Chapter XXX
Antispam Approaches Against Information Warfare

Hsin-Yang Lu
Technology Marketing Corporation, USA

Chia-Jung Tsui
Syracuse University, USA

Joon S. Park
Syracuse University, USA

ABSTRACT

The term "spam" refers to unsolicited bulk e-mail that people do not want to receive. Today it is gradually becoming a serious problem that results in significant cost both to e-mail receivers and to ISPs (Internet Service Providers). More and more people have become concerned about the issue and are making efforts to develop various anti-spam approaches, some of which are in-process proposals, while others are currently in use. In this chapter, key anti-spam approaches that include filtering, remailers, e-postage, hashcash, and sender authentication, are analyzed and discussed how these antispam approaches can be used against information warfare and cyber terrorism. Furthermore, we analyze vulnerabilities in each approach and recommend possible countermeasures. Technical details and comparisons of each antispam approach are not discussed in this chapter because of space limitations.

BACKGROUND

According to the Federal Bureau of Investigation (FBI), cyber terrorism is "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by sub-national groups or clandestine agents" (Pollitt, 1997). While the FBI focuses cyber terrorism more on political aspects, some people define it as "any occurrence that can compromise the integrity of an electronic business operation" (Gustin, 2004).

Today, cyber terrorists' major weapons include Trojan horses, viruses, worms, denial-of-service (DoS) programs, password/ID theft tools, and other malicious software. The term "spam" refers to unso-

licited and inappropriate bulk e-mail that recipients do not want to receive (Cerf, 2005; Denning, 1992; Neumann & Weinstein, 1997). A cyber terrorist can exploit spam techniques as complementary ways to use their weapons in information warfare.

The e-mail system is one of the most common communication platforms these days, and there are always some people who lack security awareness, no matter how much antiterrorism programs or knowledge is disseminated. Therefore, from a cyber terrorist's point of view, spamming millions of people with malicious codes or links to false Web sites is one of the most effective ways to reach as many gullible people as possible to compromise security. In this chapter, we analyze key antispam approaches, including filtering, remailers, e-postage, hashcash, and sender authentication, and we discuss how antispam approaches can be used against information warfare and cyber terrorism. Furthermore, we analyze vulnerabilities in each approach and recommend possible countermeasures.

SPAM FILTERING

Typically, there are two categories of spam filtering: rule-based (heuristic) and Bayesian-based (statistical) approaches.

The rule-based filtering approach was the most used until 2002. It checks predefined lists and patterns that indicate spam is present (Park & Deshpande, 2005). In essence, e-mail from senders defined in the black lists is considered to be spam and, consequently, are filtered out, whereas e-mail from those senders defined in the white lists are considered to be legitimate messages. For effective usage, these lists should be kept up to date constantly. As for the patterns, they include, but are not limited to, specific words and phrases, many uppercase letters and exclamation points, malformed e-mail headers, dates in the future or the past, improbable return addresses, strange symbols, embedded graphics, and much fraudulent routing information (Androutsopoulos, Koutsias, Chandrinos, & Spyropoulos, 2000; Cournane and Hunt, 2004; Cranor & LaMacchia, 1998; Hidalgo, Opez, & Sanz, 2000; Ioannidis, 2003). The filter scores each message scanned. Those whose scores exceed a threshold value will be regarded as spam. The main drawback of a rule-based filter is that e-mail headers can be easily manipulated with the very real possibility that a spammer has falsified the header information, including the fields for domain name service (DNS) names, senders' e-mail addresses, and delivery paths, so the e-mail appears to be from a legitimate source. Since the rules are static, spammers can usually find ways to tune e-mails in order to circumvent the filter, once new rules are set. If the filter is available to the public, then spammers can even test their spam on the filter before sending it out.

On the contrary, the Bayesian-based (Androutsopoulos et al., 2000; Sahami, Dumais, Heckerman, & Horovitz, 1998; Schneider, 2003) filtering approach is more dynamic, since it learns over time what each user considers spam to be. Basically, it uses the knowledge of prior events to predict future events. If a user marks messages as spam, the Bayesian filter will learn to automatically put messages from the same source or with the same kind of patterns into a spam folder the next time such messages are delivered. If the user does not mark those messages as spam, the filter will learn to consider them legitimate. Because Bayesian filters can be trained, their effectiveness improves continually. On the other hand, since they need to be trained, a user has to rectify them every time they misclassify an e-mail. Fortunately, the more examples or patterns that are learned by the filter, the less additional work will be required of a user.

One major role that spam plays in cyber terrorism is "phishing," an emerging criminal technique that solicitesusers for their personal or financial information. For example, spammers can make spam almost identical to official bank e-mails, requesting customers' financial information, assuming some recipients happen to be targets. In that case, the rule-based filtering approach described above checks predefined lists and patterns that indicate spam. In order to pass the list-based filtering, namely black lists and white lists, phishing e-mail can simply use a bank's official outgoing e-mail address since spammers do not expect