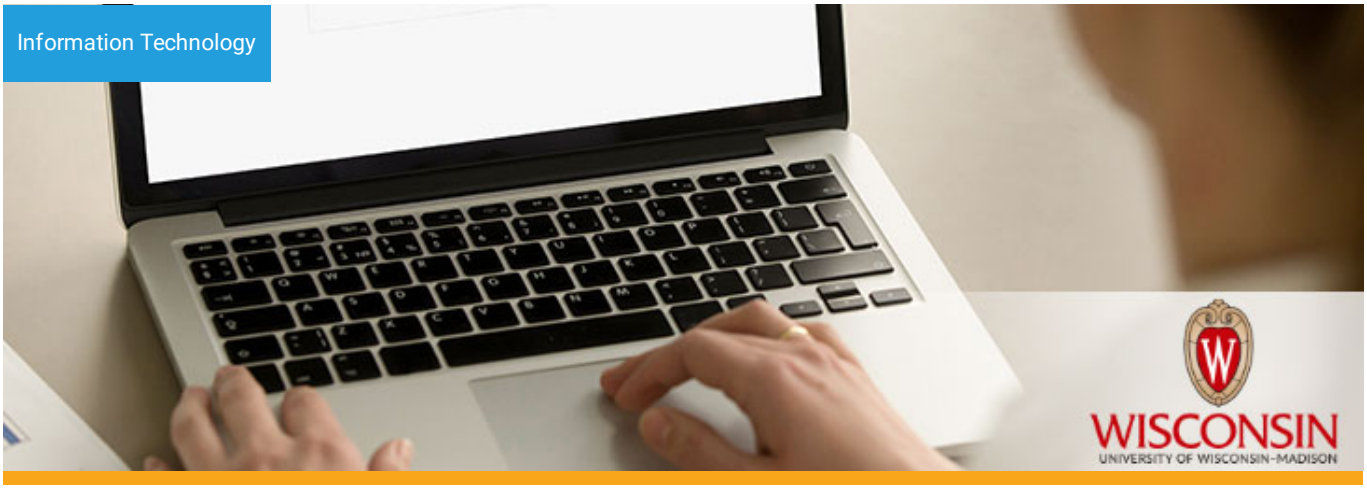
Information Technology



Scalable Monitor of Malicious Network Traffic

View U.S. Patent No. 8,015,605 in PDF format.

WARF: P05182US

Inventors: Paul Barford, Vinod Yegneswaran, David Plonka

The Wisconsin Alumni Research Foundation (WARF) is seeking commercial partners interested in developing an improved, scalable device that attaches to unused addresses and monitors communications to detect malicious network traffic.

Overview

UW-Madison researchers previously described a system of analyzing malicious network traffic to automatically generate signatures that may be used by a network intrusion detection system (NIDS) to protect computer networks from worms, viruses and other malicious software (see WARF reference number P05038US).

The Invention

The researchers have now developed an improved, scalable device that attaches to unused addresses and monitors communications to detect malicious network traffic. The device includes an active responder that simulates communication by an actual computer, but which requires fewer processing resources and may be readily scaled to monitor large numbers of network addresses. Preferably, the active responder provides a response based only on the previous statement from the malicious source. In most cases, this is sufficient to promote additional communication with the malicious source, presenting a complete record of the transaction for analysis and possible signature extraction. Experiments in a controlled laboratory situation as well as in a case study showed this device is efficient, scalable and useful.

Applications

- Detection and analysis of malicious network traffic

Key Benefits

- Discriminates between different types of attacks to the system
- Provides a high degree of scalability
- Allows a single computer to handle thousands of times more connections than a standard system
- Largely immunized against exploitation by the malicious traffic it is monitoring
- Capable of pruning irrelevant data from a statement to improve the accuracy of the responder
- Works across different communications protocols and different operating systems assumed by malicious traffic
- Capable of generating real-time alerts or periodic summaries of detected malicious activity
- Allows pre-filtering of data forwarded to the responder to improve scalability of the system
- Increases the variety of malicious data monitored
- Learns from malicious data over time
- Does not interfere with legitimate network traffic
- Works with the system described in WARF reference number P05038US

Additional Information

For More Information About the Inventors

- Paul Barford

Related Technologies

- WARF reference number P05038US describes an improved method for automatically generating signatures that are highly effective at identifying malicious network traffic.

Tech Fields

- Information Technology : Hardware
- Information Technology : Networking & telecommunications

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