PRIYA

STUDENT, MASTER OF INFORMATION SYSTEMS SECURITY AND ASSURANCE

A SURVEY ON POLYMORPHIC MALWARE ANALYSIS TECHNIQUES AND TOOLS

In information systems, malware can do involuntarily changes into the system and cause a damage to network attached devices. Polymorphic malware changes its attack vector by different means such as dead code insertion into the payload, code permutation, random modification of registers, branching or pseudo-random index decryption and code expansion. This survey focuses on the dynamicity of polymorphic malwares and how they avoid detection . The objective of our research is to compare state-of-the-art techniques and tools for polymorphic malware analysis. We are interested in assessing their effectiveness for advanced polymorphic viruses in typical malware scenarios. Tools we are using include VirusTotal, Cuckoo Sandbox, Volatility and Sophos for root cause analysis. Techniques for malware analysis that are in the scope of our research includes signature-based and behavioral based techniques.

Research Advisors: Dr. Pavol Zavarsky, Dr. Dale Lindskog