UCF Stands For Opportunity

THE DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, CS DIVISION

Presents the Fall 2012 EECS Seminar Series

Dr. Geroge Kesidis

The Pennsylvania State University

"Salting Public Traces with Attack Traffic to Test Flow Classifiers "

Thursday, November 1, 2012 ● 2:00 p.m. ● HEC 101

ABSTRACT

We consider the problem of using flow-level data for detection of botnet command and control (C&C) activity in the broader context of packet-flow classification (which we will summarize). We find that current approaches do not consider timing-based calibration of the C&C traffic traces prior to using this traffic to salt a background traffic trace. Thus, timing-based features of the C&C traffic may be artificially distinctive, potentially leading to (unrealistically) optimistic flow classification results. We first observe that round-trip times (RTT) of the C&C traffic are significantly smaller than that of the background traffic. So, the timing-based features of the "replayed" botnet traffic are calibrated by estimating eligible RTT samples from the background traffic. We then salt C&C traffic, and design flow classifiers under four scenarios: with and without calibrating timing-based fea- tures of C&C traffic, without using timing-based fea- tures, and calibrating C&C traffic only in the test set. Results are given for several supervised classifiers, evaluating botnet C&C traffic classification precision, recall, and overall classification accuracy. Our experiments reveal to what extent the presence of timing artifacts in botnet traces leads to changes in classifier results. Under the flow feature-set we employed, Zeus C&C activity on port 80 was poorly separated from background web traffic.
This motivated more recent work on domain adaption and anomaly detection which we will also summarize.

BIOGRAPHY

George Kesidis received his M.S. and Ph.D. in EECS from U.C. Berkeley in 1990 and 1992 respectively. He was a professor in the E&CE Dept of the University of Waterloo, Canada, from 1992 to 2000. Since 2000, he has been a professor of CSE and EE at the Pennsylvania State University. His research, including several areas of computer/communication networking and machine learning, has been primarily supported by NSERC of Canada, NSF and Cisco Systems URP. He served as the TPC co-chair of IEEE INFOCOM 2007 among other networking and cyber security conferences. He has also served on the editorial boards of the Computer Networks Journal, ACM TOMACS and IEEE Journal on Communications Surveys and Tutorials. Currently, he is an Intermittent Expert for the National Science Foundation's Secure and Trustworthy Cyberspace (SaTC) program. His home page is http://www.cse.psu.edu/~kesidis

DEPARTMENT OF ELECTRICAL ENGINEERING & COMPUTER SCIENCE