Malicious Manipulation in Service-Oriented Network and Software Systems: Threats and Defenses

by

Dakun Shen

By taking advantage of design flaws in software security, cyber attackers are able to breach the service system for large and small organizations in both the public and private sector. In this dissertation, I will present two approaches we have been designed to tackle threats and challenges in software security. First, I will show a new class of content masking attacks against the Adobe PDF standard, causing documents to appear to humans dissimilar to the underlying content extracted by information-based services. I will also describe a lightweight alternative mitigation method against these attacks. Then, I will describe a research agenda that protects sensitive data in binaries from being corrupted by cyber attackers. In this work, the Intel Software Guard Extensions (SGX) technology is applied to create memory isolation in a way such that data-oriented attacks cannot use traditional memory corruption methods to tamper with sensitive variables.

Publications and Patents

4) Yao Liu, Zhuo Lu, Ian Markwood, and Dakun Shen, “Content Masking Attacks Against Information-Based Services And Defenses Thereto”, (Under Submission)