Developing VoIP Honeypots: a Preliminary Investigation into Malfeasant Activity

Craig Valli
Secau – Security Research Centre
Edith Cowan University
Perth, Western Australia
c.valli@ecu.edu.au

ABSTRACT

30 years ago PABX systems were compromised by hackers wanting to make long distance calls at some other entities expense. This activity faded as telephony became cheaper and PABX systems had countermeasures installed to overcome attacks. Now the world has moved onto the provision of telephony via broadband enabled Voice over Internet Protocol (VoIP) with this service now being provided as a replacement for conventional fixed wire telephony by major telecommunication providers worldwide. Due to increasing bandwidth it is possible for systems to support multiple voice connections simultaneously. The networked nature of the Internet allows for attackers of these VoIP systems to enumerate and potentially attack and compromise a wide range of vulnerable systems. This paper is an outline of preliminary research into malfeasant VoIP activity on the Internet.

Keywords: VoIP, honeypot

INTRODUCTION

Voice over IP systems are replacing conventional switched wire telephone devices, these systems rely on Internet connectivity for the transmission of voice conversations. Many large corporations have been successfully using these types of systems over a number of years to lower communications costs relating to telephony. We are now seeing this technology being placed into homes through such initiatives as the UK-based BT Home, Australian based iinet BOB and various American offerings. These systems work by replacing conventional fixed line telephony with broadband connected wireless enabled routers that provide not only Internet access but VoIP services within the home or business.

Some 30 years ago computer hackers compromised PABX systems to facilitate cheap long-distance calling through the rerouting of their modem calls through these compromised systems. This illegal rerouting enabled the hackers for the cost of a local call to stay connected to long-distance phone calls for any period of time that they wished to. The actual costs for such long-distance calls was borne by the owner of the PABX system not the hacker and diagnostics on these systems often only indicated that the calls originated from the PABX. This mode of attack started to decrease as PABX developers hardened their devices against attack by these interloping attackers by placing countermeasures in the PABX. This coupled with long distance telephony becoming cheaper and eventually broadband digital services such as ADSL and ISDN replacing acoustic modems and the PSTN as the main carrier for Internet traffic.

Due to technological restraint it was relatively difficult to have more than a one-to-one connection between the attacker and responding devices. This paradigm has now changed with the introduction of VoIP systems where an attacker can control many telephony sessions from the one device.

VoIP is most typically sent as a clear text transmission and is relatively trivial task to intercept with a simple packet sniffer. The transport for the supporting protocols of VoIP are typically UDP based. In addition there are already a variety of tools that can intercept and replay voice conversations that are conducted over VoIP channels. Not all of the tools capable of interception or enumeration are in the realm of hacker based tools some are legitimate packages such as Wireshark or NMAP.

VoIP systems suffer from the same Achilles' heel that all core services do in that for it to be useful it must be available for connection from unknown parties. In the same way that a Web server serves web pages to requesting clients likewise a VoIP server must allow unknown connections to start for a voice conversation to occur. As a result much of the authentication and authorisation has to be open, disallowing the provider of the service basic protections against malicious activity from parties who are interested in enumerating or compromising a system.

THE CURRENT LANDSCAPE – FACTORS INTERSECTING

There are various tools available for the enumeration and subsequent compromise of VoIP systems. The following table represents some of the more common tools and indicates their abilities many of these tools have been freely available since 2005.

Name	Description/Modus Operandii
SIPVicious Tool Suite - svmap, svwar, svcrack	svmap lists the SIP devices found in an network. svwar maps active extensions on a PBX. Svcrack is a password cracker for SIP
sipflanker	Many (if not most) VoIP devices have available a Web GUI for their configuration, management, and report generation. And unfortunately it is also common for the username and password to have the default values.
sipcrack	Sipdump finds SIP logins, then sipcrack is used bruteforce passwords on the identified logins

Name	Description/Modus Operandii
steganrtp	SteganRTP is a steganography tool which establishes a full-duplex steganographic data transfer protocol utilizing Real-time Transfer Protocol (RTP) packet payloads as the cover medium. The tool provides interactive chat, file transfer, and remote shell.
sipp	Test tool and traffic generator
sipsak	sipsak is a small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications. It can be used for some simple tests on SIP applications and devices.
VoIPER	VoIPER is a security toolkit that aims to allow developers and security researchers to easily, extensively and automatically test VoIP devices for security vulnerabilties
UCSniff	UCSniff is an assessment tool that allows users to rapidly test for the threat of unauthorized VoIP eavesdropping. UCSniff supports SIP and Skinny signaling, G.711-ulaw and G.722 codecs, and a MITM ARP Poisoning mode.

In addition to this, there have been numerous articles in the literature that relate to vulnerability in the VoIP protocol [1-3] some even describe how to use the above tools to achieve enumeration or even exploit of a VoIP system. There also several books on the exploitation of VoIP [4]. This level of information availability, coupled with the increasing numbers of encoded ready to use hostile tools is a malevolent landscape waiting to happen.

In the last three to five years many large infrastructure providers as previously mentioned have started to offer integrated IP/Telephony/VoIP solutions for the home user. This current status quo now provides the attackers with not only knowledge that has moved from tacit (theoretical attack) to explicit (code tools for exploit) but also an increased opportunity for exploit and compromise of hosts through the deployment of VoIP systems in homes sees for the first time viability of attacking these systems for gain.

MOTIVATIONS FOR ATTACKING VOIP

Most of the key drivers for motivation of attacking and compromising VoIP systems is built around financial gain in a similar fashion to the PABX compromises of past. The attacker's motivation is to use the victim system as a conduit for malfeasant traffic and have the victim bear the charged cost of any such activity. The other motivations of course are still classic disruption or denial of service to the victim.

FINANCIAL GAIN

There are numerous telephone calling cards one can use to call cheaply overseas that utilize systems legitimately and use technology such as VoIP to lower costs for providers of the service. The low cost is enabled through the use of VoIP technologies. The use of a calling card normally involves calling a legitimate number and then keying in the long distance number you wish to call. As a result of keying in the number you are then normally redirected through a cheaper service typically VoIP and calls are initiated to the requested number. The call quality of these systems is sometimes degraded but then the costs are significantly lower for users of these systems.

The illegitimate use of these systems would see compromised VoIP systems being utilised to route the incoming calls to the destination at the expense of the owner of the compromised system. The other method is to use rerouting to dial premium subscriber-based phone lines that charge a set rate per minute for the connection to the end user typically on a range of between $1 - $8 a minute again typically depending on the type of service offered. The difference in price after servicing fees from the provider of the premium number then becomes the profit that is sent to the entity that set up the premium number service for providing the service normally the compromiser of the system.

Malicious users could hide much of their activity by distributing the call load across a multitude of compromised devices in essence a distributed compromise of service. By spreading the call load across a wide range of compromised devices it affords the malicious users good protections from detection by the owners of the systems. Modifying one of John Paul Getty sayings illustrates this concept “it is far easier to steal a $1 from 100 people than to try and steal $100 from one”. By using this *modus operandi* not only do attackers lower their forensic fingerprint but also make it difficult for intrusion detection systems and other methods of monitoring to detect a malfeasant call.

DENIAL OF SERVICE

Denial of Service (DoS) is a simple and well proven attack method which can be achieved by flooding network connections, socket/port exhaustion, or resource exhaustion of a service or server by overloading with the end result being memory or CPU exhaustion. This exhaustion of service can have catastrophic outcomes resulting in servers halting and rebooting or simply service to be useless due to performance degradation. Motivations for this could be blackmail as has been evinced already in businesses where availability is crucial for business e.g online casinos where if you want to be able to collect revenues you have to be available and online. This availability nexus is as previously mentioned an Achilles heel for service of this kind.

The other motivation is to gain a competitive advantage over a competitor remembering not all businesses behave ethically. If people cannot contact you on the phone service you are using it becomes increasingly difficult to conduct business with you and they will seek out an alternative. A DoS in these types of cases does not have to be 24/7 to be effective, attacks at key times during a business calendar can have devastating consequences for any business sustainability or viability.

DETECTION OF MALICIOUS ACTIVITY

The use of intrusion detection systems whether they be host based or network based is one preferred way of detecting malicious activity on a network directed towards VoIP systems. Many of the attack or enumeration tools such as SIPvicious tool suite [5]when used in default mode are overt, verbose and readily identified. The following extract from a system log file is an example of a transaction between a system and the SIPvicious tool suite

```
UDP message received [416] bytes :
OPTIONS sip:100@xx3.xxx.xxx.xxx SIP/2.0
Via: SIP/2.0/UDP 10.160.67.18:5061;branch=z9hG4bK-
2559388112;rport
Content-Length: 0
From: "sipvicious"<sip:100@1.1.1.1>;
tag=6362613137353765313363340131303635333036333336
Accept: application/sdp
User-Agent: friendly-scanner
To: "sipvicious"sip:100@1.1.1.1
Contact: sip:100@10.160.67.18:5061
CSeq: 1 OPTIONS
Call-ID: 1020236891970287777884434
Max-Forwards: 70
```

As can be clearly seen as highlighted there are hallmarks or indicators of a SIPvicious based attack on a system. It is a simple task to write some intrusion detection system rules from this exchange. An example Snort rule could be

```
alert UDP any any → any (msg:”sipvicious default
scan”; content: “|736970766963696f7573|”;)
```

This rule simply traps for any UDP connection that has the string sipvicious in it. Alternatively the string friendly-scanner could also be trapped. With the use of dynamic rules one could also for instance trap the next 500 packets from the attackers IP to be able to examine any connections or activity being undertaken by the attacking IP.

The caveat on these types of attacks is that the use of these tools is as provided by the author and that are typically initiated by inexperienced attackers often referred to as script kiddies or n00bs. The inexperienced attacker does often not know or often understand the tool they are using and that they are leaving behind a large forensic fingerprint. One could further postulate that these types of attacks are not organised criminals or experienced cyber criminals searching for vulnerable VoIP systems. These attackers instead will utilise methods that are relatively anonymous and will avoid detection by intrusion detection rule sets in use. This exact scenario now presents another problem for providers or users of VoIP systems who wish to protect the service. The problem is that to protect a VoiP system from compromise one has to assume that all connections are malicious and subject them to intense inspection and scrutiny and or use a whitelist which defeats the purpose largely of having a open connection. One of the known degraders of any network based system and in particular VoIP based systems performance is latency, by performing any form of packet inspection packet latency will be increased. Hence remedy through the enforcement of large rulesets and packet inspections may in fact be worse than the overall complaint.

USING SIMPLE HONEYPOTS TO DETECTING SCANNING OR ENUMERATION

A talk by Sjur Usken [6] outlines a method for using *SIPp* [7] and a packet logging tool *Daemonlogger* [8] as a simple honeypot for the detection of scanning and enumeration by an attacker of VoIP systems. The *SIPp* suite is a test tool or traffic generator for the SIP protocol that is legitimately used to test systems. It enables call establishment, call flow analysis, message statistics and the testing of a range of features found in VoIP systems. This suite provides the basis for low level interactions with the attacking entity.

Daemonlogger is a program that can sniff network traffic and either spool it to disk or redirect it to another network interface. In the executing of the current research it is used to write the potentially malicious traffic to disk and log it for later forensic analysis. Daemonlogger uses rulesets in tcpdump syntax an example rule follows

```
dst port 5060 or dst port 16384 or dst port 5061 or
dst port 1720
```

will trap for connections on ports 5060, 16384, 5061, 1720. Once there are packets trapped then action is initated to record the packets.

The system being used in our research utilizes rudiments of the system proposed and used by [6]. The system is replicated across a number of sensors we have installed in a honeypot system that utilizes Surfnet IDS as its supporting infrastructure. SurfnetIDS uses a collection of sensors that are connected back to logging infrastructure via VPN. In our setup there is a multitude of recordings occurring.

Basic SQL	The sensors report their VoIP activity back to a customized SQL database for logging of attack data. No packets are captured.
Daemonlogger	File based logging that daemonlogger provides on each sensor, any files produced by daemonlogger are sent back via SCP to the central logging server for storage and analysis. This is in addition to a full dump of the Ethernet connection using tcpdump –w
SurfIDS_Snort	The sensors report via VPN to a Snort based database using custom IDS based rules that respond as a result of a known VoIP attack. These records are incorporated into the SurfnetIDS reporting mechanisms. In this record the attacking IP numbers are also matched against the GeoIP suite for country of origin information.

As the honeypot research is formative and utilizing empirical learning to modify and adapt the honeypot previous experience in deploying honeypot research indicates that there is a scientific need to capture attack data with a multitude of types. The use of multiple streams or samples also allows the use of multiple tools and techniques to validate findings or investigate observed phenomena.

TECHNIQUES UNDER DEVELOPMENT

Apart from deep packet inspection in Wireshark and other packet analysis tools, the research is attempting to find suitable methods for automated alert and response to VoIP oriented attacks.

AUTOMATED ALERTING DEVELOPMENTS

This is already enabled by the research modus operandii to some degree by the use of Snort and custom IDS rulesets we are developing for VoIP systems. IDS systems in combination with analysis consoles such as ACID or Base or SnortAlert allow for much of this systematic alerting or monitoring to occur. Or in the case of this research enable timely inspection and review of attacks on the systems.

The research is also looking at methods for using daemonlogger to redirect output to another interface that becomes a trigger response i.e any traffic on that interface indicates potential malicious activity. This could be a idle VPN connection that when triggered will initiate connection that then results in an escalation of response or monitoring.

The on-demand production of graphical representation of activity using Graphviz [9] produced images using Afterglow is also another approach being developed in the research. The need for using graphical methods for analysis in combating the complexity of alert data received by network systems is well established. The ability to generate graphs on demand allows a new lense or view of the dataset.

AUTOMATED RESPONSE DEVELOPMENT

Automated response is largely enabled by IDS in this case Snort and development of dynamic rules in combination with firewall or host.deny responses. This dynamic use of IDS as always is a balancing act between false positives and legitimate usability of the system. Another factor that increases problems is that VoIP systems use UDP for transport and the resulting transmissions lack the formal controls and discipline with respect to packet sequence, latency and other attributes that a TCP based transmission can be afforded.

As mentioned previously the use of dynamic rules in Snort allows for a variety of actions not all of them need be a complete denial of route to be effective. The triggered recording of attack sessions allows for smaller analysis parcels to be produced rather than having to trawl large packet capture for small packet sequences this produces significant efficiencies in analysis.

Response via device fingerprint spoofing is a well used paradigm in honeypots and honeyd [10] is just one exemplar of the technique. The honeypot system will use known robust fingerprints of a device to fool the attacker into believing they are in fact scanning or interacting with a real device when in fact it is the honeypot. The current research is attempting to generate reliable system fingerprints using NMAP an active network fingerprinter and p0f a passive network fingerprinter for commonly used ADSL VoIP enabled routers. In addition via the production of simple PERL scripts we are also trying to emulate basic service responses to probes by some of the commonly used tools. The aim of the scripts is not to provide perfect emulation of service but merely to mimic standard responses in an attempt to get the attacker to escalate the attack to a higher level of interaction and attack.

CONCLUSION

The research is currently ongoing and should produce systems capable of a more realistic emulation of vulnerable VoIP systems. The research purposefully focuses on VoIP system vulnerability and not standard honeypot systems as there is a significant and successful body of knowledge based around these systems already. It should however, be noted that much of the research is underpinned by successful techniques and methods from within the existing honeypot knowledge domain.

The research has already uncovered increasing levels of probing and enumeration of VoIP systems from a variety of locations on the Internet. The next stage of the research is to start classifying the level of enumeration and attack being undertaken by these attackers to determine if the activity is mere scanning or escalatory in nature and activity that is genuinely seeking to compromise the systems.

REFERENCES

1. Herculea, M., T.M. Blaga, and V. Dobrota, *Evaluation of Security and Countermeasures for a SIP-based VoIP Architecture*, in *7-th International Conference RoEduNet 2008*. 2008: Cluj-Napoca, Romania.
2. Bradbury, D., *The security challenges inherent in VoIP*. Computers & Security, 2007. **26**(7): p. 485-487.
3. Jouravlev, I., *Mitigating Denial-Of-Service Attacks On VoIP Environment.* The International Journal of Applied Management and Technology, 2008. **6**(1): p. 183-223.
4. Endler, D. and M. Collier, *Hacking exposed VoIP: voice over IP security secrets & solutions*. 2006: McGraw-Hill Professional.
5. Guac, S., *SIPVicious tool suite*. 2010.
6. Usken, S.E. *VoIP - Voice over IP or haVock over IP?* 2009; Available from: http://www.honeynor.no/data/honeynet-voip-presentation-anonym.pdf.
7. Gayraud, R. and O. Jacques, *SIPp*. 2010.
8. Roesch, M., *Daemonlogger - Packet Logger & Soft Tap*. 2006, Sourcefire Inc.
9. Ellson, J. and E. Gansner, *Graphviz*. 2008.
10. Provos, N. *Developments of the Honeyd Virtual Honeypot* 2007 [cited 2010 2nd March]; Available from: http://www.honeyd.org/.