Intrusion Detection and E-Mail Security

Technology #m02-030

“Lead Inventor: Salvatore J. Stolfo Ph.D.

STV Reference: IR M02-030 & M02-031

Cyber Attacks on Computer Systems on the Rise:
The number and sophistication of intrusion attacks on computer systems are on the rise. Intrusion detection systems such as antivirus, antimalware/spyware, and other security software are used to protect data and computer systems, be it individual users or large infrastructure computer networks. As threats evolve, these security systems must keep pace. Traditional intrusion detection relies either on signature-based identification methods or rule structures that are hard coded into the detection algorithms. Signature-based methods however only protect against "known" malicious programs and hard coded rule systems cannot dynamically adapt to evolving intrusion methods.

Email Security and Intrusion Detection System:
These technologies represent two novel dynamic algorithms for intrusion detection which can identify anomalous activity in e-mail traffic and the sequential execution of system processes. The first uses statistical information about prior e-mail traffic through the system to predict whether or not an e-mail is violating security policy. One embodiment involves the grouping of e-mail recipients into cliques based on prior traffic. A security violation may be identified when recipients of an e-mail belong to different cliques. The second technology detects intrusion based on anomalous sequences of system calls as compared to a predictive model based on prior activity. The algorithm can dynamically change the number of system calls in the sequence to better identify anomalous activity.

Applications:
• Incorporation in unified threat management (UTM) software for more complete protection
• Identification of malicious e-mail on an exchange server based on content, behavior, and past e-mail traffic patterns
• Intrusion detection software for identifying ‘unknown’ threats

Advantages:
• Can detect ‘unknown’ threats and can dynamically adapt to the changing threat landscape
• Models are based on previous normal activity and require little supervision
• Reliably detects violations of e-mail security policy and intrusions in the operating system

Patent Status: Patent Issued (US 7,162,741) and Pending (US20030167402A1) ~ see links below.

Licensing Status: Available for Licensing and Sponsored Research Support

Publications: Salvatore J. Stolfo, Shlomo Hershkop, Chia-Wei Hu, Wei-Jen Li, Olivier Nimeskern, Ke Wang "Behavior-based Modeling and its Application to Email Analysis"

Inventors

Salvatore Stolfo