VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series

National Capital Region

Toward Automated Forensic Analysis of Obfuscated Malware

Speaker: Prof. Xinyuan (Frank) Wang
Department of Computer Science
George Mason University

Friday, April 7, 2017
1:00PM-2:00PM

Abstract

Malware analysis, forensics, and reverse engineering reveal a deeper understanding of the inner workings of malware and the mechanics behind attack detection, which enables us to develop better defenses against increasingly sophisticated malware. Despite its importance, the current state of forensic analysis requires notable manual effort due to various obfuscation techniques used by malware. In this talk, I will describe our work on how to automate forensic analysis of obfuscated malware and novel tools that can automatically pinpoint and recover hidden, obfuscated malicious code within memory dumps and network traffic captures. Our novel solution combines static binary analysis, dynamic binary analysis, symbolic execution, binary instrumentation, and taint analysis. It automatically and accurately pinpoints the exact start and boundaries of attack code, even if disjointed and misaligned within random bytes. Additionally, it comprehensively handles self-modifying code and extracts the complete hidden, incremental, and transient code without using any signature or pattern, even if protected by multiple layers of sophisticated encoders. Our method can monitor live network applications, even with complex external libraries such as OpenSSL.

Biography

Xinyuan Wang is an Associate Professor in the Department of Computer Science at George Mason University. He received his PhD in Computer Science from North Carolina State University in 2004 after years' professional experience in networking industry. His main research interests are around computer network and system security. Xinyuan Wang is an Associate Editor of IEEE Transactions on Dependable and Secure Computing (TDSC). He is the leading inventor of 10 US patents and a recipient of the 2009 NSF Faculty Early Career Development (CAREER) Award.