Announcing the Final Examination of Jeffrey Spaulding for the degree of Doctor of Philosophy

Time & Location: June 12, 2018 at 1:00 PM in Research 1 Conference Room 307
Title: D-FENS: DNS Filtering & Extraction Network System for Malicious Domain Names

While the DNS (Domain Name System) has become a cornerstone for the operation of the Internet, it has also fostered creative cases of maliciousness, including phishing, typosquatting, and botnet communication among others. To address this problem, this dissertation focuses on identifying and mitigating such malicious domain names through prior knowledge and machine learning. In the first part of this dissertation, we explore a method of registering domain names with deliberate typographical mistakes (i.e., typosquatting) to masquerade as popular and well-established domain names. To understand the effectiveness of typosquatting, we conducted a user study which helped shed light on which techniques were more "successful" than others in deceiving users. While certain techniques fared better than others, they failed to take the context of the user into account. Therefore, in the second part of this dissertation we look at the possibility of an advanced attack which takes context into account when generating domain names. The main idea is determining the possibility for an adversary to improve their "success" rate of deceiving users with specifically-targeted malicious domain names. While these malicious domains typically target users, other types of domain names are generated by botnets for command & control (C2) communication. Therefore, in the third part of this dissertation we investigate domain generation algorithms (DGA) used by botnets and propose a method to identify DGA-based domain names. By analyzing DNS traffic for certain patterns of NXDomain (non-existent domain) query responses, we can accurately predict DGA-based domain names before they are registered. Given all of these approaches to malicious domain names, we ultimately propose a system called D-FENS (DNS Filtering & Extraction Network System). D-FENS uses machine learning and prior knowledge to accurately predict unreported malicious domain names in real-time, thereby preventing Internet devices from unknowingly connecting to a potentially malicious domain name.

Major: Computer Science

Educational Career:
Bachelor’s of Engineering & Management, BS, 2003, Clarkson University
Master’s of Computer & Information Science, MS, 2013, SUNY Polytechnic Institute

Committee in Charge:
Aziz Mohaisen, Chair, Computer Science
Gary T. Leavens, Co-Chair, Computer Science
Mostafa A. Bassiouni, Computer Science
Xinwen Fu, Computer Science
Clay Posey, Management

Approved for distribution by Aziz Mohaisen, Committee Chair, on May 30, 2018.

The public is welcome to attend.