Analyzing Feasibility of Providing Secured Encrypted Email Service

Sudhir Chawla, Angelo State University, sudhir.chawla@angelo.edu , (325) 942 2383
Management & Marketing Department, Angelo State University, San Angelo, TX 76909

Parag Dhumal, Angelo State University, Parag.Dhumal@angelo.edu, (325) 942 2383
Management & Marketing Department, Angelo State University, San Angelo, TX 76909

ABSTRACT

Consumers consistently send and receive numerous emails a day without much thought about what they receive and what happens after they click the send button. Such email communication faces possible dangers from viruses, phishing, fake emails, spam, and eavesdropping. Customers can be protected from such possible dangers if they use a secure and private encrypted email service. This study was conducted to find out feasibility of providing a new secured email service.

Research methodology includes thorough analysis of two focus groups followed by survey of email users to find out how much people know and care about privacy of their emails, how much they are willing to pay if such service is offered and how can you reach to them. Based on survey responses we conduct thorough analysis to provide recommendations.

Key words: Email Security, Feasibility Analysis

INTRODUCTION

Millions of emails are sent everyday throughout the United States and the world. People consistently send and receive numerous emails per day without much thought about what they receive and what happens after they click the send button. Email communications over internet consistently faces possible dangers from viruses, phishing, fake emails, spam, and eavesdropping [1, 2].

Email users can be protected from possible dangers if they use a secure and private encrypted email service [3]. But such service will cost the users. Do the users have enough knowledge about possible dangers of using unsecured email? Do they believe their information is worth the price they have to pay for secure email service? And how much they are willing to pay? Thus a study was conducted to find out feasibility of providing a new secured email service.

LTURATURE REVIEW

Internet has accelerated the process of globalization. It connects the people and businesses worldwide and continues to bring them closer [4]. Email provides one of the quickest modes of communicating large amount of information inexpensively over internet. Due to its benefits use of emails has drastically gone up in the last decade. People are sending more and more information via email. It has also become official channel of communication between government agencies, businesses and customers. As the use of email has gone up the possible dangers from viruses, phishing, fake emails, spam, and eavesdropping is continuously increasing. Spam or "junk mail" refers to unsolicited emails sent in bulk, usually trying to sell a product or service that the receiver of the email has no interest in [5, 6]. Computer viruses are tiny software programs that replicate themselves and spread from one computer to another and effect the operation of an infected system [7]. In 2003, nine of the ten top viruses that year were spread through email. Phishing involves the use 'spoofed' emails to lead consumers to counterfeit websites [8]. Fake email refers to send an email that looks like it is coming from somewhere or someone that it is not. Unencrypted and unsecure email servers can leave email messages open to eavesdropping or snooping by various sources.

Due to such possible dangers use of emails is decreased among businesses. According to survey by Pew Internet and American Life Project, 22% of respondents reduced the use of e-mail while 67% stopped using it. People are concerned that computers and technology is able to invade their privacy. One of the survey found that 54% of the respondents express at least some degree of anxiety about this. More concern is expressed about financial data than any other type of data. They also found that people who go online are no more concerned about this than those who don't [9]. Due to increasing threats to the privacy and security of customer information sent via email we see the potential for developing and providing secured encrypted email service. But the feasibility of offering such service needs to be thoroughly analyzed because such service will cost users. Even though people are concerned about security they may not necessarily want to pay for it is available free of charge through internet service providers or from companies like Yahoo, Google. To find out how much people know and care about privacy of their emails, how much they are willing to pay for secured email and how can you reach to them this study was conducted. Research methodology of this study is explained in the next section.

METHODOLOGY

Two focus groups were conducted to gather information of participants' general feelings about internet and email security and privacy. The questions were open ended and participants were encouraged to expand on their thoughts of the various subjects

discussed. This was followed by email survey. Survey instrument was prepared based on purpose of study, past literature and focus group results. Survey questions were close ended and data gathered is used for statistical analysis.

RESULTS AND CONCLUSIONS

Survey and focus group results and recommendations for providing secured encrypted email service will be presented in the conference.

REFERENCES

[1] Sunner, M. (2005). Email security best practice. *Network Security, 2005*(12), 4-7.

[2] Steele, S., & Wargo, C. (2007). An Introduction to Insider Threat Management. *Information Systems Security*, *16*(1), 23-33.

[3] Larkin, E., & Philips, M. (2007). How to Protect E-Mail From Prying Eyes. *PC World*, *25*(12), 70.

[4] Parameswaran, M., Xia, Z., Whinston, A., & Fang, F. (2007). Reengineering the Internet for Better Security. *Computer*, *40*(1), 40-44.

[5] Wang, C., & Chen, S. (2007). Using header session messages to anti-spamming. *Computers & Security*, *26*(5), 381-390.

[6] Kang, L., Zhenyu, Z., & Ramaswamy, L. (2009). Privacy-Aware Collaborative Spam Filtering. *IEEE Transactions on Parallel & Distributed Systems*, *20*(5), 725-739.

[7] Heron, S. (2008). Parasitic malware: The resurgence of an old threat. *Network Security*, *2008*(3), 15-18.

[8] Forte, D. (2009). Anatomy of a phishing attack: A high-level overview. *Network Security*, *2009*(4), 17-19.

[9] Attitudes toward the Internet and Technology –Section V. (1999). *Pew Research Center.* Obtained through the Internet: http://people-press.org/reports/display.php3?PageID=342 [accessed 09/30/2009]

[10] Horrigan, John B. (2005). Broadband Adoption at Home In the United States: Growing But Slowing. *Pew Internet and American Life Project*. Obtained through the Internet: http://www.pewinternet.org/Reports/2005/Broadband-Adoption-in-the-United-States-Growing-but-Slowing/Report/1-Executive-Summary.aspx?r=1 [accessed 09/30/2009]

[11] Federal Trade Commission – Identity Theft Survey Report. (2003). Synovate. Obtained through the Internet: http://www.ftc.gov/os/2003/09/synovatereport.pdf [accessed 09/30/2009]

[12] Ye, R., Zhang, Y., Dat-Dao, N., and Chiu, J. (2004). Fee-Based Online Services: Exploring Consumers' Willingness to Pay. *Journal of International Technology and Information Management*, Obtained through the Internet: http://www.iima.org/JITIM/JITIM%2013%20Downloads/P12-Ye.pdf [accessed 09/30/2009]

[13] Huberman, B., Adar, E., & Fine, L. (2005). Valuating Privacy. *IEEE Security & Privacy*. Obtained through the Internet: http://www.hpl.hp.com/research/idl/papers/deviance/deviance.pdf [accessed 09/30/2009]

[14] Is your privacy important? Are you losing it? (2008). MSNBC. Obtained through the Internet: http://www.msnbc.msn.com/id/14850268/ [accessed 09/30/2009]