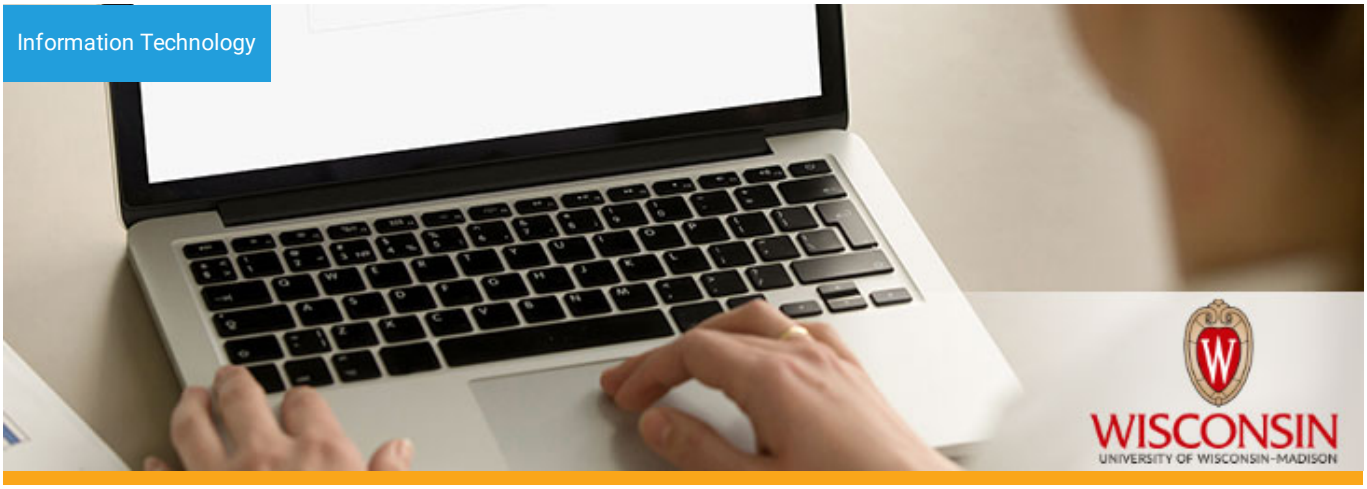
Information Technology



Protomatching Network Traffic for High Throughput Network Intrusion Detection

View U.S. Patent No. 8,220,048 in PDF format.

WARF: P06192US

Inventors: Somesh Jha, Barton Miller, Shai Rubin

The Wisconsin Alumni Research Foundation (WARF) is seeking commercial partners interested in developing a quick method of malware identification.

Overview

Network intrusion detection systems (NIDS) use signature-based detection of malicious software, or malware, to identify suspicious patterns in network traffic. Malware can be disguised by changing data encodings so that the signature is different but the function is the same.

NIDS use three steps—protocol analysis, normalization and signature matching—to identify encoded malware. When performed on all network traffic, these steps can be redundant, and may lead to a reduction in network speed, especially in high throughput networks.

The Invention

UW-Madison researchers have developed a quick method of malware identification that can increase network throughput by as much as 25 percent. The protocol analysis, normalizing and signature-matching steps are blended into one operation, called a superset protomatcher, so that the most of the network data is only inspected once. The superset protomatcher identifies most of the benign traffic immediately so that only a few strings of data require normalization.

Applications

- Malware detection

Key Benefits

- Increases efficiency of NIDS
- Eliminates duplicate analysis of many strings
- Can be used for intrusion prevention or as a passive system
- Reduces memory required for NIDS
- Provides better protection for high throughput networks

Additional Information

For More Information About the Inventors

- Somesh Jha
- Barton Miller

Tech Fields

- Information Technology : Networking & telecommunications

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