On Security Analysis of Adaptation and Implementation of Self-Protecting Systems

Charilaos Skandylas
charilaos.skandylas@lnu.se
Supervisor: Narges Khakpour
Co-supervisor: Jesper Andersson

Linnaeus University
Växjö Sweden

Abstract

As Modern day life is increasingly tied to the use of computer systems, computer systems are required to perform operations that range from every day activities to essential tasks for human life. As the complexity of systems increases, so do the vulnerabilities that attackers can compromise, while crafting effective defenses against attacks is raised to a difficult task. A self-protecting system is a system that is able to automatically protect itself against threats. To do so, a system needs to be able to detect incoming attacks, measure and analyze its current state and plan effective defenses for each attack. To design and implement such systems with proven assurances, there is a necessity for robust techniques based on a mathematical and logical background.

In this presentation, I will cover our past work on analyzing the security of and providing self-protecting capabilities to component based systems. The security analysis techniques are based on graphical threat models and logic-based reasoning. Two analyses, one based on security metrics and one based on temporal logic, in addition to two self-protecting system architectures will be presented. Furthermore, I will present an approach to secure decentralized systems via adaptive trust based decentralized information flow control. The presentation will conclude with directions toward future work.

Acknowledgment: This is work performed in the context of the PROSSES (Provably Secure Self-Protecting Systems) project supported by Swedish Knowledge Foundation (No. 20160186).

Keywords: Self-Protection, Self-Adaptive Security, Formal Security Analysis