FIGHTING SPAM: MOTIVATING AN ACCOUNT-BASED APPROACH

Guido Schryen
Institute of Business Information Systems • RWTH Aachen University
Templergraben 64 • 52062 Aachen • Germany
schryen@winfor.rwth-aachen.de

ABSTRACT

Spam as unsolicited e-mail to a large number of recipients is known to become an increasingly disturbing and costly issue of electronic business and Internet traffic. Mainly technical-oriented approaches are applied with a focus on blocking, filtering, and authentication mechanisms based on the domain name system. They come along with different drawbacks and have all low effectiveness in common. The article sketches these approaches, shows its limitations, and proposes an account-based approach where the number of e-mails per day and account is restricted.

KEYWORDS

e-mail, spam, filtering, blocking, LMAP, SMTP account

1. INTRODUCTION

Spam as unsolicited e-mail to a large number of recipients is known to become an increasingly disturbing and costly issue of electronic business and Internet traffic. Companies, non-profit organizations, and individuals get this kind of e-mail to an extent that has certainly crossed the border of just being bothersome. For example, as of mid-2003 about 83% of the e-mail messages received by Microsoft Hotmail was spam. That was around 2.5 billion out of nearly 3 billion messages on a typical day (Microsoft Corporation, 2004).

Internet service providers (ISP) as well as e-mail receiving organizations have to address a couple of times more e-mail messages than necessary by using higher bandwidths, faster hardware, and spam filtering software. This eventually leads to additional costs. Moreover, spam binds employees' attention and time not only due to the deleting operation but more due to reading the spam e-mail before classifying it as unsolicited mail. All this is reason enough to be concerned about the Internet's future capability to maintain the unique feature of a world-wide, ubiquitous, and cheap communication system.

Although many very different approaches have been proposed, the main defense strategies implemented nowadays are content based filtering and source based blocking mechanisms, heuristics still struggling with several problems sketched below. Recently, approaches were proposed where sender authentication bases on extended DNS (domain name system) entries. This article describes the main shortcomings of theses approaches and motivates an account-based approach against spam.

.

2. FILTERING, BLOCKING, AND AUTHENTICATION

The most important approaches are either legal/regulatory, social, economic, or technical ones. Blocking e-mails is a broadly used mechanism where an e-mail passes or is rejected due to the IP address of the sending e-mail mail transfer agent (MTA). When e-mail MTAs, sometimes called relays, are known to support spamming they are put on a black list and each time an e-mail comes from such an address it is blocked. Black lists work more affectively when they are synchronized with their counterparts on other servers or stored centrally. Spamhous Block List (The Spamhaus Project, 2004) is an example for an Internet

service offering a real time block list. Analogously, white lists contain trustful IP addresses. However, black lists and white lists suffer from IP spoofing where spamming e-mail MTAs label IP packets with wrong IP numbers. Moreover, spammer often change their relays and hence their IP numbers. Blocking whole ISP or ESP might be acceptable even when solicited e-mails might be blocked, but blocking whole regions or countries can easily lead to a digital divide.

Recently, grey lists (Harris, 2003) are brought into operation: They take advantage of the fact that spamming e-mail MTAs often don't implement the standardized "resume feature" according to which a once rejected e-mail is sent again after some minutes. When during a specific time window the same e-mail arrives a second time it may pass.

While blocking is strictly IP-based, filtering can rely on all e-mail data. If it is restricted to meta data mostly found in the header it is called origin-based filtering; this can include the content of the FROM field, of the SUBJECT field, or/and the RECEIVED field and even the used character set refering to the sender's country. Unfortunately, these data can be easily spoofed by a spammer, as the Simple Mail Transfer Protocol (SMTP) as the regular Internet mail protocol was not designed to live in a "dirty world".

Content-based filtering relies on the body data and often looks for keywords or specific patterns characterized by sequences of semicolons and the first 32 non-printing ASCII characters like "CR" (carriage return). A well accepted and effective probabilistic content-based filtering approach is Bayesian filtering (Provost, 1999; see http://www.niedermayer.ca/papers/bayesian/bayes.html for a good introduction into Bayesian basics and networks).

Blocking as well as filtering suffer from two possible classification failures: "false-negative e-mails" are spam e-mails although delivered, false-positive e-mails are innocent emails that get mistakenly identified as spams. The latter ones are probably the most critical ones since important information remains unread. A prominent example is the case of the British „House of Commons" where members didn't got discussion papers regarding the "Sexual Offences Bill" due to a too restrictive filtering mechanism (BBC, 2003).

Spammers often exploit that the sender's identification is not mandatory; hence, they spoof the sender's e-mail address. A family of DNS-based (domain name system) approaches has occurred where it is checked whether a message that claims to be from `buffy@sunnydale.com` was actually sent from the `sunnydale.com` organization or not. If not, the mail is a forgery. Each receiving MTA can use the extended mail exchange record (MX record) of the sender´s domain in order to verify if the sender´s IP address is a valid one attached to the sender´s domain. Reverse MX (RMX) (Danisch, 2003), Designated Mailers Protocol (DMP) (Fecyk, 2003), Sender Policy Framework (SPF) (Lentczner and Wong, 2004) partially realized and tested by AOL, and Microsoft's Caller ID for E-Mail (Microsoft Corporation, 2004) belong to the most discussed approaches. They aim at authentication of the sending MTA and belong to the Lightweight MTA Authentication protocols (LMAP) (Levine et al., 2004). The Anti-Spam Research Group (ASRG) of the Internet Research Task Force (IRTF) hasn't made a standardization decision yet.

ICANN (Internet Corporation for Assigned Names and Numbers) has just presented a candidate for a new TLD (top level domain), called .mail and proposed by Spamhaus (ICANN, 2004). According to this approach, each mail server must be registered with a .mail suffix, i.e. ICANN's mail server (currently being `icann.org`) would have to be changed into `icann.org.mail`. Then, the DNS-based approaches are set up.

However, the DNS-based approaches are annulled when Trojan horses, worms, or viruses are embedded into unsuspecting client computers (Garfinkel, 2004) and employ the client's e-mail address, smtp server, and its access data. Then, all DNS-based tests succeed. The German IT magazine "c't" reports that spammer buy addresses of computers affected with Trojan horses from people consciously distributing them (Heise, 2004). These Trojan horses can serve as spam robots.

3. AN ACCOUNT-BASED APPROACH

Another way to prevent spamming is to restrict the number of e-mails per day and account in a way that normal e-mail communication is not affected but spammers cannot go on sending junk mail. This addresses the need of spammers to send easily a huge number of e-mails, generally millions. In principle, each time a user wants to send a queue of e-mails he has to set up a SMTP (simple mail transfer protocol) connection to that e-mail server managing the account for his outgoing e-mails. Before accepting an e-mail the server

checks if the sender has still e-mail credits, i.e. his counter has not reached the limit. If this test fails the server rejects the e-mail by sending the reply code “554 Transaction failed” or – even better – a new error code “xyz No mail credit available” yet to be defined. If the user has still credits then the e-mail is accepted and the counter gets incremented. The counter has to be reset to 0 on midnight or at another fixed time.

In order to make this approach successfully and effectively work the following requirements have to be met:

- fixing an appropriate number of e-mails allowed to be sent
- providing exceptions for regular e-mail newsletters
- secure maintenance of counters
- use of SMTP Service Extension for Authentication (Myers, 1999)
- demand to set up an e-mail account manually

On one hand the number of e-mails allowed to be sent per day and account must not restrict regular e-mail behavior, on the other hand it should be chosen as small as possible. Problems may occur in order to support regular newsletters, solicited mass e-mail. Exceptions regarding exceeding usual credits have to be provided. Either there is no restriction for specific accounts or there are sufficiently high credits arranged. Mechanisms for fixing (possibly dynamic) appropriate limits have still to be found.

The counters must be protected from any unauthorized change, no user shall be enabled to fiddle its value.

Like accounts for incoming mails (POP accounts or IMAP accounts) it is important to protect SMTP accounts from unauthorized access as getting e-mail addresses and SMTP server data is no big challenge for spammers. With SMTP Service Extension for Authentication (SMTP-AUTH) there is a mechanism for authentication and an optional negotiation of a security layer for subsequent protocol interactions. Unfortunately, many SMTP servers do not use SMTP-AUTH and are open for everybody (open relays). However, SMTP-AUTH allows authentication without negotiation of a security layer. This allows attackers to hijack the SMTP connection and send e-mails to the SMTP server before the regular user can close the SMTP connection.

To prevent spammers from sending millions of e-mails it is also necessary to restrict the number of SMTP e-mails accounts. Setting up one must not be performed automatically but has to require little manual work, e.g. getting a number or word out of a picture provided by the email service provider (ESP) and entering it into a submission form to activate the account. This procedure is a visual CAPTCHA process (Completely Automated Public Turing test to tell Computers and Humans Apart) that is implemented by some e-mail providers like Yahoo and Hotmail. However, current implementations have been already compromised: Mori present an algorithm and program that captures the texts of 92% of Yahoo’s pictures; spammers can exploit this weakness and finally set up an arbitrary number of e-mail accounts automatically. Another attack at visual CAPTCHA processes proceeds as follows: the spammer puts the ESP’s picture on his own web site and asks users to read the text and enter it in a text field manually to gain access to adult information. The spammer puts the text field’s content in the corresponding text field of the ESP’s form. All this can be done automatically.

Provided that the requirements above are met, let 200 be the number of e-mails that can be sent from an account per day, then a spammer would have to set up 5000 e-mail accounts manually in order to send one million e-mails, a quantity that is common for spammers.

4. CONCLUSION

Current approaches against spam e-mails and their coaction have not shown satisfying effectiveness. An account-based approach restricting the number of e-mails per day and account might help to improve this dilemma by also preventing attackers from spamming from infected computers. However, there is much detailed work to do regarding conceptualization and implementation. The Institute of Business Information Systems of the RWTH Aachen University is currently developing such a (spam prevention) approach where e-mail clients remain unaffected and only little modifications of e-mail protocols are necessary.

REFERENCES

BBC (2004) *E-mail vetting blocks MPs' sex debate* [Internet]. Available from <http://news.bbc.co.uk/1/hi/uk_politics/2723851.stm> [Accessed 26 April, 2004]

Danisch, H. (2003) *The RMX DNS RR and method for lightweight SMTP sender authorization* [Internet] Internet Draft (category: experimental). Available from <http://www.ietf.org/internet-drafts/draft-danisch-dns-rr-smtp-03.txt> [Accessed 26 April, 2004]

Fecyk, G. (2003) *Designated Mailers Protocol - A Way to Identify Hosts Authorized to Send SMTP Traffic* [Internet] Internet Draft (category: experimental). Available from <http://www.pan-am.ca/dmp/draft-fecyk-dmp-01.txt> [Accessed 26 April, 2004]

Garfinkel, S. (2004) *False Hope for Stopping Spam* [Internet] MIT Enterprise Technology Review, 04 February, 2004. Available from <http://www.technologyreview.com/articles/wo_garfinkel020404.asp> [Accessed 26 April, 2004]

Harris, E. (2003) *The Next Step in the Spam Control War: Greylisting* [Internet]. Available from http://projects.puremagic.com/greylisting/ [Accessed 26 April, 2004]

Heise (2004) *Uncovered: Trojans as Spam Robots* [Internet], 21 February, 2004. Available from <http://www.heise.de/english/newsticker/news/44879> [Accessed 26 April, 2004]

ICANN (2004*) New sTLD RFP Application .mail* [Internet]. Available from http://www.icann.org/tlds/stld-apps-19mar04/mail.htm [Accessed 26 April, 2004]

IEEE Computer Society Conference on Computer Vision and Pattern Recognition. 16.-22. June, 2003. Wisconsin. *Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA*. Mori, G. and Malik, J. Available from http://www.cs.berkeley.edu/~mori/research/papers/mori_cvpr03.pdf Accessed 26 April, 2004]

Lentczner, M. and Wong, M.W. (2003) *Sender Policy Framework (SPF) - A Convention to Describe Hosts Authorized to Send SMTP Traffic* [Internet] Internet Draft (category: experimental). Available from <http://spf.pobox.com/draft-mengwong-spf-00.txt> [Accessed 26 April, 2004]

Levine, J. et al. (2004) *Lightweight MTA Authentication Protocol (LMAP) Discussion and Comparison* [Internet] Internet Draft (category: experimental). Available from < http://asrg.kavi.com/apps/group_public/download.php/31/draft-irtf-asrg-lmap-discussion-00.txt> [Accessed 26 April, 2004]

Microsoft Corporation (2004) *Caller ID for E-Mail: The Next Step to Deterring Spam* [Internet]. Available from <http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.mspx> [Accessed 26 April, 2004]

Myers, J. (1999) *RFC 2554 – SMTP Service Extension for Authentication* [Internet] Request for Comments 2554 (category: standards track). Available from < http://www.ietf.org/rfc/rfc2554.txt?number=2554> [Accessed 26 April, 2004]

Provost, J. (1999) *Naive-Bayes vs. Rule-Learning in Classification of Email*. Technical Report AI-TR-99-284. University of Texas at Austin, Artificial Intelligence Lab. Available from <http://www.cs.utexas.edu/users/jp/research/email.paper.pdf> [Accessed 26 April, 2004]

The Spamhaus Project *The Spamhaus Block List (SBL) Advisory Frequently Asked Questions* [Internet]. Available from <http://www.spamhaus.org/sbl/sbl-faqs.lasso> [Accessed 26 April, 2004]