<td>PRACK</td>
<td>Caller</td>
<td>No effect.</td>
</tr>
<tr>
<td>5</td>
<td>200 OK</td>
<td>Callee</td>
<td>No effect.</td>
</tr>
<tr>
<td>6</td>
<td>180 Ringing</td>
<td>Callee</td>
<td>Caller will not enter conservation state. His/her phone gets stuck in the dialing screen.</td>
</tr>
<tr>
<td>7</td>
<td>PRACK</td>
<td>Caller</td>
<td>No effect.</td>
</tr>
<tr>
<td>8</td>
<td>200 OK</td>
<td>Callee</td>
<td>Caller keeps hearing the alerting tone.</td>
</tr>
<tr>
<td>9</td>
<td>200 OK</td>
<td>Callee</td>
<td>Caller keeps hearing the alerting tone.</td>
</tr>
<tr>
<td>10</td>
<td>ACK</td>
<td>Caller</td>
<td>No effect.</td>
</tr>
<tr>
<td>11</td>
<td>Voice Packets</td>
<td>Caller /Calle</td>
<td>Call drops or voice quality downgrades.</td>
</tr>
<tr>
<td>12</td>
<td>BYE</td>
<td>Caller</td>
<td>Callee gets stuck in the conversation state for 20s. Afterwards, the call is terminated.</td>
</tr>
<tr>
<td>13</td>
<td>200 OK</td>
<td>Callee</td>
<td>No effect.</td>
</tr>
</tbody>
</table>

Wi-Fi calling Call Flow
Four Call Attack Variants

• Attack Wi-Fi signalings
  • Annoying-Incoming-Call Attack
    • Victim is callee:
      • **He/she keeps receiving incoming calls**
      • **By discarding 180 Ringing message or 183 Session Progress message**
  • Zombie-Call Attack – a call cannot be ended
    • Victim is caller:
      • The callee has answered the incoming call.
      • However, the caller’s device gets stuck in the dialing screen and will keep hearing the alerting tone.
      • **The conversation is never started.**
    • **By discarding 200 OK message**
Four Call Attack Variants (cont.)

- Attack Wi-Fi voice packets
  - Mute Call Attack – a muted call
    - Can only mute a call for 8s, call will be terminated by network
    - Not terminate the call but only mute the call
  - Telephony Denial-of-Voice-Service Attack
    - Can make the conversation be hardly continued

<table>
<thead>
<tr>
<th>Drop Rate (%)</th>
<th>Voice Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>20%</td>
<td>No clear impact.</td>
</tr>
<tr>
<td>40-60%</td>
<td>Some noises.</td>
</tr>
<tr>
<td>70-90%</td>
<td>Conversation is hardly continued.</td>
</tr>
<tr>
<td>100%</td>
<td>Call is terminated by the network.</td>
</tr>
</tbody>
</table>
Real-world Impact

• We find that Wi-Fi calling users will suffer from the devised proof-of-concept attacks, specifically for the users who are using campus Wi-Fi
  • Usually provide their faculty, staff, students, and guests with free Wi-Fi
  • However, they are not always secure (cannot defend against our attacks)
    • MSU
    • New York University
    • University of California Berkeley
    • Northeastern University
    • etc
Solutions
Solutions

• Short-term: Using Virtual Private Network (VPN) service
  • It aims to increase the **difficulty** of launching side-channel attacks
  • Adversaries cannot easily infer each Wi-Fi calling service signalings/voice/text packets

• Long-term: Revisit Wi-Fi calling service standards
  • Stipulate required security mechanisms which defends against the state-of-the-art Wi-Fi based attacks
  • Empower both Wi-Fi calling device and infrastructure to detect whether users are under the attack by monitoring the quality of Wi-Fi calling services and take actions (e.g., excluding malicious Wi-Fi networks)
  • Revise the current service continuity procedure from security perspective
Conclusion

- We conducted the **first security study** on exploring the dark side of operational Wi-Fi calling services provided by three major U.S. operators as well as their commodity Wi-Fi calling devices.

- Four security vulnerabilities are discovered, which stem from **design defects** of Wi-Fi calling standards, **operational slips** of operators, and **implementation issues** of Wi-Fi calling devices.

- We demonstrate the **negative real-world impacts** (e.g., WiFi DoS) by two proof-of-concept attacks and provide recommended remedies.

- Our lessons learned can secure both Wi-Fi calling service users and operators and facilitate its global deployment, as well as provide new design insights for upcoming 5G networks.
Thank you! Questions?