Systems and Methods for Testing and Evaluating a Network Intrusion Detection System

INVENTORS • Somesh Jha, Shai Rubin, Barton Miller

WARF: P04220US
View U.S. Patent No. 7,941,856 in PDF format.

The Wisconsin Alumni Research Foundation (WARF) is seeking commercial partners interested in developing a powerful and systematic means of testing a NIDS or other intrusion detection system.

OVERVIEW

Network intrusion detection systems (NIDS) alert a system administrator each time an intruder attempts to penetrate the network. A signature-based NIDS (see WARF reference number P05038US) uses a table of malicious signatures to define penetration. If ongoing network activity matches a signature in the table, an alarm is generated. However, a signature-based NIDS is unable to recognize an attack that differs even slightly from the signature it uses.

THE INVENTION

UW-Madison researchers have developed a method for determining if a set of signatures provided to an intrusion detection system for a given attack is sufficient to detect all possible modifications of that attack. They developed a formal set of transformation rules that represent mutations that might be used to disguise an attack. These rules can be applied in any combination to a known attack instance to generate variations on the attack. The variations can then be input to a NIDS for testing. Failure of the NIDS to detect an attack instance indicates a vulnerability in the system.

APPLICATIONS

• Testing network intrusion detection systems

KEY BENEFITS

• Provides a powerful and systematic means of testing a NIDS or other intrusion detection system
• Allows the system administrator to modify a NIDS or set of signatures based on testing results so the system will detect additional attacks
ADDITIONAL INFORMATION

Related Technologies
For a signature based NIDS, see WARF reference number P05038US.

Tech Fields
Information Technology - Network technologies

CONTACT INFORMATION

For current licensing status, please contact Emily Bauer at emily@warf.org or 608-960-9842.