Blocking Spam Sessions with Greylisting and Block Listing based on Client Behavior

Pin-Ren Chiou*, Po-Ching Lin*, Chun-Ta Li*

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

{cpj97u,pclin,lcta99m}@cs.ccu.edu.tw

***Abstract*—Greylisting and real-time block listing are two common mechanisms for spam filtering. The former can efficiently reduce the number of spam sessions, but can be easily evaded if spammers retry spam delivery within a period of time. The latter can detect and reject the clients with poor reputation during SMTP sessions by looking up an external blacklist. Its weaknesses are the high false-positive rate and a lack of locality. We design a method of dynamically updating the greylist and block list based on the delivery behavior of spammers to block spam sessions in time. The method is implemented on a mail gateway in a senior high school. In our experiments with the real-world mail traffic for a month, the method can block 70.29% and 69.21% of the known and possible messages in the spam sessions with greylisting and block listing. The forward and reverse DNS lookups are also adopted to further reduce the false-positive rate to under 0.01%. Therefore, the required system resources for further spam filtering on mail servers can be greatly saved by blocking most of the spam sessions in time.**

***Keyword*—Greylist, block list, spam, IP reputation, delivery behavior.**

Pin-Ren Chiou (S'12) received the B.S degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan, in 2012. He is currently a graduate student majoring in computer science and information engineering at National Chung Cheng University, Chiayi, Taiwan. His research interests include network security and network traffic analysis. He is also a student member of the IEEE.