BREAKING AND FIXING VOLTE: EXPLOITING HIDDEN DATA CHANNELS AND MIS-IMPLEMENTATIONS

Analysis of a WhitePaper Mapped to VoIPShield Systems

Alan Stranaghan
Product Management

alan.stranaghan@voipshield.com

December, 2015

References and Acknowledgement

This paper references the following publications, with acknowledgment to the authors:

1. **Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations**
   Authors: Hongil Kim, Dongkwan Kim, Minhee Kwon, Hyungseok Han, Dongsu Han, Yongdae Kim.
   KAIST, formerly the Korea Advanced Institute of Science and Technology, Republic of Korea.
   Authors: Yeongjin Jang, Taesoo Kim.
   Georgia Institute of Technology, United States of America.

2. **Vulnerability Note VU#943167: Voice over LTE implementations contain multiple vulnerabilities.** www.kb.cert.org/vuls/id/943167
   Author: Garret Wassermann.
   CERT, Software Engineering Institute, Carnegie Mellon University. Sponsored by the US Department of Homeland Security Office of Cybersecurity and Communications.

This paper, where appropriate, uses direct quotes, concepts and explanations from the above.

Purpose

The purpose of this analysis is to:

- Summarise the VoLTE security exploits defined in the paper;
- Match the corresponding vulnerability from the list defined in the Vulnerability Note;
- Indicate areas where VoIPshield Systems can address and thus add value with our VoIPguard™ Technology integration into McAfee Network Security Platform solution.

Background

With higher bandwidth and lower latency, Long Term Evolution (LTE) has become the dominant cellular network technology in recent years.

The VoLTE business drivers are:

- Operator cost savings, with the eventual elimination of 3G radios in cell towers etc.;
- Carrier revenue potential, with better integration of voice and data applications leading to increased adoption of products and services.

VoLTE benefits:

- Simultaneous voice and data calls – Ability to access the internet at the same time as making a voice call. Some Operators have provided this, however it becomes table-stakes with VoLTE and will drive better integration of voice and internet apps.
- Better call quality and faster call connection – Often referred to as 'high definition (HD) calling', however this requires that the recipient also have a VoLTE-enabled device and both parties have VoLTE service.

VoLTE adoption:

- By April 2015, 16 operators in 7 countries had commercially launched VoLTE services and 90 operators in 47 countries are investing to deploy VoLTE services in the near future.

VoLTE security:

- VoLTE security is becoming a topic of concern, as highlighted by the above publications. Since VoLTE operates on the cellular network, it is not only exposed to VoIP-related issues, but also inherits security issues due to the LTE implementation, as well as the architecture of the VoLTE-enabled phones themselves.

VoLTE implementation basics

In order to use VoLTE services one needs:

- A VoLTE-enabled device;
- Access to a 4G LTE mobile network where the Operator provides VoLTE service.

VoLTE-enabled devices

A VoLTE-enabled phone typically is a next-generation smartphone. Examples include the latest offerings from LG, Samsung and Apple as well as other manufacturers. These differ from earlier smart phone models which, although they can use 4G LTE service for calling and internet access, they cannot use the additional benefits of VoLTE service.

In circuit-switching (2G/3G) mobile networks, the signal processing and radio communication is conducted by a communication processor (CP) in a mobile phone, whose detailed implementation is proprietary to a few chip manufacturers. On the contrary, VoLTE-compatible devices perform signal processing purely in their application processor (AP): e.g., via a software-based SIP client. In these phones, the CP is used for only the on-board microphone and speaker. This is an important distinction, especially when one considers security implications.

VoLTE service on 4G LTE

The major difference between 2G/3G and LTE networks is in the way they deliver data in the core network. The 3G network separates network domains into packet-switching for the Internet connection and circuit-switching for phone calls.

In contrast, **the LTE network only operates through the packet-switching domain**; as it does not have a circuit-switching domain, its voice calls either fall back into the 2G/3G network (also known as Circuit Switched Fallback, or CSFB in short) or, the 4G LTE Operator provides a VoLTE solution to transfer both voice calls and data to the packet-switching domain, which does not require any fallback to the 2G/3G circuit-switching network.

Unlike VoIP services, the LTE network provides a communication channel (**the default *bearer channel*)** with guaranteed bandwidth, once a VoLTE-enabled phone connects to the network. Call signaling uses this channel.

Every phone supporting VoLTE is assigned **two IP addresses: one for voice and the other for data.**

When a call session is established, a ***dedicated bearer channel*** is created to identify voice-related traffic and all voice packets are transferred through this dedicated bearer. Upon call termination, the bearer used for the voice session is released.

VoLTE security

As with general-purpose computers, VoLTE relies completely on Internet Protocol (IP) for packet delivery. Consequently, well-known offensive techniques targeting IP are also applicable for abusing or attacking VoLTE-based devices.

Since VoLTE operates on the cellular network, it also inherits security issues from the cellular network, such as adversaries being able to interpose the signal processing itself.

VoLTE Exploits as identified in the whitepaper

1. Direct Communication – Phone-to-Phone or Phone-to-Internet

Exploit specifics

- The default bearer for VoLTE signaling messages is always established as long as the device is turned on. Each call party has the IP address for the default VoLTE bearer.
- The sending phone can, therefore, send SIP messages via **direct communication** to the receiving phone, bypassing the SIP server, if that practice is not blocked by the Operator.

Example Use Cases and implications

- The receiving phone does not return the SIP 'OK' message to the SIP server, that would cause the call accounting system initiate billing. Result: **Free calling hence loss of Operator revenue.**
- The sending phone can connect to the internet, hence initiate calls to other phones using a fake calling number **(call spoofing).** Result: **potential for phishing, harassment calls etc.**

Corresponding CERT Vulnerability: CWE-284: Improper Access Control

"Some networks allow two phones to directly establish a session rather than being monitored by a SIP server, thus such communication is not accounted for by the provider. This may be used to either spoof phone numbers or obtain free data usage such as for video calls."

Technical analysis and identified solutions

Use case / vulnerability	McAfee NSP/ VoIPshield Solution	Possible customer / operator solution	Remarks
Direct communication.			
1) Call Accounting / Billing for VoLTE call starts when a SIP server receives OK (200) from UE-B, the receiver. Thus, if UE-B	In general, all direct SIP to SIP communications can be blocked via McAfee NSP firewall rules for SIP service and IP ranges that	Since all communications (even direct) are going through the VoLTE infrastructure, firewalls/other filtering	

Use case / vulnerability	McAfee NSP/ VoIPshield Solution	Possible customer / operator solution	Remarks
does not send OK (200) to the SIP server, then the call may not be charged.	represent UEs. McAfee NSP is able to recognize SIP messages regardless of the port on which they originated and then implement policy dependent actions, such as a firewall policy-based or IPS policy-based.	could be set in place to block direct communication between phones.	
2) Phone-to-Internet (when UE uses VoIP IP address to access the internet)	McAfee NSP firewall capabilities can be used to block all traffic between VoIP IP and a non-VoLTE server IPS. Also, see above.	Communication to the internet from a VoIP IP address could be blocked by VoIP equipment or firewall.	

2. Lack of Authentication

Exploit specifics

- A SIP server should authenticate every SIP message to determine whether it is from a valid user. Some Operators do not perform proper user authentication.

Example Use Cases and implications

1. The sending phone generates a modified SIP INVITE message and sends it to the SIP server. Since the Server does not authenticate this number to the user, a fake caller number could be used, i.e. **Call Spoofing** could be performed. Result: **potential for harassment calls, phishing, fraud etc.** Also **charging the owner of the number used for the fake calling.**

2. The sending phone generates a BYE message and sends it to the SIP server, causing an on-going call to terminate prematurely. This is a type of **Denial of Service** at the phone.

Corresponding CERT Vulnerability: CWE-287 Improper Authentication

"Some networks do not properly authenticate every SIP message, allowing spoofing of phone numbers."

Technical analysis and identified solutions

Use case / vulnerability	McAfee NSP/ VoIPshield Solution	Possible customer / operator solution	Remarks
No authentication.			
A SIP server should	1) User authentication	1) A SIP server should	**VoIPshield is**

Use case / vulnerability	McAfee NSP/ VoIPshield Solution	Possible customer / operator solution	Remarks
authenticate every SIP message to determine whether it is from a valid user. However, according to the paper, two of the Korean operators do not perform proper user authentication. As a result, we could make a call with a fake phone number by sending a manipulated INVITE message.	check– cannot be achieved by McAfee NSP as we can't have list of phone numbers/user mappings in it and user/password. 2) Direct SIP communication blocking to assist vendor workaround can be implemented (see above).	authenticate every SIP message to determine whether it is from a valid user. 2) Disable direct SIP communication to prevent skipping server authentication.	**developing an incremental analytics solution.**

3. Lack of Session Management

Exploit specifics

- When the SIP server receives a SIP INVITE message, it should open a session for each message and manage each session independently. Often not the case with Operators.
- Normally, a user can make one call at a time with the native calling app on a phone. A tampered phone could transmit a virtually unlimited number of INVITE messages.
- Each INVITE results in a dedicated bearer channel and these are expensive in terms of LTE call control processing.

Example Use Cases and implications

1. A phone sends a large number of SIP INVITES. Result: Overloading the SIP server and paralyzing the IMS network for VoLTE service. This is a type of **Denial of Service at the Core Network,** performed **using a single mobile device,** where such an attack usually requires a large number of bots.

2. Calling a large number of phones **simultaneously**.

3. Generating a large number of bearer channels to establish a **hidden peer-peer network**.

Corresponding CERT Vulnerability: CWE-384 Session Fixation

"Some networks allow a user to attempt to establish multiple SIP sessions simultaneously rather than restricting a user to a single voice session, which may lead to denial of service attacks on the network. An attacker may also use this to establish a peer-to-peer network within the mobile network."

Technical analysis and identified solutions

Use case / vulnerability	McAfee NSP/ VoIPshield Solution	Possible customer / operator solution	Remarks
No session management.			
According to the paper, apart from one operator in Korea, none of the operators manages call sessions correctly. As a result of incorrect session management in SIP servers, an adversary can create multiple SIP messages to make a phone call to many people simultaneously. It should be disallowed, as more than one call session should not be established. Furthermore, this could be used to launch control plane Denial of Service attacks resulting in resource depletion: When UE-A sends an INVITE, the dedicated bearers are established both for UE-A and UE-B, even if UE-B does not respond to the call.	1) Intel Security solutions have connection and rate limiting / reconnaissance functionality that can be used in this regard.	Limit number of SIP sessions in Vendor equipment	
	2) Regarding DoS with malicious packets – McAfee NSP can detect the case when malicious packets are used. Also it would protect the target UE from bad packets if direct communication was still established or	See above.	

Use case / vulnerability	McAfee NSP/ VoIPshield Solution	Possible customer / operator solution	Remarks
	when SIP server did not filter out bad content and passed it to client.		
	3) Even though research in the article was conducted manually, some SIP generating tools can be used and our solution detects some of these.	See above.	

4. SIP Tunnelling

Exploit specifics

- The default bearer can be exploited by SIP Tunneling to send actual payload data for VoLTE. Recall that the default bearer channel is always established as long as the device is turned on. Each call party has the IP address for the default VoLTE bearer. (This manipulation is referred to in the Whitepaper as a 'Hidden Data Channel'.)

Example Use Cases and implications

1. The sender embeds actual data within the SIP messages themselves, (either in the SIP header fields, or message body, or to the end of the message) and these messages are sent through the default bearer channel. Result: **Free data usage hence loss of Operator revenue.**

Corresponding CERT Vulnerability: CWE-284: Improper Access Control

"Some networks allow two phones to directly establish a session rather than being monitored by a SIP server, thus such communication is not accounted for by the provider. This may be used to either spoof phone numbers or obtain free data usage such as for video calls."

Corresponding CERT Vulnerability: CWE-384 Session Fixation

"Some networks allow a user to attempt to establish multiple SIP sessions simultaneously rather than restricting a user to a single voice session, which may lead to denial of service attacks on the network. An attacker may also use this to establish a peer-to-peer network within the mobile network."

Technical analysis and identified solutions

Use case / vulnerability	McAfee NSP/ VoIPshield Solution	Possible customer / operator solution	Remarks
SIP tunneling.			
The payload is embedded in SIP			**Solution is unique to VoIPshield.**

Use case / vulnerability	McAfee NSP/ VoIPshield Solution	Possible customer / operator solution	Remarks
messages, and these messages are sent through the default bearer.			
1) Data payload squeezed in SIP header fields.	1) We check for length of some SIP mandatory headers (not all) - partial cover. 2) We check that certain SIP header line does not correspond to header structure e.g. not <name>:value.		**Solution is unique to VoIPshield.**
2) Data payload squeezed in SIP body attributes.	1) We check for lengths of body attributes thus reducing the amount of data that can be transferred. 2) We check that certain SIP body line does not correspond to attribute structure e.g. not <name>=value.		**Solution is unique to VoIPshield.**

5. RTP Tunnelling

Exploit specifics

- When a call session is established, a **dedicated bearer** is created and all voice packets are transferred through this channel. The protocol used by most Operators is RTP (Real-Time Protocol). Can be exploited by RTP tunneling to send data. (Referred to in the Whitepaper as a 'Hidden Data Channel'.)

Example Use Cases and implications

1. Sending data 'as is'
2. Sending data encoded as voice data
3. Generic data injections

Results:

- Free data transfer hence loss of Operator revenue
- Rogue data transfer avoids surveillance hence potential illegal activity

Corresponding CERT Vulnerability: CWE-284: Improper Access Control

"Some networks allow two phones to directly establish a session rather than being monitored by a SIP server, thus such communication is not accounted for by the provider. This may be used to either spoof phone numbers or obtain free data usage such as for video calls."

Corresponding CERT Vulnerability: CWE-384 Session Fixation

"Some networks allow a user to attempt to establish multiple SIP sessions simultaneously rather than restricting a user to a single voice session, which may lead to denial of service attacks on the network. An attacker may also use this to establish a peer-to-peer network within the mobile network."

Technical analysis and identified solutions

Use case / vulnerability	McAfee NSP/ VoIPshield Solution	Possible customer / operator solution	Remarks
RTP Tunneling.			
1) Rogue data is sent 'as is' via the RTP channel.	Possibly can be achieved by matching non-RTP packets going phone to phone. Requires some research and vendor confirmation that only RTP can go directly phone to phone via UDP, if not - make a list of other protocols and ignore those.		**Solution is unique to VoIPshield.**
2) Rogue data is encoded as a voice.	Can't be detected via IPS means, as significant resources would be needed to decode RTP into voice and then determine if that is voice. Theoretically some algorithms could make data look as voice even after decoding. Note: this requires both participants to have software that can encode-decode data into RTP. To prevent an issue on		**Requires further research.**

Use case / vulnerability	McAfee NSP/ VoIPshield Solution	Possible customer / operator solution	Remarks
	a mass scale, session limiting may help as well.		
Generic data injections	Using existing encoder detection signatures may catch some data injected into SIP that was encoded to avoid detection.		**Solution is unique to VoIPshield.**

6. Exploits at the VoLTE-enabled phone

The use cases of core network exploits lead to potential exploits at the phone:

Altering encryption

SIP messages are usually protected using IPsec tunneling with AES encryption. It has been shown possible to change the encryption from AES to null, by changing the configuration file for SIP on the phone. SIP call flows were also observed in plain text.

Access to the Phones Application Processor (AP) software

- The IPsec daemon on the phone wraps packets with a specific SIP port into the IPsec tunnel. By utilizing this daemon, SIP messages could be sent to a SIP server.
- The native SIP client on the sender phone is listening on a pre-defined port. Other apps cannot use this port. However, it seems most Carriers allow their SIP servers to accept other source ports. This offers the potential for malicious app to initiate VoLTE sessions.

Malicious Android Apps

This involves the use of these apps to send data to the internet and hence message a SIP server to call other people. The calling state not displayed hence user doesn't know the phone making calls. Hence phone DoS and possible overbilling can occur, especially if video calls are made.

Corresponding CERT Vulnerability: CWE-732: Incorrect Permission Assignment for Critical Resource

"The Android operating system does not have appropriate permissions model for current LTE networks; the CALL_PHONE permission can be overruled with only the INTERNET permission by directly sending SIP/IP packets. A call made in such a manner would not provide any feedback to the user. Continually making such calls may result in overbilling or lead to denial of service. Apple reports that iOS uses a different permission model and is not affected by this particular issue."