Security Analysis and Protection of Architecture based Self-Adaptive Systems

Charilaos Skandylas
Department of Computer Science and Media Technology
Linnaeus University
Växjö, Sweden
charilaos.skandylas@lnu.se

***Abstract*—Computer systems are complex and highly evolving, requiring constant alteration in order to cope with their ever changing environment and requirements. Self-adaptive systems have been proposed in order to achieve that purpose. However as is the case with all software systems, self-adaptive systems are prone to security attacks. In this presentation I will discuss an approach for vulnerability analysis of architecture based self-adaptive systems based on threat modeling and formal analysis. A formal(predicate based) model is extracted from the system architecture and the vulnerabilities of its components. Subsequently utilizing the predicate model, a logical attack graph, able to illustrate the possible attacker strategies to exploit different vulnerabilities, is generated. Furthermore, a set of attack graph based security metrics that allow quantitative evaluation of a system's adaptation will be discussed. The approach can then be incorporated into the self-adaptive system feedback loop in order to enable the system to dynamically reason about its security at run-time and therefore choose the most secure adaptation possible according to its goals, enabling run-time self-protection. The approach has been automated and implemented in Rainbow, a well known self-adaptive system development framework and evaluated over two candidate systems. The results indicate that a trade-off between security and other qualitative goals of the system can be achieved where the system's security can be maintained at an acceptable level. I will finally discuss ongoing work related to more formal approaches for security analysis of architecture based self-adaptive systems based on model checking.**