Simulating a Variation of the XML-Based Mitnick Attack

Master's Project, Spring 2010

Jerry Kuzhuppallil

Advised by Dr. Haiping Xu

University of Massachusetts Dartmouth

Abstract

The Mitnick attack is related to the man-in-the-middle attack (MITM), which exploits the weakness of IP-based authentication systems, and compromises the victim host when two hosts are trying to make a TCP connection using a three-way handshake. Since Mitnick attack is a multi-phased distributed attack, it is very difficult to be detected over the network. Similarly, an XML-based Mitnick attack is a multi-phased distributed attack on web services. An XML-based Mitnick attacker first attacks web services on host A, which is a trusted host for host B. Upon the failure of services on host A, the attacker disguises itself as host A to provide fake or malicious services to host B for unauthorized access.

This project simulates a variation of the XML-based Mitnick attack on web services, which uses XDoS (XML-based Denial of Services) attack to take down services deployed on a trusted host. Then it provides fake information to another host in order to make illegal profits. To demonstrate the effectiveness of this type of attacks and provide a test bed for development of defensive strategies, we implemented a service-oriented medical diagnoses prototype system that can prescribe and provide medicines with their cost. In the simulation, an attacker mimics the operation of a trusted medicine service with much higher prices. The attacker can successfully direct all medicine requests from a normal client to itself by making the trusted medicine services become unavailable using XDoS attacks.