In-Application Attack Surface Management in Distributed Energy Systems

Executive Summary

Motivation Identifying functionality abuse has always been a challenging task. The consequences of these abuses are often significant and can result in catastrophic problems. Software exploitation, data breaches, service unavailability, and account takeover are just a few examples of more prevalent incidents. This issue becomes even more concerning in distributed energy systems where several software systems have been designed for remote management and are designed to handle critical tasks and valuable data. This proposal, which we collectively call **SENTINEL**, will develop an in-application defense mechanism for **Attack Surface Management (ASM)** and real-time attack inferencing for the energy ecosystem. SENTINEL provides three crucial enhancements over the state-of-the-art: **(1)** it offers fine-grained in-application forensics data about run-time behavior of remote agents when interacting with software systems without introducing any human intervention in the loop, changing the underlying logic of web applications or modifying the service functionality, **(2)** SENTINEL shifts the entire defense mechanism on the background without involving end-user in the process while incorporating more robust techniques against randomness and behavior perturbation, **(3)** SENTINEL can quickly predict when the behavior of remote agents diverges from the expected behaviors while interacting with web services.

Intellectual Merits. The **goal** of this project is to develop an attack surface management layer to reverse the asymmetric power of adversaries in attacking critical software systems in energy systems. Our core **insight** draws on a key observation that defenders should have complete visibility over software systems functionality usage at the closest layer to the software system. Our prior work in software security lays the foundation for this project to develop the following research components:

Component I: In-Application Forensics Layer (§2.2.1). We pursue a rethinking of conventional behavioral monitoring at the application layer. An immediate challenge is how to develop an efficient forensics layer that is agnostic to underlying technologies in software systems while collecting all the forensically relevant information for building the behavioral prediction models. The second challenge is to answer how to perform intent inferencing in a real-time fashion. We will develop a customized instrumentation layer that is tailored for recording run-time functionality usage over time. The engine will arm us with a critical data source for building the behavioral prediction model in the next step.

Component II: Unsupervised cataloging and Response (§2.2.2). The goal of this phase is to quickly catalog each session based on the corresponding temporal characteristics. To this end, we will develop a novel encoding mechanism that will transform the collected traces to a generalizable representation for behavioral similarity testing. We will take advantage of advances in unsupervised machine learning to conduct similarity testing across vectorized data to catalog run-time traces and create a knowledge base of known behavior. We will deploy the trained models to identify emerging trends on how the exposed web services are used. We will propose algorithmic methods to perform automated attack summarization for review by human experts for validation and response.

Broader Impacts. The overall impact of the SENTINEL project is potentially substantial. Web-based software systems serve an important role in managing, configuring, and monitoring distributed energy systems. These software systems are commonly used to handle critical tasks (e.g., software update, configuration management) and valuable data. Their critical role make them an attractive target for adversaries that aim to hijack the control of the entire distributed environment. Implementing Attack Surface Management (ASM) as an integrated in-application defense service will develop important research underpinnings for making more resilient and trustworthy cyberspace and preempting adversarial attempts before attacks damage mission-critical services. Furthermore, the project will also provide a natural mechanism to strengthen diversity in cybersecurity research. The PIs work three Hispanic students. If funded, the project will support one of the students who will start her Ph.D. in Spring 2022