TEXAS A&M UNIVERSITY at QATAR

The Electrical and Computer Engineering Program presents
ECEN Seminar Series

Detecting domain-fluxing botnets through DNS traffic analysis

Dr. Narasimha Reddy
Texas A&M University

Monday, 14 January 2013, 12 – 1 p.m.

Lecture Hall 238

Light lunch will be served

Botnets have become one of the main threats to Network security. Botnets have been used to stage denial of service attacks, spam campaigns, stealing user passwords and other malicious activities. Detecting botnets has become an important priority for network security.
Recent Botnets such as Conficker, Kraken and Torpig have used DNS based "domain fluxing" for command-and-control, where each Bot queries for existence of a series of domain names and the owner has to register only one such domain name. In this paper, we develop a methodology to detect such "domain fluxes" in DNS traffic by looking for patterns inherent to domain names that are generated algorithmically, in contrast to those generated by humans. In particular, we look at distribution of alphanumeric characters as well as bigrams in all domains that are mapped to the same set of IP-addresses and higher domain names. We present and compare the performance of several distance metrics, including KL-distance, Edit distance and Jaccard measure. We train by using a good data set of domains obtained via a crawl of domains mapped to all IPv4 address space and modeling bad data sets based on behaviors seen so far and expected. We apply our methodology to packet traces collected at a Tier-1 ISP and show that we can automatically detect domain fluxing botnets with minimal false positives.

Narasimha Reddy received a B.Tech. degree in Electronics and Electrical Communications Engineering from the Indian Institute of Technology, Kharagpur, India, in August 1985, and the M.S. and Ph.D degrees in Computer Engineering from the University of Illinois at Urbana-Champaign in May 1987 and August 1990 respectively.

Reddy is currently a J.W. Runyon Professor in the department of Electrical and Computer Engineering at Texas A & M University. Reddy's research interests are in Computer Networks, Storage Systems, Multimedia systems, and Computer Architecture. During 1990-1995, he was a Research Staff Member at IBM Almaden Research Center in San Jose.

Reddy holds five patents and was awarded a technical accomplishment award while at IBM. He has received an NSF Career Award in 1996. He was a faculty fellow of the College of Engineering at Texas A&M during 1999-2000. His honors include an outstanding professor award by the IEEE student branch at Texas A&M during 1997-1998, an outstanding faculty award by the department of Electrical and Computer Engineering during 2003-2004, a Distinguished Achievement award for teaching from the former students association of Texas A&M University and a citation "for one of the most influential papers from the 1st ACM Multimedia conference". Reddy is a Fellow of IEEE Computer Society and is a member of ACM.

FOR MORE INFORMATION:

Noha Ezzat
noha.ezzat@qatar.tamu.edu
+974.4423.0152

Qatar Foundation
TEXAS A&M UNIVERSITY at QATAR