VirginiaTech

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series, 2014

National Capital Region

Dissecting Bad Codes with Chatter and AVMeter

Speaker: Dr. Aziz Mohaisen
Verisign Labs

Friday, April 11, 2014
1:00PM- 2:00PM, NVC 325

Abstract

Malware classification and family identification are not new problems. However, the rapid evolution of the malware attack and defense ecosystem has enabled much more fruitful research. In this talk, we present our contributions to the domain by reviewing two systems that we at Verisign Labs have named Chatter and AVMeter.

Chatter is a system for representing and leveraging the sequence of events in a malware execution. Whereas calculating and exposing low-level feature values might have ill scalability or gamesmanship effects, Chatter tersely and efficiently captures execution patterns. By creating an alphabet/language to represent runtime behavior, techniques from n-gram processing are used to train a binary classifier that is capable of distinguishing different malware samples with high accuracy. We validate the performance of Chatter on various manually vetted malware families.

AVMeter, is a system for evaluating the performance of antivirus scans and labels. Researchers rely heavily on these outputs in establishing ground-truth for their methods and companies use them to guide mitigation and disinfection efforts. However, there is a lack of research that validates the performance of these antivirus vendors. Utilizing malware samples that have been manually labeled by expert analysts, we reveal dramatic errors in the correctness, coverage, and consistency of current antivirus offerings. We invite the community to challenge assumptions about relying on AV scans and labels as a ground truth for malware analysis and classification.

Biography

Aziz Mohaisen is a senior research scientist at VeriSign Labs. His research interests are broadly focused on the security, privacy, measurement, and analysis of complex and emerging network systems. His recent work has emphasized data-driven security and its applications in malware analysis, network routing, information sharing, and Internet-scale reputation. He obtained his Ph.D. in computer science from the University of Minnesota in 2012. More on his work can be found at: http://www.mohaisen.net