Edith Cowan University
Research Online

Australian Information Security Management Conference

Conferences, Symposia and Campus Events

2011

Evaluation of users' perspective on VOIP's security vulnerabilities

Alireza Heravi
University of South Australia

Sameera Mubarak
University of South Australia

DOI: 10.4225/75/57b530f9cd8bc
Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/115

EVALUATION OF USERS' PERSPECTIVE ON VOIP'S SECURITY VULNERABILITIES

Alireza Heravi, Sameera Mubarak
School of Computer and Information Science
University of South Australia
Heray004@mymail.unisa.edu.au, Sameera.Mubarak@unisa.edu.au

Abstract

Voice over Internet protocol (VoIP) represents a major newish trend in telecommunications and an alternative to traditional phone systems. VoIP uses IP networks and therefore inherits their vulnerabilities. Adding voice traffic to IP networks complicates security issues and introduces a range of vulnerabilities. A VoIP system may face either an exclusive attack or an attack to the underlying IP network. The significance of security and privacy in VoIP communications are well known, and many studies mostly from the technical perspective have been published. However to date, no known research has been conducted to evaluate users' perspectives on these issues. In light of this scarcity, we carried out a survey to evaluate users' awareness of VoIP security vulnerabilities, and their attitudes towards privacy in VoIP communications. An overall finding highlights the fact that the majority of participants are neither concerned about VoIP privacy (eavesdropping) or VoIP security.

Keywords
VoIP Security, VoIP Privacy, VoIP vulnerabilities

INTRODUCTION

For almost a century, person-to-person communication was dominated by Bell's legacy, the traditional telephony system. Due to recent advances in the Internet since the 1990s, the "Internet Telephony" technology has now enabled person-to-person communication to take place via computer networks on a global scale.

VoIP is an umbrella term for the technologies that enable voice to be transmitted over packet-switched IP networks, such as the Internet. VoIP is comprised of a large number of components including, end user equipment (traditional handsets, softphones or PCs and IP phones), end user applications (Skype, X-Lite, Net-Meeting, etc.), call managers, gateways, switches, routers and protocols.

The lower cost and greater flexibility that characterize the main advantages of VoIP over the public switched telephone network (PSTN) are mostly related to the method that voice is transmitted. However, this method - the convergence of voice and data in IP networks - complicates security issues and introduces new vulnerabilities (Douglas & Tom 2004). VoIP systems are vulnerable to both VoIP-specific attacks and attacks to the underlying IP network. Consequently, VoIP systems require additional security controls (Gupta & Shmatikov 2007).

In the literature, VoIP security has been addressed from technical and industrial perspectives. However, no known research to the best of the researcher's knowledge has evaluated users' perspectives on VoIP security and privacy vulnerabilities. To bridge this gap, an on-line questionnaire was designed to collect information to evaluate the users' awareness and attitude towards privacy and security issues in VoIP communications. The remainder of this paper is organized as follows. Section II contains a brief overview of VoIP security. The research methodology is presented in Section III followed by the findings and discussions of this study in section IV. The conclusion of this research is provided in section V.

VOIP SECURITY

VoIP refers to a class of technologies that enables multimedia (text/voice/video) traffic to be transferred over IP networks. The fundamental concept of VoIP is the digitization and packetization of the human voice. The speech (voice analogue signals) is converted into digital signals by appropriate coders/decoders and it is then broken into packets and transferred over Internet Protocol (IP)-based networks like the Internet (Porter et al. 2006a, p. 6).

For data to be transmitted over IP networks, a large number of parameters have to be configured. Many of these parameters are configured dynamically and since a wide range of configurations is involved, networks suffer from potentially vulnerable points (Kuhn, Walsh & Fries 2005). Generally, VoIP uses the existing IP networks and therefore inherits their vulnerabilities. Adding voice traffic to IP networks complicates security issues and introduces a range of vulnerabilities. This is because VoIP requires VoIP-specific configurable parameters in addition to the existing ones in the underlying IP networks, such as call processing components. These parameters change dynamically each time VoIP services are started or restarted.

VoIP/PSTN security: a comparison

It is generally assumed that Public Switched Telephone Network (PSTN) is more secure than VoIP. Basically, PSTN security is based on the physical security of the core network equipment and the related components on the customer's premises. This model known as 'physical wire security' seems to be efficient enough for PSTN since attacks which require physical access usually do not scale in a distributed environment. However, an eavesdropper can wiretap PSTN by physically accessing telephone lines which is much easier than to wiretap VoIP systems. Security issues in PSTN are discussed in (Porter et al. 2006a, pp. 114-118).

On the other hand, the nature of VoIP security is such that it is not based on wire security. However, by gaining access to traffic on a VoIP network that is not well secured, VoIP packets could be captured, modified, reassembled or controlled to overturn the security behaviour. VoIP systems may be attacked by non-specialists using free VoIP-sniffers such as Vomit (http://vomit.xtdnet.nl/) and VoiPong (www.enderunix.org/voipong), but hacking PSTN generally requires specialist knowledge.

Myths about VoIP security

Myths surrounding VoIP have been discussed in Cherry (2005) and Sundquist and Service (2006). In both studies the myth about VoIP security has been described alongside other myths. However, Patrick (2009, pp. 14-15) merely addresses the myths about VoIP security and cast light on them. These myths are summarized in Table 1.

Myth	Reality
1- Traditional phone systems (PSTN) are more secure than VoIP systems	The biggest concern in relation to this myth is wiretapping. It has to be noted that wiretapping PSTN is much easier than wiretapping VoIP. This is because an eavesdropper can wiretap PSTN by physically accessing telephone lines which are not well secured (like outside buildings). However, an eavesdropper, to be able to sniff voice packets has to locate his sniffing tool on the same broadcasting domain as the VoIP devices. This is very hard for external hackers to do due to the fact that VoIP devices are located in places which are either well secured (network equipment's in IT centers) or at least have some level of security (IP phones/cables at offices or residences.
2- To protect network and VoIP end users against threats, strict encryption and authentication is sufficient	It is obvious that encryption and authentication is crucial for securing networks; however, some advanced attackers get through by impersonating, and then bypassing the authentication and encryption process.
3- Securing underlying IP networks can secure VoIP networks as well	From the network layer perspective, securing the IP network will partially protect VoIP data. However, from the application layer perspective this does not apply. This is because security devices like firewalls generally are not able to detect VoIP specific application layer attacks, such as malformed H.323 or SIP messages which target the servers. Security devices should be VoIP aware and this can be achieved by employing VoIP security devices/modules. To retain a secure VoIP system, both IP network and VoIP-specific security issues must be addressed.

Table 1 The three myths about VoIP security

VoIP Threat Taxonomy

Vulnerabilities and threats to VoIP systems have been discussed and classified in various studies (Kuhn, Walsh & Fries 2005; Frost 2006; Porter 2006, pp. 3-25; Stanton 2006; Butcher, Xiangyang & Jinhua 2007; Dantu et al. 2009; Patrick 2009, pp. 19-44). However, the Voice over IP Security Alliance's -VOIPSA (www.voipsa.org) document, 'VoIP Security and Privacy Threat Taxonomy' (www.voipsa.org/Activities/taxonomy.php) provides the most comprehensive classification of security and privacy threats which VoIP's systems may face. These threats are categorized as:

- Misrepresentation
- Theft of Services
- Unwanted Contact
- Eavesdropping
- Interception and Modification
- Service Abuse
- Intentional Interruption of Service
- Other Interruptions of Service

RESEARCH METHODOLOGY

The on-line questionnaire was designed to collect information in order to evaluate the users' awareness of VoIP security vulnerabilities, and their attitudes towards privacy and security in VoIP communications. The 'Recruitment email' was sent to all students at the University of South Australia's School of Computer and Information Science (CIS), to encourage them to answer the questionnaire. Out of 300 recruitment email sent, 107 valid responses were received. To analyze the collected data, SPSS (PASW Statistics 17.0 (release 17.0.2)) and Microsoft Excel 2007 were used and to determine if the relationship between variables is statistically significant, chi-square test was used.

THE RESULTS AND DISCUSSION

It should be emphasized that in this study privacy is considered as eavesdropping while VoIP security is considered to be other violating actions such as toll fraud. However, the occurrence of privacy breaches indicates that the system is not well secure. In that sense, privacy breaches in the VoIP system are synonymous to security vulnerabilities.

Nationality

There were no relationships between nationality and awareness/attitude towards security/privacy issues in VoIP. This is due to the fact that most of the countries (13 out of 18) had either 1 or 2 participants. In all 60% the respondents are Australian, while the rest of the participants (40%) are from 17 other countries.

Average monthly talking time

In regard to users' awareness and attitude towards VoIP privacy and security, the average monthly talking time is related to the participants' concern about VoIP privacy and security issues. Those who speak more are more concerned. However, it has to be pointed out that although the results highlight that the participants who spend more than 7 hours/month on the phone/mobile are more concerned about VoIP privacy (eavesdropping) and VoIP security, there is no technical reason to support this belief. If a VoIP system is vulnerable to privacy/security breaches, the duration of the communication will not affect the system's level of security and consequently will not affect the users. For instance, in Zhu and Fu's (2010) study, the duration of Skype calls is not a metric in their proposed traffic analysis attacks on Skype calls. This indicates that if one uses Skype more often, he or she is not more vulnerable to such attacks. Similarly, in Benini and Sicari's (2008) research the risk assessment method they proposed when assessing the risks of intercepting VoIP calls is not related to the duration of calls.

Using computers to make calls/voice chat

The majority of the participants who use computers for making calls/voice chat believe that privacy breaches are less possible in VoIP than in traditional telephony. This attitude may refer to the network knowledge that computer users have. It has been pointed out in Porter et al. (2006a, pp. 114-118) that eavesdropping VoIP is harder in comparison to eavesdropping PSTN. This is due to the fact that PSTN security is considered to be physical wire security while for wiretapping VoIP attackers must have access to the communication channel of VoIP parties. This is due to the distributed environment of IP networks being more difficult to penetrate.

Convenience is the main reason for choosing specific software for making calls/voice chat by computers, although the respondents are least concerned about the security features of the software they use. In this regard, Skype is the most common service that participants use. There is no relationship between the time they spend on a computer for making calls/voice chat and the choice of Skype as software. However, those who speak more on phone/mobile also spend more time on computers for making calls/voice chat. Furthermore, most of the respondents who use computers to make calls/voice chat use Skype.

Preferred way to make international calls

The majority of the respondents regardless of their preference for using either computers or landline/mobile for making international calls use Skype. Analyses reveal that 55.5% of the respondents who prefer to use computers for international calls and 42% of those who prefer landline/mobile over computer use Skype. This indicates that Skype is the most common service for making international calls either via computer or landline/mobile.

It is obvious that the reason for choosing a service by those who are most concerned about "lower cost" when making international calls, is the lower cost that the service offers. However, the same trend does not apply to those who chose a service for other reasons such as convenience, friend/family suggestion, quality and security. Analyses reveal that 42.4% of the respondents who are most concerned about lower cost when making international calls want a service that is cheaper. Therefore, the feature that the respondents are most concerned about when making international calls matches the reason that they choose a service for making such calls. This is not the case for those who chose a service for convenience (74%) and lower cost (27.5%) when making international calls since the reason for selecting a service differs from the concerned feature. This may indicate that the respondents did not accurately answer the questions.

Concerned features when making international calls

Participants are most concerned about lower cost followed by quality, convenience and security. Therefore, they are least concerned about security and this is probably due to the fact that generally people who make international calls talk to their relatives/friends and the content of their conversations is not confidential. Confidential and sensitive conversations go through end-to-end secure lines, which is common in enterprises and government-sensitive sectors.

The majority of the respondents who are most concerned about "Convenience, Quality and Security" when making international calls are concerned about VoIP privacy (eavesdropping). In contrast, most of those (68.4%) who are most concerned about "Lower cost" are not concerned about VoIP privacy. This demonstrates that when most participants are paying less for their calls they are not concerned about the privacy of their conversations. This is consistent with the participants' opinions about the possibility of privacy and security breaches in VoIP. Answers reveal that most of the participants did not expect VoIP providers to offer the best facilities and privacy since they offer low-cost services.

Privacy concerns when making calls

In all, 43.9% of the participants are not concerned or are little concerned about privacy (eavesdropping) when making calls/ voice chat. In contrast, 38.3% of the participants are seriously concerned about privacy, and 15% remained neutral on this issue.

The majority of the participants who are concerned about VoIP privacy and VoIP security are also concerned about privacy when making calls via traditional telephony and vice versa. This indicates that participants' concern about privacy/security when making calls is not related to the service they use. In other words, these participants are concerned about privacy/security when making calls either by traditional telephony or VoIP.

Comparison of security between international/long distance calls and domestic calls

More of the respondents (35.5%) do not know whether international/long distance calls are less secure than domestic calls. Only 27.1% believe that international/long distance calls are less secure than domestic calls. Additionally, 44.8% of the respondents who believe international/long distance calls are less secure than domestic calls (regardless of the used service) also believe that PSTN is more secure than VoIP (Table 2). This is due to the fact that VoIP is much more likely to be used for international than domestic calls.

Chi-Square value of the relationship: Pearson Chi-Square - Asymp. Sig. (2-sided): .013

Comparison of security between international/long distance calls and domestic calls			Possibility of privacy breaches in VoIP versus traditional telephony				Total
			Don't know	No*	Same	Yes**	
(International/long distance calls are not more secure than domestic calls)	Don't know	Count	18	9	3	8	38
		%	47.4%	23.7%	7.9%	21.1%	100.0%
	No	Count	8	4	3	8	23
		%	34.8%	17.4%	13.0%	34.8%	100.0%
	Same	Count	4	1	6	4	15
		%	26.7%	6.7%	40.0%	26.7%	100.0%
(International/long distance calls are more secure than domestic calls)	Yes	Count	5	13	3	8	29
		%	17.2%	44.8%	10.3%	27.6%	100.0%
Total		Count	35	27	15	28	105
		%	33.3%	25.7%	14.3%	26.7%	100.0%

Table 2 international/long distance calls is more secure than domestic calls?

* Possibility of privacy breaches in traditional telephony is not more than possibility of privacy breaches in VoIP
** Possibility of privacy breaches in traditional telephony is more than possibility of privacy breaches in VoIP

Concern about VoIP privacy (eavesdropping)/security

The majority of the participants neither are concerned about VoIP privacy (eavesdropping) nor about VoIP security.

Participants' concern about VoIP privacy and security is consistent. The majority of those (65.9%) who are concerned about VoIP privacy (eavesdropping) are also concerned about VoIP security, and the majority of participants (67.9%) who are not concerned about VoIP privacy are also not concerned about VoIP security.

It has to be pointed out that in the on-line questionnaire privacy is considered to be eavesdropping and VoIP security is considered as other violating actions such as toll fraud.

Discussing security/privacy issues with service providers

Most of the participants (88.8%) never discussed security/privacy issues with their service provider.

This is in line with participants' most concerned feature when making calls/voice chat. For international calls via PSTN participants are most concerned about lower cost (59%) and least concerned about security (2%). For calls/voice chat via computers participants are most concerned about convenience (51%) and least concerned about security (3%). This indicates that participants either using PSTN or VoIP are least concerned about security.

Comparison of VoIP and traditional telephony from privacy/security perspective

As it is shown in Table 3, more of the participants believe that traditional telephony (landline/mobile) is more secure than VoIP. However, they do not know that the likelihood of privacy breaches in VoIP is more or the likelihood of privacy breaches in traditional telephony (landline/mobile) is more.

This is in line with Patrick's (2009, pp. 14-15) study where myths about VoIP security were addressed. He argues that although it is generally assumed that the traditional phone system (PSTN) is more secure than VoIP, this is not necessarily true. It has to be noted that PSTN security is based on physical security. Therefore, an

eavesdropper can wiretap PSTN by physically accessing telephone lines which is much easier to do than to wiretapping VoIP systems.

Chi-Square value of the relationship: Pearson Chi-Square - Asymp. Sig. (2-sided): .002

Possibility of privacy breaches in VoIP versus traditional telephony			Traditional telephony security versus VoIP security				Total
			Don't know	No*	Same	Yes**	
	Don't know	Count	12	7	2	14	35
		%	34.3%	20.0%	5.7%	40.0%	100.0%
(Possibility of privacy breaches in traditional telephony is not more than possibility of privacy breaches in VoIP)	No	Count	3	6	2	16	27
		%	11.1%	22.2%	7.4%	59.3%	100.0%
	Same	Count	2	3	6	4	15
		%	13.3%	20.0%	40.0%	26.7%	100.0%
(Possibility of privacy breaches in traditional telephony is more than possibility of privacy breaches in VoIP)	Yes	Count	4	13	2	9	28
		%	14.3%	46.4%	7.1%	32.1%	100.0%
Total		Count	21	29	12	43	105
		%	20.0%	27.6%	11.4%	41.0%	100.0%

Table 3 Traditional telephony security versus VoIP security

* Traditional telephony is not more secure than VoIP
** Traditional telephony is more secure than VoIP

CONCLUSION

The findings of this study revealed that the majority of participants are neither concerned about VoIP privacy (eavesdropping) or VoIP security. They also do not expect to have the best facilities and privacy features when using VoIP since VoIP providers generally offer low-cost services. Also, the findings indicate that participants are most concerned about lower cost and least concerned about security when making international calls. However, most respondents who make international calls (either using VoIP or traditional telephony, and either by phone or via computer) are at some level concerned about privacy (eavesdropping). The same trend applies to domestic and interstate calls as well.

For other participants where security/privacy is not a major concern, it is believed that the content of their conversations does not contain sensitive information (calling family, etc.). However, these participants are concerned about security/privacy issues if they are having a business/private conversation.

Most of the participants believe that traditional telephony (landline/mobile) is more secure than VoIP. However, they are not aware that whether the likelihood of privacy breaches in VoIP is more or the likelihood of privacy breaches in traditional telephony (landline/mobile) is more. This does not apply to the majority of the participants who use computers for making calls/voice chat since they believe that privacy breaches are less possible in VoIP than in traditional telephony.

It is commonly believed that, regardless of the used service (VoIP/landline/mobile), privacy breaches are very possible and therefore one should not talk about anything sensitive or important. There is also a widespread belief that conversations are monitored and analyzed by governments for reasons of national security.

There is a relationship between conversation duration and awareness and attitude towards security/privacy issues in VoIP. Those who spend more time talking either by phone or via computers, are more concerned about security/privacy. However, the respondents who prefer computers over landline/mobile for international calls are less concerned about VoIP privacy and vice versa.

REFERENCES

Benini, M & Sicari, S 2008, 'Assessing the risk of intercepting VoIP calls', Computer Networks, vol. 52, no. 12, pp. 2432-2446.

Butcher, D, Xiangyang, L & Jinhua, G 2007, '15-Security Challenge and Defense in VoIP Infrastructures', *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on,* vol. 37, no. 6, pp. 1152-1162.

Cherry, S 2005, 'Seven myths about voice over IP', *Spectrum, IEEE,* vol. 42, no. 3, pp. 52-57.

Dantu, R, Fahmy, S, Schulzrinne, H & Cangussu, J 2009, 'Issues and challenges in securing VoIP', *Computers & Security,* vol. , vol. 28, no. 8, pp. 743-753.

Douglas, CS & Tom, L 2004, 'VoIP Security: Not an Afterthought', ACM Queue, vol. 2, no. 6.

Frost, N 2006, 'VoIP threats - getting louder', *Network Security,* vol. 2006, no. 3, pp. 16-18.

Gupta, P., & Shmatikov, V. (2007). *32-Security Analysis of Voice-over-IP Protocols.* Paper presented at the Computer Security Foundations Symposium, 2007. CSF '07. 20th IEEE.

Kuhn, DR, Walsh, JT & Fries, S 2005, *Security Considerations for Voice Over IP Systems*, National Institute of Standards and Technology, U.S. Department of Commerce, viewed on 10 April 2010, <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>.

Patrick, P 2009, Voice over IP Security, Cisco Press, Indianapolis, USA.

Porter, T 2006, 'Threats to VoIP Communications Systems', in *Syngress Force Emerging Threat Analysis*, Syngress, Rockland, pp. 3-25.

Porter, T, Kanclirz, J, Zmolek, A, Rosela, A, Cross, M, Chaffin, L, Baskin, B & Shim, C 2006a, 'PSTN Architecture', in Practical VoIP Security, eds. P Thomas, K Jan, Z Andyet al, Syngress, Burlington, pp. 91-121.

Stanton, R 2006, 'Secure VoIP - an achievable goal', *Computer Fraud & Security,* vol. 2006, no. 4, pp. 11-14.

Sundquist, J & Service, N 2006, *Top 10 Myths about VoIP*, Epygi Technologies Ltd., viewed on 3 March 2011, <http://www.epygi.com/pdf/WhitePapers/Epygi%20white%20paper%20-%2010%20VoIP%20Myths.pdf>.

Zhu, Y & Fu, H 2010, 'Traffic analysis attacks on Skype VoIP calls', Computer Communications, vol. In Press, Corrected Proof.