Type of submission: Paper

Title: Intrusion Detection and Isolation Protocol: Automated Response to Attacks

Topic: Innovative Approaches

Speaker: Jeff Rowe
UC Davis
530-752-2149 (Phone)
530-752-4767 (Fax)
CS Dept
1 Sheilds Ave
Davis, CA 95616
rowe@cs.ucdavis.edu (email)

Other contributors to this work:
Dan Schnackenberg, Daylan Darby (Boeing)
Karl Levitt, Chris Wee, David Klotz, Jason Schatz (U.C. Davis)

Dr. Jeff Rowe is a Researcher in the UC Davis Security Laboratory. He bears primary responsibility for the evaluation and deployment of the GrIDS network intrusion detection system. He also leads the UC Davis team in developing components of the IDIP automated response system. Dr. Rowe is also working on a system that correlates multiple intrusion detection reports with network management information as a means to reduce false alarm rates

Subject: Automated responses

Intrusion Detection and Isolation Protocol: Automated Response to Attacks

Abstract:

With current intrusion detection technology, it is possible to detect attacks in real time. Typically, when an IDS system is triggered, a human operator is notified. The system is then adjusted manually in response to the intrusion. Many types of attacks, however, can only be thwarted if the response is quick. Responding quickly, without considering the self-inflicted damage that a response might inadvertently cause, however, is equally dangerous. Should the attacker discover the response mechanism, a willful triggering could be a denial-of-service attack in itself.

Our Intrusion Detection and Isolation Protocol (IDIP) automates attack response. IDIP is a protocol whereby filtering routers, firewalls and host-based response modules cooperate with intrusion detection systems (IDS) to trace the attack back to the source and stop it. To be able to initiate a quick response that halts an attack in progress, while still maintaining the ability to issue the optimum response minimizing self-inflicted damage, our system employs a staged response approach.

The first response stage relies only upon information available locally. The triggered IDS broadcasts a "Have you seen this attack?" query to its neighboring IDIP enabled devices (a firewall or router). All IDIP enabled devices maintain a log of recently forwarded traffic. Upon receiving the query, a device consults its traffic log and, if seen, will implement a filter blocking further attack activity for a brief period. They then forward the same attack query to their immediate neighbors. In this manner, the attack is quickly traced back to its true origin, with filters in place at each device along its path, preventing attack completion.

Clearly there is the opportunity for the attacker to deliberately trigger a greater denial-of-service through IDIP traffic blocking than could be obtained otherwise. To alleviate this problem, the IDIP network components also forward their reports and activity to a centralized Discovery Coordinator (DC). The IDIP DC operates on a global level, incorporating information from multiple IDS reports and IDIP enabled sources. It contains a map of network topology and a list of major services with their relative values. It recognizes coordinated attack patterns, determines the optimal response and the placement in the network that minimizes the impact upon critical services. If the least costly response is worse than the potential damage due to the attack, no response is issued.