2006

Voice over IP: Forensic Computing Implications

Matthew Simon
University of South Australia

Jill Slay
University of South Australia

DOI: 10.4225/75/57b13904c7058
Originally published in the Proceedings of the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006.

Voice over IP: Forensic Computing Implications

Matthew Simon and Jill Slay
Enterprise Security Management Lab,
Advanced Computing Research Centre
University of South Australia,
MAWSON LAKES, SA 5095
SIMMP002@students.unisa.edu.au

Abstract

The issues faced by law enforcement authorities concerning VoIP are very different from that of traditional telephony. VoIP provides strong encryption and a decentralised data-based network. Wiretapping is not applicable to VoIP calls and packet capturing is negated by encryption. New methods are required to collect evidence from systems running VoIP software. This paper presents work in progress and, based on a literature review of the field, explores a methodology that may be used to advance this research area.

Keywords

Voice over Internet Protocol , Forensic Computing

INTRODUCTION

Voice over Internet Protocol (VoIP) technology, while still not prominent, is set to radically change the way voice data is communicated and thus to revolutionise the Australian Telecommunications industry. With the tremendous growth in popularity and bandwidth of the Internet, technology has emerged that allows phone calls to be routed over Internet infrastructure rather than the traditional Public Switched Telephone Network (PSTN) infrastructure. The technology, called Voice over Internet Protocol (VoIP), uses the Internet Protocol (IP) to route packets containing small portions of voice conversations between the callers.

TELEPHONY

The Internet and the common telephone are two instrumental communication tools in today's society. These technologies have vastly different methods of transmitting data between locations, both use a variety of common media and have a digital architecture but little other similarities. With the tremendous growth in popularity and bandwidth of the Internet, VoIP technology has allowed phone calls to be routed over Internet infrastructure rather than the traditional Public Switched Telephone Network (PSTN) infrastructure. VoIP utilises the Internet Protocol (IP) to route packets containing small portions of audio from the conversations between the callers.

There are several advantages of using a VoIP implementation over a PSTN implementation. This advantage exists for both the home-user and large telecommunication companies. Some advantages of using VoIP are reduced call costs, greater ability to integrate new services and a significant increase in scalability . In contrast, there are also disadvantages and potential problems associated with VoIP such as lower quality of service, increased security risks, denial of service and determining physical location of callers .

PUBLIC SWITCHED TELEPHONE NETWORK

The PSTN has evolved from the early days of analogue signals passing through manual switches controlled by people, to a highly complex and monolithic digital network . The PSTN connects callers through a series of switches and dedicated lines in what is called a circuit switched network. When a call is established between two callers, a set amount of bandwidth is reserved for the time the connection is active. In Australia, 64 kbps is reserved for each active connection. T1 cables are used for most telephone lines which have a maximum capacity of 1.5 Mbps allowing a total of 24 simultaneous reserved connections . The 64kbps bandwidth was chosen based

on the Nyquist theorem which states that good quality voice transmission is achieved by sampling at twice the highest frequency on the line .

One of the main problems with PSTN technology is that the 64 kbps of bandwidth is reserved even when there is no data being sent (e.g. a silence between the two callers) and the entire bandwidth isn't needed . The actual requirement for bandwidth is usually only a small amount of what is reserved . Another issue with the PSTN is that it does not integrate with new features easily . PSTN uses in-band signalling, this means that data sent for the purpose of creating and ending calls (as well as data sent during a call which is not data from the conversation) is sent in the same frequency as the conversation data . This is illustrated when dialling a telephone number. When each button is pushed, a tone made by the phone is sent across the line that is then interpreted at the telephone's exchange. To develop new services for the PSTN (e.g. caller ID or call waiting), the application developers have only in-band signalling and a small number of other signal mechanisms to use. There are a number of other techniques for overcoming the small number of signals such as dialling special purpose numbers, for example a 1800 prefix .

VOICE OVER INTERNET PROTOCOL (VOIP)

VoIP is telephony that uses the same technology as that which is the foundation of the Internet; this is a packet switched network . Packet switched networks differ from circuit switched networks as a set bandwidth is not reserved for a single connection, in fact, the Internet inherently has no concept of a connection. Small sections of data, called packets, are sent from the end-point through a series of routers, each of which forward the packet closer to its destination. Many different data streams can be sent over the same connections because the bandwidth is not reserved for one particular stream of data. Essentially, VoIP sends data packets between smart devices (e.g. computers) over a relatively unintelligent network, whereas traditional telephony sends voice data between dumb devices (telephones) through a super smart central network .

VoIP telephony is becoming very attractive to users and telecommunication providers alike for a number of reasons. One of the main reasons is decreased costs . Switching data across a packet switched network is much cheaper than establishing a circuit over a circuit switched network because less bandwidth is required. Using the Internet infrastructure is also cheaper as its ownership is not concentrated in a limited number of private companies. Many organisations, including private companies, Governments, Universities and other organisations, own and maintain various parts the infrastructure .

VoIP services are often used in conjunction with PSTN by using media gateways. In the case of a PSTN to SIP network, the media gateways convert the PSTN in-band signalling to Session Initiation Protocol (SIP) messages and voice data to Real-Time Transport Protocol (RTP) packets (or the other way around if travelling from IP to PSTN) . SIP and RTP are common protocols used in VoIP implementations and will be discussed further below. Long distance and international calls benefit from VoIP as the majority of the distance can be travelled via IP networks and rejoin the PSTN at a local call distance from the target destination. One major telecommunication company in the United Kingdom is expected convert from a PSTN to an IP backbone by the year 2007. Customers utilising the company's infrastructure will likely not know the calls are travelling via the Internet . Telecommunication companies also see VoIP as a method of offering existing customers additional multimedia services such as video-calls .

Another reason for the increased use of VoIP is extensibility and scalability . VoIP is capable of integrating almost any feature imaginable. The limitations are in the end devices and protocols rather than in the network (as is the case with PSTN). With an IP network, in-band signalling is not required, separate data streams are used for data and signalling . To integrate new features within the PSTN network, the complex central switches have to be reprogrammed which is an involved task .

VoIP telephony relies upon various protocols and methods to establish calls and transmit data. Skype software uses proprietary protocols that are also encrypted. Many VoIP implementations, however, use SIP and RTP. The SIP protocol is used for call initiation, call teardown and other call related data sent during the conversation. This is analogous to the PSTN in-band signalling mechanism, Dual Tone Multi-Frequency (DTMF). SIP is a text

based application level protocol and relies heavily on other protocols for transport (such as IP and UDP) . VoIP implementations that use SIP generally rely on a SIP proxy server to which the users must authenticate their login credentials. This proxy is also used to route call and signalling data. Clients can find each other and forward SIP messages via this proxy . Communications using SIP are not only used for initiating and to teardown calls, they are also used for changing call parameters or other features such as integrating more callers into a conference session. shows the exchange of SIP messages between two clients. It shows the use of SIP registrars and the proxies which allows callers to create new call sessions. SIP registrars are additional servers used to locate other users; generally, the SIP proxy also acts as the registrar.

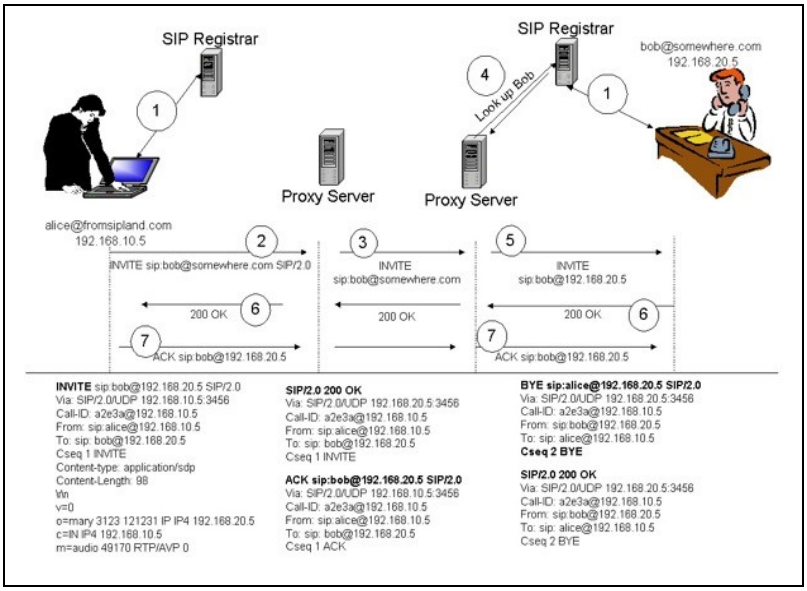

Figure 1 The exchange of SIP messages between two callers

RTP is used for data that is real time in nature. It is not specifically designed for use with VoIP, but rather any generic data of a delay-sensitive nature sent over an IP based network. RTP is transported within UDP packets to reduce overhead, which leads to greater transmission speed and therefore better call quality. The UDP protocol does not support the concept of a stream and consequently RTP incorporates sequencing numbers and timestamps in its packet header to detect jitter and packet loss . Additional mechanisms are also added to RTP to allow for Quality of Service (QoS) metrics, content recognition and compression.

There are numerous advantages of using VoIP telephony over traditional PSTN technology, but there are currently issues that affect the viability of the technology. Quality of Service is a measure of the acceptability of performance from the perspective of the user. The Internet does not inherently support real-time message passing and traditional applications have not required such constraints. A delay of three seconds would not affect an email in transit but would have a significant impact on a VoIP phone call. There are three issues which affect real time data that are not a problem for other data, these are latency, jitter and packet loss . Latency occurs when packets arrive too slowly from the source and this can cause gaps in conversation. Jitter occurs when packets arrive out of order and packet loss occurs when packets do not arrive at all (if the packet arrives too late then it will be dropped and have the same affect as a lost packet) .

The security of VoIP is another major issue, as VoIP must contend with a whole range of threats to which the PSTN is not exposed. Denial of Service (DoS) (including Distributed Denial of Service - DDOS), subscription hijacking and eavesdropping are among the more common threats to VoIP . The risks of running VoIP also extend to the underlying network, protocols and other devices on the network . Issues with VoIP and the underlying network are an especially complicated problem as VoIP has very different requirements to that of a data network. Network Address Translation (NAT) routers create problems with routing call data (predominantly adding latency), whilst firewalls often stop VoIP applications from using dynamic port allocation. Security of the

call data (including call metadata) is another issue with VoIP. Although eavesdropping (packet sniffing VoIP call packets as it crosses the network) has been negated in many VoIP implementations with strong encryption, a compromised VoIP device such as a SIP proxy, could collect information about calls such as destinations, origins, durations and call parameters . In addition to the threats which are faced by VoIP exclusively, traditional threats to network connected devices such as viruses, spam, unauthorised access and malware all still remain applicable to VoIP .

Much has been done to protect networks and allow VoIP implementations to be secured. Protocols such as SIP inherently support encryption and Secure RTP (SRTP) has been developed to add encryption to real time data. Issues such as DoS can be negated by good network design, as they can with a traditional data-centric network . Kuhn, Walsh & Fries suggest a novel approach to protecting data-centric networks while integrating a fully functional VoIP network using the same physical infrastructure. They recommend using two logically separate networks, with exclusive address blocks, Dynamic Host Configuration Protocol (DHCP) server and firewalls for each network. This will allow the networks to have different configurations (especially within the firewall) to allow for optimal performance and security for each while only having to maintain one physical network. The logical networks can implement additional measures to stop data flowing between the networks illegally.

CALL INTERCEPTION

VoIP is a developing technology and the social and legal issues surrounding it are still being realised. How VoIP is affected by legislation that was designed for traditional PSTN telephony is still unclear in many cases. In the United States, the Communication Assistance for Law Enforcement Act (CALEA) governs the legal responsibilities of communication providers and the rights of law enforcement agencies. One of the stipulations of the act requires that all digital switched PSTN telephony switches be wiretap enabled . Bellovon, Blaze & Landau report that the Federal Communications Commission (FCC) ruled that VoIP implementations (i.e. non-carrier VoIP) must also comply with CALEA. Although this is ambiguous, it seems that non-carrier VoIP, such as Skype, is not subject to CALEA where as carrier VoIP must comply (i.e. purpose built VoIP phones which connect through a VoIP carrier) . The distinction between carrier VoIP and non-carrier VoIP, is that non-carrier VoIP is regarded as an information service, which is not covered by CALEA . The FCC ruling means that non-carrier VoIP would also have to comply with CALEA and a major overhaul of protocols would need to be implemented . Forcing non-carrier VoIP to comply with CALEA is a dangerous move as it leaves foreign spies, hackers and terrorists (as well as the intended government law-enforcement agencies) a method of eavesdropping thus causing major security implications.

PROBLEM ARISING FROM USE OF VOIP

The popularity of VoIP is increasing as the cost savings and ease of use is realised by a wide range of people and corporations. The technology is attractive to criminals, especially the non-carrier VoIP, as it often does not require verification of any details to commence using the service. The security of placing such calls may also be appealing to criminals, as many implementations use strong encryption to secure both the voice payload as well as control messages. Skype uses 256 bit AES encryption while Google Talk does not encrypt its payload (but will support encryption in the future) .

The following hypothetical situation illustrates the ease of which this technology can be used in criminal activity:

An organised crime ring operates within Australia, distributing illicit drugs throughout the country. The operators of the crime ring decide that by using Skype software they can anonymously communicate when necessary. From a criminal perspective, there are several disadvantages of using the traditional PSTN telephone system. There is the possibility that a law enforcement body could wiretap the connection should they become suspicious, all calls made and received are logged by the service provider, and using a PSTN phone fixes someone to a given location (i.e. the physical location of the phone). As an alternative solution, criminals can use laptops running Skype, create profiles in the same way as a regular user and communicate when necessary. If

law enforcement should investigate, there is no line to wire tap, no call logs and no ability to tie a person to a specific geographic location. The criminals using Skype can also be contacted or make contact from different locations, providing flexibility.

Although this particular situation is only hypothetical, it is possible. The smallest through to the largest criminal organisations, including international terrorists, could potentially communicate using VoIP, as it incorporates the flexibility of email, the richness of voice and the safety of a decentralised system using strong encryption algorithms.

RESEARCH IN FORENSIC COMPUTING

Forensic computing is an emerging field of computer science that is currently in a transitional phase that will see the field mature into a solid and respected science . New technologies are constantly emerging into the marketplace and the forensic computing field must be vigilant in updating practices and knowledge to account for such technologies. In recent years, there has been a massive increase in the number of devices with embedded logic and storage. There have also been remarkable increases in data storage capabilities in household computers, laptops and dedicated servers. The field of forensic computing must constantly research new technologies as they emerge, as well as review methods and tools that already exist in order to keep methods, practices and knowledge up to date. Many common devices have embedded processing and storage capabilities. These devices could potentially be used during criminal activity and as such, may contain data that could be used as evidence. Devices such as personal digital assistants (PDA), mobile phones, household computers, laptop computers, iPod's, USB storage devices, removable hard drives and other proprietary technologies (e.g. a Blackberry) have the potential to hold information of evidentiary value that could be used in the course of a criminal, civil or internal investigation.

Research within the field of forensic computing is multifaceted. New technologies must be thoroughly examined to determine how they work. This will provide a base for procedures to be developed, allowing a process where relevant data can be extracted in a forensically sound manner. Developing forensically sound tools with which to perform this procedure is an important element of the process.

The goal of research in forensic computing is to determine the 'what' and 'how' of the data on the device or computer. The 'what' is to determine what data is relevant and can be used as evidence in an investigation. The 'how' is to determine the means of collecting and storing the data. If techniques for extracting and storing data cannot be proven forensically sound, it will likely loose integrity and becoming inadmissible in a court of law.

Research within forensic computing needs to be versatile as multiple techniques may be required for any particular situation during an investigation. Forensic computing investigators often face the problem of encountering live systems, that is, a computer or device that is switched on. Forensic investigations are rarely conducted using the target system or on original evidence sources . The target system usually needs to be powered down so that the data on the disk drives cannot be altered, and can subsequently be removed (if practical), secured, and then entered as evidence. The investigator must consider all factors when deciding whether to power down the relevant devices. The computer or device may be powered down using a number of different methods from shutting down normally to removing the battery or plug. If the computer or device is left on, it may be possible for the investigator to extract information from the main memory, although this is more likely with a computer than a proprietary device. Tools and methods have been developed to gain information from memory that is lost once the machine is powered down (e.g. current running processes, memory resident worms etc) .

Situations often arise in forensic computing investigations that require special procedures or tools because a particular technology or situation encountered. Forensic computing research requires constant investigation into new devices and technologies, as well as new methods and procedures for existing technologies. This will equip law enforcement bodies and other forensic investigators with the knowledge and abilities to allow thorough and safe investigation of digital devices. It is thus essential that computer forensic research evaluate the use of VoIP technology and devise methods to allow law enforcement agencies to overcome some of the aspects that are

advantageous to criminals. Wire-tapping is not applicable to VoIP communications and therefore other methods of recovering evidence and information are required.

In his work, Jones (2005) identifies a range of social and technical research questions that focus on the security and privacy issues through the capture of VoIP packets and logs by diverse technological means. He also alludes to the corollary to this issue, which is the positive use of such captured packets and logs for either intelligence or forensic computing purposes.

FORENSIC COMPUTING AND VOIP – POTENTIAL METHODOLOGY

Using Jones (2005) concepts, we turn to memory forensics which is a relatively unexplored area of computer forensics. There are numerous reasons for the lack of use of this technique but is mainly due to the fact that the process of imaging the memory is not verifiable. Little investigation into tools and processes for sound memory dumping techniques has been performed in forensic computing research .

The volatile memory of a system potentially contains tremendous amounts of information about the system including (but not limited to) open files, active processes, terminated processes and device drivers. This source of data is lost when the target system is turned off in the course of securing the non-volatile data sources. Situations can occur in forensic investigations where a target system cannot be turned off. Servers are a prime example as downtime generally leads to loss of revenue or essential services. Imaging the memory of a target machine allows evidence to be collected without any downtime. Imaging memory in general investigations allows an extra source of data from which evidence can be inferred.

Dumping of the memory from a system requires some method of interfacing with the data. Linux Systems contain a memory device similar to devices representing hard disks. Memory can be imaged by copying the data from this memory device . Windows XP does not have an equivalent memory device and must use a section object to gain access to the memory. A section object allows a mapping to memory pages which can subsequently be accessed by multiple processes .

Our work in progress thus examines the question “What VoIP related evidence can be recovered from the volatile memory of a system running VoIP software?”. A number of sub-questions have been devised to divide the research into sections so that each can be focused on individually. Our work is incomplete and still in progress but we see that these questions can be feasibly answered in the relatively short-term

CONCLUSION

Imaging memory for forensic purposes is gaining recognition as an area in need of further research. Burdach has published a number of papers on techniques of finding evidence in both Windows and Linux memory images. The scope of memory forensics is large because and has potential to add a diverse source of potential evidence. The lack of research needs to be addressed to promote greater use of such techniques.

REFERENCES

COPYRIGHT