IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 7, September 2014.
www.ijiset.com
ISSN 2348 – 7968

Cyberspace Tracing: Study and Generation of Security Model for Spam and Bulk Email Prevention

Shrikant Thakar [1], Dr. Vikram Kaushik [2]

[1] I.N.S.B. Institute of Information Technology and Management Studies, BCA College, Idar, Gujarat, 383430, India.

[2] Nootan Sarv Vidhyalay Kelvani Mandal Sanchalit , MCA College, Visnagar, Gujarat, 384315, India

Abstract

To examine the traceability on the Internet how actually works. Failures of traceability, with consequent unintentional anonymity, have continued as the technology has been changed. The lack of traceability at the edges is stealing another person's identity on an Wide Area Network that existing tools and procedures would entirely fail to detect. Especially governments see preserving activity logs,, as essential for the traceability of illegal cyberspace activity. Present a new and efficient security model of processing email server logs to detect machines sending “bulk email \ spam" or “email infected with viruses" using IP Address Based Cyberspace Tracing. Want to create a content-blocking system with a hybrid design. The systems database holds details of the traceability of content, as viewed from a single location at a single time.

1. Introduction

Traceability is the ability to map events in cyberspace, particularly on the Internet, back to real-world instigators, often with a view to holding them accountable for their actions [1]. Anonymity is present when traceability fails.

The process of mapping from an event occurring in the cyberspace world of the Internet to the everyday world we're familiar with is known as tracing and the property of interest, the ability to do that tracing, has become known as traceability. In contrast, the ability to use the Internet without others being able to determine that “you are responsible” is now referred to as anonymity.

Academics have researched into anonymity for decades, building elaborate systems that interact communications in time or space so that it becomes impractical to untangle them. However, there has been little academic interest in traceability, which is often - incorrectly - seen as trivial or obvious.

In the Internet Service Provider (ISP) world, traceability has long been a key issue [2]. In just a dozen years, the Internet has been transformed from an academic research network, with a few thousands of hosts, into an all-pervasive, mass-market commercial entity with hundreds of millions of hosts.

Despite this transformation, the ISPs that operate the individual networks that make up the global Internet have remained entirely independent entities, yet to permit their users to inter-work they must co-operate with every other ISP. If users do things that are anti-social, then the ISP that hosts them must act to preserve the reputation of their business. Without traceability, the disruptive user will remain hidden and the ISP risks becoming a pariah that no other networks will communicate with, which is a sure recipe for a commercial disaster [3].

These investigators have learnt that they can employ traceability to locate the miscreant although, as we shall see, their requirements are sufficiently different from those of ISPs as to cause substantial practical difficulties. A small proportion of users are doing things on the Internet that are illegal and that law enforcement officials wish to investigate.

A small proportion of users are doing things on the Internet that are illegal and that law enforcement officials wish to investigate. These investigators have learnt that they can employ traceability to locate the miscreant although, as we shall see, their requirements are sufficiently different from those of ISPs as to cause substantial practical difficulties.

2. E-Mail Spam

Spam is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam.

E-mail spam, known as unsolicited bulk Email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. Spam in e-mail started to become a problem when the Internet was opened up to the general public in the mid-1990s. It grew exponentially over the following years, and today composes some 80 to 85% of all the email in the world, by a "conservative estimate" [4]. Spam can be used to spread computer viruses, trojan horses or other malicious software.

A 2009 Cisco Systems report lists the origin of spam by country as follows [5]:

Rank	Country	Spam messages per year (in trillions)
1	Brazil	7.7
2	United States	6.6
3	India	3.6
4	South Korea	3.1
5	Turkey	2.6
6	Vietnam	2.5
7	China	2.4
8	Poland	2.4
9	Russia	2.3
10	Argentina	1.5

Table-1: Cisco System Report

Spammers collect e-mail addresses from chat rooms, websites, customer lists, newsgroups, and viruses which harvest users' address books, and are sold to other spammers. They also use a practice known as "e-mail appending" or "epending" in which they use known information about their target (such as a postal

ISSN 2348 – 7968

address) to search for the target's e-mail address. Much of spam is sent to invalid e-mail addresses. Spam averages 78% of all e-mail sent [6]. According to the Message Anti-Abuse Working Group, the amount of spam email was between 88-92% of email messages sent in the first half of 2010 [7].

2.1 Spam Protection Technique of Gmail

Gmail doesn't filter all the spam messages that could reach your inbox. When you click on the "Mark as spam" button, Gmail uses that information to stop similar future messages not only for you, but for all Gmail users. But spam is also evolving and it's harder to block, especially when it uses images and literary texts.

"Many Google teams provide pieces of the spam-protection puzzle, from distributed computing to language detection. Gmail supports multiple authentication systems, including SPF (Sender Policy Framework), Domain Keys, and DKIM (Domain Keys Identified Mail), so we can be more certain that your mail is from who it says it's from. Also, unlike many other providers that automatically let through all mail from certain senders, making it possible for their messages to bypass spam filters, Gmail puts all senders through the same rigorous checks [8]."

Gmail's spam filters also work in our IMAP client by automatically diverting messages that are suspected of being unwanted messages into Gmail Spam and keeping them out of your inbox. If we find a message that should be marked as spam, just move it to Gmail Spam. This is just like clicking 'Report Spam' in the Gmail web interface and helps us to improve our spam filters [9].

If we find a message wrongly classified as spam, we can move the message out of '[Gmail]/Spam' to the appropriate folder in your client.

2.2 Spam Protection Technique of Yahoo Mail

A Yahoo security upgrade that caused chaos for thousands of BT customers who use their own domain name to send email has been temporarily removed after protests from users.

The upgrade was intended to stop spam being sent through the BT/Yahoo mail servers. Early versions of spam-generating malware would install a mail server on the infected machine, and could send out thousands of junk emails per hour. But internet service providers (ISPs) then blocked any traffic on port 25 (used for sending email) that did not go through their servers. Newer malware uses the settings from the infected machines to send spam through the authorised servers - but will still have fake From: addresses [10].

To combat this, Yahoo tried to filter out messages whose From: did not match the user name - but that caught thousands of BT users who use their own domain. BT/Yahoo intended that anyone doing so should just add that domain to an "approved list" - but apparently had not counted on the large number of people who choose something other than a BT/Yahoo sender's email. BT apologised for the confusion, while Yahoo has set up a web page to clarify the process (btyahoo.com/verify). BT added: "Protection of our customers is paramount."

Yahoo licenses out Domain Keys, and recently said it is working with Cisco to combine their anti-spam technologies and create a new authentication system. IBM is promoting its technology with developers, saying it wants to help them build more effective antispam filters [11].

2.3 Spam Protection Technique of Hotmail

When an external user sends email messages to a Windows Live Hotmail account, Smart Screen filter technology evaluates the content of the messages and assigns the message a rating based on the probability that the message is junk or spam email. This rating is stored as a message property called a Spam Confidence Level (SCL) within the message itself. The SCL rating stays with the message as it is sent to other anti-spam protection layers within Windows Live Hotmail [12].

Rules inside Windows Live Hotmail are set to handle email messages with various SCL ratings. If a message has an SCL rating lower than a certain threshold, it is considered spam and a rule then deletes the message rather than send the message to the users' junk email folders. If the message has a higher SCL rating than the threshold, the email is delivered to the user's junk email folder rather than to the inbox [12].

Microsoft has started pushing its Sender ID anti-spam technology by running it on Hotmail. Users are given an on-screen alert every time the sender of an e-mail does not use the Sender ID framework will certainly add weight to people fears, but at the same time a large number of Internet users will be glad that something is being done to tackle an ever-increasing problem. However the suggestion by director of Microsoft's Technology Care and Safety Group, Craig Spiezle, that e-mail sent by companies that don't use Sender ID will be put in a junk mail folder or even deleted, will inevitably lead of accusations of abuse.

Microsoft is pushing Sender ID as a system for identifying and thwarting unwanted e-mail. The technology works by verifying that e-mails originate from the domain from which they claim to have been sent. It checks the sending server's address against a registered list of servers that the domain owner has authorised to send e-mail.

Microsoft is not the only major technology player promoting an anti-spam technology. Yahoo has an authentication technology called Domain Keys, and IBM has rolled out a new anti-spam technology called Fair UCE, or Fair use of Unsolicited Commercial Email [13].

2.4 McColo Web Hosting Service Provider Affected By Spam

McColo was a San Jose-based web hosting service provider [14]. In late 2008, the company was shut down by the two upstream providers, Global Crossing and Hurricane Electric, because a significant amount of malware and botnets had been trafficking from the McColo servers [14].

In November 2008 a large source of the world's spam, the McColo network, was taken offline. Prior to that, spam levels had been holding relatively constant. But when McColo went offline, we saw spam drop by 70% compared with previous levels. However, spammers are recovering with vigour.

While spam is still down overall, it's important to note its rate of growth. Spam levels are up by 156% since November 2008. As spammers recover, the increased rate of spam growth will likely have total spam volumes back to pre-McColo levels within a few months.

ISSN 2348 – 7968

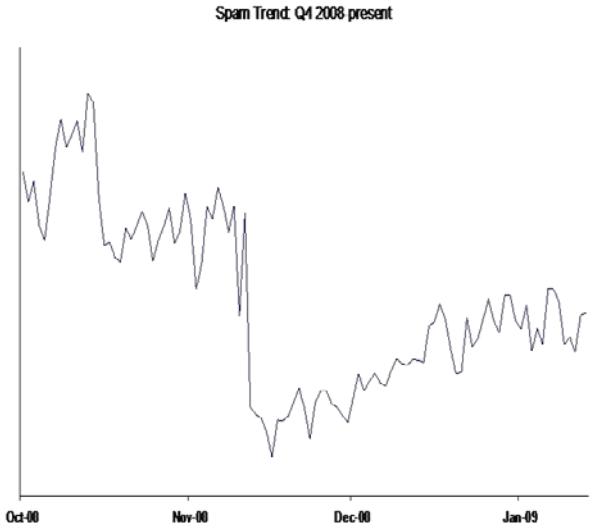

Figure-1: McColo affected by spam

Although McColo received a lot of attention, the highest volume of spam in 2008 actually came on April 23, which was an all-time high spam level for Google Message Security data canters. That day, the average number of spam messages blocked per user was 194. This peak was driven by an unprecedented number of non-delivery receipt (NDR) attacks we saw in April. One customer who was the target of a specific NDR attack said that their users were receiving an average of 100 emails every minute [15].

The volume of spam in circulation fell by as much as two thirds after upstream providers pulled the plug on McColo, which harboured many of the command and control servers that controlled the world's spam distribution. Immediately prior to McColo's shut down, these three botnets were ranked first, second and fifth the world's most prolific sources of spam, altogether responsible for nearly 70 per cent of junk mail, according to net security firm Marshal8e6 [16].

We can also expect that viruses and malware will continue to be a key tool and area of focus for spammers to upgrade their platforms [17].

McColo's termination followed closely on the heels of an incendiary report released by researchers from numerous security organizations and companies, including McAfee, Trend Micro and Arbor Networks, detailing shady criminal practices of ISPs like McColo and their connection with spam and cyber crime [18].

3. Objective

To examine how traceability on the Internet actually works. Failures of traceability, with consequent unintentional anonymity, have continued as the technology has been changed.

An analysis that ascribes these failures to the mechanisms at the edge of the network being inherently inadequate for the burden that traceability places upon them. The underlying reason for this continuing failure is a lack of economic incentives for improvement. The lack of traceability at the edges is stealing another person's identity on an Ethernet Local Area Network that existing tools and procedures would entirely fail to detect. Preserving activity logs is seen, especially by Governments, as essential for the traceability of illegal cyberspace activity**.**

The present a new and efficient security model of processing email server logs to detect machines sending "bulk email \ spam" or "email infected with viruses" using IP Address Based Cyberspace Tracing. We want to create a content-blocking system with a hybrid design. The systems database holds details of the traceability of content, as viewed from a single location at a single time.

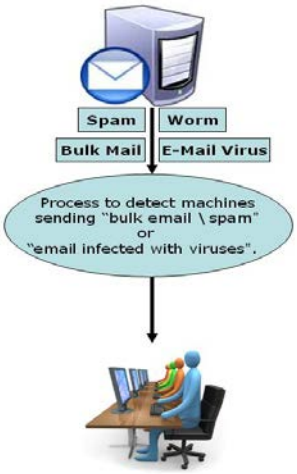

Figure-2: Anti spam technique

4. Conclusion

This research is primarily set out to identify and consolidate the prevention mechanism associated with spam and to formulate a security model to handle these issues. The insights that will be gained from the research are expected to form a set of guidelines for designing this system in the form of a structured framework for evaluation for prevention mechanism.

References

[1] "Glossary," ASME Boiler and Pressure Vessel Code, Section III, Article NCA-9000, Internet: http://en.wikipedia.org/wiki/Traceability, May 5, 2011 [March 19, 2011].

[2] Broder Kleinschmidt, "An International Comparison of ISP's Liabilities for Unlawful Third Party Content" Internet: http://ijlit.oxfordjournals.org/content/early/ 2010/07/09/ijlit.eaq009.abstract, [March 19, 2011].

[3] "Internet" Available: http://en.wikipedia.org/wiki/Internet, [March 16, 2011].

[4] "Email Metrics Report" Internet: http://www.maawg.org/email_metrics_report, [April 20, 2011].

[5] "Brasil assume a liderança do spam mundial em 2009, diz Cisco." Internet: http://idgnow.uol.com.br/seguranca/2009/12/08/brasil-assume-a-lideranca-do-spam-mundial-em-2009-diz-cisco/, December 8, 2009 [April 22, 2011].

[6] Dan Fletcher, "A Brief History of Spam" Internet: http://www.time.com/time /business/article/0,8599,1933796,00.html, November 2, 2009 [April 22, 2011]

[7] "Email Metrics Report" Internet: http://www.maawg.org/sites/maawg/files/news/ MAAWG_2010-Q1Q2_Metrics_Report_13.pdf, November 2010, [April 20, 2011].

[8] "How Gmail Blocks Spam" Internet: http://googlesystem.blogspot.com/2007/10/ how-gmail-blocks-spam.html, October 29, 2007 [April 28, 2011].

[9] "Gmail Help articles" Internet: http://mail.google.com/support/bin/answer.py? answer=78759 January 24, 2011 [April 29, 2011].

[10] Laura Marcus, "Yahoo downgrades anti spam measure after causing BT email chaos" Internet: http://www.guardian.co.uk/technology/2008/may/15/yahoo.spam, May 15, 2008 [May 2, 2011].

[11] Laura Marcus, "Yahoo downgrades anti spam measure after causing BT email chaos" Internet: http://www.guardian.co.uk/technology/2008/may/15/yahoo.spam, May 15, 2008 [May 2, 2011].

ISSN 2348 – 7968

[12] "Junk Email Filters" Internet: http://mail.live.com/mail/junkemail.aspx, [May 4, 2011].
[13] Kieren McCarthy, "Microsoft forces Sender ID on Hotmail users" Internet: http://news.techworld.com/security/3908/microsoft-forces-sender-id-on-hotmail-users/, June 23, 2005 [May 9, 2011].
[14] Krebs Brian, (November 12, 2008). "Host of Internet Spam Groups Is Cut Off". January 27, 2009. Available: http://en.wikipedia.org/wiki/McColo [May 13, 2011].
[15] "2008 The year in spam" Internet: http://googleenterprise.blogspot.com/2009/01/ 2008-year-in-spam.html, January 26, 2009 [May 12, 2011].
[16] John Leyden, (21st November 2008). "McColo shutdown" Available: http://www.theregister.co.uk/2008/11/21/mccolo_shutdown_analysis/ [May 13, 2011].
[17] Google Team, "2008 the year in spam" Internet: http://googleenterprise. blogspot.com/2009/01/ 2008-year-in-spam.html, January 26, 2009 [May 12, 2011].
[18] Stefanie Hoffman, (November 12, 2008). "ISP McColo shut down after connection found to spammers" Available: http://www.crn.com/news/security/ 212002220/isp-mccolo-shut-down-after-connection-found-to-spammers.htm, [May 13, 2011].

First Author: - I have completed bachelor degree (B.Sc.) in 2002 and master degree (M.C.A.) in 2005. I have been appointing as a assistant professor in INSB Institute of Information Technology and Management Studies BCA College, Idar since 2007 which is affiliated to North Gujarat University, Patan. I am working as a research scholar in Mewar University Chhittogarh (Rajasthan) since 2010. My research interest is in IP routing, Network Protocols, server mirroring etc...

Second Author: - Dr. Vikram Kaushik have been working as a director in N.S.V.K.M.S., MCA College, Visnagar, situated in Mahesana district in Gujarat. He had PhD degree in ERP system from Hemchandracharya North Gujarat University, Patan.