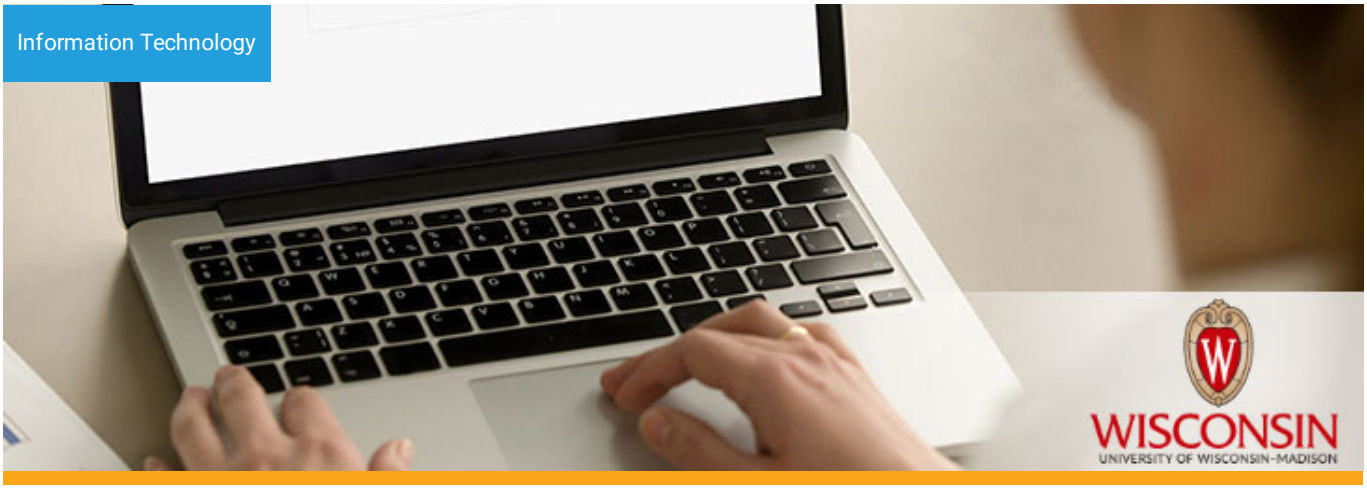
Information Technology



Semantically-Aware Network Intrusion Signature Generator

View U.S. Patent No. 8,065,722 in PDF format.

WARF: P05038US

Inventors: Paul Barford, Somesh Jha, Vinod Yegneswaran, Jonathon Giffin

The Wisconsin Alumni Research Foundation (WARF) is seeking commercial partners interested in developing an improved method for automatically generating signatures that are highly effective at identifying malicious network traffic.

Overview

Network intrusion detection systems (NIDS) can help protect computer networks from worms, viruses and other malicious software. Today's NIDS rely on a set of simple signatures to identify malicious network traffic; however, generating signatures is a burdensome and error-prone task because of the constantly changing nature of the malicious traffic.

The Invention

UW-Madison researchers have developed an improved method for automatically generating signatures that are highly effective at identifying malicious network traffic. The method involves collecting malicious traffic on dark-space addresses (routable network addresses not used by legitimate systems), assigning multi-packet samples from the collected traffic to connections and/or sessions, and normalizing each packet sequence. Cluster analysis of the transformed sequence data is then used to organize the malicious network traffic into groups with similar characteristics. Finally, machine learning is used to generate semantically-aware signatures that identify all variants in each cluster. An analysis showed that the resulting signatures have extremely low false alarm rates compared to standard NIDS signature sets.

Applications

- Identification of malicious network traffic

Key Benefits

- Tapping into the network address dark-space provides a rich source of easily identified malicious network data.
- Normalization removes many common forms of traffic obfuscation.
- Cluster analysis allows isolation of core features of the malicious traffic.
- Modular features allow the system to take advantage of different cluster analysis techniques.
- Signatures may be expressed as finite-state machines for compactness and to allow identification of many variants, possibly including future variants, on the sampled traffic.
- Looking at both the connection and session level improves resulting signature sets.
- Examining both the context and contents of data packets (semantic awareness) particularly improves the ability of signatures to identify a broad set of attacks, including multi-step attacks.
- Offers a compact and flexible way of expressing signatures
- Provides an automated mechanism for generating signatures
- Allows *a priori* judgments of the significance of particular data

Additional Information

For More Information About the Inventors

- Paul Barford
- Somesh Jha

Tech Fields

- Information Technology : Networking & telecommunications

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