Addressing Spam E-Mail Using Hashcast

Kevin Curran, University of Ulster, UK
John Stephen Honan, University of Ulster, UK

ABSTRACT

This paper investigates the problem of e-mail spam and identifies methods to efficiently minimize the volumes. It is argued that the usefulness of e-mail and its potential for future growth are jeopardized by the rising tide of unwanted e-mail, both SPAM and viruses. This threatens to wipe out the advantages and benefits of e-mail. An important flaw in current e-mail standards (most notably SMTP) is the lack of any technical requirement that ensures the reliable identification of the sender of messages. A message’s domain of origin can easily be faked, or “spoofed”. We focus on the Hashcash proof-of-work approach and investigate the feasibility of implementing a Hashcash-based solution. We conclude that a hybrid antispam system in conjunction with a legal and policy framework is best. However, this needs to be agreed on and implemented by the main industry players and technical bodies to be successful.

Keywords: e-mail; e-mail message filtering; hashcash; information and communication technologies; information filtering; Internet technologies; junk mail; spam

INTRODUCTION

Spam can be defined as unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups. Spam can be categorized as follows:

- **Junk mail**: mass mailings from legitimate businesses that is unwanted.
- **Non-commercial spam**: mass mailings of unsolicited messages without an apparent commercial motive including chain letters, urban legends, and joke collections.
- **Offensive and pornographic spam**: mass mailings of adult advertisements or pornographic pictures.
- **Spam scams**: mass mailings of fraudulent messages or those designed to con people out of personal information for the purpose of identity theft and other criminal acts.
- **Virus spam**: mass mailings that contain viruses, Trojans, malicious scripts, and so forth.
Spoofing (Templeton & Levitt, 2003) is a technique often used by spammers to make them harder to trace. Trojan viruses embedded in e-mail messages also employ spoofing techniques to ensure the source of the message is more difficult to locate (Ishibashi et al., 2003). Spam filters and virus scanners can only eliminate a certain amount of spam and also risk catching legitimate e-mails. As the SoBig virus has demonstrated, virus scanners themselves actually add to the e-mail traffic through notification and bounceback messages. SMTP is flawed in that it allows these e-mail headers to be faked and does not allow for the sender to be authenticated as the “real” sender of the message. If this problem can be solved, it will result in a reduction in spam e-mail messages, more security for existing e-mails, and allow e-mail viruses to be tracked down and stopped more effectively (Schwartz & Garfinkel, 1998). This approach is known as “Trusted E-mail”. The Simple Mail Transport Protocol is the basic protocol used by servers to send e-mail messages to each other (Schwartz & Garfinkel, 1998). It defines how the conversation should take place and the format of the data that is exchanged during the conversation. The e-mail is composed in the senders Mail User Agent (MUA); this is usually a piece of software on the senders PC, such as Outlook or Eudora, but can also consist of a Web-based e-mail system, such as Yahoo! or Hotmail. The message might look as shown in Example 1.

There are two parts to the above message: the header and the body. The header contains information about the message, such as who it is to be sent to. The body contains the actual text of the message. When the sender clicks the “Send” button in their MUA, some additional headers are automatically added to the message by the MUA. See Example 2 for an example (the new headers added by the MUA are in bold).

The message Id is a unique identifier added by the MUA, the X-Mailer is the name and version of the MUA software used to compose the e-mail. To deliver the

**Example 1.**

Date: Thursday, 1 Apr 2004 12:40:30 -0000
From: you@yourhost.com
To: John & Kevin < jhonan@silveronion.com>
Subject: Party on Sat night

"There’s a party on Saturday night, would you like to go?"

**Example 2.**

Date: Thursday, 1 Apr 2004 12:40:30 -0000
From: you@yourhost.com
To: John & Kevin < jhonan@silveronion.com>
Subject: Party on Sat night
Message-Id: <002d01c444ca$bdaa3e70$5b92cbc1@yourhost.com>
X-Mailer: Microsoft Outlook Express 6.00.2800.1409

"There’s a party on Saturday night, would you like to go?"
Related Content

Optimized Communication Architecture of MPSoCs with a Hardware Scheduler: A System-Level Analysis
www.igi-global.com/chapter/optimized-communication-architecture-mpsocs-hardware/74247?camid=4v1a

Retained-Key Encryption
www.igi-global.com/article/retained-key-encryption/79277?camid=4v1a

Distributed and Fixed Mobility Management Strategy for IP-based Mobile Networks
www.igi-global.com/article/distributed-fixed-mobility-management-strategy/60239?camid=4v1a
Resource Allocation in Heterogeneous Broadband Wireless Access Networks
Chetna Singhal and Swades De (2014). Convergence of Broadband, Broadcast, and Cellular Network Technologies (pp. 51-76).
www.igi-global.com/chapter/resource-allocation-in-heterogeneous-broadband-wireless-access-networks/108088?camid=4v1a