VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series, 2010

National Capital Region

Artificial Malware Immunization

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

Friday, October 15, 2010
1:00PM-2:00PM, NVC 325

Abstract

Computer malwares (e.g., botnets, rootkits, and spyware) are one of the most serious threats to all computers and networks. Most malwares conduct their malicious actions via hijacking the control flow of the infected system or program. Therefore, it is critically important to protect our mission critical systems from malicious control flows.

Inspired by the self-nonself discrimination in natural immune system, this research explores a new direction in building the artificial malware immune systems. Most existing models of self of the protected program or system are passive reflection of the existing being (e.g., system call sequence) of the protected program or system. Instead of passively reflecting the existing being of the protected program, we actively assign a unique mark to the protected program or system. Such a dynamically assigned unique mark forms dynamically assigned sense of self of the protected program or system that enables us to effectively and efficiently distinguish the unmarked nonself (e.g., malware actions) from marked self with no false positive. Since our artificial malware immunization technique does not require any specific knowledge of the malwares, it can be effective against new and previously unknown malwares.

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 – including malware analysis and defense, attack attribution, anonymity and privacy, VoIP security, digital forensics. He has first demonstrated that it is feasible to track encrypted, anonymous peer-to-peer VoIP calls on the Internet. Xinyuan Wang is a recipient of the 2009 NSF Faculty Early Career Development (CAREER) Award.