Evaluation of Security for a H.323-based VoIP Emulated Architecture

Eng. MARIUS HERCULEA, Professor VIRGIL DOBROTA Ph.D.

Abstract

Evaluation tests were conducted on H.323 Cisco Gatekeeper, Gateways and several H.323 software clients from the security point of view. The tools involved refereed to information gathering, session and signaling hacking, traffic interception, eavesdropping, session teardown and stress-testing with malformed messages. The responses were appreciated in regards to the capabilities of the targeted systems to withstand and recover after the attacks.

1 Introduction

One of the most widely used VoIP protocols is the by now consecrated H.323. It was published by ITU-T and can be seen as an umbrella recommendation of several protocols. These allow for interoperability between different vendor implementations of telephony and multimedia applications across IP-based networks. H.323 provides support for real-time audio, video and data communications.

From a security point of view, assuring a H.323 safe environment is a complex task. The multitude of associated protocols as well as the large number of vendor implementations complicates the implementation of security measures as every vendor imposes its own security features. This issue translates into a number of vulnerabilities affecting the H.323 entities [1]. Awareness of these security flaws can make the difference between deploying a safe VoIP H.323 based environment and having a vulnerable one.

2 Classification of tests and types of attacks

The first step in any attempt to test a VoIP network is to find the VoIP capable devices. This is known as information gathering. In the H.323 case it can be done rather easily using a sniffer tool to intercept RAS Gatekeeper Discovery or Register Request messages. These messages contain valuable information like IP addresses, E.164 numbers, H.323 aliases, and vendor which can clearly identify the presence and type of different H.323 elements.

Because H.323 uses for authentication MD5 hashes and timestamps, by intercepting signaling messages, an attacker can retrieve passwords using an offline brute-force attack method. Authentication is also vulnerable to replay attacks. This is done by sniffing MD5 hashes from signaling and then creating a similar message including the intercepted hash value. The message will be sent later on to the gatekeeper, falsely identifying the attacker as a legitimate user. This attack can be performed using the *nemesis* [2] packet injection tool and a modified raw packet to be sent. Other H.323 attacks rely on the fact that at the gatekeeper, by default, authentication is done by providing a valid H.323 ID or E.164 number. Thus by sniffing H.323 messages an attacker can find out a user`s alias. Then by performing a DoS on the legitimate endpoint and then submitting a message with the victim`s alias, one can receive authorization from a gatekeeper. This attack is known as alias spoofing/hopping.

Registration reject attacks can be performed on a H.323 network if an attacker can send to a registered H.323 endpoint, a registration reject packet to unregister it. If the victim tries to re-register one can simply send another registration reject packet. This attack can also be performed with the *nemesis* packet injection tool and a previously modified H.323 registration packet. Another way to do it is by intercepting signaling messages on the path between the gatekeeper and endpoints. For every request, a tool like *H225regregject* **[**3**]** can inject a dynamically created registration reject packet to the endpoint, for every terminal or gateway that tries to register to the gatekeeper. Registration messages are still forwarded to the Gatekeeper so it remains oblivious to the attack. The *H225regregject* can also inject reject packets into a call to effectively end the call setup attempt.

Sending malformed H.323 messages might result in a system crash (DoS) for the attacked H.323 element. The process in which a system is tested to see how it reacts to malformed input data is called fuzing. PROTOS [4] is such a H.323 fuzzing tool. It sends modified Setup-PDUs that carry H.225 initial signaling information. Every message has the information element variables malformed so the result is an unexpected H.323 message. Because PROTOS uses call setup messages and can be tweaked to send them to the destination at high rates, it can also be used as a flooding testing tool.

Eavesdropping involves extracting audio information from the sniffed packets. Also the RTP injection and mixing attacks [5] can be performed in the H.323 environment as well, resulting in new audio to be inserted into the conversation heard by two users. The following table illustrates a list of tools that can be used for each specific attack.

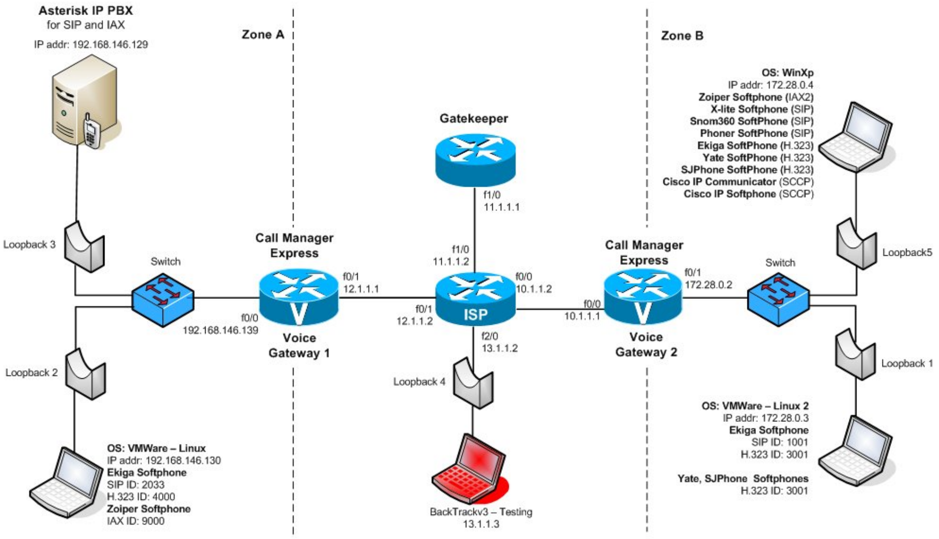
Tools available Tests/Attacks	Cain&Abel	Nemesis	Netdiscover	Nmap	PROTOS	Rtpinsertsound	Rtpmixsound	H225regreject	ettercap	Wireshark
Info, Gathering	x		x	x					x	
Authentication		x								
Eavesdroping	x									x
Register attacks		x						x		
Call setup DoS		x			x					
Session teardown		x						x		
RTP media injection						x				
RTP media mixing							x			
Fuzzing					x			x		

Table 1: List of tools associated with supported types of attacks

3 VoIP Architecture

The VoIP environment implemented functions using the following equipments: HP Laptop with Intel Core 2 Duo at 2.2GHz CPU and 2GB of RAM, Running a WinXP OS The actual environment comprises of 2 Ubuntu Virtual Machines with the Ekiga softphone version 2.0.3 installed, one Debian Linux Virtual Machine on which an Asterisk IP PBX resides, and a BackTrackv3 Virtual Machine for testing purposes. These elements are connected as in Figure.1 with two emulated Cisco 2691 Routers with Integrated Services. These Routers act as H.323 Gateways and as Call Manager Express entities. Both register to a Cisco 7206VXR Router that acts as a H.323 Gatekeeper [6].

All routers are emulated using GNS3 [7] and dynamips tools. The network interfaces of the virtual machines are linked with GNS3 via loopback interfaces in the OS of the physical laptop. These loopbacks act as bridges. The physical network interface of the Laptop is connected to the environment via its 10/100 Intel 82568t Network Card. Additionally on the Linux 2 distribution, Yate v2.0 and SJPhone v1.65 H.323 softphones are also installed. The WinXP OS runs with the following softphones: X-Lite, Snom360, Phoner (SIP), Zoiper (IAX2), Ekiga, Yate, SJPhone (H.323), Cisco IP Communicator, and Cisco SoftPhone (SCCP). This was done with future testing in mind, for evaluating the environment in which all VoIP protocols are used in a Unified Communication environment.



Router IOS images

Gatekeeper	7206VXR	IOS : c7200-js-mz.122-11.T
Gateway 1 w/ CME	2691	IOS: c2691-adventerprisek9_sna-mz.124-13b
Gateway 2 w/ CME	2691	IOS: c2691-adventerprisek9_sna-mz.124-13b
ISP	7206VXR	IOS: c7200-js-mz.122-11.T

Figure 1: Architecture used for security testing

4 Attacking the VoIP environment

4.1 Registration Attacks

Using ettercap a traffic interception was acquired on the link between the ISP and Gatekeeper. Then by using H225regregject, for every registration attempt made by the terminals and Gateways, a registration reject was sent back as if originating at the Gatekeeper.

The following H225regregject command was used, where parameter –a is given so that the registration attack can be performed for all incoming RAS register messages.

```
# python H225regreject.py -a
```

Several tests were performed to see which type of Registration Reject message is more efficient, by changing the GatekeeperRejectReason field so that if falls in one of these categories: Invalid Alias, security Denial (default), full Registration Required, Invalid Terminal Aliases, Generic Data Reason, Needed Feature Not Supported, Security Wrong Sync Time.

The FullRegistrationNeeded message was found to be most effective. Besides successfully performing the registration reject, it also creates a loop in that for every registration attempt 1000 RAS messages are created.

All softphones were affected by this attack, resulting in the inability to register while H225reject was running. The Gateways also displayed alerts of failed registration attempts but after 2 retries could eventually register.

Another registration attack was performed using the nemesis injection tool and an H.323 injection file to send a fake Register Reject message to the H.323 endpoints.

```
# nemesis –x 1719 –y 1719  –S 11.1.1.1 –D 172.25.0.3 –P iSEC.Registration.Reject
```

The following parameters were introduced: the 1719 source an destination ports specific for H.323 RAS signaling, the source 11.1.1.1 IP address of the Gatekeeper the destination IP address 172.25.0.3 of the H.323 terminal and the file to be injected. After receiving the Registration Reject message all of the tested softphones displayed the same unregistered message to the Gatekeeper alert.

4.2 Authentication spoofing and replay attack

By sniffing the network, valuable information like the IP address 172.28.0.3 and the 3001 H.323 alias of the Ekiga softphone in ZoneB were retrieved. Next the endpoint was attacked by using a DoS method or an registration reject one. Finally using a simple softphone the H.323 account was spoofed resulting in the successful registration at the Gatekeeper.

For the replay attack, a MD5 hash was retrieved from a sniffed RAS RegisterRequest message (1D4656912D7A5B8419E36C2847E4F36E). This value was inserted in another RegisterRequest message that in turn was stored in the Registration.Request.Auth file. Then by using nemesis the message was “re-submitted” to the Gatekeeper, resulting in the successful authentication. The following command was used:

```
# nemesis –x 1719 –y 1719  –S 172.28.0.3 –D 11.1.1.1 –P iSEC.Registration.Request.Auth
```

The source 172.28.0.3 address is that of the endpoint, the destination address 11.1.1.1 belongs to the Gatekeeper, and iSEC.Registration.Request.Auth is the modified register packet in a raw file form.

4.4 Fuzzing and DoS attacks

The PROTOS fuzzing tool was used on the H.323 endpoints and Cisco Gateways. First test was conducted on the Ekiga softphone with the H.323-ID of 3001, then on the Yate softphone and SJPhone at the Linux 2 Virtual PC from Zone B. The following command was issued where the host 172.28.0.3 parameter is the IP address of the h.323 endpoint:

```
# java –jar c07-h2250v4-r2.jar –host 172.28.0.3
```

Tests indicated that all the softphones crashed after 300 call initiation attempts using malformed messages. On the Ekiga softphone, any attempt to unregister or re-register during the test resulted in the inability to use the phone even after the attack stops. It`s Linux process remains “hanging” and has to be killed manually. Tests revealed that PROTOS can be used as a DoS tool.

Another series of tests were conducted on the same softphones (Ekiga, Yate, SJPhone) while running on the WinXp OS of the physical laptop, via the 10/100 Intel 82568t network interface. This was done to evaluate differences between the behavior of the softphones under test in the virtual environment and in “physical” one. Test revealed the same results as in the previous experiment.

Next, the PROTOS tool was used against the Cisco Gateways using the following commands:

```
# java –jar c07-h2250v4-r2.jar –host 10.1.1.1
# java –jar c07-h2250v4-r2.jar –host 12.1.1.1
```

As a result even if the routers displayed alert messages in the CLI, their functionality was not affected. They were able to register to the Gatekeeper or handle H.323 signaling messages.

4.5 Session Teardown with Registration Reject messages

First a call was initiated between 3001 (Zone B) and 4000 (Zone A). Then a Registration Reject packet was injected into the call towards the Zone B endpoint. The H225regregject tool was used to disconnect H.323 calls, where 172.28.0.3 is the endpoint and 11.1.1.1 is the Gatekeeper:

```
# python H225regreject.py 172.28.0.3 11.1.1.1
```

The attack successfully disconnected calls between the two communicating parties.

5 Conclusions

Test revealed that a number of security issues the existence of a Gatekeeper, which introduces a single point of failure for the architecture. Compromising the signaling at the Gatekeeper can have drastic consequences on availability and functionality of the VoIP environment.

While testing with PROTOS, results revealed the problem is also insufficient bounds checking of H.323 messages as they are parsed and processed by H.323 systems. These means that they are vendor related issues, as everyone implements the H.323 stack in it`s own way. The effect of weak designs is apparent based on the fact that all the softphones crashed as opposed to the Cisco IOS that performed well under fuzzing tests.

Future work will be done in testing and securing an environment with H.323-SIP –IAX interoperable solutions, as well as developing automated tools that make use of all the vulnerabilities and exploits found in these networks and supporting protocols.

References

[1] T. Porter, *Practical VoIP Security,* Syngress Publishing Inc., August 2008, pp. 239-263
[2] J. Nathan, *Nemesis Tool*, SourceForge, 2009. *http://nemesis.sourceforge.net/index.html*
[3] Z. Lackey, *Registration Reject DoS Tool*, iSEC Partners, 2009. *http://www.isecpartners.com*
[4] Oulu University, *PROTOS H.323Test-Suite,* PROTOS Project, 2008. *http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/h2250v4/index.html*
[5] M. Herculea, V. Dobrota, *"Evaluation of Security and Countermeasures for SIP-based VoIP Architecture", Proceedings at 7-th RoEduNet International Conference*, August 2008, pp. 30-34
[6] K. Wallace, *CCVP:Implementing Cisco Gateways and Gatekeepers*, Cisco Systems Inc., 2009
[7] J. Grossman, X. Alt, , "*Grafic Network Simulator 3*", 2009, *http http://www.gns3.net*

Biography

Herculea is in the sixth year studying at the Technical University of Cluj-Napoca, Faculty of Electronics, Telecommunications and Information Technology, specializing in Telecommunications. His interests include communication network architectures and protocols with a special emphasis on security, multimedia and unified communications. His current research focuses on VoIP Security. He is also a member of the Board of European Students of Technology (BEST) organization and Association Internationale des Etudiants en sciences Economiques et Commerciales (AIESEC), in Cluj-Napoca.

End.Dipl. MARIUS HERCULEA, M.Sc. Student
Technical University of Cluj-Napoca
Faculty of Electronics, Telecommunications and Information Technology
G. Baritiu Str., 26 – 28 No., 400027, Cluj-Napoca, ROMANIA
e-mail: marius_hm@student.utcluj.ro