



UNDERSTANDING SECURITY FOR VOIP AND VOLTE SERVICES IN UNIFIED COMMUNICATION

Siddarth Kaul¹, Dr Anuj Jain²,

¹Research Scholar, ²Assistant Professor

Bhagwant University,

Rajasthan India

July 3, 2018

Abstract

This paper proposes a framework for security services for Voice over IP (VoIP) and Voice over LTE (VoLTE) in commercial networks using Unified Communication. The VoIP/VoLTE services are exposed to several security threats such as Denial- of-Service (DoS) attack, network sniffing, unauthorized services access, and VoIP spam. The conventional security services for VoIP/VoLTE suffer from the lack of flexible security rule installation and dynamic security rule update. The security service framework for VoIP/VoLTE .This paper suggests an advanced way to deal with different security threats, the framework can flexibly install new rules and dynamically update these rules. **Keywords:**

1 Introduction

Unified Communications (UC) have the potential to dramatically simplify and improve enterprise communications, reducing costs and improving revenue opportunities. However, these benefits do not come without risks. The introduction of an IP-based UC

solution brings an array of new vulnerabilities into the enterprise, exploited by a growing number of malicious programs. This paper presents the most common of risks faced by the major dominant technologies used in unified communications solutions and an approach to mitigate them.

Traditionally, the voice traffic elements of mobile telephone networks consisted of very smart core/edge network functions which were accessed by relatively simple end-user terminals (i.e. mobile phones) using a reasonably secure family of protocols designed for circuit-switched mobile networks. The mobile operators also had very tight guidelines through which they restricted the end user mobile devices that were allowed on their wireless networks. All these characteristics provided a certain degree of security for the end user, the mobile operator and the network as a whole.

1.1 Security for VOLTE in Unified Communication

However, mobile networks began to change drastically when highly programmable and powerful computing devices, such as iPhone and Android phones, were introduced. Those types of devices offered an opportunity to would-be attackers for exploring potential security gaps in the mobile operators networks. This opportunity has been exacerbated by the switch to more direct IP connectivity from the handsets to the network core, via Volte. Any attacker that can take control of a smartphone can potentially use it to launch attacks towards the operators network. Taking control over the smartphone (or terminal) can be achieved via technical vulnerabilities in the software/firmware of the terminal, but it is usually as simple as having an unsuspecting (or inexperienced) user allowing the attacker in, similarly as an unsuspecting users personal computer is infected by a virus or malware. Attackers can also build their own attack devices using commercially available components.

With this in mind, French consultancy P1 Security recently published a whitepaper of security risks in VoLTE networks. To summarize, P1 Security claim to have identified several attack vectors, and possibly security gaps, in VoLTE mobile networks, as

follows:

- Mobile terminals (such as smartphones) could be used as the source of a DDOS attack directly aimed at the mobile network. If a large number of phones can be taken over by the attacker this will form a potent form of botnet.
- An attacker could discover the phone numbers that are serviced by a particular mobile operator network and use the information for illegal purposes.
- Attackers could embed arbitrary information in SDP to cause buffer overflows. This is a special case of more general malformed packet attacks.
- Attackers could impersonate other users, if authentication procedures are not correctly implemented.
- The mobile network could be leaking fingerprinting information in messages sent to the attacker, making the topology of the core network easier to deduce, and thereby aiding the attacker with their exploration and exploitation of the network.
- The terminal equipment identity (IMEI) of a called party could be leaked by the mobile network, and the attacker could use it for nefarious purposes.¹
- Geolocation information of a callee could be leaked by the mobile network to the attacker.

P1 Security is correct that all of the above are possible attack vectors. So we thought it would be interesting to dive a little deeper into the assessment. For the most part, these are attack vectors that have already been addressed by Volte standards via the definition of the P-CSCF.² Those which are not directly addressed by standards are addressed by network-hardened mobile network functions, such as a Session Border Controller (SBC), which often houses the P-CSCF function.

Let's have a closer look at some of the attacks to focus on each in more detail:

Possible ways to attack VOLTE in Unified Communication with few scenarios.

Attack 1: DDOS attack from mobile terminals

Traditionally we think of botnets as being comprised of large numbers of compromised computers. Not only are modern smartphones pocket-sized computers, they have an always-on direct IP connection to the core telecoms network. A successful worm might compromise a large number of smartphones without the users even knowing. They can then be coordinated to launch a wide range of DDOS attacks - including carefully crafted DDOS attacks using SIP registers that require a large amount of processing to handle.

Defense 1: Hardened SBC DDOS handling

This attack highlights the need to protect the telecoms network with an SBC. These devices are designed to handle DDOS attacks aimed at telecoms networks - discarding the attack traffic efficiently, and blacklisting the devices carrying out the attack.

Attack 2: SIP INVITE phone number enumeration

An attacker who has a registered phone on a mobile network can make calls to any number, one at a time. The response message and/or response code received for each call attempt will let the attacker know whether that specific number is serviced by the operator. Once the attacker has completed the scan of all the numbers in the attack list, the attacker can move on to using the information for other purposes, such as selling it in the black market or to initiate more severe attacks.

Defense 2: INVITE rate-limiting function

An SBC should be deployed to police a sensible rate of INVITEs per endpoint. This will ensure that any brute force attempt to gather information in a sensible timeframe will trigger the SBC to identify and blacklist the compromised endpoint.

Attack 3: Embed information in SDP

The attacker can include arbitrary information in SDP without breaking protocol flows. An example attack using this mechanism

is execute a buffer overflow attack on a telecoms target by sending in a large message. And a carefully-crafted attack might ensure that the payload of the buffer overflow contains executing code that is designed to compromise the target system and gain root access!

Defense 3: Limit the size of SDP

Any attempt to execute a buffer overflow attack would involve sending in very large messages. The SBC should protect devices in the network from this attack by limiting the size of SDP to a sensible value for valid communications.

Attack 4: Source ID spoofing

The attacker can customize certain SIP header fields (From: and P-Preferred-Identity:) of a SIP INVITE request to impersonate other callers. This fake information could be received by the callee and trick them into thinking the caller is someone else - e.g. the employee of a bank asking for account details.

Defense 4: Policing by SBC

The SBC should policy the INVITE requests it receives to check their credentials. It should compare the source IP address to the information in the From: header, and it should check the URIs against those allowed by the S-CSCF at registration time. In this way the SBC will ensure the integrity of callers trying to initiate calls through it.

Attack 5: Topology leak on key SIP headers

Attackers can inspect the SIP messages they receive at the endpoint to see what information is included in the SIP headers. This information could contain details of the server types and versions of devices in the core network. The attacker could then use this information to craft attacks that exploit specific vulnerabilities of those devices.

Defense 5: SBC strips out unnecessary headers

The SBC removes non-essential SIP headers as SIP messages traverse core network boundaries. This means that information defining the topology of the network never reaches the attacker.

Attack 6: Leaking IMEI information

RFC 7255 defines the Uniform Resource Name (URN) pattern for GSMA. This guarantees uniqueness by including the IMEI of the mobile phone user in the '+sip.instance' parameter of the Contact: header. When the attacker sends an INVITE to initiate a call this information may be included in the responses sent to the attacker, which can be used to build an attack profile for the callee.

Defense 6: Dont include the information on responses

The network core shouldn't include this information on responses sent to INVITE requests. If it does, then the SBC can also be configured to strip this out as the security device at the edge of the network.

Attack 7: Geolocation information

In some IMS implementations the Cell ID of the callee is included in the P-Access-Network-Info header of responses. This Cell ID could be used by the attacker to narrow down the location of the callee to a specific cell tower.

Defense 7: SBC strips out unnecessary headers

Same as Defense 5, the SBC removes non-essential SIP headers as SIP responses traverse core network boundaries.

So in actuality, the P1 Security paper reinforces the need for a hardened SBC and CSCF to protect against attacks from within the mobile access side of the operator network. Any operator deploying a P-CSCF implementation that hasnt been designed with strong security principles in mind from the start could find themselves the victim of a wide range of attacks.

2 Security for VOIP in Unified Communication

Various strategies implemented within an IT infrastructure to protect Voice over Internet Protocol (VoIP) communication services from potential network threats. These preventative tactics offer security and added performance to a company or

VoIP provider when business-critical voice communications are transmitted over a VoIP network.

Organizations using VoIP communications need to understand that while the service is convenient and makes efficient use of under-utilized network resources, without proper security measures in place problems can arise. VoIP network security works to preserve optimal communication performance within a business's network by preventing possible threats such as viruses, Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks. When a VoIP network encounters harmful traffic, it is deprived of the vital resources and services it requires to provide efficient communications. This can result in transmissions that degrade voice quality, making it unintelligible and rendering the system useless. Fixing these problems can cost businesses both time and money. With these reasons, it is easy to see why implementing proper VoIP network security is so important. With an efficient communications security strategy in place, companies can improve VoIP functionality and drive overall business performance. Unified Communications (UC) networks have the potential to transform business Communications by connecting employees, peers and customers through a rich ecosystem Of multimedia applications and services. Driving this transformation is the ubiquity of IP-based networks and the robustness of SIP session management to control real-time Communications. Yet at the very core of widespread UC adoption is the requirement for Secure IP communications. Should UC initiatives fail this security test, enterprises will pay a

Substantial price both literally and figuratively. In order to ensure that UC systems have the requisite level of security and privacy Protection, government and industry have stepped forward with guidelines and standards That define enterprise communications in general, and IP-based enterprise communications

Specifically. Failure to adhere to these standards can cost enterprises brand equity, Customer confidence and, in many cases, hefty fines levied by industry regulations. This is Especially true for information-sensitive industries such as finance and healthcare, which Find themselves frequent targets of malicious network attacks for the purpose of profit or Other exploitation.

3 UC Introduces Security Risk

Network attacks on the data side of the enterprise network are well documented: stolen Credit card numbers, compromised passwords, exposed e-mail addresses, identify theft, Unauthorized access to confidential patient information, etc. But Voice over IP (VoIP) Networks also face risks and figure prominently in UC deployments, exposing the enterprise To a greater number of threats including ANI/caller ID spoofing, Telephony Denial of Service (TDoS) attacks and IP eavesdropping. In order to protect consumer privacy and ensure Standardized compliance on the part of enterprises, both government and industry have Created security regulations that define to what extent enterprises must protect personal Information.

Examples of Security Mandates That Affect Enterprises

Source	Goal	VoIP Security Requirements
Gramm-Leach-Bliley Act	Protect customer financial information	Encrypt VoIP calls, authenticate call center/IVR access & secure wireless communications
Health Insurance Portability and Accountability Act	Protect patient information	Secure authorized internal & external access to patient data
Sarbanes-Oxley Act	Audit public companies	Prevent unauthorized network access via VoIP channels
Federal Information Security Management Act	Ensure IT security of government agencies	Prevent/detect network intrusions via VoIP & block VoIP-carried malware
Payment Card Industry Data Security Standard	Protect cardholder information & prevent credit card fraud	Encrypt VoIP sessions, authenticate call center/IVR access, track/monitor VoIP sessions & block TDoS attacks

4 Conclusion

The various aspects of security in VOIP and security in VOLTE have been presented in the paper however more efforts are required in future with emerging technology to ensure smooth security standards.

References

- [1] <https://www.sonus.net/sites/default/files/2017-08>
- [2] <https://www.avaya.com/en/documents/securinguhealthcase.pdf?t=0>
- [3] https://www.cisco.com/c/dam/global/es_mx/assets/docs/pdf/Secure_Unified_Communications.pdf
- [4] <http://www.oracle.com/us/industries/communications/making-unified-secure-wp-1985070.pdf>
- [5] <http://www.ipcsit.com/vol2/52-B138.pdf>

