A SMS Based Security Providing for an Email ID by Creating an Email Server

R. Kaviarasi[1], S. Anitha[2] and K. Suganya[3]

**[1]AP, Department of Computer Applications,
Bharathidasan Institute of Technology, Anna University,
Tiruchirappalli**

**[2]PG Student, Department of Computer Applications,
Bharathidasan Institute of Technology, Anna University,
Tiruchirappalli**

**[3]PG Student, Department of Computer Applications,
Bharathidasan Institute of Technology, Anna University,
Tiruchirappalli**

Abstract

Email is a method of exchanging digital messages from an author to one or more recipients. Email communication is responsible for spreading the majority of virtual infections and poses one of the greatest security risks for companies today. Furthermore, unprotected email messaging also violates compliance regulations in terms of sending highly sensitive information over the Internet. The users' fears of losing control of their own email id information data can become a significant barrier to the wide adoption of mail services. In this paper we protects the email id from unauthorized access and inspection by sending the information about the email id details such as IP address of recently visited system with date, time and also the location, to user mobile device as message by using the SMS gateway. Thus way the user can able to know about the email account information. It is one of the efficient ways to protect the email id.

Keywords- Email Server, SMS, Email Security, A SMS Based Security Providing for an Email ID by Creating an Email Server(SPECES), Mobile Phone, SMS gateway.

I. Introduction

Email security is increasingly moving away from a focus on a single type of protection, such as antivirus, toward a focus on broad protection from a wide range of emerging threats to enterprise security. While antivirus software remains the foundation of email security, emerging threats are forcing organizations to approach email security with a more comprehensive solution. Corporate concerns about spam, viruses, worms, legal liability, regulatory compliance, and employee productivity are driving the need for a more complete solution. Moreover, there is an increasing need for integration between individual security technologies in order to reduce the cost and time associated with managing point products.

The current design of some email systems make them difficult to use for SMB applications. For example, while some email server products are adding functions—such as support for PDAs, smart phones and team collaboration—their growing administrative complexity plus their increasing requirements for more powerful hardware and the newest operating system software can exceed the IT expertise and budgets of smaller organizations. In fact, the complexity of some email servers often requires at least one full-time employee dedicated to installing, monitoring, maintaining and updating the system, adding the overhead of an employee to the other monthly capital expenses.

On the opportunities side, more developers and hosted-service providers are designing their offerings for the usability, IT staffing and economic requirements of SMBs.

Security—This issue is becoming extremely important for SMBs. While they have been historically less targeted by email threats and exploits, SMBs are increasingly drawing the attention of the burglars and thieves of cyberspace because of their more relaxed security practices, especially when compared to the higher level of security now in place at larger enterprises.

Mobility—With more employees being on the road, mobility is also becoming vitally important for SMBs. Anywhere-to-anywhere communications provide mobile staff with more accurate and real time data, helping on-the-road workers stay in touch and within reach through their PDAs, smart phones or laptops.

Collaboration—Productivity almost always improves when local and remote team members interact and work collaboratively by sharing emails, calendars, contacts, task lists, notes and more. Many email servers and hosting services are now offering affordable and easy-to-use groupware collaboration tools.

Administration—For the SMB, an email server should be easy to use, requiring about the same amount of knowledge required to use a personal workstation. The email servers for the SMB should provide secure messaging, mobility and collaboration and require very little attention or intervention. They should also provide for fast and easy disaster recovery for businesses with limited IT professional support.

Email for small-to-medium businesses can be secure, mobile, collaborative and easy to use, plus affordable. It can also provide services such as wireless access, groupware collaboration, secure instant messaging, Sync ML data synchronization, web mail, mailing lists and, if needed, integration with the groupware functions of Microsoft Outlook. Archiving and backing up, plus fast and easy disaster recovery procedures should also be available. While offering new and innovative features, email designed for SMBs can run on economical hardware with older operating systems, plus require little, if any, IT professional support.

1.1 Related Work

M. Tariq Ban day, proposed to make e-mail communication secure and private, e-mail servers incorporate one or more security features using add-on security protocols. The add-on security protocols provide a reasonable security but have several limitations. This paper discusses limitations of e-mail security protocols, analyzes and evaluates their effectiveness in e-mail servers. It also proposes methods to improve efficiency of e-mail servers in detecting spoofed e-mails from domains that do not follow any standard anti-spoofing protocol. Further, it presents results of studies carried out to appraise e-mail user practice; knowledge of security protocols and their confidence in e-mail system.

Vernon M Neppe, FRSSAf, this paper is based on a detailed consensus-based analytic comparison of the four major technologies for secure email, X.509/PKI, PGP, IBE, and Zmail. General usability and security metrics are applied to rate available secure email systems, This work thus confutes the conventional thinking that usability and security are like a seesaw; if usability goes up, security must go down, and vice-versa. This apparent antinomy can now be seen as a synergy: With more usability in a secure system, security increases. With less usability in a secure system, security decreases. A secure system that is not usable will be left aside by users. As both a limitation and an objectively strong point of the method used in this work, these are findings based on models for usability and security, not user focus groups and penetration testing analysis.

Matt Blaze, This paper examines mechanical lock security from the perspective of computer science and cryptology. We focus on new and practical attacks for amplifying rights in mechanical pin tumbler locks. Given access to a single master-keyed lock and its associated key, a procedure is given that allows discovery and creation of a working master key for the system. No special skill or equipment, beyond a small number of blank keys and a metal file, is required, and the attacker need engage in no suspicious behaviour at the lock's location. Countermeasures are also described that may provide limited protection under certain circumstances. We conclude with directions for research in this area and the suggestion that mechanical locks are worthy objects for study and scrutiny.

Sugata Sanyal, Ajit Shelat, Amit Gupta, trend increases as more and more web-based applications are made available over the Internet. The Insider threats are generally caused by current or ex-employees, contractors or partners, who have authorized access to the organization's network and servers. Theft of confidential information is often for either material gain or for wilful damage. Easy availability of hacking tools on the Internet, USB devices and wireless connectivity provide for easy break-ins. The net result is losses worth millions of dollars in terms of IP theft, leakage of customer / individual information, etc. This paper presents an understanding of the Insider threats, attackers and their motives and suggests mitigation techniques at the organization level.

II. SPECES Framework

A SMS Based Security Providing for an Email ID by creating an Email Server (SPECES) plays a major role for the security for Email application by sending SMS to the user about the mail information such as IP address of the recently visited system date, time and location through SMS gateway.

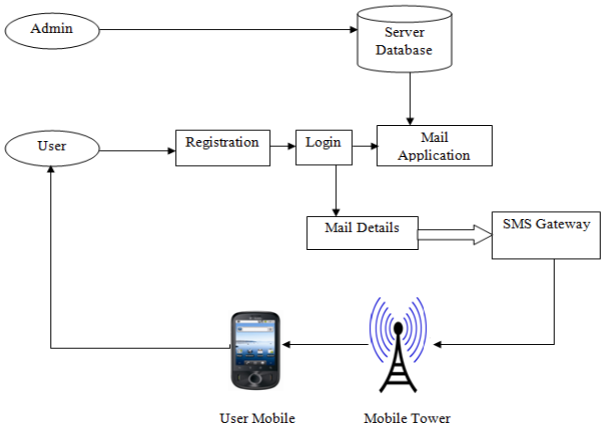


Fig 2.1 SPECES Framework architecture

The above Framework contains Mail Application, Mail server, Mobile device, SMS gateway, Server database.

The user register their details like Name, Email id, Mobile number etc. When the user login into amail server, the user get the message such as the visited system IP address, date, time and location through the SMS gateway.

In such a way, received mails in their inbox are sending to the user mobile phones as a text message by using the SMS gateway. The admin store all the user details in the server database.

The above process are implemented in an own mail server named as amail server. It is similar to Gmail, yahoo mail, hotmail etc. The user can able to create account in an amail server. It is mainly developed for the security purpose. It prevents security from the unauthorised users and from hackers.

III. SMS Gateway

An SMS gateway is a telecommunications network facility for sending or receiving Short Message Service (SMS) transmissions to or from a telecommunications network that supports SMS. Most messages are eventually routed into the mobile phone networks. Many SMS gateways support media conversion from email and other formats.

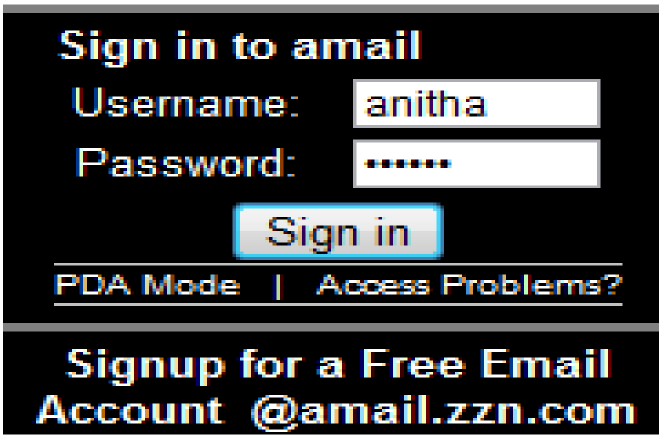
Several operators have true fixed-wire SMS services. These are based on extensions to the ETSI GSM SMS standards and allow fixed-fixed, fixed-mobile and mobile-fixed messaging. These use frequency-shift keying to transfer the message between the terminal and the SMSC. Terminals are usually DECT-based, but wired handsets and wired text-only (no voice) devices exist. Messages are received by the terminal recognising that the CLI is that of the SMSC and going off-hook silently to receive the message.

A direct-to-mobile gateway is a device which has built-in wireless GSM(Global System For Mobile Communications) connectivity. It allows SMS text messages to be sent and/or received by email, from web pages or from other software applications by acquiring a Subscriber Identity Module (SIM card) . Direct-to-mobile gateways are different from SMS aggregators because they are installed on an organization's own network and connect to a local mobile network. The connection to the mobile network is made by acquiring a Sim card from the mobile operator and installing it in the gateway. Typically, direct-to-mobile gateway appliances are used for low 100s or 1,000s texts per month. More model appliances now offer the capability of send up to 100,000 messages each day. Several vendors that have historically provide GSM Gateway equipment for voice also have an SMS capability. Some are more primitive than others. The more sophisticated devices are engineered with SIM management to regulate the number of SMS messages per SIM; ODBC to connect to a database and HTTP interfaces to interactive with third party applications.

A direct-to-SMSC gateway is a device which allows SMS text messages to be sent and received by email, from web pages or from other software applications. The gateway connects directly to a mobile operator's SMSC via the Internet or direct leased line connections. It converts the message format into a format understood by the SMSC, typically this is the SMPP protocol. Direct-to-SMSC gateways are used by SMS aggregators to provide SMS services to their clients. Typically they serve for high volume messaging and require a contract directly with a mobile operator.

IV. Results and Discussion

This model is developed for providing the security in Email server application and also provides the security in the server application the data owner also receives an alert message about the fake users through SMS gateway sends a message to the mobile device.



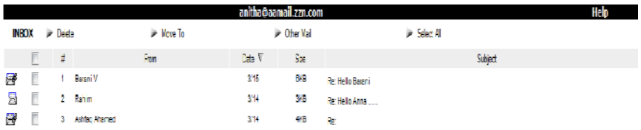
Sign in to amail

Username: anitha

Password: •••••••

Signup for a Free Email Account @amail.zzn.com

Fig 4.1 Login Form



anitha@aamail.zzn.com

	□	#	From	Date ∇	Size	Subject
	□	1	Barani V	3/15	8KB	Re: Hello Barani
	□	2	Rahim	3/14	3KB	Re: Hello Anna .....
	□	3	Ashfac Ahamed	3/14	4KB	Re:

Fig 4.2 Mail Form

V. Conclusion

Internet has changed and has been changing greatly over the years, and this has made our concern about the security more today, particularly for those who are transmitting their personal and sensitive data over the internet. E-mail users are losing confidence in e-mail security because they have insufficient awareness of security protocols and only some of users use them to secure their emails. There is a need to undertake a major educational campaign to aware e-mail users about e-mail security issues and train them in use of security protocols and procedures. This paper is mainly developed for the security purpose. It is used to secure our email id from unauthorised users and from hackers.

VI References

[1]. Klensin, (2001) ‘Simple Mail Transfer Protocol’ IETF RFC 2821.

[2] Mir, F.A., Banday, M.T. (2010). “Control of Spam: A Comparative Approach with special reference to India”, Journal of Information Technology Law,UK,19(1),pp.22-59,DOI: 10.1080/13600831003589350,URL:http://dx.doi.org/10.1080/13600831003589350.

[3] Banday, M.T., Qadri, J.A. (2010). “A Study of E-mail Security Protocols,” eBritian, ISSN: 1755-9200, British Institute of Technology and E-commerce, UK, Issue 5,Summer 2010, pp. 55-60, available online at: http://www.bite.ac.uk/ebritain/ebritain_summer_10.pdf.

[4] Banday, M.T., Mir, F.A., Qadri, J.A., Shah, N.A. (2011). “Analyzing Internet E-mail Date Spoofing”, Journal of Digital Investigation, UK, 7, pp. 145-153, doi:10.1016/j.diin.2010.11.001.

[5] C. E. Landwegr, C. L. Heitmeyer, and J. D. McLean, (2001) “A security model for military message systems: Retrospective,” Naval Research Laboratory, Washington, DC,2001.http://www.chacs.nrl.navy.mil/publications/CHACS/2001/2001landwehr-ACSA.pdf, accessed 20 November 2009.

[6] R. Oppliger, (2004) “Certified Mail: the next challenge for secure messaging”, Communications of ACM, Vol. 47, No. 8, pp. 75-79.

[7] M. Jakobsson and S. Myers (Eds.), (2006) “Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft”, Adobe E-Book, Wiley Publication, ISBN: 978-0-470-08609-4.

[8] T. R. Surmacz, (2007) “Reliability of e-mail delivery in the era of spam”, International Conference on Dependability of Computer Systems, DepCoS-RELCOMEX’07, 198 – 204.

[9] Apu Kapadia, (2007) “A Case (Study) For Usability in Secure E-mail Communication”, IEEE Security & Privacy, pp. 80-84.

[10] P. Tzerefos, C. Smythe, I. Stergiou and S. Cvetkovic, (1997) “A comparative study of Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) and X.400