Moving Target Defenses for Computer Networks

By Dr. Simon Ou and Dr. Scott A. DeLoach

This presentation will discuss the proposed design and some initial simulation results for a prototype moving-target defense (MTD) system, whose goal is to exponentially increase the difficulty of attacks on enterprise networks. In most computer networks, services are run on well-known ports and are located at fixed IP addresses that can be easily identified through reconnaissance, which provides attackers with a great advantage. The goal of our MTD system is to continuously adapt the network configuration over time in ways that seems random or chaotic to attackers, thus negating their advantage. The novelty of our approach lies in the use of runtime models that explicitly capture a computer network's operational and security goals, the functionality required to achieve those goals, and the logical and physical configuration of the system. Our MTD system uses these runtime models in concert with a novel conservative attack graph to analyze both known and unknown vulnerabilities to ensure that adaptations occur often enough and in the right areas to protect the system against specific attacker profiles.