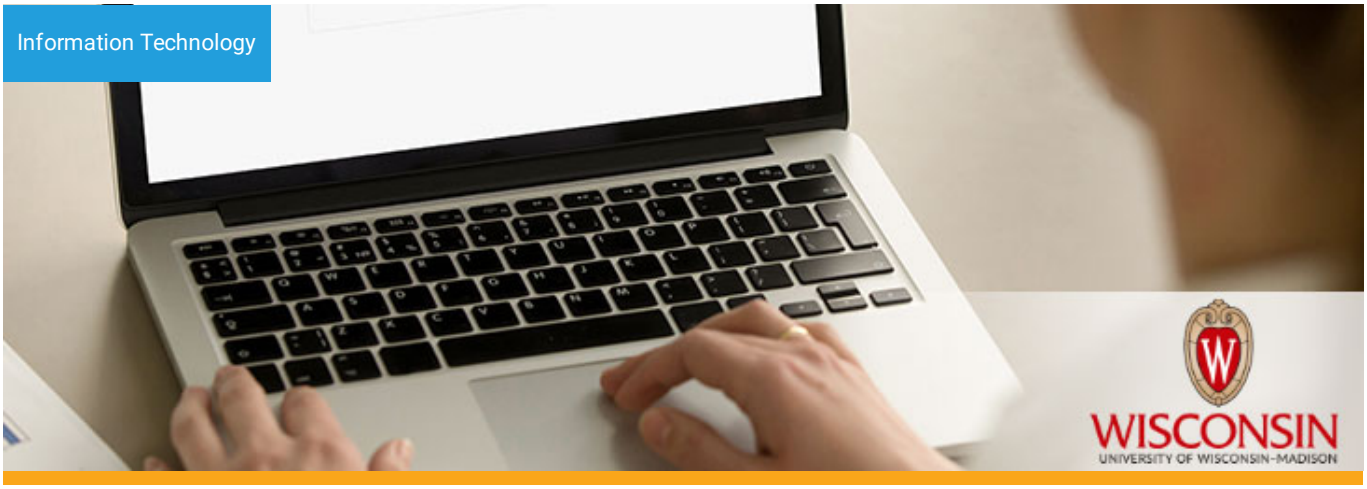
Information Technology



SAFE: A Dynamic Malware Detection and Prevention System

View U.S. Patent No. 8,065,728 in PDF format.

WARF: P07396US

Inventors: Somesh Jha, Hao Wang

The Wisconsin Alumni Research Foundation (WARF) is seeking commercial partners interested in developing a behavior-based system, known as "SAFE," that is capable of detecting and stopping known and unknown malware.

Overview

Detecting and stopping malware—viruses, trojans, bots and spyware—from infecting a computer is a challenge because of its rapidly changing nature. Existing techniques either use signature-based scanning, which is ineffective against novel malware, or require heavy-weight techniques, such as static analysis and virtual machines, which cannot be readily deployed by end users.

The Invention

UW-Madison researchers have developed a behavior-based approach capable of detecting and stopping known and unknown malware. Most malware can be detected by observing malware-generated events, such as creating files or making network connections, from inside the "kernel," the central component of the operating system. These events are essential to the function of the malware and not easily disguised.

The inventors have developed a program to monitor kernel events associated with all processes being executed on a computer. Code or programs from unverified sources are allowed to run in a controlled and isolated environment that restricts access to critical system resources, such as network and host system files. Before a kernel event associated with one of these unverified processes is committed to a system resource, it is evaluated against a set of policies that describe sequences of such events that are associated with malicious behavior. If a kernel event is identified as being malicious, the monitoring program stops the execution of the process and quarantines it for removal.

Applications

- Detecting malicious software

Key Benefits

- Effective against both known and unknown malware—allows the user to specify generic descriptions of suspicious behavior that cover an entire family of malware, instead of individual instances of malware
- Makes early ("zero-day") and reliable detection of malware possible
- Monitors and controls kernel events within the operating system to protect against being disabled by the malware
- Operates in real time with very low overhead
- Can be easily integrated into a running computer with no significant effect on performance
- Applicable to the widely used Windows® operating system
- Capable of preventing all drive-by downloads, a common means of malware infection
- Detects trojans, which stealthily download and install new programs on a host

- Can detect malware that operates over a long time period

Additional Information

For More Information About the Inventors

- Somesh Jha

Tech Fields

- Information Technology : Networking & telecommunications

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