Analysis of a PBX Toll Fraud Honeypot

N. McInnes, E.J. Zaluska, G. Wills
School of Electronics and Computer Science
Faculty of Engineering and Physical Sciences
University of Southampton
United Kingdom

Abstract

Organisations are moving over from legacy telecommunications to Voice over IP (VoIP), enabling greater flexibility, resilience and an overall cost reduction. Session Initiated Protocol (SIP) is considered to be the main VoIP protocol in the business-to-business market, but the correct implementation and configuration is not always well-understood. The failure to configure SIP systems correctly has led to significant fraud exploiting a range of vulnerabilities and billions of dollars every year being stolen from companies of all sizes through PBX Hacking via the medium of Toll Fraud. Previous research into this area is now dated but suggested fast-changing approaches by attackers. Industry organisations such as the Communications Fraud Control Association (CFCA) acknowledged this is a fast-growing problem. To quantify the size of the current problem, a Honeypot experiment was undertaken using a popular phone system used by businesses. The Honeypot ran for 10 days and recorded just under 19 million SIP messages. This research has identified attackers are using various sophisticated methods to attempt to gain access and trick a PBX into making calls. When comparing previous research, the rate of attack is approximately 30 times more aggressive and the countries from where attacks originate are distributed over 75 countries.

1. Introduction

Voice over Internet Protocol (VoIP) is a group of protocols that enables voice communication over an IP network.

Current telephone networks are in the process of moving from a closed legacy approach in network design (traditionally copper cable infrastructure using Signalling System No. 7 (SS7) technologies) to an open approach based on other mediums (for instance IP). This transition enables telephone costs to be significantly reduced, it also enables users of such systems greater flexibility over their communications eco system.

However, as the market for VoIP paid calls grows, it also increases the possibility of misuse and fraud. Billions of dollars a year is being lost through various activities such as toll fraud, where calls are made to phone numbers (through a hacked component) where the calling party receives revenue from such calls at the expense of the victim – completely unknown and undetected until they receive their telephone bill [1].

Annual fraud figures published by the Communications Fraud Control Association (CFCA) suggest that around $38 billion are lost to fraud [2] and PBX hacking itself has increased by over 60% resulting in losses of over $7 billion in 2015 [3]. This crime is now becoming such a concern, national bodies such as the City of London Police through its subsidiary ‘Action Fraud’ are specifically now collecting details about this kind of crime [4].

Previous research using VoIP Honeynets to assess the impact of attackers is now over 5 years old. One of the results of these early studies was that the attackers changed their behaviour over time [5]. This article provides a comparison and discusses the methodology and results of a Honeypot experiment that ran for just 10 days to provide an up-to-date view on the attack methods currently being used by attackers.

2. Background Literature

Ahmed et al. states many consumer-based services are value-added and peer-to-peer in nature, often using their own proprietary protocols [6] (Skype, Viber and WhatsApp are examples). In these cases, protocols are closed, custom built and have dedicated mobile phone applications.

In comparison, business services typically focus on interoperability, because most businesses want to use existing equipment, which requires the use of a common protocol. As suggested by Abdelnur et al, SIP is the-IETF recommended protocol for VoIP. [7].
2.1. SIP

SIP is the industry recommended VoIP Protocol for interconnectivity and an open standard (IETF RFC 3261) [8]. This has enabled a number of manufactures, namely Cisco, Avaya, Yealink and software vendors such as Asterisk, Sangoma, Freeswitch to build products and platforms that work together.

SIP works by separating a phone call into signalling and media elements [9]. The signalling, which carries messages containing the initial call message to begin a session (called an ‘Invite’) includes the initial call details such as destination number, origination number and other parameters such as privacy information and audio codec to be used. This is usually on User Diagram Protocol (UDP) port 5060 [8]. The audio channels are set up on 2 random UDP ports (for example in the case of Asterisk these ports are between 10,000-20,000 for bi-directional audio).

SIP uses Uniform Resource Identifiers (URI) adopting the following format: SIP/Extension@IP [10]. This approach is similar to other web protocols, for instance a web URL or File Transfer Protocol (FTP) address.

SIP is regularly used in one of 2 modes depending on the context it is to be used within: IP Authentication or Registration (to be able to identify a user). IP Authentication is regularly used for SIP trunking (equivalent to a trunk line) between a provider’s switch and a customer’s Private Branch Exchange (PBX), where registration is most often used to register a handset to a PBX.

IP authentication requires a PBX to have a dedicated public IP where the PBX is public facing. For the scope of this article, it is usually at this interface that attacks from the Internet will occur.

2.2. Private Branch Exchange (PBX)

A PBX is a phone system that is usually located inside a business’s office and has desk phones connected to it. PBXs originally had complex command line interfaces, however as web technologies have improved more PBXs have entered the market with easy-to-use Graphical User Interfaces (GUI).

User devices can regularly change IP, therefore a device needs to periodically register with a SIP server. This can be to a PBX to reconfirm where to send Invites (for receiving or making a call) [11]. Registration is performed by username and password authentication and is used between a PBX and a device (e.g. handset), although both types can be used in other use cases (i.e. a trunk can also be username/password based). Fig. 1 shows a normal use case of how the SIP protocol is used in business communications.

Figure 1. Normal Business SIP Use Case

Many workers work remotely (home workers). This requires a firewall to accept incoming traffic from the general internet. This introduces new sets of challenges that PBX owners need to consider. To achieve this use case, a PBX generally requires a dedicated public IP.

A PBX having a dedicated IP allows a business not only to be able to connect to their provider using IP Authentication, but supports working patterns that are becoming more popular in a changing society. For instance, teleworking which can involve working from home or on the go. However, due to the nature and impracticality and shortage of IPv4 addresses, not many mobile devices or consumer broadband services (which a VoIP phone would connect to) have a dedicated IP. This presents a challenge to businesses of how to limit access to the PBX through a firewall.

2.3. VoIP Vulnerabilities and Types of Attacks

Many potent VoIP vulnerabilities have been identified. Rebahi et al. studied more than 220 different vulnerabilities [12]. Proprietorial software, services and open source all appear to have their own vulnerabilities.

Skype users have reported account breaches via a login vulnerability (weak credentials) or SIP not encrypting signalling or media.

In contrast, Sengar suggests that most SIP vulnerabilities are not due to the weaknesses in the protocol itself, but result from poor SIP credentials and misconfigured systems [13]. Other researchers such as Hoffstadt et al. [14] and Gruber et al. [15] support this assessment.

2.4. PBX Penetration Studies

Hoffstadt et al. [14] from the University of Duisburg, Essen, Germany have become leading researchers in VoIP Attacks for fraudulent purposes. Their paper presented at the IEEE 2012 Conference on Trust, Security and Privacy in Computing and Communications began with them building a Honeynet (a collection of Honeypots) setup as an Intrusion Detection System (IDS), located in Germany and the USA.

This Honeynet collected over 47.5 million messages over approximately a 2-year period. Hoffstadt et al. used a novel method to collect not only messages contacting their systems, but also the entire subnet (monitoring the Level 3 Switch). On building
the Honeynet, Hoffstadt et al. analysed previous work and established low level interaction Honeypots have weaknesses by not being able to provide full overview and only enable basic "fingerprinting". Hoffstadt et al. identified that considerable amounts of data will be available and could use Packet Capture (PCAP) and UDP Sockets for SIP Traffic analysis. They did this by building 2 networks, one with SIP components, the other without.

Hoffstadt et al. [14] discovered that to determine if a device is SIP enabled, attackers would send out Option messages to probe whether a device is SIP enabled or not (where the device would reply if it was). An Option is a message sent out to a SIP server which replies with a list of features it supports. This led Hoffstadt et al. categorising an attack into 4 stages [14]:

1. Initial SIP Server Scan – Scan IP with Option messages looking for replies
2. Extension Scan – Scan for extensions looking at differences in error messages (404 not found, 403 Forbidden, 401 Unauthorised)
3. Extension Hijacking – Using dictionary attacks on extensions
4. Toll Fraud – Making successful calls.

In Essen’s analysis of the signalling details, Hoffstadt et al. noted that tools such as SIPVicious were being used to automate an attack. This confirms claim by Ronniger et al. that there are tools available to attack VoIP Infrastructures [16].

Hoffstadt et al. established that once a non-SIP component was open to the public internet, it appeared to be continually under Option attacks [14].

In contrast, when a SIP component replied, little to no Options were further received, but attackers moved onto stage 2. Stage 3 of the attack used typically 10,000 various usernames with different password combinations (over 55,000 attempts) which took a little over a minute to complete. On successfully registering, it was observed that after some time, Toll Fraud began (stage 4) where various prefixes (numbers) were used to dial out (i.e. 011 for an international line the US and 00 for an international line in Germany) [14].

Although most attacks were automated when scanning and brute forcing, the author discovered that stage 4 would happen several months after successfully registering with an extension [14]. The victim may have difficulties in researching the hack as evidence may already have been destroyed by natural log cycles in order to save storage space.

In further papers [17], Hoffstadt et al. extend their work to introduce logic. This allowed them to dynamically create extensions where that extension was being probed by giving the impression the extension is valid.

Furthermore, a system was introduced to answer calls for random periods to simulate a call. This enabled Hoffstadt et al. to follow attackers from stage 1, where multiple IP addresses may be involved [17]. Later on, Hoffstadt et al. created a Generic Attack Replay Tool (GART) allowing the replaying of attacks by capturing key information to assist in building tools that can detect and prevent attacks at a later date [18].

Repeated studies found that once an attacker has gained access, they attempt to call premium-rate numbers or high-cost numbers in various countries, suggesting attackers earn money for doing so [14,15]. Gambia, Palestinian territories and Somalia appear to be regularly attempted. Gruber et al. goes further suggesting that most calls go to African countries [5].

Since 2011, researchers at Vienna University of Technology have also been running a Honeynet. Their findings coincide with Essen’s in that many calls were to African countries (Ethiopia and Egypt) and when attempts are made, most of the time the attempt is made from an Egyptian IP address [15].

Researchers at the University of Duisburg partnered with Researchers at the Network Systems Group to develop novel methods for implementing and improving monitoring nodes around distributed Honeynets with monitoring points in China, Norway and Germany. This reconfirmed their initial conclusions that attackers scan large segments of the internet. Moreover, they determined not all attackers were involved in the different stages of attacks, concluding that attackers share information about potential victims with other attackers [19].

### 3. Methodology

Researchers at Essen and Vienna, both developed Honeynets (the collection of Honeypots) to monitor SIP messaging at different geographical locations. These studies did not facilitate the use of a PBX, but only certain software engines used by PBX software.

At the SIP Signalling level, messages can contain metadata regarding the software configurations and versions to replies in Invites, Options and Registration requests. This requires a high interactive Honeypot.

To meet the requirements of having a high interactive VoIP engine, the decision was taken to use a popular open source PBX software package known as FreePBX.

FreePBX is a feature rich platform, which claims over 1 million installs. This means that if hackers are actively seeking out VoIP Systems to attack, then this would be a good candidate because of its wide installation base.

As FreePBX is lightweight in nature, a Virtual Machine is sufficient to run the Honeypot which is located in the United Kingdom. In this experiment, the Honeypot would reply with the Server type as FPBX-VERSION where VERSION is the version of...
FreePBX being used in the SIP Messaging. FreePBX is built on top of the Open Source Asterisk Engine.

3.1. PBX Configuration

For ease of setup, monitoring and collecting data, it is important that the PBX is setup in a way which maximises opportunities to collect and study how a PBX hack attempt has occurred while minimising and reducing risk.

The overall goal is to study a hack attempt, not to allow the system itself to get infected by malware or similar. Certain flows will be allowed to allow toll fraud, but overall the system is to be locked down and no actual calls can be made as it is not connected to a phone provider.

The PBX is installed via the ISO disk image provided by FreePBX which allows a straightforward installation. The ISO is built on the Linux Centos 7 Operating System.

FreePBX comes with several built-in security features such as Fail2ban which will block an IP for a period of time if the incorrect credentials are provided. However, for the purpose of this experiment to assist in obtaining a full understanding of the scale of the current problem, Fail2ban was disabled. (Leaving Fail2ban enabled could limit the number of attacks on the PBX.)

To secure all ports, the Virtual Machine (VM) provider provides a free virtual firewall which provides the ability to block all connections except a select few TCP and UDP ports.

For the purpose of this experiment the following ports were opened and monitored:

- TCP: 5060-5070
- UDP: 5060-5070, 10,000-20,000

As shown by Hoffstadt et al. [14] and Gruber et al. [15], attackers would scan extensions looking at the replies to determine if an extension exists. Therefore, to trigger different responses, various extensions have been created to provide an illusion of a live production system (reinforcing metadata replies to SIP requests). These extensions can be seen in Table 1.

To record SIP interactions on the PBX, different methods could be used. SIP interactions could be recorded in the Asterisk log or via a Packet Analysis. Packet Analysis is preferred over the Asterisk Log as it allows for detailed inspection of all events that occur over the network interface of the system which may not be recorded via the Asterisk Log.

Using a utility such as Wireshark, knowledge was gained to determine whether previous findings in previous studies are still valid and what new techniques are being used. Wireshark also contains tools that were used for summarising certain types of SIP events using tools such as SIP statistics that is part of Wireshark. For these reasons, Wireshark was used.

### TABLE 1. SAMPLE EXTENSIONS CREATED ON HONEYPOT

<table>
<thead>
<tr>
<th>Username (Extension)</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>fdfAS243%32</td>
</tr>
<tr>
<td>1002</td>
<td>1002</td>
</tr>
<tr>
<td>1003</td>
<td>1003</td>
</tr>
<tr>
<td>1125486</td>
<td>Dfgg35DGS24g</td>
</tr>
<tr>
<td>10000</td>
<td>10000</td>
</tr>
<tr>
<td>50000</td>
<td>50000</td>
</tr>
<tr>
<td>100000</td>
<td>100000</td>
</tr>
<tr>
<td>5001</td>
<td>5001</td>
</tr>
<tr>
<td>5003</td>
<td>dfdfSDG3435s</td>
</tr>
</tbody>
</table>

In addition to the above, using the Virtual Machine Provider’s Tools, Bandwidth Data and Machine Resources will be monitored to see what impact if any an attack has on the VM.

The specification of the Virtual Machine was 1 x 2.4Ghz Intel virtual core with 1024gb of RAM and SSD storage.

4. Results

The data analysed was collected over a 10-day period (24rd September 00:00 BST – 3rd October 23:59 BST 2018). During this period, just under 19 million SIP messages were received from malicious actors. These were split into the following SIP Message Types as seen in Table 2. For the purpose of this experiment, Register, Invite and Option has the meaning set out by IETF RFC 3261 [8]. For instance:

- Register allows the PBX to know where the device connecting to it is.
- Invite contains parameters on a call and Invites a device to begin a session.
- Option allows a device to understand the capability of another device.

The IP of the Honeypot was not publicly advertised and real devices were not connected to the SIP system. Therefore, it can be presumed that all inward SIP traffic was malicious.

During the period the Honeypot ran, less than 0.02% of all registration attempts successfully registered where the only successful registrations was when the password was the same as the extension. When analysing packet data to investigate credential combinations, some attempts were with the same credential combination. The attack on the 3rd October were all with the same credential combination.
### TABLE 2. DAILY BREAKDOWN OF SIP MESSAGE TYPES RECEIVED

<table>
<thead>
<tr>
<th>Date</th>
<th>Register</th>
<th>Invite</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/09/2018</td>
<td>1,494,872</td>
<td>1,488</td>
<td>78</td>
</tr>
<tr>
<td>25/09/2018</td>
<td>45,247</td>
<td>1,667</td>
<td>91</td>
</tr>
<tr>
<td>26/09/2018</td>
<td>2,014</td>
<td>2,266</td>
<td>84</td>
</tr>
<tr>
<td>27/09/2018</td>
<td>478,208</td>
<td>1,153</td>
<td>66</td>
</tr>
<tr>
<td>28/09/2018</td>
<td>12,037</td>
<td>1,636</td>
<td>121</td>
</tr>
<tr>
<td>29/09/2018</td>
<td>3,030,372</td>
<td>1,667</td>
<td>114</td>
</tr>
<tr>
<td>30/09/2018</td>
<td>2,770,527</td>
<td>2,774</td>
<td>91</td>
</tr>
<tr>
<td>01/10/2018</td>
<td>1,914,163</td>
<td>315</td>
<td>34</td>
</tr>
<tr>
<td>02/10/2018</td>
<td>1,921,432</td>
<td>34,778</td>
<td>102</td>
</tr>
<tr>
<td>03/10/2018</td>
<td>7,204,257</td>
<td>10,471</td>
<td>95</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>18,873,129</td>
<td>58,215</td>
<td>876</td>
</tr>
</tbody>
</table>

### 4.1. System Resources

During the 10-day period the Honeypot ran, approximately 20GB of SIP traffic was recorded which averaged 2GB per day due to inward SIP Messages.

The highest average bandwidth utilisation recorded by the Virtual Machine provider was 600Kbps. The highest average CPU utilisation recorded by the Virtual Machine was 30% and the average SIP dictionary registration attack was for 12 hours (excluding 3rd October). During these times the above average results of bandwidth and CPU utilisation were observed during the period. Fig. 2 shows an IO graph exported from the Wireshark tool which demonstrates the intensity of packets per second.

![Figure 2. Data IO Graph 24/9/2018](image)

### 4.2. Attack Origination

The PBX was attacked from multiple sources. Our experiment observed IP subnets from over 75 destinations across 886 subnets. Fig. 3 demonstrates these in detail. Where countries not shaded were not witnessed, but the darker the shade, the more IP /24 subnets that were observed.

![Figure 3. Attack IP /24 Subnet Country Origination (attack sources)](image)

This data is further broken down by top countries of observed IP /24 subnets in Table 3. This displays the highest to lowest of how many IP /24 subnets (4th Octet removed) were observed from each country.

### TABLE 3. TOP COUNTRIES OF IP /24 SUBNETS OBSERVED

<table>
<thead>
<tr>
<th>Destination</th>
<th>Numbers observed of individual IP /24 Subnets</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>157</td>
</tr>
<tr>
<td>Brazil</td>
<td>113</td>
</tr>
<tr>
<td>France</td>
<td>96</td>
</tr>
<tr>
<td>China</td>
<td>80</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>55</td>
</tr>
<tr>
<td>Germany</td>
<td>33</td>
</tr>
<tr>
<td>Canada</td>
<td>26</td>
</tr>
<tr>
<td>Netherlands</td>
<td>23</td>
</tr>
<tr>
<td>Ukraine</td>
<td>20</td>
</tr>
<tr>
<td>Indonesia</td>
<td>17</td>
</tr>
<tr>
<td>Iran</td>
<td>16</td>
</tr>
<tr>
<td>Palestinian Territories</td>
<td>15</td>
</tr>
<tr>
<td>Other</td>
<td>235</td>
</tr>
</tbody>
</table>

During this experiment, the highest number of IP /24 subnets observed was from the United States, although not displayed in Table 3, only 7 /24 subnets were witnessed from the United Kingdom.
4.3. Volume of Attacks

In section 4.2, it was claimed that the United States was the most frequent country by different IP /24 subnets to attempt to gain access in some way to the PBX Honeypot. Yet, this does not necessarily mean that most attacks were witness from the United States. Instead, as displayed in Fig. 4, the most amount of data transferred were based on attacks which originated from the Netherlands.

The majority of traffic from the Netherlands and Iceland originated from 1 IP /24 subnet, where in comparison it was balanced for French, Russian and US IP subnets.

4.4. 3\textsuperscript{rd} October Registration Attack

The attack witnessed on the 3\textsuperscript{rd} October 2018 was multiple times bigger than any other attack. Instead of the approximate 12-hour attacks (Fig. 2) witnessed on other days, 3\textsuperscript{rd} October had a continual 24-hour period attack (with a short break in between) where 7.2 million registration attempts were made. The user agent used in the SIP messaging appeared to be from MGKsip release 1110. This attack intensity can be seen in Fig. 5.

4.5. User Agents

During the 10 days the Honeypot ran, various user agents appear to have been used by third parties to send messages to the system were observed.

<table>
<thead>
<tr>
<th>Register</th>
<th>Invite</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vaxsipuseragent/3.1</td>
<td>Linksys-SPA924</td>
<td>Friendly-scanner</td>
</tr>
<tr>
<td>MGKsip release 1110</td>
<td>SIPCLI/V1.8 (some were V1.9)</td>
<td>Avaya</td>
</tr>
<tr>
<td>VoIPSIP V11.0.0</td>
<td>Pplsip</td>
<td>Cisco-sipgateway/IOS-12.X</td>
</tr>
<tr>
<td>Eyebeam</td>
<td>voipxx</td>
<td>sipvicious</td>
</tr>
<tr>
<td>FPBX</td>
<td>Various random characters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- zazann,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- xcvfdfl1</td>
<td></td>
</tr>
</tbody>
</table>

Some of these were a combination of random letters and numbers, others were known user agents, desk phones or phone systems. The breakdown based on SIP Message type can be seen in Table 4.

4.6. Unauthenticated Invite Attempts

It was observed that third parties were attempting to dial the PBX without prior authenticating by sending Invites. Attackers usually attempted to call real phone numbers by trying different prefixes in front of the number. This concept is similar to that of dialling 9 for an outside line. Hundreds, if not thousands of variations were observed for many of the numbers attempted. For example:

- 9[number]
- 900[number]
- *9[number]
- +[number]

What is of interest is that almost all Invite messages were setup to originate from the Honeypot IP address. For example, in the “from” header in the Invite, instead of it normally containing the...
origination number and IP of the device that generated
the call, it would mostly be a valid extension on the
PBX and the IP of the PBX. For example, 1001@honeypotIP.

In this experiment, the majority of call attempts
(Invites) were to United Kingdom phone numbers,
even though the United States used the most amount
of numbers. In total, calls were attempted to 25
different countries (26 if you include internal
extensions). Table 5 shows in more detail the
countries where different numbers were observed
along with their corresponding percentage of call
attempts based on individual calls (which can contain
multiple Invites) being attempted.

Overall there were 58,215 Invite messages, but
only 44,157 call attempts. On some occasions the
Honeypot was sent the same Invite multiple times, but
on many other occasions an attacker would attempt to
send a call attempt without prior registering, the
Honeypot would then reply back with a “401
Unauthorised” SIP message, where the attacker would
then send another Invite but this time with various
credentials. Table 5 displays the percentage of these
call attempts for each country.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Numbers observed</th>
<th>% of call attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>44</td>
<td>4.2%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>24</td>
<td>61.9%</td>
</tr>
<tr>
<td>Israel</td>
<td>18</td>
<td>1.7%</td>
</tr>
<tr>
<td>Poland</td>
<td>12</td>
<td>29.7%</td>
</tr>
<tr>
<td>Unknown</td>
<td>10</td>
<td>0.3%</td>
</tr>
<tr>
<td>Internal Ext.</td>
<td>5</td>
<td>1.7%</td>
</tr>
<tr>
<td>Sweden</td>
<td>4</td>
<td>0.4%</td>
</tr>
<tr>
<td>Russia</td>
<td>3</td>
<td>0.1%</td>
</tr>
<tr>
<td>Other</td>
<td>22</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

What is of particular interest, is call attempts to
Poland where these call attempts would use very long
prefixes. Unlike other countries where there was
potential logic for attempting to dial out (various
combinations for 9 or 8 etc. for an outside line), in
many cases, the prefixes were 6 or more numbers
long.

The countries where the Invites were originated
from based on IP /24 subnets are displayed in Fig. 6.

Most Invites originated from France, followed by the
United States.

5. Discussion of Results

The date period within this experiment is 10 days.
The experiment performed by Hoffstadt et al. (Essen
Project) between late 2009 and early 2012
experienced 47.5 million SIP messages [14].

In contrast, our experiment has experienced just
under 19 million SIP messages in only 10 days. This
gives a mean average of 1.9 million messages per day.
In 1 day alone (3rd October), over 7.2 million SIP
messages were received which is over 15% of what
Essen witnessed across multiple locations combined
over a 2-year period.

Based on our results, if this experiment ran for the
same time period to that of the Essen experiment, it is
expected to result in over 1.4 billion SIP messages.

This represents a rate of attack 30 times more
aggressive than in the Essen experiment. This view
reinforces the trend observed by the CFCA that PBX
hacking has increased significantly in recent years [3].

When a dictionary attack was being performed, the
resources being consumed by the PBX were
significant which would question whether a negative
impact of service would be experienced by a business
user or owner of a PBX that was being attacked. A
large amount of upload bandwidth was consumed by
a rate of approximately 600Kbps.

For businesses that do not have a leased line and
rely on ADSL, this could have significant
consequences by reducing the quality of calls due to
bandwidth constraints imposed by technologies and
providers.
In addition, 30% of the CPU was being consumed by these attacks which could limit the call capacity of the PBX where both would have the symptoms of audio breaks in the calls, also known as choppy calls.

A final consequence on the bandwidth being used in these attacks are where businesses pay per GB of data transferred or have a monthly bandwidth quota. It is still common among business ADSL lines to have data quotas applied to a broadband line with additional fees applying for exceeding this threshold.

The large CPU resources being consumed by these attacks can be explained by the multiple processes that occur when a SIP message is received. Asterisk would receive a message and if a Register or Invite was received Asterisk would have to perform an SQL lookup in a database (to check credentials) and provide a reply while at the same time writing events to a log. Many PBX systems do not have an SSD, but a hard disk. If a basic PBX had to deal with this volume of connection attempts, then the PBX would most likely become overloaded or not be usable by a business due to IO constraints.

Unlike previous similar experiments, little to no Options were received. This could be because we have not specifically checked whether the research conclusion from Essen are still correct (i.e. the PBX is continually being sent Option SIP messages until the PBX responds and after responding, few further Options will be received).

As from previous studies from over 5 years ago [14,15], several user agents are still being used such as friendly-scanner and user agents with various random characters. Of interest though are user agents which give the impression of real, widely-used devices such as Avaya, Cisco-SIPGateway and Linksys-SPA942. This would suggest that attackers are either spoofing these user agent names or hardware has been compromised into some form of botnet. This hardware is usually expensive at the higher end of the market. The significant attack on the 3rd October appeared to originate from an attacker using MGKsip Release. This demonstrates that the approach taken during these attacks today have developed in sophistication compared to that seen in previous research [14,15].

Unlike other documented experiments, an actual PBX was used, although the SIP process would remain the same, the metadata exchanged would contain information regarding the PBX which would give information about the software being used. This would lead an attacker to believe the system is genuine and a production system. This may partially explain why this experiment witnessed significantly more attacks.

Hoffstadt et al. concluded that not all attackers were involved in various stages of attack and potentially shared information with other attackers. Based on anecdotal evidence physical hardware appearing to be involved in attacks, this could reinforce the idea that data is shared but via a botnet of infected machines. This concept is further discussed below.

During the Honeypot period, only a very small percentage (<0.02%) of attempts successfully registered to any of the PBX extensions. Although on most days, when an attack was under way, different credentials were being attempted. On the 3rd October, all 7.2 million attempts used the same details. This could be explained by a botnet which is automated and, in this case, misconfigured, but more concerning due to the volume could be seen as a Denial of Service attack as the result it could have on a business.

As witnessed in Fig. 2 and Fig. 5 attacks would run and then stop, suggesting hackers were trying a set of predetermined data in their registration attacks. In both graphs, a sudden, but short spike in requests are made. This would have a detrimental impact on the performance of a PBX as described above due to IO limitations.

The Honeypot observed that although the United States had the highest number of individual IP /24 subnets attempting connections, the Netherlands had the most amount of data transfer. This could suggest that hackers are either geo-locating their attacks (Netherlands has considerably less latency to the UK than from the USA) or there is a coordinated botnet of systems all interconnected which perform different tasks. This reinforces Hoffstadt et al. idea as discussed above that data is shared, but as our experiment showed, the Invite IP subnets were rarely the same as the Registration attempt IP subnets. In this experiment, the attackers knew exactly what extensions the Honeypot had and attempted Invites appearing from those extensions. This appears to have evolved in terms of attackers behaviour. This suggests there is anecdotal evidence that a botnet exists of compromised VoIP systems for PBX Toll Fraud where each system performs different task. A simplified view could be:

1. Compromised System A is for Options to see if a system is SIP enabled
2. Compromised System B is for registration attack to determine accounts on a PBX
3. Compromised System C is to launch Invites to appear from the accounts
4. Compromised System D is to brute force registration on known accounts.

This sophisticated nature could suggest a single or handful of organised criminal networks for Toll Fraud considering how much money is thought to be involved.

In addition, this demonstrates that systems from many countries are involved in terms of IP Space and this provides insight into the challenges PBX and Network administrators would have as even though a
PBX administrator may attempt to only allow VoIP Traffic from the specific country, there is a high probability that registration attempts will also come from that country. Although the Fail2ban feature may help, it could still be problematic where a user accidentally blocks themselves due to entering their password incorrectly too many times. In addition, a PBX dealing with these levels of attacks prior to blocking can still cause system load.

Invites being constructed in a way that make it look like a call has originated from an extension of the PBX may suggest that PBXs currently being used are either vulnerable to an attack or may be badly configured which suggest that the PBX may believe that the call has originated on a loopback interface and may accept the call.

In addition to this, it appears that attackers are also attempting to brute force via call attempts by sending multiple Invites with different credentials. Although there were no large dictionary attacks witnessed, this does in theory leave scope that large brute forcing attacks potentially could occur via Invites rather than through Registrations which currently accounts for most message types. Although in the case of Invites, it appeared the attackers already new the extensions which reinforces the idea that data is being shared.

The combination attempts of Polish numbers did not make logical sense. In these attempts, the prefix appeared to be very long, longer than what may be considered reasonable for an outside line or attempting to brute force a pin code than can be required to call an outside line and international. These long prefixes are common when connecting to a VoIP Trunk provider where each prefix is unique to a customer to assist in identifying and routing calls. This could suggest 2 theories that in this case, the entire dial string is sent to the PBX allowing a call to route (perhaps it is a pin number) or the theory that VoIP Provider Servers accept calls from other PBX Systems are badly configured and therefore the attacker is presuming this use case and attempting various prefixes on the chance it may go through due to a software vulnerability or misconfiguration.

The majority of numbers in observed Invites were to low cost numbers and in most countries were regular fixed line numbers that would not generate a premium for an attacker. This would suggest that in the Eco System of Toll Fraud, the criminals appear to call out just to prove the principle that they can actually call out. It could be argued that attackers are using mostly low cost numbers to mask their high cost numbers until they know they can call out at which point it is thought they will then use their high cost numbers to generate revenue.

Reinforcing the idea previously discussed that attackers are possibly geo-locating their attacks, this is reinforced as the majority of Invites came from French IP subnets. This could be because the Honeypot was located in the United Kingdom.

Additionally, the majority of Invite attempts were to numbers in the United Kingdom. This could be because the attackers are presuming local calls geographically located close to the PBX may not be as noticed as much when compared to international calls when they are attempting to initially call out. This could be different if the Honeypot was located for instance in Japan. The only way to determine this is to rerun the Honeypot in multiple locations around the world and analyse any similarities between Honeypot location and attack locations.

6. Conclusions

The data gathered in this 10-day Honeypot experiment has yielded interesting findings and established that VoIP Attacks are not only still occurring, but are significantly greater in numbers (up to 30 times more aggressive than previous studies) and new software and possibly compromised hardware is being used to generate these attacks which could suggest a wider problem from a PBX Hacking botnet.

Previous documented user agents still occur in some occasions, but this is outweighed by new appearing user agents. In addition, attacks are of the size that could congest business broadband connections resulting in further indirect charges.

The United States had the greatest number of individual IP /24 subnets of any one country witnessed, but the majority of SIP Messages overall originated from the Netherlands. Where in comparison the majority of Invites appeared to originate from France. There is anecdotal evidence to suggest that there is an international botnet of potentially compromised VoIP systems being used to hack PBXs where different systems perform different roles in attempting to gain access.

Building off the previous paragraph, this experiment has shown that attackers are attempting to trick PBX’s into believing that calls being made are from either a) extensions on the PBX or b) an allowed unique prefix which could be making use of a software vulnerability or misconfiguration in a PBX or other VoIP software.

Finally, there is evidence to suggest that attackers are geo-locating their attacks based on where a PBX is located. For example, in this experiment, most Invites went to low cost numbers in the United Kingdom potentially suggesting an attacker is trying to call out without being noticed.

7. References


8. Acknowledgements

This work was supported by the Digital Economy programme, led by the Engineering and Physical Sciences Research Council on behalf of UK Research and Innovation.