SPIT: Spam Over Internet Telephony

Kevin Curran
University of Ulster, Magee Campus, UK

Ciaran O Donnell
University of Ulster, Magee Campus, UK

INTRODUCTION

Spam in the computer does not simply mean ads. Spam is any message, article, or ad that repeats itself an unacceptable number of times so that it causes annoyance. The content of the spam is of no importance. It could contain your simple "Make Money Fast" hyperlink or a beautiful piece of poetry, but if the message is continuously repeated it becomes spam. The term spam is thought to have been taken from a famous Monty Python sketch. In that sketch spam came with everything the people ordered and the waitress would be constantly saying the word spam. Therefore the meaning of spam is something that repeats itself causing much anger or annoyance. Spam can be categorized as follows:

- **Junk mail:** Mass mailings from legitimate businesses that is unwanted.
- **Noncommercial 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 (Schwartz & Garfinkel, 1998) 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, Yamai, Abe, & Matsuura, 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 (Geer, 2004). This article looks at a new type of spam known as spam over Internet telephony (SPIT).

SPAM

Spam has been used for a few different types of techniques. One was to overrun the computer with so much data and information that it crashes. Another technique is to send unwanted messages to people during a chat session by using a computer program known as a spambot. A spambot is used to get e-mail addresses from the Internet so that it can build a mailing list for sending unwelcome e-mail. A spambot can gather e-mail addresses from anywhere including Web sites, message boards, and chat rooms. Unwanted messages being sent to an e-mail address is also called spam or more affectionately "junk mail." This is the most popular type of spam (Boutin, 2004).

Spam has grown because of the new advances being made in communication connectivity. The first major type of spam was flooding message boards with unwanted messages (Simpson, 2002). This first happened around 1993 when the first giant spam was made by a Clarence Thomas. This spam contained a religious theme stating that our sins were to blame for the destruction in the world. This caused widespread controversy. Although Clarence caused the first giant spam, the most famous spam was caused by two lawyers called Canter and Siegel. In this instance, they flooded the message boards with spam offering the chance for people to take part in a Green Card Lottery. This

spam also received a lot of complaints but went on to make the two men quite famous. When e-mail became widely used among home users, spammers saw this as the perfect way to advertise products and services. The vast quantities of modern spams offer get rich quick schemes, adult Websites or the perfect body in days. Some also contain viruses and worms hoping to break into a system. Some estimates claim that over 50% of all e-mail is spam (Littauer, 2004).

As technology developed, people began using chat rooms to keep in contact with friends and colleagues. The spammers once again are viewing this as the perfect opportunity to advertise. This resulted in the birth of SPam over Instant Messaging (SPIM). Spim is caused by spambots that collect instant messaging user names off the Internet and imitate a human user by sending spam to the user names through an instant message. The spim will contain a link to a Web site that the spim is trying to advertise. The main difference between instant messaging and e-mail is that e-mail is open to anybody while instant messaging is controlled by companies such as AOL and Microsoft. This means that there is more control over spam on the instant messengers than on e-mail. The IP address of the spimmer can be traced and blocked from using that site again. However, spim still remains an attractive option for the advertisers as once the spim is sent, users will see it in a dialogue box. This means the advertiser will know the message has been read, unlike e-mail spam which could be deleted without it been opened. This advantage over spam has seen spim grow at about three times the rate of the normal e-mail spam.

METHODS USED TO MINIMIZE SPAM

Here are the main methods being used to prevent spam, together with their pros and cons (Graham, 2003).

Complain to the Spammer's ISP

When spam volumes were quite low, it was often effective enough to send a complaint e-mail to the ISP of the spammer. The ISP could then investigate and close down the spammers account. The advantages of this approach are that it can achieve direct action from the ISP to get the spammer shut down fairly quickly. The disadvantages are that the volumes of spam are now too high to allow a complaint to be sent and followed up on for every spam that is sent. In addition, it is often difficult to determine from the headers who the ISP of the spammer actually is. Spammers shut down in one ISP or hosting company will just open accounts with someone else. The spam blocking efficiency of this method is medium. It may block one spammer, but others will get through. False positives however do not occur (Goodman & Rounthwaite, 2004).

MAIL SERVER IP BLACKLISTS

An IP blacklist is a list of the IP addresses of spammers' mail servers, or relay servers (unsecure servers which allow spammers to forward e-mail). These lists are maintained by volunteer groups and antispam organizations. ISPs can then subscribe to these lists and refuse to accept e-mail from any listed IP addresses. This is a very precise method of blocking potential spam; however, these blacklists can never hope to list every single IP address that spammers use. Spammers often end up listing legitimate IP addresses, or blacklisting an entire domain (1,000 ordinary users could get blacklisted for the actions of one spammer). The source IP is spoofable by the spammer, which means the spammer can bypass the blacklist. The Spam blocking efficiency is high. IT blocks all spam from given IP addresses; however, false positives are quite likely. If a legitimate sender uses a blacklisted IP block, their e-mail will get stopped (Tserefos, Smythe, Stergiou, & Cvetkovic, 2005).

Signature Based Filtering

This method compares incoming e-mails against a signature database of known spam e-mails. The system calculates a checksum signature of an incoming spam message, and adds it to the database. Any incoming e-mails are then compared to this database to see if the e-mail is spam. The advantages of this are that it is an accurate way of matching spam. It can achieve very low "false positives" because only definite spasm are matched based on the hash signature of their contents. The disadvantages are that in order to be detected as spam, the message will have to exist in the database of pre-sent spam messages. If the spam is new, it may not exist in the database at this stage, and therefore won't get blocked. The database must be kept up to date (Graham, 2003). The main problem however, is