Cyber Attack Simulations for Cloud Environments

Viktor Engström
vengs@kth.se

May 19, 2021

1 Abstract

Migrating computing capabilities to cloud platforms is increasingly common. Securing the resulting cloud environments remains difficult, however. Particularly at scale, cloud environments can consist of many interrelated services and rapidly changing segments. Moreover, realistic attacks might exploit chains of vulnerabilities and misconfigurations across systems and cloud services. Assessing the security of such environments in a timely manner quickly becomes overwhelming, even for entire security teams.

Our proposed solution is a combination of threat modeling and cyber attack simulations. The latter spans methods for generating attacker behaviors by executing dynamic models. This presentation covers three main points based on our research thus far. First is an introductory description of attack simulations as either tactical, strategic, or impact-based. Of particular interest to us are tactical simulations, which focus on the detailed actions taken by attackers to reach particular goals.

Second is a description of our automated security assessment method for Amazon Web Services (AWS) environments using the Meta Attack Language (MAL). Specifically, a domain-specific modeling language for AWS has been developed using MAL that is capable of describing AWS environments. The modeling elements contain the pre-defined attack and defense logic required to construct a tailored attack graph. This graph is traversed during the attack simulations to produce attack paths detailing the steps required to compromise the modeled environment.

Last is a discussion of an ongoing project to validate the quality of such simulation-derived attack paths. The aim is to qualitatively compare the reasoning expressed by the simulations to that of human experts. Inspired by the Feigenbaum test, the study will have a human judge evaluating anonymized attack paths produced by either humans or simulations.

Keywords: attack simulation, cloud security, threat modeling, security assessment, automation