Chapter 2
Voice Over IP:
Privacy and Forensic Implications

Jill Slay
University of South Australia, Australia

Matthew Simon
University of South Australia, Australia

ABSTRACT

With the tremendous growth in popularity and bandwidth of the Internet, VoIP technology has emerged that allows phone calls to be routed over Internet infrastructure rather than the traditional Public Switched Telephone Network (PSTN) infrastructure. The issues faced by law enforcement authorities concerning VoIP are very different from that of traditional telephony. Wiretapping is not applicable to VoIP calls and packet capturing is negated by encryption. This article discusses experimental work carried out to explore methods by which electronic evidence may be collected from systems where VoIP conversations play an important role in suspected criminal activity or communications. It also considers the privacy issues associated with the growing use of VoIP.

INTRODUCTION

Voice over Internet Protocol (VoIP) technology, a growing technology, is set to radically change the way voice data is communicated and thus to revolutionise the Australian and International 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. It is currently estimated that there will be more than 24 million VoIP users in the USA by the end of this year, 2008.

This article reports on research designed to provide significant input into the current concern regarding the security and privacy implications of widespread adoption of Voice over Internet

DOI: 10.4018/978-1-60960-515-5.ch002

Protocol (VoIP) for personal and business telecommunications. The aims of the project were to:

- Examine the potential threat to the privacy of telecommunications users' by the capture and reassembly of VoIP packets from a computer or network after a VoIP conversation has taken place and
- Evaluate the potential use of such reassembled packets in forensic computing investigations.

This work is intended to inform policymakers on the legislative issues surrounding privacy, telecommunications interceptions and electronic evidence preservation. It also advises, technically, as to whether this technology should be used in restricted environments, and will drive future technological security control developments.

VoIP and Security

In our previous work (Simon & Slay, 2006; 2007;) we have illustrated how VoIP technology, while still not prominent, is set to radically change the way voice data is communicated, and thus to revolutionise the Australian and International Telecommunications industry. With the growth in popularity and speed of the Internet, this technology is emerging rapidly, allowing phone calls to be sent via Internet infrastructure rather than the traditional Public Switched Telephone Network (PSTN). There are many advantages to using VoIP technology instead of the current PSTN system. The primary benefit is cheaper call costs for local, long distance and international calls. VoIP is also an advantage in terms of regional and remote users since it avoids large-scale roll-out of cable and cuts costs in large organisations with extensive internal phone systems.

Like any new and emerging technology, many potential problems have been raised with regard to security, and thus to privacy. Recently, the Voice over IP Security Alliance (VoIPSA) released a detailed review of threats faced by VoIP technology. The most serious of the threats are 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.

As indicated above, the purpose of our research into VoIP security and forensics was to inform policymakers on the legislative issues surrounding privacy, telecommunications interceptions and electronic evidence preservation and also to advise technically, as to whether this technology should be used in restricted environments, and to drive future technological security control developments, given the security problems identified. The corollary to this issue is that insecure implementations of VoIP may easily provide valuable electronic evidence and this issue needs to be made known to law enforcement.

VoIP is still a developing technology and the social and legal issues surrounding VoIP are still being realised. In his work, Jones (2005) identifies a range of social and technical research questions which focus on the potential breach of privacy of VoIP communications through the capture of VoIP packets and logs by diverse technological means. In our own work (Simon & Slay 2006) we have identified the existence of VoIP packets in a computer's memory after a VoIP call has taken place. Thus we see an urgent need to be able to identify how much of a conversation might remain in memory and be accessible to a targeted hacking attack, thus breaching privacy. There is an equal interest in determining the extent to which any remnant packets might be reconstituted to provide electronic evidence for intelligence gathering or for forensic investigation.

We have found little other published research in this area of IT Security / Forensic Computing. Neumann, Tillwick, & Olivier (2006) explore the information exchanged in VoIP call control messages and the implications this has on personal privacy. Chen Wang & Jajodia (2006) examine the privacy and security aspects of peer-to-peer