EMAIL CRIME MITIGATION BY ITS FORENSICS AND LEGAL PROSECUTION

Dr. Jigar Patel,
MCA Department, Kalol Institute of Management, India.

ABSTRACT

Email sending and receiving is almost every day exercise of Internet user. Billions of Emails are transmitted via Internet and even the numbers increasing drastically. Email is becoming more and more sophisticated and faster way of communication opens the new challenges and legal issues nowadays. This paper is focus on what are the current Email related issues and crimes occurred everyday and possible ways of proactive use of Email communication. Paper also aims for what is the security measures required for the safer Email communication and also what kind of Email abuse prevailing in the society. The paper concludes with all legal provisions that can be useful if one is victim of Email related crime.

KEYWORDS - Cyber Law, Email, Forensic, Security, Spam

INTRODUCTION

According to Wikipedia, Electronic mail, most commonly referred as Email or e-mail since approximately 1993. It is very popular method to transfer the message from one sender to one or many recipients. Earlier system of Email exchange required both sender and recipient online but today the Email are worked based on stored and forward method, just we need to connect the Email server to retrieve the Email messages. The Email consist mainly three components like envelope, header and body. Generally Email send by Simple Mail Transfer Protocol (SMTP) for the text only message but now, one can transfer multimedia content attachments via Multipurpose Internet Mail Extension (MIME). At the other end for retrieving Emails from the mail server we use the Application Layer protocol like Internet Message Access Protocol (IMAP).

Email is becoming very fast and even cost effective way of communication nowadays. Therefore, up to 2013 there were total 3.3 billion of Email accounts created and it's likely to increase in next few years as well. Most of the Email account owners are from India and China as expected because these two are most populated countries in the world. Bigger part of the all Email accounts are of the consumer Email account and corporate Email accounts. Social Networking as well as Apple and Android based mobile devices is also reason of increasing Email popularities among the users and due to it currently 34% of Emails are accessed via such mobile devices [1]. In connection of that the numbers of Email related crime continue to rise with high rate worldwide in last few years. The spamming and spreading viruses and worms are serious problems between the Email users and lots of such crime related incidents are reported almost in every year [2]. The survey conducted by the Computer Security Institute and Federal Bureau of Institute shows the shocking figures of such crime related things [3].

As shown in the Fig.1 entire Email crime mitigation process is divided in the mainly five steps. First step of the process is to basics of sending and receiving the Emails and how the Email related coding and programming should be carried out so that users can use the Email system error free. Second step in the process explained the necessity of security in the sending and receiving an Email by using secure protocols as well as other security majors at both client and server sides. Third step shows even after security mechanism crime can be take place and we need to aware about all possible Email related crimes. In the forth step it is explain what to do if someone committing the Email related crimes and one is victim of Email related crime. Therefore, here digital forensic plays the role of how you can trace the Emails and reach to the criminals. In the fifth and final steps in the process it is shown that after arresting the criminals how the prosecution can be take place in the court of law and criminal will be punished under the Cyber laws drafted by the different countries.

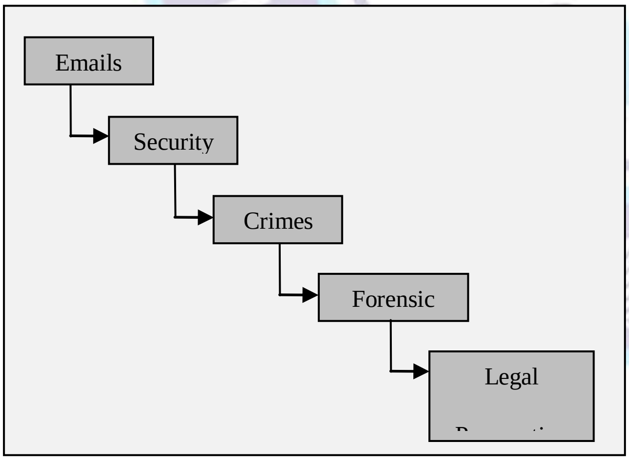

Fig.1. Email Crime Mitigation Process

Here in the paper all these steps are explained in the three distinct sections. In the first section of this paper it is explained how Email related crimes are growing nowadays and classification of Email related crime. In the second section in the paper it is explained how you can carried out secure Email exchange and prevent you from such crime and what are the Email related best practices. How the network security can be helpful for such prevention. Third sections contain all the legal prosecution related aspects and law provisions available against such crime in different countries around the globe.

EMAIL RELATED PROBLEMS AND CRIMES

As we know the use of Emails are increasing day by day results the risk of misuse of the Email system therefore, attacks committed by the Cyber criminal cannot be underestimated. The problem with any individual Email account is the password. Today's criminals are using numerous techniques to crack the Email password and afterword they are getting the valuable information from that Email account. Cyber criminals can also send the Email to any user which contains the virus and worms in the attachments. Sometimes the Email contain the text or image as clickable link and when user click it the Trojan can be planted in the user's computer which gives remote control of one's computers to the attackers. The other possible problem for the Email system is it can be crash and Cyber criminals can get the vulnerable information from that by hacking the Email server. Various techniques used by the hackers to hack the Email server like scanning or sniffing or exploiting other vulnerabilities [5]. Email bombing is also one kind of attack by which user's cannot access his Email account for certain period of time and such attacks is work like Denial of Service (DoS) attack [6].

Most critical kind of the Email related problem is describes in consensus the ubiquitous phenomenon of receiving Unsolicited Bulk Email (UBE) commonly known as SPAM [7]. It is associate with the commercial context commonly refer to Unsolicited Commercial Email [8]. According the report publish by Semantec corporation in 2012 there is global ration in Email traffic was 68.8 percent. Out of that most the share occupied in the dating related Email which is done by .com top level domain. Further in the analysis it has been found 36.8 percent of spam Emails were less than 5Kb while 24.9 percent were between 5 to 10 Kb and remaining 38.3 percent of Email having size greater than 10Kb of size which definitely causes the heavy network payload [9]. It also causes the economic damages to business firms as well as the time spent by the employees is also indirect loss of such firms.

The crucial work done by SPAM Email sender is to obtain the users Email addresses trough various techniques. In the dictionary attack spammer tries to get the first and last name from the database. Afterword he tried all random combination of those names and sending the bulk Email without worrying about how many Emails are bounces back. Other source of getting Email addresses is to read the web pages to search the Email address. Users are generally putting their Email address on the social networking websites or blog or any other website can be used by the spammer for sending such a SPAM Emails.

The Emails have two limitations, first is there is no encryption mechanism at the sender side and no integrity check at the receiver side. Second is the most used Email protocol Simple Mail Transfer Protocol hasn't any mechanism for source authentication and Email header which containing information about sender and path along which the Email message is traveled can be easily modified. It has been also observed by researchers even installing antivirus software, filters, scanners and firewall is not enough for the securing Email communication [10].

POSSIBLE EMAIL SECURITY, FORENSIC & BEST PRACTICES

As discuss in second section there are many ways used by criminals to abuse Email nowadays. This section discuss about what are the possible ways of securing our Email. In the second subsection it is explained even after all the security provisions one can suffers in Email related crimes, then how investigator and Email users are altogether know about which kinds of Cyber crime they are suffered from. In the last subsection it is also explain what are the best practices that must be keep in mind by normal Email user.

As far as Email security is concern first of all organizations can use the highly effective filtering systems to block the delivery of most of the unsolicited Email being sent to such business organizations. Researchers have designed and implemented an intelligent Email virus filtering with an embedded system. It is also proposed intelligent Embedded Email Virus Filter (EEVF) system acts as a standalone Email gateway to filter inbound messages by successfully enforcing Email virus filtering policies. In addition, a new systematic Associative Petri Net (APN) model construction algorithm is proposed to make malicious Email reasoning possible [12][13].

Queuing model propose a novel method to study the impact of three types of attacks like password cracking, sending malicious Email and Email bombing on the Email systems. Researcher construct a multiple queuing model to characterize three types of attacks integrally, and study the performance metrics of system security such as system availability, average queue length and information leakage probability [14]. Companies need to take a more holistic approach to Email security, putting stringent, formalized policy procedures in place alongside aggressive detection methods. By choosing an 'in the cloud' approach to security, ICI outsources the responsibility of protection to a trusted partner who protects their business at its first line of defense – the Internet. Emails are monitored outside the corporate network and any suspicious looking Emails or spam will be stopped, before they reach the network boundary. This effectively pushes the problem back to the spammers [11].

Even such Email security measures anyhow criminals are still succeeding to bypass and committing crimes every day. In this regard Email forensic is new area which is helpful to catch the criminals after such Email related crimes happened. Digital forensic is required trained investigator having all access privileges to catch the criminals. There are various tools and technology is used for the digital forensic especially for the Email related crime. The main task of investigator is to find out the originator of the specific Email message. Therefore, Email authorship is core issue in this kind of Email investigation process. It has been proven using similarity in the text we can find the author of Email with different techniques and models [15]. As a result of growing e-mail fraud, investigators need efficient automated methods and tools for analyzing Emails. Different framework offers different functionalities ranging from Email storing, editing, searching, and querying to more advanced functionalities such as authorship attribution and Email account localization. Extending traditional authorship identification techniques, it is proposed an Email mining using different techniques like classification, clustering and other statistical analysis methods helps in such forensic investigation process. Email social networks need to be further explored; they are rich sources of learning about Cyber criminal activities [16].

As far as best practices is concern user has to understand few points to avoid major Email related problems as below.

- Never trust on the username, it can be forged.
- Do not rely on the sender name. Culprit always uses the other person's name and Email address.
- Never trust on the Email content, any link or file given in the Email because it can cause the damage or spread the virus in your computer.

- Never delete the controversial Email from your account. Retain such message in the Email program or in other media. The stored Email messages can be useful for the further investigation.
- Do not reply the person who is unfamiliar with you, because the replying message encourages that person to communicate further.
- Do not agree under the any circumstances to meet with the person personally.

LEGAL ASPECT OF EMAILS

Over the years, a number of laws and regulations have been drafted in the world, which covers the subject of Email monitoring and prosecution. In 2000, the UK government passed the Regulation of Investigatory Powers Act (RIPA) which clarifies how and why organizations can monitor individuals, and protects employees' rights [17]. Australian parliament has passed the Spam Act 2003 for the setting up a scheme for the regulation of commercial Email and other types of commercial electronic messages. It restricts spam, especially Email spam and some types of phone spam, as well as Email address harvesting, however there are broad exemptions. Fighting Internet and Wireless Spam Act (FISA), is Canada's anti-spam legislation applying for "all communications sent by Canadian companies, to Canadian companies or messages simply routed through Canadian servers.

United States has also developed CAN-SPAM which derives from the bill's full name: Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. This is also a play on the usual term for unsolicited Email of this type of spam. CAN-SPAM defines a "Commercial electronic mail message" as any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service. As the other countries according to Indian IT Act any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to two three years and with fine. Even after such provision of punishment the implementation of such laws related to Cyber world the number of cases and prosecution in the courts of law under the Cyber law are not match with the number of cases occurred every day. The problems behind the prosecution is collection of digital evidence and its reliability and the technical knowledge related to computer and its network among the person involved in the prosecution are playing the vital role in the entire process.

CONCLUSIONS

Email communication is becoming quite common day by day for the business, education, social networking and military data transfer the security, reliability and integrity is becoming serious problems nowadays. Email security and preventing users computer from virus and malware is most required things today. Lots of researcher has tried to enhance the security for Email communication but still there are number of reasons behind the Email related crimes. All Email users should aware of risk related to Email and protect themselves against the crime. Government can play crucial role in the implementation of Cyber laws and prosecution process in the court of laws to strengthen laws and order in the Cyber world.

REFERENCES

1. Sara Radicati, “Email Statistics Report”, The radicati group, inc. a technology market research firm, 2012.
2. A. Coulthard, T.A. Vuori, Computer viruses: a quantitative analysis, Logistics Information Management 15 (5), 2002, pp. 400–409.
3. R. Richardson, 2010/2011 Computer Crime and Security Survey. Available at: https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey 2010.pdf 2012.
4. Wikipedia, the free encyclopedia, Available at: http://en.wikipedia.org/wiki/Email, 2013.
5. Yang Wang, Chuang Lin, Quan-Lin Li, “Performance analysis of Email systems under three types of attacks”, Performance Evaluation 67,2010, pp. 485-499.
6. Y. Wang, C. Lin, Q.L. Li, Y. Fang, A queueing analysis for the denial of service (DoS) attacks in computer networks, Computer Networks 51, 2007, pp. 3564-3573.
7. Spamhaus, “The definition of spam”, Available at http://www.spamhaus.org /definition.html.
8. CAUCE: Coalition against unsolicited commercial Email, Available at http://www.cauce.org.
9. Symantec Intelligence, “Symantec Intelligence Report”, November 2012,
10. Teng J, Ma J, Lai I, Li Ying, “E-mail authorship mining based on svm for computer forensic”, In: Proc. third international conference on machine learning and cyhemetics, Shanghai; August 2004.
11. Mark Sunner, “Email security best Practice, Network Security”, December 2005.

12. Dong-Her Shih, Hsiu-Sen Chiang, David C. Yen, Shin-Chuan Huang, "An intelligent embedded system for malicious Email filtering", Computer Standards & Interfaces, 35,(2013, pp. 557–565
13. D.H. Shih, H.S. Chiang, B. Lin, "A generalized associative Petri net for reasoning", IEEE Transactions on Knowledge and Data Engineering 19 (9),2007, pp. 1241–1251.
14. Yang Wang, Chuang Lin, Quan-Lin Li, "Performance analysis of Email systems under three types of attacks", Performance Evaluation 67, 2010, pp. 485-499
15. Abbasi A, Chen H., "A Stylometric Approach to Identitylevel Identification and Similarity Detection in Cyberspace", ACM Transactions on Information Systems March-2008.
16. Rachid Hadjidj, Mourad Debbabi, Hakim Lounis, Farkhund Iqbal, Adam Szporer, Djamel Benredjem, "Towards an integrated e-mail forensic analysis framework", digital investigation 5, 2009, pp. 124 – 137.
17. Ken Watt, "Legal Email – Email monitoring and UK legal landmines", Computer Fraud & Security, pp. 18-19.