한국항행학회 논문지 제13권 제2호 2009년 4월

조직 내부에서의 인스턴트 메시징 보안 정책에 대한 연구

A Study on The Instant Messaging Security Policy in The Organizations

페루자 사타로바[*], 김석수[*], 최민규[*], 조은숙[*], 김태훈[*]

Feruza Sattarova[*], Seok-Soo Kim[*], Min-Kyu Choi[*], Eun-Suk Cho[*] and Tai-Hoon Kim[*]

요 약

현재 인스턴트 메시징은 다양한 분야에서 많은 장점을 제공하고 있기 때문에, 여러 조직 내부에서 여러 상황에 맞추어 새로운 의사소통수단으로 빠르게 변모하고 있다. 긴급한 메시지의 전파, 파일의 전송 등, 인스턴트 메시징은 한 조직의 의사소통체계를 훨씬 용이하게 만들어 주는 귀중한 자산으로 자리매김 할 수도 있으나, 만약 부주의하게 사용된다면, 개인의 사생활을 침해할 수 있을 뿐만 아니라 조직 전체에 악성 프로그램을 유포하는 데 악용될 수도 있다. 본 논문에서는 인스턴트 메시징이 사용되는 방식을 분류하고, 인스턴트 메시징으로 야기될 수 있는 위협요소에 효율적으로 대처할 수 있는 보안 정책을 연구하고 제안하였다.

Abstract

A policy of instant messaging usage is offered in this article. First, a brief introduction of instant messaging system structure is described. The main threats and vulnerabilities of Instant messenger (IM) are described in the second part of the paper. Instant messaging applications offer so many advantages in so many different fields that they're fast becoming the preferred communication tool for a number of different professional scenarios. When properly implemented, instant messaging can be a true asset to the business by making communications easier throughout the organization. If instant messaging is carelessly implemented, though, it can cause problems with privacy and may expose the organization to various forms of malware. The solution offered in this paper is one of the effective ways against threats of IM. However, the system cannot be secured entirely. All we can do is reducing the risks.

Key words : Instant Messaging, Security Policy, Messaging Security

I. Introduction

Nowadays it is nearly impossible to imagine everyday life without Instant Messaging as this service offers many benefits to an ordinary user and organizations. Today more than double the amount of instant messages are sent with comparison to email. Some organizations use instant messaging as their primary communication mechanism. Instant Messaging service offers these advantages: low communication costs, instant response, quicker turn

[*] 한남대학교 멀티미디어 공학부 (Department of Multimedia Engineering, Hannam University.)

· 교신저자(Corresponding Author) : 김태훈

· 투고일자 : 2009년 3월 22일

· 심사(수정)일자 : 2009년 3월 23일 (수정일자 : 2009년 4월 23일)

· 게재일자 : 2009년 4월 30일

around, instant file sharing, collaborative approach. IM as a business tool can be quite effective, but any tool can be abused, especially if unmanaged. When properly implemented, instant messaging can be a true asset to the business by making communications easier throughout the organization. If instant messaging is carelessly implemented, though, it can cause problems with privacy and may expose the organization to various forms of malware [2].

To understand the threats and vulnerabilities of IM we must know how it works first. While instant messaging may seem like a new technology, it is actually decades old. The first system, IRC, was developed in 1988 by Jarkko Oikarinen. Still in use, this system allows users to form ad-hoc discussion groups, chat with one another, and exchange files. Since the introduction of IRC, many new IM systems have been launched; for example, ICQ, AOL Instant Messenger, MSN Messenger, and Yahoo Messenger. While each of these offers different features, they all provide the same basic zxservice: peer-to-peer real-time chatting and file transfer capabilities. Virtually all IM systems employ the same basic client-server architecture. Users install instant messaging clients on their client machines―-desktop computers, wireless devices, or PDAs, for example―and these clients communicate with an IM server in the messaging provider's infrastructure to locate other users and exchange messages. In most instances, messages are not sent directly from the initiating user's computer to the recipient"s computer, but are sent first to an IM server, and then from the IM server to the intended recipient. (See Fig. 1.)

While most instant messaging systems use centralized servers to transmit all messages, some systems do offer peer-to-peer messaging. In such a model, clients contact the IM server to locate other clients. Once the client chat program has located its peer, it contacts the peer directly. (See Fig. 2.)

The peer-to-peer scheme offers better security than the client-server client scheme (shown in Fig. 1.) when both users are on the same local area network because messages do not travel over the Internet. However, if one user is located outside the corporate network, messages sent between machines are exposed to potential eavesdroppers, just as in the client-server-client scheme [1].

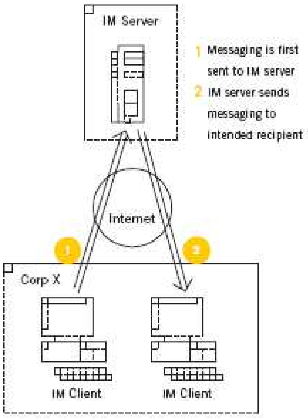
IM Server
1 Messaging is first sent to IM server
2 IM server sends messaging to intended recipient
Internet
1
2
Corp X
IM Client
IM Client

Fig. 1. Client-server instant messaging [2]

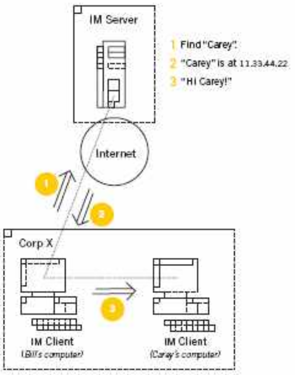

Fig. 2. Peer-to-Peer instant messaging [2]

Ⅱ. Threats and Vulnerabilities of Instant Messaging

Instant messaging is useful at work for these reasons: informal, friendly and quick, it can facilitate fast answers to questions and strengthen good will at the same time. But instant messaging also has several down sides. It can be a major time-waster and distraction. But more importantly, it adds vulnerability to the informational environment. Vulnerability is increased in several ways.

Firstly, there is an array of malicious programs designed to attack IM protocols. Secondly, vulnerabilities in the client program make it a target for hackers. Thirdly, confidential information sent over IM is easy pickings for competent and motivated people who want it. Add to the mix a disgruntled or disloyal company employee with a will and a way to transfer confidential data out via IM, and the reasons why you should start worrying right now become compelling.

Sybari's survey revealed that the majority of companies questioned are extremely aware of the benefits that instant messaging can bring to their business with over 81% listing real-time communication as a main advantage. On average, those questioned estimated that IM would decrease their phone bills by approximately 11%.

Just under 90% understood that IM should be managed at server level, with 77% expressing concern over potential security threats attached to IM communication. However, in spite of the fact that their employees may be installing their own choice of IM applications (ie Skype, MSN, Yahoo), more than 56% had no plans to install an IM solution at a managed server level.

Three-quarters of businesses saw the threat of viruses and worms through instant messaging as a primary concern. This was closely followed (68%) by those who were worried about information theft and loss of sensitive data or information that would have an 'extreme impact' on their business, especially those who are aware of compliance with government and industry regulations and legislation. Moreover, 54% of the companies surveyed were concerned with making sure that their employees' computers were not vulnerable to remote controlling 'hijackers', and 40% were concerned about IM conversation spying.

Surprisingly, only 13% of those surveyed cover IM usage in their current corporate e-mail usage guides. Over 55% do not include IM and 28% do not currently have a corporate messaging policy of any kind [2].

Fig. 3. shows the chief threats connected with IM usage. The leak of confidential information(42.3%) takes pole position with risks arising from virus attacks and improper use of IT resources attracting around a fifth of the votes each. Spam and advertising garnered 10%. Only 7.6% of respondents considered IM usage free from risk.

The introduction of a robust information security policy is, perhaps, the simplest means of reducing risk from IM. Despite this, 62.0% of respondents stated that their companies did not have such policies in place with only 14.9% of respondents regarding their companies' policies as effective. Multiple answers were permitted [3].

So what can be done to reduce the risks? Here are some solutions:

1. Establishing Security Policy of IM usage.
2. Monitoring IM traffic for policy compliance.
3. Installation of Firewall or local Anti-virus software, which is managed centrally.
4. Enabling encryption for transmission of confidential data.
5. Isolating corporate IM system.

However it is impossible to secure system entirely. All we can do is to reduce the risks.

In the next part of our paper we offer the Instant Messaging Policy which can be implemented to an organization.

Ⅲ. Proposition of Policy of Instant Messaging Usage

The proposed policy consists of seven parts: content, scope, purpose, policy, definitions, rules, and policy update and notifications. You can insight the Policy below.

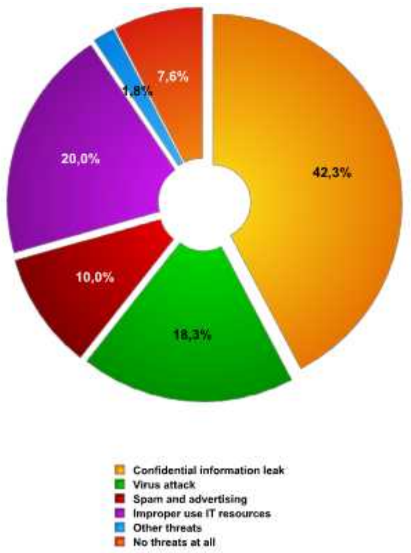

Fig. 3. Threats arising from IM usage

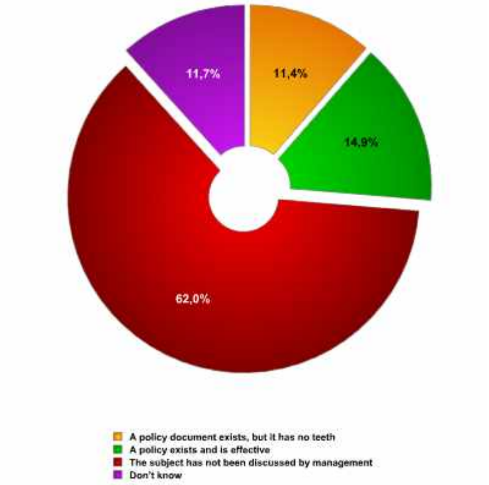

Fig. 4. IM-policy enforcement across the company

3-1. Instant Messaging Policy

I. Content

1. Scope. 2.Purpose. 3. Policy. 4. Definitions. 5. Rules. 6.Policy update and Notifications.

II. Scope. This policy applies to all Users of Company X.

III. Purpose. This policy describes the rules concerning to the use of Instant Messaging technology in a Company X to protect Company X from technology abuse and misconduct. The rules described in this policy outline the limitations of the use of this technology, protect company information, and describe the expectation of privacy when using the company provided system.

IV. Policy. Internet, intranet, and extranet-related systems, including but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, World Wide Web browsing, IM, and FTP are the property of Company X. These systems are used exclusively for business purposes in serving the interests of the company, our clients, and our customers in the course of normal operations. The use of Instant Messaging technology is limited to the capabilities provided by company on internal network services. Users must use the Instant Messaging service provided in a manner that protects company assets and Confidential Information.

V. Definitions. 5.1. IM - Instant Messaging: A technology that gives users the ability to identify people online and to exchange messages with them in real time. The instant messaging system alerts you whenever someone on your "buddy list" is online and is trying to contact you via your computer. You can then initiate a chat session with that person and type text messages back and forth. 5.2. Technology resources - Company X's technology resources comprise of computing, networking and software applications that can be accessed by authorized Company X users. 5.3. User -Anyone with authorized access to Company X's technology resources including permanent and temporary Usersor third party personnel such as temporaries, contractors, consultants, and other parties with valid Company X access accounts. 5.4. VoIP - Voice over Internet Protocol (VoIP): An application that encodes and digitizes a voice signal, converts the signal to data packets, and transports the packets over a data network running Internet protocol (IP). 5.5. Chat - A real time conferencing capability between two or more users on a local network (LAN) or on the Internet. 5.6. Confidential Information - Any information that meets any of the following criteria, whether in electronic or print media, oral or written: protected health information; sensitive information; proprietary information; certain employment-related records and information specifically protected under federal or state law; provider and facility credentialing and re-credentialing information and records; third party information, data, software, manuals and other materials that company has agreed to maintain in confidence pursuant to a written contract or nonagreement, information otherwise protected by state or federal law. 5.7. Hired employee - A person who is hired to work for a Company for a certain short time, or a person who is in his/her probation period.

VI. Rules. 6.1. Users are prohibited from downloading and using personal, consumer-grade IM software (ex..AOL Instant Messenger, Yahoo Messenger, or MSN) to transmit messages via the public Internet. The type of allowed IM software is decided by a Company security administration. Use of any other external IM provider is prohibited. Users who violate this rule are subject to termination. 6.2. Use of the company Instant Messaging service is for business purposes only. No personal use of the Instant Messaging service is permitted. 6.3. Information sent or received via the company Instant Messaging service is stored for 14 days only. 6.4. All IM traffic must go through an IM proxy. Access to the IM proxy must be approved by the employee's manager. 6.5. Users should be aware that any data (such as IM user list, message content, etc.) they create on corporate systems remains the property of Company X. Only users with a supervisor's prior documented approval can use IM. 6.6.All IM communications and information transmitted, received, or archived in the company's IM system belong to the company. 6.7.Users have no reasonable expectation of privacy when using the company s IM system. 6.8.The company reserves the right to monitor, access, and disclose all employee IM communications. 6.9.Always use professional and appropriate language in all instant messages. 6.10. Users are prohibited from sending abusive, harassing, threatening, menacing, discriminatory, pornographic, disrespectful, or otherwise offensive instant messages. 6.11. Users are prohibited from sending offensive jokes or materials, rumors, gossip, or unsubstantiated opinions via IM. 6.12. Users may not use IM to transmit confidential, proprietary, personal, or defamatory statements and embarrassing information about the company, Users, clients, business associates, or other third parties. 6.13.Users may not share confidential, proprietary, or potentially embarrassing business-related or personal IMs with the media, competitors, prospective employers, or other third parties. 6.14. Illegal use of IM may include, but not limited to: obscenity, child pornography, threats, harassment, theft, and violation of copyright, trademark, or defamation laws. 6.15. Users are to share their IM usernames with colleagues strictly on a need-to-know basis. 6.16. A user may not save or publish another user's message(s) or attachment(s) unless authorized. 6.17. Hired employees can not be provided with or given access to confidential information of the company.

6.Policy update and notification. Company X reserves the right to revise the conditions of this policy at any time by giving notice. Users are responsible for understanding or seeking clarification of any rules outlined in this document and for familiarizing themselves with the most current version of this policy.

We have read Company X's IM policy and agree to abide by it. We understand that violation of any of the above policies and procedures may result in discipline, up to and including my termination.

After reading the Policy a user signs it and puts the date.

3-2. Implementation of the Instant Messaging Policy to a Company

The IM Policy offered in this article can be implemented to protect a Company from technology abuse and misconduct. But can a Company apply this policy to the employees that were hired for a Company for a short period or for a person who is in a probation period in that company? Yes. The offered policy can be applied to a hired employee too. But to protect the confidential information of a Company, a hired employee cannot be given access to any confidential information of the company. This rule is given in 6.17 section of the policy.

The 6.1. point of the Policy prohibits users from using personal consumer-grade IM software. The studies show that [4] most IM software are of high vulnerabilities and risks, because they were created for home users initially not for business purposes. It is easy to hack that software and loose confidential information exchanged via that IM software. It is recommended to use IM created for business purposes. The 6.2. section allows users to exchange information via IM only with business purposes. IM can be useful for the activity of a Company, but also it can harm it too [5]. If used properly it will probably lead to the first expectation. It is better to prohibit the personal use of IM because it leads to the lost of company resources such as time, IT resources, energy and others. Sections 6.3-6.17 refer to the terms of company security terms and privacy. Company has a right to monitor all traffic and information exchanged by its employees. The employees who violate the rules are subject to termination.

Ⅳ. Conclusions

This work has presented a Policy for Instant Messaging usage that can help to improve the effectiveness of using IM within the organization and reduce it's vulnerabilities and leakage of confidential information.

Acknowledgement

This paper has been supported by the 2009 Hannam University Research Fund.

References

[1] Semantyc Enterprize Security "Securing Instant Messaging" white paper. www.semantyc.com

[2] "Security Threats of Instant Messaging" Camsoft Solutions, Johannesburg, 18 May 2005, http://www.camsoft.co.za

[3] Alexey Dolya, "Instant Messenger: making business friendlier but less secure", August 20, 2007. http://www.viruslist.com/en/analysis?pubid=204791959#i3

[4] Gunter Ollmann "Instant Messenger Security: Securing Against the Threat of Instant Messengers" Aug 16, 2006, http://www.windowsecurity.com/whitepapers/Instant-Messenger-Security.html

[5] Ricky M. Magalhaes "Instant Messaging: Friend or Foe?" Nov 05, 2008 , http://www.windowsecurity.com/articles/Instant-Messaging-Friend-Foe.html?printversion

Feruza Sattarova Yusufovna

2003-2007 B.S., in Economics and Management, Tashkent University of Information Technologies.
Currently, M.S., in Multimedia Engineering, Control and Assurance Laboratory, Hannam University.
Research interests : security, insider threats, innovation, security assurance, SCADA

Seok-soo Kim

1989 Received a B.S. degree in computer engineering from Kyungnam University , Korea.
1991 M.S. degree in Information engineering from Sungkyun-kwan University, Korea.
2002 Ph D. degree in Information engineering from Sungkyun-kwan University, Korea.
2003 professor in Department of Multimedia Engineering, Hannam University.
Currently, Member of KCA, KICS, KIMICS, KIPS, KMS, and DCS. He is Editors in Chief of IJMUE.
Research interests : Multimedia Communication systems, Distance learning, Multimedia Authoring, Telemedicine, Multimedia Programming, Computer Networking. Information Security.

Min-kyu Choi

2008 B.S. degree in Department of Multimedia, Hanam University
Currently, M.S. candidate in Department of Multimedia, Hanam University
Research interests : information security, security evaluation, information assurance

Eun-suk Cho

1994 Associate in Dept. of Nursing Science, Suwon Women Colleage.
2000 B.L. in Dept. of Law, Korea National Open University
2003 Ed. M. in Dept. of Education, Ajou University
Currently, Integrated Course for M..S and Ph.D. in Dept. of Multimedia Engineering, Hannam University.
Research interests : Hospital Security, Patients' privacy, U-healthcare system.

Tai-hoon Kim

1995 B.S., 1997 M.S., 2002 Ph.D. degrees in Electric, Electronic, and Computer engineering, Sung Kyun Kwan University.
1996~1999 Researcher, Technical Research Institute sindoricoh.
2002~2004 Senior researcher, Korea Information Security Agency.
2006~2007 Research professor, Ewha women university.
Currently, assistant professor, Hannam university.
Research interests : information security, security evaluation, information assurance