ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

Developing an Email Violation Prevention Model Using Web 3.0 Technology

Apoorva Kanavalli[1], Haritha.P[2]

U.G. Student, KLES's BCA, P.C. Jabin Science College, Huballi, Karnataka, India[1]

U.G. Student, KLES's BCA, P.C. Jabin Science College, Huballi, Karnataka, India2

ABSTRACT: Email is one of the most important Internet applications for most computer users. The usage of email is increasing from time to time. However, together with this growth comes a variety of problems, such as increase of spam and the widely spread of computer worms via emails. The current scenario poses a challenge on ways to manage email efficiently, especially in avoiding the sending and receiving of spam email. Recent development in web technology such as Semantic Web provides an infrastructure that enables web pages, databases, and services to both consume and produce data on the web. Application developer can use this information to search, filter, and prepare information in new and exciting ways to assist the web user. With these features, Semantic Email, one of Semantic Web application, is believed to be able to help control spam by using semantic filtering and filing of email. This paper reports the current practice of email violation prevention method by Internet Service Providers in Malaysia, and later proposes a measure to prevent email violation in Malaysia through Web 3.0 technology. The development of an email violation prevention model based on Web 3.0 elements signifies the theoretical contribution of this study.

KEYWORDS: Computer worms, emails, semantic web, spam, semantic filtering, internet service providers, web 3.0 technology.

I.INTRODUCTION

There has been much alarm about Internet abuse in the past decade. Claims of Internet-related crimes such as homicides, suicides, and child neglect have received widespread media attention across the globe. Almost 10 percent of adult Internet users are identified as Internet addicts and 31 percent of Facebook users admitted that they are addicted to Internet applications. In India, according to local Internet Service Provider Jarring, reported the recent abuse of the Internet, in which 38 computer servers belonging to local educational, government and private.

Organizations were hacked and used as the launching pads for the online abuse in 1999. The Web technology is evolving day by day. Starting with Web 1.0, the first generation of web technology was static and read-only applications that followed strict categorization and naming of web element representations. At the transaction level, these applications are a complete backward and forward communication to the server for each of the user requests. In other words, each request had to be serviced by the server. Web 2.0 aims to enhance creativity, information sharing and collaboration among users. User participation is exaggerated through user's involvement in the application, abilityto contribute and share interest in the group that they are associated. Control over data hosted on the application provides scope for creative data management, usage and representation. This transforms application usage experience from a static to a participative operator of the application. The current new generation of Web applications is Web 3.0. Web 3.0 extends Web 2.0 applications by completely upsetting the technology of the traditional computer application industry. Major web sites with the Web 3.0 technology will undergo transformation into web services and will effectively expose their information to the community. This study aims to explore the current practice of Internet Service Providers (ISP) in India on handling email violation problem and their prevention method of the problem. Based on the information gathered, an email violation prevention model is developed by integrating Web 3.0 technology into the current practice framework

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

II.RELATED WORK

Email privacy is a broad topic dealing with the issues of unauthorised access and inspection of electronic mail. This unauthorised access can happen while an email is in transit, as well as when it is stored on email servers or on a user computer. In countries with constitutional guarantee of this secrecy of correspondence, whether email can be equated with letters and get legal protection from all forms of eavesdropping comes under question because of the very nature of email.The related works are summarized as follows:

1. There are certain technological workarounds that make unauthorized access to email hard, if not impossible. However, since email messages frequently cross nation boundaries, and different countries have different rules and regulations, governing who can access and email, email privacy is complicated issue.
2. There are certain technological workarounds to ensure better privacy of email communication. Although it is possible to secure the content of communication, protecting the meta-data of (who sends the email to whom) is fundamentally hard. Even though certain technological methods exist, the widespread adoption is another issue because of reduced usability.
3. Emailing from home is likely to grant you a reasonable expectation of privacy, but even then, it's not very difficult for prying eyes to gain access to your emails. Because your emails are stored locally, at your ISP, and on the receiving end, there are multiple points that hackers or law enforcement can gain access to.
4. Government employees have even less privacy than the little privacy a typical employee in the private sector may have. Under various public records acts and the freedom of information (FOIA), the public can gain access to almost anything the government employee writes down.

III. EXPERIMENTAL RESULTS

Figures shows the results of the email violation prevention model and how it can be achieved using various practices.

Figure 1 shows a full email header, in an email, the body is always preceded by header lines that identify routing information of the message. Figure 2 shows the spam firewall architecture that is it optimises the processing of each email to maximise performance and process millions of messages per day. Figure

Figure 1. A full email header

Figure 2. Spam Firewall Architecture

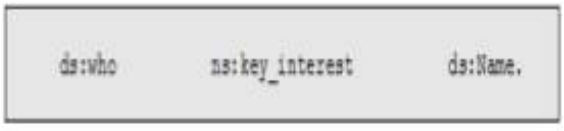

Figure 3. Domain specific relations

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

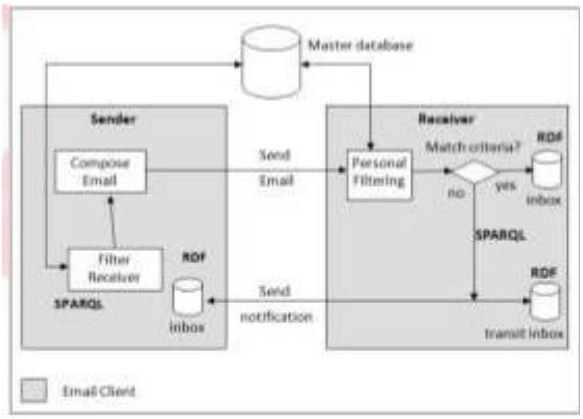

Figure 4. Email violation prevention model by filtering the receiver of the e-mail based on preset criteria.

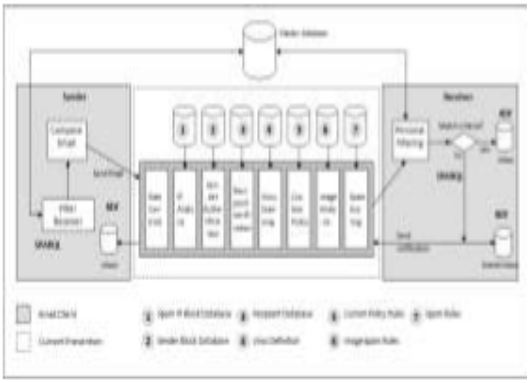

Figure 5. Overall view of the proposed email violation prevention model together with the current prevention model.

IV.CONCLUSION

This seminar discusses the email violation definition in the perspective of ISP. The definition is slightly different from what we got in the literature review since it is depends on the customer of the ISP. The current practice by theISP in handling the email violation cases by their customer is by studying the email contents. If the email is categorized as spam email, the ISP will check the full email header to get the more information such as IP address and routing information. For email violation prevention in their own organization, the ISPs are using off the shelf software and hardware. The number of software used is depends on the organization budget. An email violation prevention model based on Web 3.0has been constructed and explains in this chapter. The model is adapting the Web 3.0 elements to prevent email sender sends email to the wrong recipients

REFERENCES

[1] Cooper, A., Morahan-Martin, J., Mathy, R. M., & Maheu, M. (2002) "Toward an increased understanding of user demographics in onlinesexual activities." Journal of Sex & MaritalTherapy, 28, 105-129
[2] Vanden Boogart MR (2006) "Uncovering the social impacts of Facebook on a college campus",Retrieved March 12, 2009 from http://hdl.handle.net/2097/181.
[3] Chia, A. "Number of Internet abuse cases quadruples to 2", 106 New Straits Times, 10th October 2003, Retrieved April 1, 2009 from http://www.cybersecurity.org.my/en/knowledge_bank/news/2003/main/detail/919/index.html.
[4] Shannon, V. (2006) "A 'more revolutionary' Web", Retrieved March 15, 2009 from http://www.nytimes.com/2006/05/23/technology/23iht-web.html
[5] Kiefer, C. (2007) "Imprecise SPARQL:Towards a Unified Framework for Similarity Based Semantic Web Tasks", Department of Informatics, University of Zurich.
[6] Hendler, J. (2009). "Web 3.0 Emerging. Digital Object Identifier", 111-113
[7] Fensel, D. (2002). "Web Intelligence", IEEE/WIC/ACM International Conference on Digital Object Identifier.
[8] Dumbill, E. (2002). "XML Watch: Finding friends with XML and RDF" Retrieved April 28,2009 from http://www.ibm.com/developerworks/xml/library/x-foaf.html