SCHOOL OF INFORMATICS, COMPUTING, AND ENGINEERING

COMPUTER SCIENCE COLLOQUIUM SERIES

Xiaojing Liao

College of William & Mary

Monday, December 4, 2017

4:00 pm

State Room West, IMU

Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks

Abstract: BulletProof Hosting (BPH) services provide criminal actors with technical infrastructure that is resilient to complaints of illicit activities, which serves as a basic building block for streamlining numerous types of attacks. Anecdotal reports have highlighted an emerging trend of these BPH services reselling infrastructure from lower end service providers (hosting ISPs, cloud hosting, and CDNs) instead of from monolithic BPH providers. This has rendered many of the prior methods of detecting BPH less effective, since instead of the infrastructure being highly concentrated within a few malicious Autonomous Systems (ASes) it is now agile and dispersed across a larger set of providers that have a mixture of benign and malicious clients.

In this talk, I will present the first systematic study on this new trend of BPH services. By collecting and analyzing a large amount of data (25 snapshots of the entire Whois IP address dataset, 1.5 TB of passive DNS data, and longitudinal data from several blacklist feeds), a set of new features are identified that uniquely characterizes BPH on sub-allocations and that are costly to evade. Leveraging such features, the whole IPv4 space is scanned and 39K malicious network blocks are detected. Then, I will show a large-scale study of the BPH service ecosystem, which sheds light on this underground business strategy, including patterns of network blocks being recycled and malicious clients being migrated to different network blocks, in an effort to evade IP address based blacklisting. This study highlights the trend of agile BPH service and points to potential methods of detecting and mitigating this emerging threat.

Biography: Xiaojing Liao is an Assistant Professor in the Department of Computer Science at William and Mary. She received her Ph.D. from Georgia Institute of Technology in 2017. Her research interests include data-driven security and web security, with the specific focus on the investigation of cybercrime and cyber threat intelligence. Her works were published in the top-tier security conference including IEEE S&P, ACM CCS, ISOC NDSS etc. and were widely covered by the mainstream media including New York Times, CNN, Fox News, etc.

INDIANA UNIVERSITY

SCHOOL OF INFORMATICS, COMPUTING, AND ENGINEERING