How Voice Service Threatens Cellular-Connected IoT Devices in the Operational 4G LTE Networks

Tian Xie¹, Chi-Yu Li², Jiliang Tang¹, Guan-Hua Tu¹

¹Michigan State University
²National Chiao Tung University
Internet-of-Things (IoT) Era

‘Things’ include a wide variety of devices

- House appliances
- Hotspot on vehicles
- Wearable devices
- Heart monitoring implants
- Cameras streaming live feed of wild animals
- Biochip transponders on farm animals
- Etc.

https://appsec-labs.com/iot-security/
Cellular IoT

- Rel-8/ Cat. 4, Rel-8/Cat. 1, etc.
- Providing wide range data rates (0.2 Mbps to 150 Mbps) with low-power consumption for IoT devices.
- Already being proposed in 4G LTE networks and can be merged with existing networks.

Non-Cellular IoT

- LoRA, SigFox, etc.
- Only for low-speed transmission (<= 50 Kbps) and low-power consumption IoT services.
Key Problem for Cellular IoT Services

- Does the existing network infrastructure support IoT services well?
Glance of Cellular IoT

1. Cellular IoT devices share the similar network architecture with non-IoT devices (smartphones).
2. Specific IoT cellular network specification.
Study of IoT Support in Cellular Networks

- **Cellular IoT Primer**
  - Cellular IoT Architecture
  - IoT Specifications

- **Vulnerability**

- **Proof-of-concept Attack**

- **Solution**
4G LTE Network Architecture for Cellular IoT

- Radio Access Network (RAN)
- Core Network (CN)
  - Management
  - Control
  - Data
4G LTE Network Architecture for Cellular IoT

• Management Plane
  • Charging Gateway Function (CGF)
  • Billing System
4G LTE Network Architecture for Cellular IoT

- Control plane
  - Home Subscriber Server (HSS)
  - Mobility Management Entity (MME)
4G LTE Network Architecture for Cellular IoT

- Data plane
  - CN connects RAN, IMS, and Internet
Cellular IoT Technologies in 4G LTE

- Various network specifications in the 4G LTE network for diverse demands from IoT services

<table>
<thead>
<tr>
<th>Technologies</th>
<th>Rel-8/Cat.4</th>
<th>Rel-8/Cat.1</th>
<th>Rel-12/Cat.0</th>
<th>Rel-13/Cat.M1</th>
<th>Rel-13/NB-IoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT types</td>
<td>Critical</td>
<td>Critical/Massive</td>
<td>Massive</td>
<td>Massive</td>
<td>Massive</td>
</tr>
<tr>
<td>Downlink peak rate</td>
<td>150 Mbps</td>
<td>10 Mbps</td>
<td>1 Mbps</td>
<td>1 Mbps</td>
<td>0.2 Mbps</td>
</tr>
<tr>
<td>Uplink peak rate</td>
<td>50 Mbps</td>
<td>5 Mbps</td>
<td>1 Mbps</td>
<td>1 Mbps</td>
<td>0.2 Mbps</td>
</tr>
<tr>
<td>Duplex mode</td>
<td>Full</td>
<td>Full</td>
<td>Half/Full</td>
<td>Half/Full</td>
<td>Half</td>
</tr>
<tr>
<td>UE bandwidth</td>
<td>20 Mhz</td>
<td>20 Mhz</td>
<td>20 Mhz</td>
<td>1.4 MHz</td>
<td>180 KHz</td>
</tr>
<tr>
<td>UE max transmission power</td>
<td>23dBm</td>
<td>23dBm</td>
<td>23dBm</td>
<td>20 or 23dBm</td>
<td>23dBm</td>
</tr>
<tr>
<td>Complexity vs. Cat.1</td>
<td>125%</td>
<td>100%</td>
<td>50%</td>
<td>20-25%</td>
<td>10%</td>
</tr>
<tr>
<td>Voice over LTE</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
<tr>
<td>Battery life</td>
<td>day(s)</td>
<td>year(s) [7]</td>
<td>&gt;10 years [20]</td>
<td>&gt;10 years [20]</td>
<td>&gt;10 years [20]</td>
</tr>
</tbody>
</table>
Vulnerability

- Conventional charging function operates on a per-bearer basis.
Improper IoT Service Charging Function

• Network Interface

Phone: enable VoLTE and mobile data

Watch: enable VoLTE and mobile data

Two network interfaces

Only one network interface

Same experiment location
Improper IoT Service Charging Function

Question: Which charging function is used on the smartwatch?

Currently, the service plan for IoT devices provided by operators is volume-based charging.

This bearer’s charging method is volume-based. Thus, the VoLTE service will be charged too. (VoLTE signaling is not free!)
Proof-of-concept Attack

• Launch an IoT overcharging unaware attack by sending a large number of VoLTE call signaling spams

Without receiving SIP Update, the callee does not ring.
Proof-of-concept Attack

• Use our previous developed application, VoLTECaller, to launch the attack.

Interrupt the dialing when observing SIP Session Progress

1. SIP Invite
2. SIP Session Progress
3. Resource Reservation
4. SIP Update
5. Ringing
6. SIP Ringing
Attack Result

Each VoLTE call attempt: 3.24 seconds
Total data consumed: 681 KB

Data usage volume per second
Accumulated data usage volume per second

177 MB
Real World Impact?

• Verizon provides a cellular IoT charging plan for IoT users ($2 for one device with 200 KB data.
• The attack can consume 681 KB in 324 seconds, which means that 200KB data can be used in 100 seconds.
  • No automatically refill: Denial of service
  • Automatically refill: Non-negligible financial loss

$2 per 100 seconds = $1440 per day for a single IoT device!
Solution

• Flow-based service charging method for IoT devices.

• Service data flow is identified by the five-tuple information:

  Source IP address or mask  Source port number  Destination IP address or mask  Destination port number  Protocol ID (TCP/UDP)

VoLTE signaling can be represented (*, *, VoLTE_Server_IP, 5060, TCP)
Solution

• Advantage of flow-based charging method
  • Compatible: Applying different charging methods to a single bearer for different services
  • Deployable: T-Mobile and Verizon provide users with free DNS services (packets over TCP/UDP destination port 53 are free of charge)
CONCLUSION

• Review the network architecture and specification for cellular IoT
• Vulnerability
  • The single bearer of IoT device servers both VoLTE services and data services.
• Proof-of-concept attack
• Solution
  • Flow-based service charging method
Thank you! Questions?