2010

Developing Robust VoIP Router Honeypots Using Device Fingerprints

Craig Valli
Edith Cowan University

Mohammed Al-Lawati
Edith Cowan University

DEVELOPING ROBUST VOIP ROUTER HONEYPOTS USING DEVICE FINGERPRINTS

Craig Valli and Mohammed Al - Lawati

secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
c.valli@ecu.edu.au

Abstract

As the telegram was replaced by telephony, so to Voice over IP (VoIP) systems are replacing conventional switched wire telephone devices, these systems rely on Internet connectivity for the transmission of voice conversations. This paper is an outline of ongoing preliminary research into malfeasant VoIP activity on the Internet. 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) this service is 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.

.

Keywords: VoIP, honeypot, honeyd

INTRODUCTION

As the telegram was replaced by telephony, so to Voice over IP (VoIP) systems are replacing conventional switched wire telephone devices. VoIP systems rely on Internet or network connectivity for the transmission of voice conversations using a range of protocols. We are now seeing as result of the spread of broadband networks VoIP 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 context. This growth of VoIP enabled systems is coupled with an increase in malfeasant activity and scanning associated with these systems as attackers seek to compromise vulnerable systems and purloin telephony services.

Some 30 years ago computer hackers compromised PABX systems to facilitate cheap long-distance calling through the rerouting of their modem calls into these compromised systems to access data services. 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 thereby avoiding the high tolls for long-distance calls. 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 compromised PABX not the actual connecting malfeasant entity. This mode of attack started to decrease as PABX developers hardened their devices against attack through reliable countermeasures. Another contributing factor to the decline of this type of attack was the lowering cost of long distance telephony tariffs and a subsequent lowering of the reward versus risk ratio. This method of attack on conventional PABX has now moved to low rate of incidence as broadband digital services such as ADSL and ISDN have all but replaced acoustic and analog modems that use the PSTN as the main carrier for Internet or data traffic.

Due to physical and technological restraint it was relatively difficult to have more than a one-to-one connection between the attacker and responding devices in fixed wire PABX systems. This restraint has now disappeared with the introduction of VoIP systems where an attacker can control many telephony sessions from the one device that is connected to a broadband connection. As network bandwidth increases and hardware capability scales there is increased capacity to carry extra telephony connections.

VoIP traffic from systems that are in default configuration is most typically sent as a clear text transmission and it is relatively trivial task to intercept this traffic with a simple packet sniffer. The main network transports for the supporting protocols of VoIP are typically UDP based. In addition there are already a variety of generic and purpose built software 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 niche hacker based tools some are legitimate security packages such as Wireshark or NMAP.

VoIP systems suffer from the same nexus that all core services do, in that for the service 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 instantiate 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, interrogating or ultimately compromising a VoIP system.

Research is needed to find out the nature of the threats being directed at VoIP systems and to develop techniques for subsequent ameliorations for same. The approach in this particular research is a five phase design to the development of robust VoIP honeypot. The phases are:

Phase 1 – Deployment of initial simple honeypot based on Usken (2009)

Phase 2 – Creation of simple IDS rules, OS fingerprinting of real ADSL VoIP routers

Phase 3 – Implementation of OS fingerprints into simple honeyd based honeypot

Phase 4 – Emulation of services (web, telnet) on ADSL VoIP routers via simple scripts

Phase 5 – Dynamic proxying of advanced or unknown methods

The research is building on existing honeypot methods and techniques and is changing where necessary the modus operandii of known tools and systems to suit detection and response to malfeasant VoIP activity. The paper will explore the current landscape, motivations for attacking VoIP, exploration of simple methods for detection of attacks and progress of the research so far.

THE CURRENT LANDSCAPE – FACTORS INTERSECTING

There are various tools freely available on the Internet for the enumeration and subsequent compromise of VoIP systems. Many of the available tools are specialised and scoped to be operated on VoIP systems and supporting protocols. The following table represents only some of the more common tools and indicates their capabilities many of these tools have been freely available since 2005.

Name	**Description or Modus Operandii**
SIPVicious Tool Suite	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
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
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 (Bradbury 2007; Herculea, Blaga et al. 2008; Jouravlev 2008) some even describe how to use the above tools to achieve enumeration, query or even exploit of a VoIP system. There are also several books on the exploitation of VoIP some of which have been in publication as early as 2005 (Endler and Collier 2006).This level of information availability, coupled with the increasing numbers of encoded ready to use hostile tools is an increasingly entropic security problem.

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 as bandwidth to the endpoint is increasingly capable of supporting it. This current status quo now has knowledge that has moved from tacit (theoretical attack) to explicit (release of code and tools for exploit) in this problem but also an increased opportunity for exploit and compromise of hosts through the deployment of commodity VoIP systems. The commodity systems deployed in home or small business environments atypically do not have strong regimes of security controls and monitoring seen in large enterprise level IT and VoIP systems. This status quo for the first time presents and enables the viability of attacking these increasing number of commodity VoIP systems for personal 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 the 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 is 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 use of a calling card normally involves calling a legitimate number and then keying in the long distance number that you wish to call. As a result of keying in the number you are then normally redirected through a cheaper service typically VoIP based systems and calls are then initiated to the requested number for you. The call quality of these systems is sometimes degraded compared to conventional modern telephony but then the costs are significantly lower for users of these systems. The illegitimate use of these VoIP 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 reroute a users VoIP system 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 initiated on a system.

Denial of Service

Denial of Service (DoS) is a well proven attack method in computer and network exploitation which can be achieved by flooding network connections, socket/port exhaustion, or realisation of resource exhaustion of a service or server by overloading it malfeasant packets with the end result being memory or CPU failure. This exhaustion of service can have catastrophic outcomes resulting in servers halting and rebooting or simply service to be unusable 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. A short denial of service during a competitive demand period for services e.g submission of competitive tendering, realisation of offer and acceptances, participation in auctions or live bidding could be catastrophic for a business.

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 (Guac 2010) 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: 10202368919702877778844 34
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: "|73697076696369 6f7573|";)

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 type of attacks are not organised criminals or experienced cyber criminals searching for vulnerable VoIP systems. The experienced attackers instead will utilise methods that are relatively anonymous and will avoid detection by intrusion detection rule sets or other countermeasures in place. 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 potentially resulting in lagged, noisy or lossy communications.

PHASE 1 - USING SIMPLE HONEYPOTS IN DETECTING SCANNING OR ENUMERATION

A talk by Sjur Usken (Usken 2009) outlines a method for using SIPp (Gayraud and Jacques 2010) and a packet logging tool Daemonlogger (Roesch 2006) 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 VoIP 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 and subsequent use in a low interaction, low level honeypot.

Daemonlogger is a program that can sniff network traffic and either spool it to disk or redirect it to another network interface for transmission to a remote server. 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 which becoming a defacto-standard for many network tools. An example of the syntax follows:

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

This ruleset will trap for connections on destination ports 5060, 16384, 5061, 1720 on either UDP or TCP connection. Once there are packets trapped then an action is initated to record the packets in the preferred mode by setting options from the command line of the tool.

The system being used in our Phase 1 research utilizes rudiments of the system proposed and used by Usken(2009). The system is replicated across a number of sensors we have installed in a honeypot system that utilizes SurfnetIDS 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 this 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.

PHASE 2 – PRODUCTION OF SIMPLE IDS RULES AND OS FINGERPRINTING

The simple honeypot has allowed us to gather intelligence about various scan types and also probes against the fake VoIP device. This intelligence in turn has enabled the development of various rudimentary Snort rules that allow us to now monitor and also detect default scanning activity from a variety of applications. These detected events are now recorded into a database for later analysis and study. In addition to the alerting there is also still full network capture of all traffic to the honeypot systems occurring concurrently and in time sync with the IDS rules.

The fingerprinting phase has involved extensive testing and probing of default commodity VoIP routers in all six different routers were extensively probed using NMAP primarily or (Fyodor, 1998). As a result of extensive testing of the routers the previous research (Valli and Al – Lawati, 2009) identified reliable operating system (OS) fingerprints that can be deployed in a honeyd honeypot architecture to allow spoofing of a realistic hardware device. The systems that have the consistent fingerprints are a D-Link (DVG-G14702S), NETGEAR (DG834GV) and O2 Wireless Box. The successful fingerprint for the D-Link (DVG-G14702S) is below

```
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=4.76%D=4/28%OT=23%CT=%CU=31140%PV=Y%DS=1%G=N%M=001B11%TM=4BD8521B%P=i686-pc-linux-gnu)
SEQ(SP=108%GCD=1%ISR=10C%TI=I%II=I%SS=S%TS=U)
SEQ(SP=107%GCD=1%ISR=10B%TI=I%II=I%SS=S%TS=U)
OPS(O1=M586%O2=M578%O3=M280%O4=M586%O5=M218%O6=M109)
WIN(W1=3E80%W2=3E80%W3=3E80%W4=3E80%W5=3E80%W6=3E80)
ECN(R=Y%DF=N%T=40%W=3E80%O=M586%CC=N%Q=)
T1(R=Y%DF=N%T=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=Y%DF=N%T=40%W=3E80%S=O%A=S+%F=AS%O=M109%RD=0%Q=)
T4(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
U1(R=Y%DF=N%T=40%TOS=0%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUL=G%RUD=G)
IE(R=Y%DFI=N%T=40%TOSI=Z%CD=S%SI=S%DLI=S)
```

PHASE 3 AND BEYOND - TECHNIQUES UNDER DEVELOPMENT

Response via device fingerprint spoofing is a well used paradigm in honeypots and honeyd (Provos, 2007) is just one exemplar of the technique. The honeypot system is now using known robust fingerprints of a fingerprinted 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 developed OS fingerprints are now in honeyd device profiles and scripts are being modified to represent the configuration interfaces on the devices. These interfaces are typically run on *http* or *telnet* protocols and normally not secured via a SSL. As a result of the lack of SSL there is no need to provide cryptography to the session and as such the modification of existing honeypot scripts can be undertaken to emulate the VoIP systems responses to commands. This current phase of research is developing a full topical enumeration of the administration interfaces into an event storyboard. Development of these digital narratives this will enable the development of highly interactive emulation scripts. The aim of the these scripts as with previous developments 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 with the VoIP router.

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 redeveloping standard honeypot systems to address the issues uncovered as a result of the applied research. It should however, be noted that much of the research is underpinned and supported 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. It has generated reliable OS fingerprints that are now being used to develop interactive scripts that will cogently and topically emulate administrative interfaces on the devices. This extended emulation will allow us to entertain a higher level of interaction with the adversary beyond simple probe and scan responses that we are currently capable of monitoring. The extended scripts will enable tracking of interactions to help develop predictive models to determine if the attack is automated or manual. Another potential outcome is to see if malware is targeting a particular firmware revision of a router.

REFERENCES

Bradbury, D. (2007). "The security challenges inherent in VoIP." Computers & Security **26**(7): 485-487.

Endler, D. and M. Collier (2006). Hacking exposed VoIP: voice over IP security secrets & solutions, McGraw-Hill Professional.

Fyodor. (1998). "Remote OS detection via TCP/IP stack fingerprinting." Retrieved 10 May, 2002, from http://www.insecure.org/nmap/nmap-fingerprinting-article.txt.

Gayraud, R. and O. Jacques (2010). SIPp.

Guac, S. (2010). SIPVicious tool suite.

Herculea, M., T. M. Blaga, et al. (2008). Evaluation of Security and Countermeasures for a SIP-based VoIP Architecture. 7-th International Conference RoEduNet 2008. Cluj-Napoca, Romania.

Jouravlev, I. (2008). "Mitigating Denial-Of-Service Attacks On VoIP Environment." The International Journal of Applied Management and Technology **6**(1): 183-223.

Provos, N. (2007). "Developments of the Honeyd Virtual Honeypot " Retrieved 2nd March, 2010, from http://www.honeyd.org/

Roesch, M. (2006). Daemonlogger - Packet Logger & Soft Tap, Sourcefire Inc.

Usken, S. E. (2009). "VoIP - Voice over IP or haVock over IP?", from http://www.honeynor.no/data/honeynet-voip-presentation-anonym.pdf

Valli, C. & Al Lawati, M. (2010) Developing VoIP Router honeypots, Proceedings of the 2010 International Conference on Security & Management, SAM 2010, Las Vegas Nevada, USA.