DREXEL UNIVERSITY
Cybersecurity Institute

Research project profile: **malware detection, classification, and mitigation**

Investigators	Bander Alsulamy	Ph.D. student	CS Dept.	Drexel University
	Raymond Canzanese	Ph.D.		Sift Security
	Marcello Balduccini	Assistant Research Professor	CS Dept.	Drexel University
	Spiros Mancoridis	Isaac L. Auerbach Professor	CS Dept.	Drexel University
	Moshe Kam	Professor	Dept. of ECE	NJIT


B. Alsulamy


R. Canzanese


M. Balduccini


S. Mancoridis


M. Kam

Research summary: Despite efforts to mitigate the malware threat, the proliferation of malware continues, with record-setting numbers of malware samples being discovered each quarter. Malware are any intentionally malicious software, including software designed for extortion, sabotage, and espionage. Traditional malware defenses are primarily signature-based and heuristic-based, and include firewalls, intrusion detection systems, and antivirus software. Such defenses are reactive, performing well against known threats but struggling against new malware variants and zero-day threats. Together, the reactive nature of traditional defenses and the continuing spread of malware motivate the development of new techniques to detect such threats. One set of techniques uses features from system call traces to infer malicious behaviors.

This research studies detecting and classifying malicious processes using system call trace analysis. The goal is to identify techniques that are 'lightweight' enough and exhibit a low enough false positive rate to be deployed in production environments. Contributions are: (1) a study of the effects of feature extraction strategy on malware detection performance; (2) the comparison of signature-based and statistical detection techniques for malware detection and classification; (3) the application of sequential detection techniques for malware detection, with the goal of identifying malicious behaviors as quickly as possible; (4) a study of malware detection performance at very low false positive rates; and (5) an extensive empirical evaluation, wherein the performance of the malware detection and classification systems are evaluated against data collected from production hosts and from the execution of recently discovered malware samples. The outcome is a proof-of-concept system that detects the execution of malicious processes in production environments and classifies them using known malware.

Publications related to this research project include:

[1] Raymond Canzanese, Spiros Mancoridis, and Moshe Kam. Run-time classification of malicious processes using system call analysis. *Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALCON)*, Puerto Rico, USA, October 2015.

[2] Marcello Balduccini and Spiros Mancoridis. Action languages and the mitigation of malware. *Proceedings of the First Workshop on Action Languages, Process Modeling, and Policy Reasoning (ALPP)*, Lexington, KY, September 2015.

[3] Raymond Canzanese, Spiros Mancoridis, and Moshe Kam. System call-based detection of malicious processes. *Proceedings of the IEEE International Conference on Software Security and Reliability (QRS)*, Vancouver, British Columbia, August 2015.

[4] Raymond Canzanese, Moshe Kam, and Spiros Mancoridis. Toward an automatic, online behavioral malware classification system. *Proceedings of the International Conference on Self-Adaptive and Self-Organizing Systems (SASO)*, Philadelphia, PA, September 2013.

[5] Raymond Canzanese, Moshe Kam, and Spiros Mancoridis. Multi-channel change-point malware detection. *Proceedings of the 7th IEEE International Conference on Software Security and Reliability (SERE)*, Washington, D.C., June 2013.

This research is partially supported by the following grants:

[1] Spiros Mancoridis (PI), Harish Sethu, Naga Kandasamy, and Steven Weber. Machine learning and big data analytics. *Comcast and University of Connecticut Center of Excellence for Security Innovation (CSI)*, January, 2015 – December, 2016. $200,000.