International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 3, No. 01 Jan-Feb; 2021

EXPLOITING VOIP SECURITY ISSUES IN A CLASSIC SCENARIO

Enkli Ylli, Igli Tafa and Fabjola Cejku
Faculty of Information Technology, Polytechnic University of Tirana, Sheshi Nënë Tereza,Tiranë, Albania

ABSTRACT

Voice over Internet Protocol (VoIP) has become mainstream in terms of the usability due to two key factors: flexibility and low cost, all of this towards classic PSTN (Public as well Service Telephone Network) based on several studies and the practical approach because your calls are no longer routed along a dedicated wire to a local exchange, but instead provider implements packet switching and the direct line needed is now performed by the VoIP provider. However, there are several concerns over security, [13] which is quite understandable. The rising issues have naturally come over the efficiency communication VoIP offers and with this being a main key, that's where companies and businesses have invested, leaving things in the open over security. This study tries to exploit the vulnerabilities VoIP shows in its classic scenario and give a few suggestions on what to do regarding the problems raised during the way. All the work was based on previous knowledge regarding VoIP as studied in Computer Networks.

KEYWORDS: VoIP risks, security, spoofing, authentication

1. INTRODUCTION

This paper tries to explore the main threats big companies and businesses face while using the VoIP technology. Why use VoIP instead of PSTN? As mentioned above two key factors stand firm and close. When being compared to the traditional services, VoIP costs less and this is attractive to people. Offering more while costing less, a win – win situation after all. Cost saving involve using a single network for carrying data and voice, the only thing you would be paying is of course the Internet service. Secondly, VoIP is flexible. It allows you to go in any end point, log in and this means that the call will be made to your specific profile at the phone, making things mobile. Raised functionality is seen with the whole profile of working mobile, as you can work anywhere you go. As it has reached its peak of usage, VoIP needs the right attention when it comes to security. As it has been accepted by many, security is one of the main keys people worry about, due to data sensitivity. Considering VoIP popularity, this technology would become a target to intruders meaning that the protocols used need improving and new techniques must be proposed. Without a shadow of doubt, VoIP has already offered security opportunities, but with risks [11] behind as well meaning that they need to be addressed.

Mainly concerned over quality and cost in the first years, VoIP has now raised attentions over security. Firstly, in this paper we will be discussing the challenges and later deploy the characteristics that must be involved in a basic scenario that will be implemented in the experimental part. Now as it has been established so far by many researchers, when it comes to VoIP the main concepts that draw the attention are jitters, latency and of course bandwidth. While explaining the basics, these will be discussed on detail. As VoIP replaced the old and traditional telephony networks, one of the challenges that remained was unreliable quality. Regarding this pointed issue, several techniques have already been suggested helping to overcome this problem. Now while the VoIP technology has become increasingly usable, applying the much-needed security has also caused problems in the services that offers. This will be explained shortly in the next section. An understanding that what happens with VoIP, would mean better measures due to the following terms: packet switching, integrity and non-repudiation. Basically, if you have good internet connection it is possible that you may get phone service over the Internet rather than the classic local phone company. The transmission here happens over a packet switching network as the information is packetized and sent as IP (Internet Protocol) packets. So far, so good. This is where the first security breach is found, VoIP packets. These transmitted packets need protection from possible attacks. In case of sniffing, the information should not be revealed. Second, integrity easily means that packets have been transmitted without any modifications, meaning that the information has by no means been compromised. Considering the popular use of VoIP in businesses and big companies, with data being at risk of being compromised, integrity is with no doubt very important. Last, but not least, non-repudiation. All parties involved in the communication cannot deny a VoIP transmission. [25, 26,27].

What we intended in here was implementing possible threats to VoIP such as eavesdropping, telephone tampering, authentication attacks, DoS (Denial of Service), identity spoofing, information gathering, extension enumeration. By looking closely at these situations, we would be exploring possible solutions over the attacks happening as per the concrete threats showing.

2. Related Work

On a basic research that we have made on the making of this paper, there is a noticeable stance on VoIP approach and methodology searching, despite VoIP being popular or said in basic terms, mainstream. Problems on security concerns rise drastically and this is why researchers in the previous years have made several studies regarding threats on VoIP security and in the other hand even big companies have worked on potential solutions to offer better service, regarding quality as follows.

In 2017, Alouneh, Abed and Ghinea explored the possible issues that VoIP technology may encounter on low or limited bandwidth networks. [1] This study showed that added security may result in the addition of traditional VoIP problems such as delay, jitters and packet loss, as a result of high encryption standards. They propose a new core infrastructure, the MPLS.

While at the same year, [2] Jingi and Muhammad wrote about the countermeasures that must be taken in order to overcome security threats and they propose authentication, encryption of the protocol that

VoIP uses, a separation between data network and VoIP, all of this in the mitigation process.

As our approach is towards business, SPIT callers [3] are a worry, and this is why in this paper there is a proposal for detecting SPIT in a network based in internet telephony without possible interferences to the sender or receiver through a social network so it will guarantee the global reputation of the caller.

The main discussion here considers network that has been attacked in the process of implementing and integrating VoIP with IP PBX which also data tracking and voice stance. A new feature is introduced VoIP as it will improve reliability, a major problem within callers. [4]

Complying with VoIP leaves opportunities in the open for big telephone companies in the voice traffic hobbling business, but vulnerabilities as well. [5] Therefore, the thesis proposed a new framework for testing the security of interconnects between MNOs and international carriers.

So far, we have mainly focused on security, [6] but to understand this we should first understand why enterprises are switching to VoIP and then the problems that may arise due to the popular use of the technology being discussed in this paper.

In another collective study, two authors have identified previously noted threats and attacks on VoIP and discuss over possible threats in detail. While studying the basic protocols, and discussing how cheap VoIP is, the authors also discussed regarding two venders which have switched to VoIP as per the needs and standards that are set by the industry. The approach both authors follow is securing and focusing on strengthening protocols as it would result in the reduction of different level attacks plus new methods. [7]

In an article about VoIP security, Telekom discusses about facts and prejudices over the mentioned technology. At first it starts with a brief explanation that IP telephony is not always the same as Internet Telephony. The article goes further saying that critics citing security weaknesses of the Internet have something to do with the security breaches on Voice Over Internet Protocol. However, even when discussing several other issues, the author tries to explain:

Over the Top providers and telecommunication companies are based on different infrastructures when offering this service. Services offered by telecommunication companies offer VoIP via secure private network due to their infrastructure. On the other hand, over the top (OTT) providers are based on public networks making them less secure.

As explaining how Telekom offers VoIP, the article arrives into several conclusions: the VoIP service from Telekom is provided, is separated from other communication services, independent of the Internet; and based what was stated above, this means that the security problems Internet has don't affect this service. [8] This by no means secures the network and what it has been implemented are the session border controllers between the carrier network and company networks. Also, an end-to-end encryption in critical calls would be of big help.

In a recent study by Velona [9] exploring DoS attacks on VoIP, the researchers come at the conclusion that DoS attacks can be standalone or be part of a major one, while preventing a specific system on functioning correctly while it can also cause major troubles on the bigger picture as well. Malformed SIP messages are sophisticated attacks that are now being implored while there has been a rise on Incomplete Transaction. [10]

The article also explores 4G VoLTE and 5G using end to end VoIP are vulnerable [12] to attacks. These attacks would not only mean revenue loss, but also reputational damage.

3. Background Information

While exploring the related works from the section above we see that there are several techniques we should be implementing to perform a full review on the VoIP technology. Before this, we should have a basic understanding on how this technology works and on the other hand have a full menu on how to perform attacks. This is exactly what we will be doing in this section.

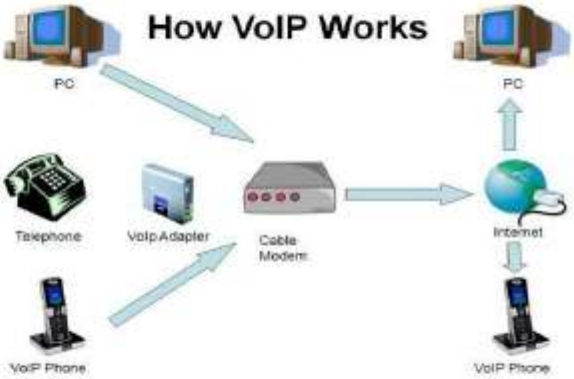


Figure 1. How VoIP works

Several definitions have been settled on what VoIP means, but what can be said is that this technology has revolutionized the telephony system. This due to the fact that with a good quality Internet connection long distance calls can easily be made. A normal service plan VoIP includes: ID, dial, waiting, call transfer, return call, repeat dial. At first, we see that there has been a replacement of circuit switching, as VoIP is a packet – switched phone network. Basically, when we discuss this technology, this opens a fast connection so it could send a message encapsulated in a packet, from the sender to the receiver. VoIP is a based IP network and as such is mainly focused on the device address. On each end of a VoIP call there are several combinations possible; analog, IP phones, soft phones acting as interfaces, while in the back we have codecs. To make a communication possible between we need to have a basic information over the protocols that VoIP uses.

First a brief discussion over the signaling protocols in which we will focus later on one of the attacks performed. The H.323 protocol is a popular protocol enterprises due to the easily integration with the previous technology that VoIP replaced, PSTN.

H.323 is a VoIP protocol and its components are: gatekeeper, gateway, MCU, BES. While we consider signaling protocols, SIP transfers basically payload in different versions of encodings.

Over the transport VoIP protocols, RTP is the most popular one as it is a simple protocol which runs above the UDP and not TCP as it doesn’t focuses on reliability, meaning that is based on “best effort” delivery. RTCP is also used, as it used for collecting data in purpose of the quality, of course in connection efficiency.

In this part of the paper we will also give a brief introduction of the attacks that will be performed in the experimental part of the study. Attackers typically target the most popular and well-publicized systems and applications. VoIP has become one of such application.

Eavesdropping. The intruder in this scenario tries to collect information through signal [19, 20] monitoring as data is being exchanged between the users. This is one of the basic steps as information is gathered to plant an attack later.

Denial of Service (DoS). As explained in one of the related works above, Denial of Service can deny the access to VoIP services. DoS [22] can be implemented differently, which are specifically for VoIP, which at the end are mainly focused on the call setup; or VoIP – agnostic that basically try to implore traffic flooding. The last one could be on physical components.

Telephone Tampering. The basic idea here is manipulation calls as they can modify the carried signal by harming the user at the other end. All of this is possible through the RTP protocol by capturing a packet and create one similar.

Authentication attacks. Despite not being a new technique as encryption has changed, we see how the old problems of password being plain text or MD5 (as it has been cracked) could make VoIP vulnerable. Prior to 2016, there were several techniques showing how AES helps in VoIP security but adds latency.

Information Gathering. Seems a bit sarcastic that this is one of the planted attacks, but before making the required steps on attacking; we see that the building process requires system information which will be important to the intruder as introduced later.
Extensions Enumeration. This is important for the SIP [23] extensions which is the basic idea of the attack in here Identity Spoofing. Identity spoofing refers to the act of assuming the identity of another as per the idea of making harm. [14]

4. Experimental Technicalities

A. The Environment
The scenario implemented is a basic VoIP scenario as shown in the figure below.

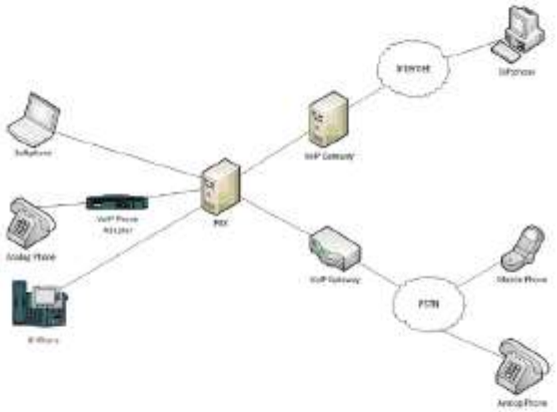


Figure 2. VoIP basic scenario

The basic idea of this VoIP is that it works as a PTN and the components in this scenario are as follows: Softphones: Zoiper and X-Lite are examples of such case; Softphone is a software that enables calls over the Internet using a computer to hardware, implemented in different. VoIP in this case is visible to the PSTN. What happens here? The intruder has a classic idea on how to perform the attack. First it is information gathering. The features being used on the devices and the intruder would like to know about the network hosts, network servers, VoIP gateways, SIP [15] clients and many more.
As we explained above SIP based VoIP protocols will be the focus and first, we need to understand the SIP [16] entities.
• User Agent (UA) – Two main agents are for client UAC and server UAS, the former is a client application that initiates requests, while the later is a server application that basically controls the first connection with the receiver after receiving a request.
• Proxy Server – It is a logical network entity, works on behalf of the client as it forwards requests or

responses.

- Registration Server – As we understand from the name, this server receives registration requests and saves address mapping.
- Redirection Server – This server responds to the received requests, with one or many addresses.
- Location Server – Provides locating services, as per the name

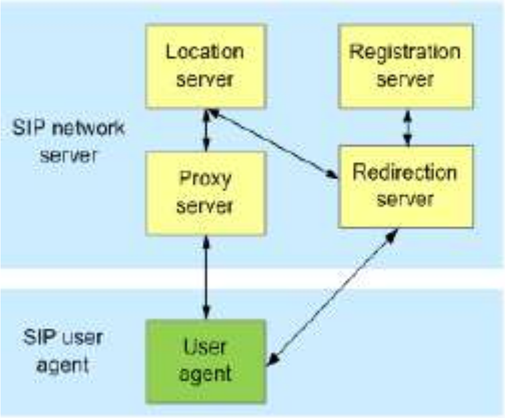


Figure 3. SIP Network Entities

To accomplish information gathering a tool has been used from the SIPVicious suite which is free for use. SVMAP is a SIP scanner.
SIPVicious is a tool which is used to evaluate SIP based VoIP systems. The tools used are:

1. Svmap
2. svwar
3. svreport
4. svcrash

We also use Wireshark which is an open – source packet analyzer.

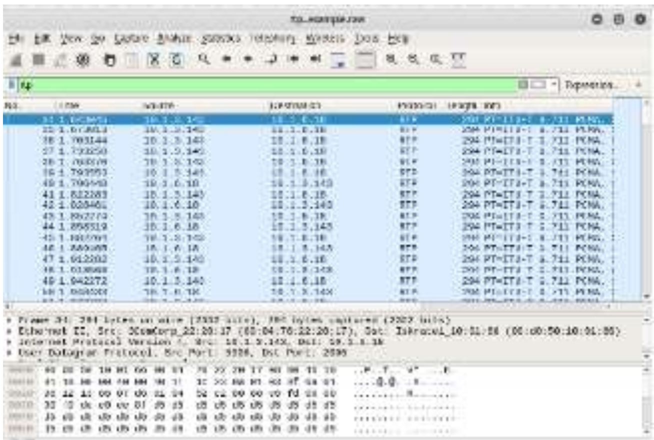


Figure 4. Example in the wireshark website

For extensions enumeration the tool used is SVNWAR.

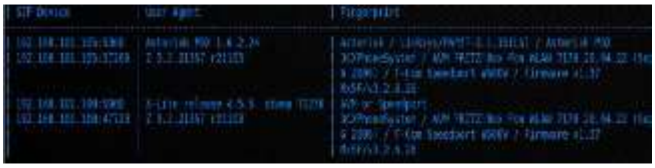
5. THE RESULTS

First, we start with the basic thing that an intruder would do,
and this is collecting information over the ‘target victim’. The basic processes that should help in network evaluation are scanning and foot printing. Foot printing is the process of data gathering for a network environment we will be considering in our study and in this case, this is done to gather information over our VoIP infrastructure. Seven basic steps are:

1. information gathering
2. determining the network range
3. identifying active machines
4. finding open ports and access points,
5. OS fingerprinting
6. fingerprinting services
7. mapping the network.

The command for network scanning:

./svmap.py 192.168.101.* -m INVITE



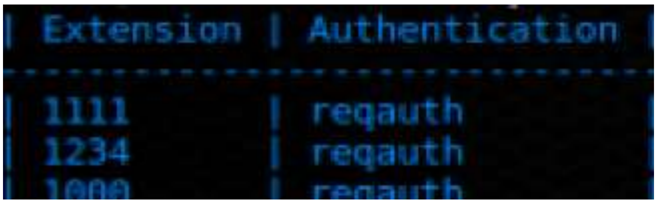
```
| SIP Device             | User Agent                  | Fingerprint
-----------------------------------------------------------------------------
| 192.168.101.125:5060   | Asterisk PBX 1.6.2.24       | Asterisk / [illegible]
| 192.168.101.125:[illegible] | [illegible]            | [illegible]
|                        |                             | [illegible]
|                        |                             | [illegible]
| 192.168.101.[illegible] | [illegible]                | [illegible]
| 192.168.101.[illegible] | [illegible]                | [illegible]
```

Figure 5. Network Scanning

As noted by the results, the scanning process has found three devices, which we know beforehand

from our scenario
explained in section A.

Extensions Enumeration. Another action being taken is Extensions Enumeration, and in the results of the command execution we see, user extensions and as explained above, the authentication of the UAC's is needed.
./svwar.py -e1000-1500 192.168.101.117



```
| Extension | Authentication |
------------------------------
| 1111      | reqauth        |
| 1234      | reqauth        |
| 1000      | reqauth
```

Figure 6. Applying Extensions Enumeration

Eavesdropping. The intruder in this scenario tries to collect information through signal monitoring as data is being exchanged between the users. This is one of the basic steps as information is gathered to plant an attack later.

Basically, the parties that are communicating have no idea over the fact that someone is secretly listening to their conversation. In that meaning we see that the packets are being somehow captured in the process.

```
0:27:a1:87:df 8:0:27:a9:4:5c 0806 42: arp reply 192.168.101.100 is-at 8:0:27:a1:87:df
0:27:a1:87:df 8:0:27:a9:4:5c 0806 42: arp reply 192.168.101.100 is-at 8:0:27:a1:87:df
0:27:a1:87:df 8:0:27:a9:4:5c 0806 42: arp reply 192.168.101.100 is-at 8:0:27:a1:87:df
0:27:a1:87:df 8:0:27:a9:4:5c 0806 42: arp reply 192.168.101.100 is-at 8:0:27:a1:87:df
0:27:a1:87:df 8:0:27:a9:4:5c 0806 42: arp reply 192.168.101.100 is-at 8:0:27:a1:87:df
0:27:a1:87:df 8:0:27:a9:4:5c 0806 42: arp reply 192.168.101.100 is-at 8:0:27:a1:87:df
```

Figure 7. Spoofing UAC with ARP Spoof

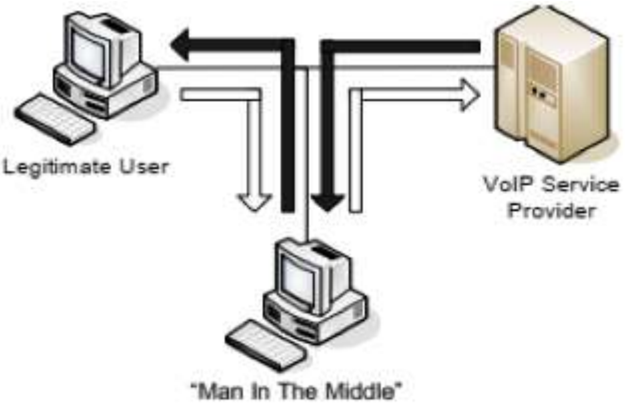


Figure 8. Implementing Man in The Middle

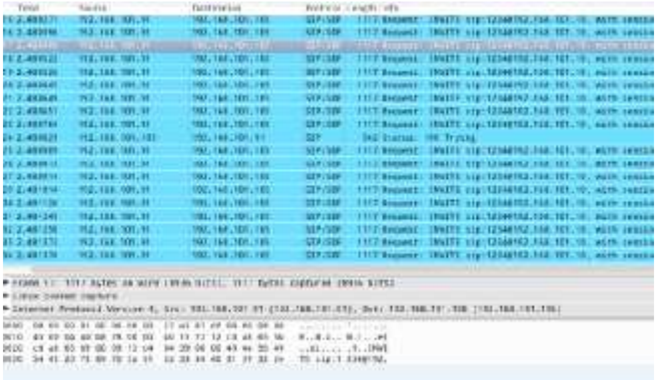
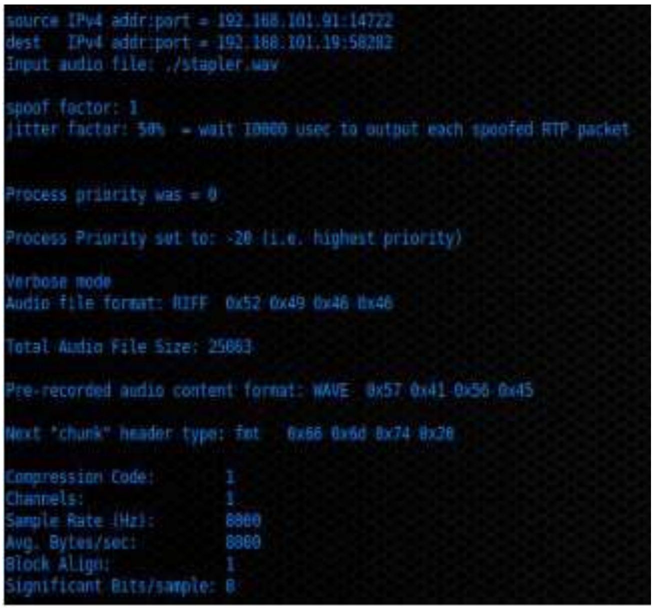


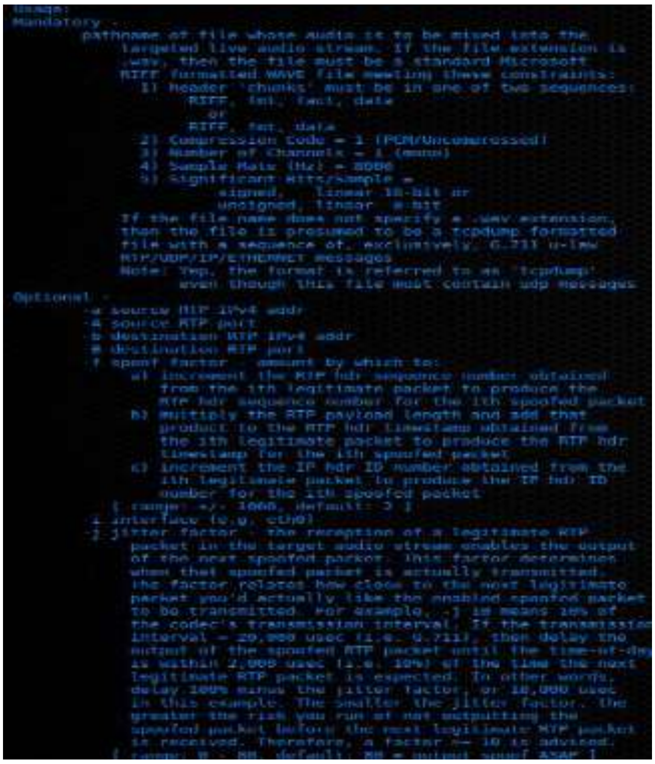
Figure 9. Call traces

Call Tampering. Call Tampering is another Man in the Middle [17] attack as explained above. Main idea is impersonation.



```
source IPv4 addr:port = 192.168.101.91:14722
dest   IPv4 addr:port = 192.168.101.19:58282
Input audio file: ./stapler.wav

spoof factor: 1
jitter factor: 50%  - wait 10000 usec to output each spoofed RTP packet


Process priority was = 0

Process Priority set to: -20 (i.e. highest priority)

Verbose mode
Audio file format: RIFF  0x52 0x49 0x46 0x46

Total Audio File Size: 25063

Pre-recorded audio content format: WAVE  0x57 0x41 0x56 0x45

Next "chunk" header type: fmt   0x66 0x6d 0x74 0x20

Compression Code:        1
Channels:                1
Sample Rate (Hz):        8000
Avg. Bytes/sec:          8000
Block Align:             1
Significant Bits/sample: 8
```

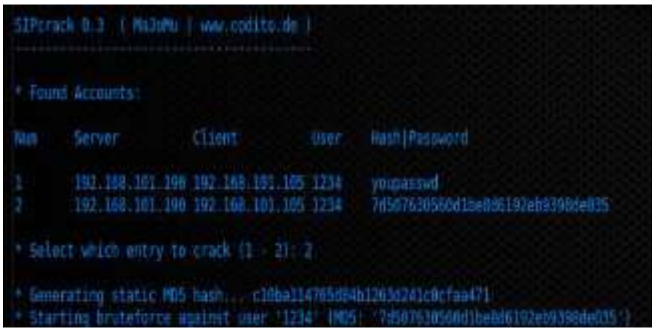
Figure 10. Call Tampering



```
Usage:
Mandatory -
        pathname of file whose audio is to be mixed into the
            targeted live audio stream. If the file extension is
            .wav, then the file must be a standard Microsoft
            RIFF formatted WAVE file meeting these constraints:
              1) header 'chunks' must be in one of two sequences:
                   RIFF, fmt, fact, data
                     or
                   RIFF, fmt, data
              2) Compression Code = 1 (PCM/Uncompressed)
              3) Number of Channels = 1 (mono)
              4) Sample Rate (Hz) = 8000
              5) Significant Bits/Sample =
                       signed,   linear 16-bit or
                       unsigned, linear  8-bit
            If the file name does not specify a .wav extension,
            then the file is presumed to be a tcpdump formatted
            file with a sequence of, exclusively, G.711 u-law
            RTP/UDP/IP/ETHERNET messages
            Note: Yep, the format is referred to as 'tcpdump'
                  even though this file must contain udp messages
Optional -
        -a source RTP IPv4 addr
        -A source RTP port
        -b destination RTP IPv4 addr
        -B destination RTP port
        -f spoof factor - amount by which to:
             a) increment the RTP hdr sequence number obtained
                from the ith legitimate packet to produce the
                RTP hdr sequence number for the ith spoofed packet
             b) multiply the RTP payload length and add that
                product to the RTP hdr timestamp obtained from
                the ith legitimate packet to produce the RTP hdr
                timestamp for the ith spoofed packet
             c) increment the IP hdr ID number obtained from the
                ith legitimate packet to produce the IP hdr ID
                number for the ith spoofed packet
           [ range: +/- 1000, default: 2 ]
        -i interface (e.g. eth0)
        -j jitter factor - the reception of a legitimate RTP
             packet in the target audio stream enables the output
             of the next spoofed packet. This factor determines
             when that spoofed packet is actually transmitted.
             The factor relates how close to the next legitimate
             packet you'd actually like the enabled spoofed packet
             to be transmitted. For example, -j 10 means 10% of
             the codec's transmission interval. If the transmission
             interval = 20,000 usec (i.e. G.711), then delay the
             output of the spoofed RTP packet until the time-of-day
             is within 2,000 usec (i.e. 10%) of the time the next
             legitimate RTP packet is expected. In other words,
             delay 100% minus the jitter factor, or 18,000 usec
             in this example. The smaller the jitter factor, the
             greater the risk you run of not outputting the
             spoofed packet before the next legitimate RTP packet
             is received. Therefore, a factor >= 10 is advised.
           [ range: 0 - 80, default: 80 = output spoof ASAP ]
```

Figure 11. Sound help command

Authentication. What happens if password is plain – text or we use MD5? Plain – text password should not be a thing anymore? Why? Because they are easily to be discovered. MD5 goes over the same way as MD5 has already been cracked. Mostly, we need something else to proceed, but let's see what happens at first.



```
SIPcrack 0.3  ( MaJoMu | www.codito.de )
----------------------------------------

* Found Accounts:

Num     Server          Client          User    Hash|Password

1       192.168.101.198 192.168.101.105 1234    youpasswd
2       192.168.101.198 192.168.101.105 1234    7d507630560d1be886192eb9398de035

* Select which entry to crack (1 - 2): 2

* Generating static MD5 hash... c10ba114765d84b1263d241c0cfaa471
* Starting bruteforce against user '1234' (MD5: '7d507630560d1be886192eb9398de035')
```

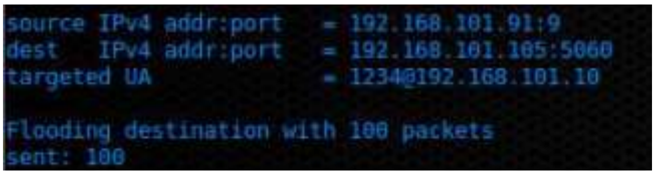
Figure 11. Sipcrack cracking passwords

DoS – There are a few basic types:

a. Flood Dos

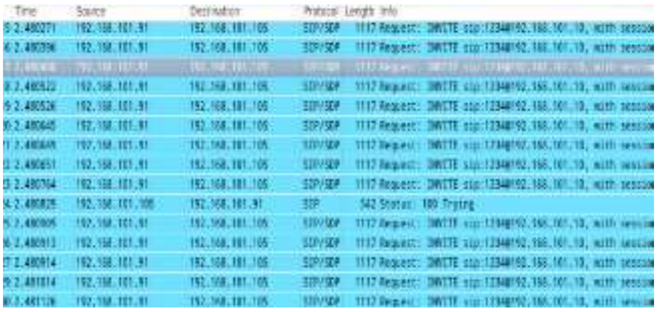
b. Flaw Dos

c. Platform Dos
d. Application – level Dos



```
source IPv4 addr:port    = 192.168.101.91:9
dest   IPv4 addr:port    = 192.168.101.105:5060
targeted UA              = 1234@192.168.101.10

Flooding destination with 100 packets
sent: 100
```

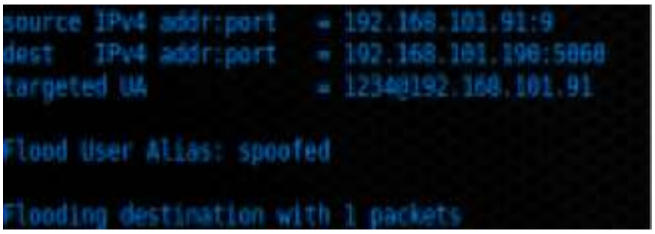
Figure 12. Flood DoS



```
Time        Source           Destination      Protocol Length Info
2.480271    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.480396    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
[illegible]
2.480522    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.480526    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.480645    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.480649    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.480651    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.480764    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.480825    192.168.101.105  192.168.101.91   SIP       542 Status: 100 Trying
2.480905    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.480913    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.480914    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.481014    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
2.481126    192.168.101.91   192.168.101.105  SIP/SDP  1117 Request: INVITE sip:1234@192.168.101.10, with sessio
```

Figure 13. Packet Registration

Spoofing Caller ID



```
source IPv4 addr:port    = 192.168.101.91:9
dest   IPv4 addr:port    = 192.168.101.190:5060
targeted UA              = 1234@192.168.101.91

Flood User Alias: spoofed

Flooding destination with 1 packets
```

Figure 14. Spoof Caller

6. INTERPRETING THE RESULTS

All the issues we presented above need addressing and the elephant in the room is security. We see that when dealing with foot – printing and scanning the network, several ideas come to mind. Based on research, there a few things we canhelp the network. You cannot stop the SIP messages from coming, but obviously setting up a firewall in the User Agent Server by ACL’s. With Access Control Lists the UAS can now only accept requests from reliable IP addresses.

Eavesdropping can be prevented by following a few basic things that may seem easy:

a. The system administrator must change the default configurations
b. Monitor advisories
c. Update session control borders
d. Encrypting VoIP calls, however as it was explored in a previous study, it adds jitters and delays

Telephone Tampering is a big issue as both the caller and the callee consider one another as trusted parties and in the cases where the attacker captures an RTP packet, this means it can duplicate the original packet and have the other user where he wants, meaning that he is being tricked.

Voice encryption can be helpful at the case, as this the best chance that the administrator must make a move in this case. Telephone Tampering is serious, so AES encryption is a must. The drawbacks in such case probably won't be a big of a deal anyway.

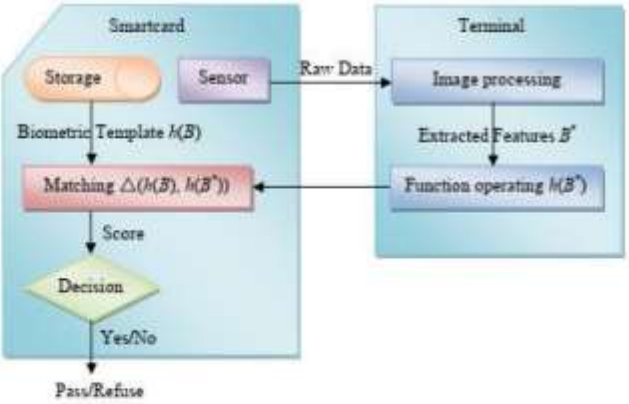


Figure 15. Procedure on biometric data

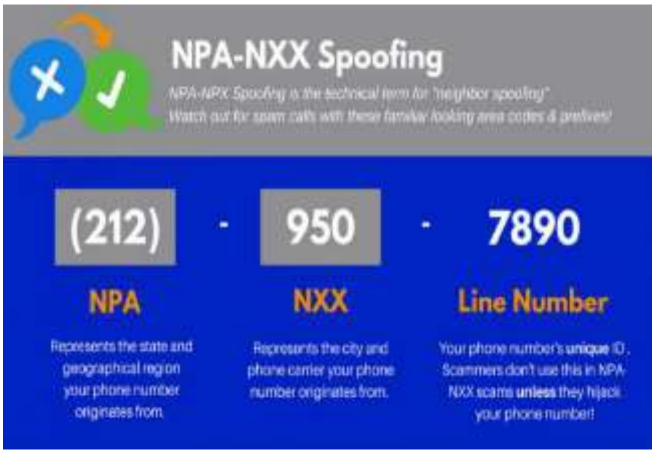

NPA-NXX Spoofing
NPA-NPX Spoofing is the technical term for "neighbor spoofing"
Watch out for spam calls with these familiar looking area codes & prefixes!
(212)
-
950
-
7890
NPA
NXX
Line Number
Represents the state and geographical region your phone number originates from.
Represents the city and phone carrier your phone number originates from.
Your phone number's unique ID. Scammers don't use this in NPA-NXX scams unless they hijack your phone number!

Figure 16. Caller Spoofing

Caller Spoofing is illegal as of 2009 and the only effective countermeasure that can be of help here is authentication of the sender party, using the header.

Figure 17. Unknown Caller

When using PKI with UAC and UAS, the client authentication can easily be made, by not every proxy may support the Public Key Infrastructures meaning that at this point, the call is not trusted.

7. Conclusions and Future Works

When dealing with VoIP we should hold into account the popular use of the technology into the enterprises and big companies. While discussing the conclusions of the paper, we view security as a big and important issue in today's world. In the end, the discussion is about money and money loss, but especially integrity is at stake when it comes to enterprises. Secure communication is important and when it comes to data sensitivity, the most affected are those who have data exchange and transmission a key factor to their work.

Therefore, we give a revision of what can be done after all:
1. Review Call Records Details: Call details allow identification of a normal activity. Reviewing the said details monthly shows the typical registrations and therefore identifies unusual traffic, call destinations, lengths etc.
2. Secure Credentials: Third parties must not be aware of the user credentials and it is indeed helpful to regenerate them in case an attack happens.
3. Establish password protocols: Best practices show that password change in 3 - 6 months help.

4. Restrict call forward options: Despite being a VoIP feature, frauds can easily cause issues through forwarding.
5. Review Security Protocols: Problems must be identified in both software and hardware
Those opinions are business wise as educating employees, but as a network administrator there are several techniques that might be helpful:

1. Port Authentication: It uses the standard 802.1.x to confirm access between user and authority. In here, the intruder must authenticate himself first with the authority to be given access, but this is very secure.
2. Categorization of traffic: Dividing both voice and data means that the probability for the attack will be divided and this means less damage overall.
3. Authenticating the signaling: [18] Maintenance of the link using the SIP protocol, as we would basically, the phone registered would show its identity in this case.

8. REFERENCES

[1] Alouneh, Sahel & Abed, Sa'Ed & Ghinea, Gheorghita. (2017). Security of VoIP traffic over low or limited bandwidth networks. Security and Communication Networks. 9. 10.1002/sec.1719.
[2] Jingi & Muhammad. (2017). VoIP Security: Common Attacks and their Countermeasures. International Journal of Computer Science and Information Security (IJCSIS),
Vol. 15, No.3, March 2017
[3] Azad, Muhammad & Morla, Ricardo & Arshad, Junaid & Salah, Khaled. (2016). Clustering VoIP caller for SPIT identification. Security and Communication Networks. 9. 10.1002/sec.1656.
[4] Fayyaz, Yasir & KHAN, Dost & FAYYAZ, Faisal & Qadri, Salman & Naweed, M. & Fahad, Muhammad. (2016).
The Evaluation of Voice-over Internet Protocol (VoIP) by means of Trixbox. International Journal of
Natural and Engineering Sciences. 10. 33-41.
[5] Naguib, Mina M.. “On the security of VoIP mobile network operator and international carrier interconnects.” (2016).
[6] Shaw, Urjashee & Sharma, Bobby. (2016). A Survey Paper on Voice over Internet Protocol (VOIP). International Journal of Computer Applications. 139. 16-
22. 10.5120/ijca2016909112.
[7] Hasan & Hussain, (2017). Collective Study On Security Threats In VOIP. International Journal of Scientific & Technology Research Volume 6, Issue 01, January 2017
[8] Telekom article on VoIP Security: Facts instead of prejudices (2017)
[9] Friar, (2018). Denial of Services attacks against VoIP systems, A white paper from Velona Systems.
[10] A. D. Keromytis, “Voice over IP: Risks, Threats and

Vulnerabilities," in Proceedings of the Cyber Infrastructure Protection (CIP) Conference, June 2009.

[11] R. Dantu and P. Kolan, "Detecting Spam in VoIP Networks," in Proceedings of the USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI), pp. 31–37, July 2005

[12] G. Zhang and S. Fischer-Hubner, "Peer-to-Peer VoIP Communications Using Anonymisation Overlay Networks," in Proceedings of the 11th Conference on Communications and Multimedia Security (CMS), May/June 2010

[13] Y. Rebahi, D. Sisalem, and T. Magedanz, "SIP Spam Detection," in Proceedings of the International Conference on Digital Telecommunications (ICDT), pp.
29–31, August 2006

[14] Y. Rebahi and D. Sisalem, "SIP Service Providers and the Spam Problem," in Proceedings of the 2nd VoIP Security Workshop, June 2005

[15] M. Petraschek, T. Hoeher, O. Jung, H. Hlavacs, and W.N. Gansterer, "Security and Usability Aspects of Manin-the-Middle Attacks on ZRTP," Journal of Universal Computer Science, vol. 14, no. 5, pp. 673–692, 2008

[16] Jayaprakash, M., Tamilarasi, A. & Gopikrishnan, S.(2012) 'QoS management in VoIP security using stream cipher', European Journal of Scientific Research, 87 (1), pp.127-136

[17] A. Fessi, N. Evans, H. Niedermayer, and R. Holz, "Pr2-P2PSIP: Privacy Preserving P2P Signaling for VoIP and IM," in Proceedings of the 4th Annual ACM
Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM), pp. 141–152, August 2010

[18] A. D. Keromytis, "A Look at VoIP Vulnerabilities," USENIX; login: Magazine, vol. 35, pp. 41–50, February 2010

[19] J. Larson, T. Dawson, M. Evans, and J. C. Straley, "Defending VoIP Networks from Distributed DoS (DDoS) Attacks," in Proceedings of the IEEE Global
Telecommunications Conference (GLOBECOM), November/December 2004

[20] J. Fiedler, T. Kupka, S. Ehlert, T. Magedanz, and D. Sisalem, "VoIP Defender: Highly Scalable SIP-based Security Architecture," in Proceedings of the 1st
International Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm), pp. 11–17, July 2007

[21] A. Talevski, E. Chang, and T. Dillon, "Secure Mobile VoIP," in Proceedings of the International Conference on Convergence Information Technology, pp. 2108– 2113, November 2007

[22] N. Aschenbruck, M. Frank, P. Martini, J. Tolle, R. Legat, and H.-D. Richmann, "Present and Future Challenges Concerning DoS-attacks against PSAPs in
VoIP Networks," in Proceedings of the 4th IEEE International Workshop on Information Assurance (IWIA), pp. 103– 108, April 2006.

[23] S. Vuong and Y. Bai, "A Survey of VoIP Intrusions and Intrusion Detection Systems," in Proceedings of the 6th International Conference on Advanced Communication Technology

(ICACT), pp. 317–322, February 2004

[24] Pérez-Botero, D. & Donoso, Y. (2011) "VoIP eavesdropping: A comprehensive evaluation of cryptographic countermeasures", Networking and Distributed Computing (ICNDC), 2011 Second International Conference on, IEEE. p192-196

[25] A. D. Elbayoumy and S. Shepherd, “A High GradeSecure VoIP System Using an Endpoint CPU
Capability Detector,” in Proceedings of the ITA05 International Conference on Internet Technologies and Applications, pp. 173–180, September 2005

[26] A. D. Keromytis, “Voice over IP Security: Research and Practice,”IEEE Security & Privacy Magazine, vol. 8, pp. 76–78,March/April 2010