Securing Risks of Electronic Mail Based on the Type of Organization

Seyyed Hossein Raja

***Abstract*—E-mail technology, has become one of the requirements of human lives for correspondence between individuals. Given this, the important point is that the messages, server and client of e-mail and correspondences that exchanged between different people have acceptable security, to make people sure to use of this technology. In the information age, many of financial and non financial transactions are done electronically, data exchange takes place via the internet and theft and manipulation of data can make exorbitant cost in terms of integrity, financial, political, economic and culture. E-mail correspondence in there is same and it is very important. Email risks and methods of securing them has been studied by different people, but the question of how to set up security for your organization's e-mail and securing which of risks has not been investigated so far. Because of our national view, in this paper we use the categories provided by the institute of information technology of Iran. We combine these categories and list of the risks, then we have offered new classification of securing risks of e-mail based on the type of organization.**

***Index Terms*—Email, security, risks of email, organizations and security of email, securing email.**

I. Introduction

With advances in computer science and entering the arena of computers, man created a new system for corresponding. The new system was the same of paper mail but its speeds is much higher than the former. In the new system that we discussed, security in the messages of correspondence that exchanged and system security is very important. The difference between traditional system and electronic system is that the importance of security in the new system increased[1].

In the field of email, there are different protocols and mechanisms and these protocols and mechanisms can contain various risks. The important thing is that:

- Know the risks.
- How can we secure these risks through existing mechanisms and reduce risk.
- Securing list of risks with regard of type of organization.

In this paper after studying the attacks and their results, Risks of e-mail server and service have examined and the methods of securing these risks have outlined.

In continue regarded to classification of organizations based on common divided by the Institute of Information Technology of Iran (fata) are discussed.

Finally, according to the type of organization, we have offered solution of securing email risks of that organization.

Manuscript received Februray 13, 2012; revised April 22, 2012.

S. H. Raja is with the DSP Research Institute, Tehran, Iran (e-mail: hosseinraja@dspri.com).

In the area of Identification of e-mail risks, Richard Bulm[2] and Curtis Smith[3] have provided a list of risks.

Stone burner and his colleagues in the field of risks of IT-based systems have offered assessment formula that many people using this formula. This formula uses two parameters: impact and overall probability[4].

This formula is presented in the form of recommendation from the NIST organization and different people use the formula provided with changed parameters in the same way. For example, in field of software and network security, McGraw presented a formula that uses two parameters: single loss expectancy and annualized rate of occurrence. It is actually renamed the parameters in the formula presented by Brenner and his colleagues.

Of course there are people that using other formulas and additional parameters. For example, in SQL injection attacks Madan and his colleagues have proposed a formula for risk assessment that have five parameters: Damage Potential, Reproducibility, Exploitability, Affected User and Discoverability[6]. Cisco IPSs assessing the risks in its 4200 series of three parameters: intensity, loyalty and uses the value of score [7].

Convery have offered formula for calculating a network known risks such as flood planning attacks, tampering, counterfeiting and other common attacks[8]. This formula uses four parameters: hardness, ease of use, frequency and impact.

In the field of classifying organizations in terms of performance, different categories of individuals are presented. But because of our national view in this paper we have used the categories provided by the information technology of Iran Institute[19].

We combine these categories and list of the risks, and we have offer new classification of securing risks of e-mail based on the type of organization.

II. Attacks

Generally attacks can't be classified into precise form. Most of categories in a way that attacks can be placed in one class, or can't placed in one class[8]. However, in this research is necessary to classify attacks, because in the field of security without having a comprehensive classification of security attacks, we cannot determine whether or not it is a safety plan.

For this reason, with study and work on existing attacks have provided the following main categories:

- Read: Gain access to unauthorized information
- Manipulate: Modify information
- Spoof: Provide false information or offer false services

- Flood: Overflow a computer resource
- Redirect: Change the flow of information
- Composite: Comprise more than one listed method

Attack Results. All attacks have specific attack results that can be categorized as one of five types[8]:

- Disclosure of Information: Disclosure of information is the dissemination of information to anyone not authorized to access that information. This includes sniffing passwords off the wire, reading parts of a hard disk drive you are unauthorized to access, learning confidential information about your victim, and so on.
- Corruption of Information: Corruption of information is any unauthorized alteration of files stored on a host computer or data in transit across a network. Examples include website defacement, man-in-the-middle (MITM) attacks, viruses that destroy data, and so on.
- Denial of Service**:** Denial of service (DoS) is the intentional degradation or blocking of computer or network resources. Most types of flooding attacks have DoS as a primary objective. Similarly, intentionally crashing network resources can create a DoS condition, as would reconfiguration of certain network devices.
- Theft of Service: Theft of service is the unauthorized use of computer or network services without degrading the service to other users. Stealing someone's password and logging on to the network is a good example, as is accessing a wireless LAN without authorization or pirating software.
- Increased Access: Increased access is the resultant unauthorized increase in user privileges that occurs when accessing computer or network services. Executing a buffer overflow attack is a good example of an attack resulting in increased access.

III. Email Risks and Their Secureness

There are many risks to electronic mail that categorized in two types: Risks for email server and risks for email service.

In the below we explain these risks and methods for securing them. The first four risks are related to the mail server and the next four risks are related to the mail service.

Network attack and network access Risks. One common rule of thumb in the network world is that if your server is connected to a network, someone will try to break into it. Even with servers connected to local area networks (LANs) protected by firewalls, you must always be on guard against intruders originating in your own organization. The first step in protecting the mail server is to disable any network services that are not being used. The inetd program is a single network program that listens for any network connection requests from remote clients. If a connection request is identified, a specific application is called by inetd and the connection is passed off to the application. By default, the inetd program supports many different types of network services, many of which are not necessarily needed on a mail server. It is a good idea to disable any services you are not using to decreases the chance that a hacker can use them to break into your server.

For more security we should disable risky commands and installing firewall and ID/PS in our email system[3].

Open Relay Risk. When a mail server automatically passes a mail message from a remote client to the proper destination mail server (other than itself), it is called relaying. When a mail server relays any message from any remote client to any remote host, that mail server is called an open relay[9].

Open relays were useful in the early days of the Internet, but they too were abused just as other components of the Internet. It didn't take long before people found out that by relaying messages through an open relay, you could easily mask the origin of the message from the recipient. Using this feature, many commercial mass marketers send out thousands of unsolicited commercial e-mails (UCE).When victims receive them, it is often difficult to track the messages back to a source e-mail address.

Because of this, most open source e-mail packages have implemented limited relaying. Instead of relaying messages from all clients, only a preconfigured subset of clients are allowed to relay messages. Any other client attempting to relay a message is blocked.

Spam Risk. As mentioned in the preceding section, UCE mail is the less controversial term for unwanted e-mail advertisements. The term UCE is often found in technical literature addressing the issue, but the more common name for UCE is spam[10].

Although most people are glad to avoid receiving spam messages, mail administrators must walk a fine line when trying to reduce spam on their mail server. An overzealous mail administrator can block out legitimate messages as well as spam messages. There are a few different techniques used to block spam[11]:

- Block messages from known spam hosts.
- Block messages with known commercial subject headers.
- Block messages from hosts listed in a worldwide spam database.
- Accept messages only from known hosts.

Installing anti-spam solutions such as SpamAssasin can also be good in preventing attacks[12].

Virus Risk. The greatest fear of the Internet community is the plague of destructive viruses. A single virus can delete any or all files on the computer, often without the user knowing what is happening.

Although the mail server itself is not normally susceptible to viruses, it can be used as a tool to help block viruses from being transmitted via e-mail to unsuspecting users.

For controlling spams, there are many methods commonly used to help block e-mails with virus[13]:

- Block all messages with a known virus subject header.
- Perform a virus scan on all mail attachments.
- Block all messages that contain an attachment.
- Block all messages with a particular type of attachment.

Risk of abuse of some commands. Hackers and

spammers are using various techniques to get information about your mail system and its users, but there are techniques that can help you to fight this problem.

With disabling some commands and also installing a firewall in front of mail system you can stop attacks and exploration to the mail system.

Risk of abuse of mail header. With abusing of e-mail headers that can be forged generating email spam and acting as open relay can be proceeded.

Another popular method of allowing remote hosts to relay messages through the e-mail server is to use an authentication method. The authentication method can uniquely identify the remote mail server so that your mail server can determine whether it is allowed to relay messages.

SASL is one of the most famous methods to confirm the identity of network connections[14,15].

Risk of being unsafe of IMAP and POP3 Servers. Many of MTA packages uses POP3 or IMAP protocols to receive messages [16,17]. The problem with these protocols is that they transfer messages across the network using plain ASCII text, which could leave your users vulnerable to network snooping by others.

To help alleviate the problem of sending plain text across the network, the Secure Socket Layer (SSL) family of protocols has been developed. SSL allows network hosts to encrypt data before sending it across the network and allows the receiving host to decrypt the data back into its normal form. By using SSL, you can create a more secure environment for your users to send and receive their mail messages[18].

Risk of insecure webmail. The increase in popularity of the World Wide Web has spawned a new line of software products in many areas. Programmers are finding that using a Web-based interface increases the usability of their programs. Most users already know how to navigate around Web pages, so little if any user training is needed to use standard Web page controls such as hot links, drop-down lists, and control buttons. E-mail client software is no different. Many companies have realized that by using Web based e-mail client software, users can access their mail messages with little training and are able to access their mailboxes from a wider variety of computers (such as laptops for mobile users).There are many popular Internet Webmail implementations, such as Hotmail and Yahoo!, where users can connect to the mail server using only their Web browsers.

Users can use any standard Web browser to access messages stored in their mailboxes. Additionally, with most Web-based e-mail packages, users can create folders and store messages on the mail server in separate folders. By maintaining mailbox messages on the server, users can read all their messages from any computer, almost anywhere[3].

Webmail is not secure in itself. To secure webmail, web server and database server must be secured and we can use SSL for communications.

The most important ingredient for a secure Webmail server is, of course, a secure Web server.The Apache open source Web server software is the most popular Web server software available for the Unix platform. The Apache project has also produced quite a number of plug-in modules that add functionality to the basic Web server product. One of these modules is mod_ssl. It is used for incorporating the SSL protocol into the standard Web server software, providing a secure method to transfer data between the client and the Web server[2].

IV. Securing Risks based on the Type of Organization

According to the division of Institute of information technology of Iran four categories of executive agencies, national organizations, sensitive organizations and executive vital organizations are exist[19].

Classification conducted by the Institute of ITof Iran have been divided into four categories: Executive, National, sensitive and Executive vital. With using this classification in terms of security organizations can put their e-mail in the following groups:

- E-mail with medium security for executive agencies.
- E-mail for national organizations with high security
- E-mail along with high security and privacy for sensitive and executive vital organizations

E-mail with medium security for executive agencies. Email security is not very important in these organizations and they only send and receive email just for individual use. Executive agencies and environments that email security are less important are in this category.

The important issue here is securing email server not securing email service. This is because we want the server persisting and continue to work. However the message content to stay safe or someone abuses IMAP or POP3 protocols and others can read the message does not matter too much.

If the virus can affect the whole server, the server will break down; or if the volume of open relay or spam to be somewhat that DOS attacks take, the server will break down. Because these reasons we recommended that to secure the following risks:

- Risks of network attack and network access
- MTA packages risk
- Open relay risk
- Spam risk
- Virus risk

E-mail for national organizations with high security. Email security is important in these organizations and take the letter to be sent and received is not sufficient for the users. National organizations belong in this category.

The important issue here is to provide security for email server and email services. Because In addition to we want the server work continues, we want the email service is not misused. But here the message confidentiality it is not necessary for everyone. Because these reasons we recommended that to secure the following risks:

- Risks of network attack and network access
- MTA packages risk
- Open relay risk
- Spam risk
- Virus risk
- Risk of abuse of some commands
- Risk of misuse of the mail header
- Risk of insecure webmail

E-mail with high security and privacy for sensitive and executive vital organizations. Email security in these organizations is very high importance and safety of the mail server and the mail service is not enough. Emails of security and military organizations and confidential e-mail letters of government agencies are in this category. Sensitive and executive vital agencies are in this group.

The importance in here addition to server and service security is confidentiality of your email messages. Because these reasons we recommended that to secure the following risks:

- Risks of network attack and network access
- MTA packages risk
- Open relay risk
- Spam risk
- Virus risk
- Risk of abuse of some commands
- Risk of misuse of the mail header
- Risk of insecure webmail
- Risk of being unsafe of IMAP and POP3 Servers
- Risk of being unsafe to content of messages

V. Summary

In this paper, we discuss about securing risks of email based on the type of organization. Email risks and methods of securing them has been studied by various individuals, but the question of how to set up security for your organization's e-mail and securing which of risks has not been investigated so far. Because of our national view, in this paper we use the categories provided by the institute of information technology of Iran(fata).

With use of classification provided by the Institute of information technology of Iran(fata) and combining it with a list of existing risks we have offered new approach to secure e-mail risks according to the type of organization.

References

[1] M. Ferris ,"New email security infrastructure", IEEE Conferences , 1994 , Page(s): 20 – 27.

[2] R. Bulm, "Open source e-mail security,", Sams, 2002.

[3] S. Curtis, "Pro open source mail: Building an enterprise mail solution", apress, 2006

[4] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30, July 2002

[5] G. McGraw, "Software security," *IEEE Security and Privacy*, vol. 2, no.2, 2004, pp. 80–83.

[6] S. Madan, "Bulwark against SQL injection attack–An unified approach," *IJCSNS International Journal of Computer Science and Network Security*, vol.10, no.5, May 2010

[7] Cisco Systems Learning,"Implementing Cisco Intrusion Prevention Systems Volume 1 Version 6.0", Cisco Press, 2006

[8] S. Convery, "Network security architectures," *Cisco Press* ,2004

[9] P. Piazza, "Closing open relays to spammers,"Tech Talk, Jul 31, 2005

[10] S. Shirali-Shahreza, A. Movaghar, "A new anti-spam protocol using CAPTCHA", *IEEE Conferences* , 2007 , pp. 234 – 238

[11] F. Faure, M. Lopusniac, G. Richard, M. Farmer, "A complexity-based method for anti-spamming," *IEEE Conferences* **,** 2007 , pp. 315 – 320

[12] A. McDonald, "SpamAssassin: A practical guide to integration and configuration",packt,2004

[13] J. Stanger, "E-mail virus protection handbook : Protect your e-mail from viruses, Trojan horses, and mobile code attacks," Syngress,Oct 30, 2000

[14] K. Zeilenga, " Anonymous simple authentication and security layer (SASL) mechanism," RFC 4505, June 2006

[15] A. Melnikov and E. Zeilenga, "Simple Authentication and Security Layer (SASL)," RFC4422, June 2006

[16] J. Myers and M. Rose, "Post Office Protocol - Version 3", RFC 1939, May 1996

[17] M. Crispin, "INTERNET MESSAGE ACCESS PROTOCOL – VERSION 4rev1", RFC 3501, March 2003.

[18] R**.** Oppliger**,** "SSL and TLS: Theory and Practice (Information Security and Privacy)" , Artech House,Sep 30, 2009

[19] Institute of Information Technology of Iran , July 2012, http://www.itc.ir