Detecting Spamming Activities by Network Monitoring with Bloom Filters

Po-Ching Lin*, Ping-Hai Lin*, Pin-Ren Chiou*, Chien-Tsung Liu**

**Department of Computer Science and Information Engineering, National Chung Cheng University, Chaiyi, Taiwan*

***CyberTrust Technology Institute, Institute for Information Industry, Taipei, Taiwan*

{pclin,lph99m}@cs.ccu.edu.tw, littlecho@cloud.littlecho.tw, netsaga@iii.org.tw

Spam delivery is common in the Internet. Most modern spam-filtering solutions are deployed on the receiver side. They are good at filtering spam for end users, but spam messages still keep wasting Internet bandwidth and the storage space of mail servers. This work is therefore intended to detect and nip spamming bots in the bud. We use the Bro intrusion detection system to monitor the SMTP sessions in a university campus, and track the number and the uniqueness of the recipients' email addresses in the outgoing mail messages from each individual internal host as the features for detecting spamming bots. Due to the huge number of email addresses observed in the SMTP sessions, we store and manage them efficiently in the Bloom filters. According to the SMTP logs over a period of six months from November 2011 to April 2012, we found totally 65 dedicated spamming bots in the campus and observed 1.5 million outgoing spam messages from them. We also found account cracking events on 14 legitimate mail servers, on which some user accounts are cracked and abused for spamming. The method can effectively detect and curb the spamming bots with the precision and the recall up to 0.97 and 0.96.

***Keyword*—spamming activities, network monitoring, botnet, Bloom filters, detection.**

Po-Ching Lin (M’06) received the B.S. degree in computer and information education from National Taiwan Normal University, Taipei, Taiwan, in 1995, and the M.S. and Ph.D. degrees in computer science from National Chiao Tung University, Hsinchu, Taiwan, in 2001 and 2008, respectively.

He was a VISITING SCHOLAR with Prof. Vern Paxson at International Computer Science Institute (ICSI), Univ. of California, Berkeley from 2007 to 2008, and became a SENIOR ENGINEER at Networks & Multimedia Institute, Institute for Information Industry from 2008 to 2009. He joined the faculty of the Department of Computer and Information Science, National Chung Cheng University (CCU), Chiayi, Taiwan, in August 2009. He is currently an Assistant Professor. His research interests include network security, network traffic analysis, and performance evaluation of network systems.

Prof. Lin is also a member of Chinese Cryptology and Information Security Association (CCISA). He was a member of technical program committee (TPC) in IEEE ICC 2008, and will be a member of TPC in IEEE Globecom 2013. He received an outstanding paper award in ICACT 2012, and a best paper award in IEEE Globecom 2012.