Abstract

Electronic Mail (e-mail) is one of the early applications of internetworks which subsequently became the first widely used application of the Internet. It created an electronic version of conventional mail system allowing massages to be sent more quickly and easily, in a manner similar to conventional postal system. Today, e-mail has emerged as an affordable, valuable and crucial worldwide business tool that not only supports conversation between parties but also supports delivery of documents and archives of diverse nature.

The primary protocol for E-mail transfer does not define any security and privacy policy and lacks security features for privacy of conversation, authentication of sending party, integrity of e-mail message, non-repudiation by sender and consistency of the envelope. It is thus not completely secure while it is being transmitted and also requires a huge storage space for backups. The arteries of e-mail have become literally clogged by spam, viruses, and any other content that can be sent via, e-mail. Spam e-mails often contain offensive, fraudulent, adult oriented and misleading material that cause several problems either directly or indirectly, to the e-mail system that include: i) network conjunction ii) misuse of storage space and computational resources iii) loss of work productivity and annoyance to users iv) legal issues as a result of pornographic advertisements and other objectionable material v) financial losses through phishing and other related attacks vi) spread of viruses, worms and Trojan Horses, and vii) Denial of Services and Directory Harvesting attacks.

Several protocols and procedures have been developed to make e-mail communication secure and private. These procedures propose the use of diverse technological, legal and socio-economic solutions. However, hackers, spammers and phishers continue to
circumvent these procedures to exploit e-mail system for their illicit gains by changing the nature of their attacks, content of spam e-mails, etc.

In this study, various aspects of e-mail system have been worked out so as to make it secure and improve its reliability and performance. The study has mainly focused on the following issues:

- To Study process of e-mail communication and identify various protocols and components used in it. Review several vital aspects of e-mail system including addressing, message formats, Multipurpose Internet Mail Extensions (MIME), Access Protocols, etc. Illustrate process of e-mail communication through Simple Mail Transfer Protocol (SMTP) by issuing the individual SMTP commands and extensions directly to transmit e-mail messages using Telnet client.

- To Identify and analyze various security issues of e-mail system especially those related to privacy of sender, sender authentication, message integrity, non-repudiation by sender, consistency of message and Spam e-mails.

- To Identify and analyze various security protocols along with their working to apprise their effectiveness and limitations in e-mail security system.

- To study SMTP server architectures, configuration options and features; analyze and evaluate their effectiveness and propose methods to improve their efficiency in detecting spoofed e-mails from domains that do not follow any standard anti-spoofing protocol. Apprise e-mail user practice, knowledge of security protocols and their confidence in e-mail system.

- To study in detail date-spoofing, its implications on users, businesses and systems, conduct experiments and surveys of date-spoofed e-mails on commercial and corporate e-mail servers and propose methods for their detection, forensics and elimination.
• To investigate spam, its different types and spamming modes, outline the routes, system components, devices and protocols exploited by each spamming mode, and analyze mail path and its categorization to identify effective anti-spam measure that may be applied for a particular spamming mode. Identify problems and economic losses caused by spam, analyze objectionable features of spam and provide categorization of technological solutions of spam. Analyze machine learning spam filtering and the statistical techniques involved in the design of famous statistical spam filters and compare them in terms of various evaluation measures to find out their comparative effectiveness and limitations.

• To discuss possible parameters in the light of trans-border legislative developments which an anti-spam legislation in India, as and when enacted, may have and also present an account of present legal solutions to the problem of spam in India taking cue from the judicial pronouncements on the subject in other jurisdictions.

• To analyze Threat e-mails and the efficiency of different types of Naïve Bayes spam filtering approaches for their classification using threat e-mail corpus created from various sources which either belongs to terrorists or keep record of terrorism or report terrorism or have some form of interaction with them e.g. terrorism websites, newspapers, data available with resource centers and databases like Terrorism and Preparedness Data Resource Center (TPDRC) and Global Terrorism Database (GTD).

• To investigation existing Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) methods and their working, identify security and usability issues of CAPTCHA methods, and to provide guidelines to improve security control and usability of CAPTCHAAs. Propose and design new clickable image-based CAPTCHA technique; evaluate its usability and security; and compare it with other similar techniques for the purpose of relative merits and demerits.