Voice Over IP And Forensics: A Review of Recent Australian Work

Slay, Simon and Irwin

Abstract

- The popularity of Voice over the Internet Protocol (VoIP) for providing voice communication over IP networks such as the Internet has resulted in VoIP becoming a global telephony service.
- VoIP applications convert analogue voice signals into a digital format, which is then encapsulated into IP packets for transmission over the Internet.
- Our research has examined both the security and privacy implications of widespread adoption of VoIP for personal and business telecommunications and also the use of VoIP calls by criminals, as many implementations of VoIP may also use strong encryption to secure both the voice payload as well as to control messages.
- We have also considered the implication of recovering electronic evidence and information from VoIP since conventional methods of eavesdropping and wire-tapping do not apply to VoIP calls.

Introduction

- Our original interest in this topic was developed after the Voice over IP Security Alliance (VoIPSA) (Kuhn, Walsh & Fries 2005) released a detailed review of threats faced by VoIP technology.
- The most serious of the threats identified were denial of service, host and protocol vulnerability exploits, surveillance of calls, hijacking of calls, identity theft of users, eavesdropping and the insertion, deletion and modification of audio streams .

Pilot Study

- Our work started with a successful pilot study (Simon & Slay 2006) in which we began to examine the potential threat to privacy by the capture and reassembly of VoIP packets by a hacker (or other criminal or terrorist) from a computer or network after a VoIP conversation has taken place.
- We have applied memory forensics to address some of the concerns with the use of VoIP.
- The results of the limited number of experiments conducted with one particular implementation of VoIP (SIP) on one specific operating system (Windows XP SP 2) showed that it was possible to recover packets from memory after the completion of a VoIP call.
- Although very few packets remained in memory in our pilot study, there was enough evidence with these few packets to prove that a call has actually been placed and between whom.

Other research

- At the time, we found little other published research in this area of IT Security / Forensic Computing.
- Neumann, Tillwick, & Olivier (2006) had explored the information exchanged in VoIP call control messages and the implications this has on personal privacy.
- Chen, Wang & Jajodia (2006) examined the privacy and security aspects of peer-to-peer (P2P) VoIP calls and show how the use of VoIP has substantially shifted the previous balance between privacy and security that exists in traditional PSTN calls.
- This paper shows the development of our work at the University of South Australia beyond that identified at our commencement in 2005-6.

Pilot study

- Our original work (Simon & Slay, 2008) was an examination of the privacy implications of VoIP.
- The result of this work was that we were able to search for packets in a memory image taken from a computer running Windows XP or Mac OS 10 and sort, order and output the packets and eventually, under specific circumstances reconstitute the packets to an audio file (audio could be heard).
- We showed that potentially a user's privacy might be breached by a hacker using software similar to that which we developed as part of this original research and that a hacker would be able to copy remnants of the data stream from the computer's volatile memory and recreate small portions of the conversation.

Pilot study

- We also showed the corollary: it was possible to extend the software developed as a tool for users to mitigate against the threat of a hacker who was able to breach their physical and logical security and extract remnant VoIP packets from memory space (in specific situations). This also meant that we had also developed our own first VoIP forensic tool
- A major problem with this research was the inability to verify the resulting memory images obtained during the memory imaging process.
- It was difficult to ascertain how much of a change the process of acquiring the image makes to the image itself.
- We saw a need to examine other operating systems, implementations of VoiP including encrypted forms and then later began to consider the effect of the widespread use of VoIP on law enforcement and police analysis and investigations.

Recovery of Remnant Information from Memory

- We extended our work on VoIP in 2009 (Smon & Slay, 2009) This research presented a study into the feasibility of recovering remnant information from the physical memory of a target computer about a particular IM setup.
- The setup emulated in this study, was Google Chat used through the Pidgin-Portable client while employing Tor to add a layer of encryption and anonymity to the entire process.
- The primary objective of the experiment was to assess if remnant data does remain in the physical memory of the system after use of the target communication technology.
- It also aimed to identify some of the influencing conditions that affect the outcome so as to define patterns in the data that was recovered.

Recovery of Remnant Information from Memory

- The results showed that remnant artefacts do remain in the physical memory during and after the execution of the target communication technology in the context tested.
- This indicates that physical memory forensics has potential for use in recovering information about the technologies tested in this research.
- While the results of this research confirmed that the recovery of communication technology artefacts was feasible, it also helped us understand the limitations of our research.
- The results showed that the information is not necessarily recoverable in all situations – the termination of the relevant processes was highlighted as one case where data was often subsequently unavailable.

Law enforcement Investigations

- We noted in 2011 (Simon & Slay, 2011) that investigation of communication technologies is an important activity that law enforcement agencies carry out.
- We noted that over the extensive lifespan of traditional communication technologies, methodologies have been built that support the acquisition of information in a legally sound and rigorous manner.
- In obtaining information about the use of traditional communication technologies, police use a combination of communication interception, access of stored information and use of post-mortem analysis.
- Two major factors support these methods, legislation and the nature of the technology.
- The legislation is effective in allowing law enforcement to carry out certain activities but also in forcing service providers to operate in certain ways that support law enforcement (e.g. collecting certain types of information).
- The 'nature of the technology' is more nuanced. It effectively relates to the low level of control the user has over the technology that largely prevents the users from circumventing law enforcement methods of obtaining information.

Law enforcement Investigations

- We argued that law enforcement investigation methods where the carriage service is an Internet application are ineffective in many instances.
- When carrying out communications interception, the provider has no legal obligation to assist law enforcement.
- The use of interception at the carrier level circumvents the carriage service provider but the service decoupling property will mean that communications may be missed, and the use of encryption will render this approach ineffective.
- Another layer of complexity is added by the lower barrier to entry and the borderless supply properties that affect both communication interception and access of stored information. The carriage service provider could potentially be anyone located anywhere in the world. This may make even attempting to interface with the provider very difficult, let alone accessing the required information.
- The increasing complexity of end-user devices is another change that works against law enforcement methodologies. Many devices now have built in encryption that can be easily activated by even technically low-skilled users. This will prevent the use of post-mortem analysis to recover any information stored on the device.
- More highly skilled users can employ advanced techniques such as data obfuscation or plausible deniable encryption to add a layer of complexity to an investigation.

Looking further and deeper into VoIP for Electronic Evidence

- Our more recent research is based on analysis of the very limited amount of VoIP data stored in the play-out buffer located in IP telephone devices.
- Examples of this kind of telephone devices include both hardware IP phone and software IP phone end-device, i.e., VoIP software running on computer, such as that implemented in Skype . The play-out buffer usually contains of 800 – 1000 milliseconds of VoIP data, which are packetized into variable length (up to 1500 bytes) UDP/IP packet format. This buffer can be used to supply electronic evidence for forensic investigation or intelligence.
- Another important feature is routing VoIP traffic through firewalls and address translators. Private Session Border Controllers are used along with firewalls to enable VoIP calls to and from a protected enterprise network by traversing symmetric NATs (network address translators) and firewalls.
- These Private Session Border Controllers also contain data that might be extracted using a suitably developed software tool to extract electronic evidence, since VoIP users through these Private Session Border Controllers must be registered with the VoIP gateways for billing purposes.

Development of Digital Forensic Tool for extraction of VoIP data

In 2011, Irwin and Slay extended the previous work by the development of a forensic tool with the following functionality:

- Reconstruction of the VoIP data packet sequence.
  - Detection of the VoIP protocol being used to packetize the voice data.
  - Reconstruct the VoIP data packet sequence order using packet sequence number.
- Interactive searching functionality.
  - The development of an interactive user interface to help the tool user search for forensic evidence within the captured RAM effectively.
  - Automatically record the search results in a format designed to fit the requirements of a court of law.

Development of Digital Forensic Tool for extraction of VoIP data

- Analysis of the voice data.
  - Discovery of the VoIP phone application being used, VoIP codec and routing protocols.
  - Identify VoIP audio in RAM using both a statistical searching algorithm to first identify the language type (English, Japanese etc) based on the characteristics of various types of languages and also spectral analysis if enough VoIP voice data is recovered.
- Trace and tracking information of the VoIP end users.
  - The recovery of VoIP application user names from the control signalling information used to initiate a VoIP call between two parties.
  - The use of a SIP phone as the VoIP application will require both end users to be registered with a SIP provider. These registration details may be recovered at a later date if the unique SIP phone number is extracted from the call setup information.

Further work

- Performing RAM forensics has successfully demonstrated the ability to recover VoIP protocol artefacts left behind in RAM after a VoIP call has taken place. Having successfully recovered packet sequence information to allow VoIP payloads to be reconstructed correctly, the next phase of the research is threefold:
  - Search RAM for unencrypted audio, if it exists.
  - Is VoIP injection possible? To perform track and trace of the end-user, the individual at the receiving end of the VoIP call. The recovered IP addresses may not necessarily include the end-user but a node within the network path between the calling and receiving party.
  - Extend the research to include VoIP applications on portable devices, primarily, mobile phones.
  - Develop a database of contact list structures and control signal information for the most common VoIP applications.