National Security Education Center

A CONSORTIUM OF LANL INSTITUTES

UNCLASSIFIED

Information Science and Technology Seminar Series

Michalis Faloutsos
University of California, Riverside

"Detecting Malware: Traffic Classification, Botnets, and Facebook Scams"

Wednesday, February 8, 2012
9:30 - 10:30 AM
TA-3, Bldg. 1690, Room 102 (CNLS Conference Room)

Abstract: In this talk, we highlight two topics of security research from our lab. First, we address the problem of Internet traffic classification (e.g. web, filesharing, or botnet?). We present a fundamentally different approach to classifying traffic that studies the network wide behavior by modeling the interactions of users as a graph. By contrast, most previous approaches use statistics such as packet sizes and inter-packet delays. We show how our approach gives rise to novel and powerful ways to: (a) visualize the traffic, (b) model the behavior of applications, and (c) detect abnormalities and attacks. Extending this approach, we develop ENTELECHEIA, a botnet-detection method. Tests with real data suggests that our graph-based approach is very promising.

Second, we present, MyPageKeeper, a security Facebook app, with 13K downloads, which we deployed to: (a) quantify the presence of malware on Facebook, and (b) protect end-users. We designed MyPageKeeper in a way that strikes the balance between accuracy and computational cost and can operate in real-time. Our initial results are scary and interesting: (a) malware is widespread, with 49% of our users are exposed to at least one malicious post from a friend, and (b) roughly 74% of all malicious posts contain links that point back to Facebook, and thus would evade any of the current web-based filtering approaches.

Biography: Michalis Faloutsos is a faculty member in the Computer Science Department at University of California, Riverside. He received his bachelor's degree at the National Technical University of Athens and his M.Sc and Ph.D. at the University of Toronto. His interests include, Internet protocols and measurements, peer-to-peer networks, network security, BGP routing, and ad-hoc networks. He is actively involved in the community as a reviewer and a TPC member in many conferences and journals. With his two brothers, he co-authored the paper on power laws of the Internet topology (SIGCOMM'99), which is one of the top ten most cited papers of 1999. His most recent work on peer-to-peer measurements have been widely cited in popular printed and electronic press such as slashdot, ACM Electronic News, USA Today, and Wired. Most recently he has focused on the classification of traffic and identification of abnormal network behavior. He also works in the area of Internet routing (BGP), and ad hoc networks routing, and network security, with emphasis on routing.

Los Alamos NATIONAL LABORATORY EST.1943

UNCLASSIFIED

For more information contact the technical host, Stephan Eidenbenz, eidenben@lanl.gov, 667-3742.
Hosted by the Information Science and Technology Center (ISTC)