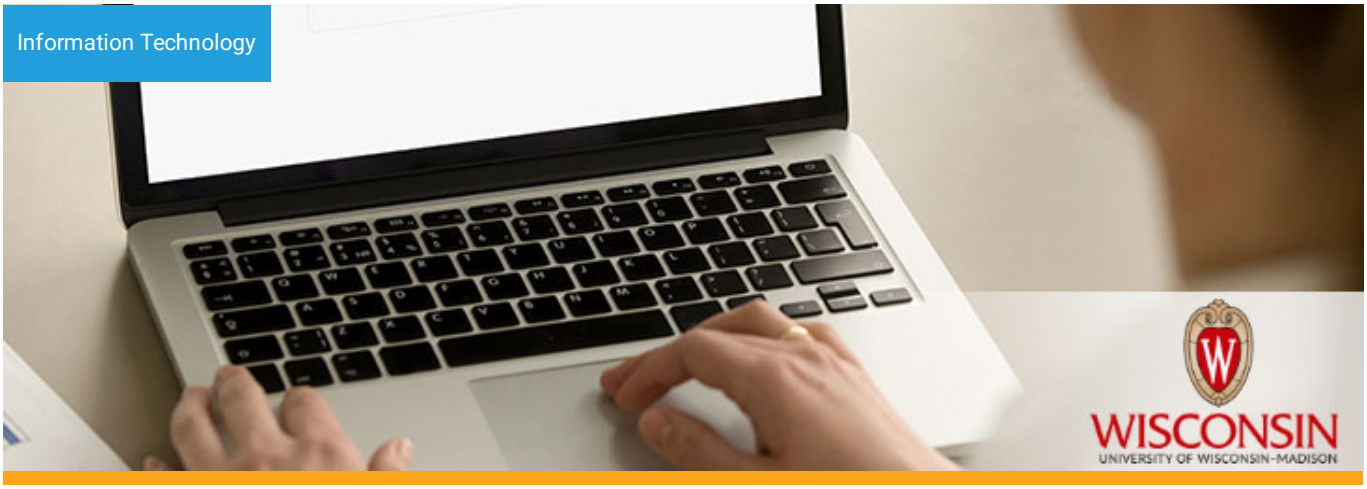
Information Technology



A Novel Method for Detecting Computer Viruses

View U.S. Patent No. 7,739,737 in PDF format.

WARF: P03146US

Inventors: Somesh Jha, Mihai Christodorescu

The Wisconsin Alumni Research Foundation (WARF) is seeking commercial partners interested in developing a novel approach to identifying malicious portions in a suspect computer program.

Overview

In the interconnected world of computers, malicious programs such as viruses have become an omnipresent and dangerous threat.

The Invention

UW-Madison researchers have developed a novel approach to identifying malicious portions in a suspect computer program.
The approach is able to detect malicious code that has been obfuscated, or disguised, by examining the function of the code rather than its “expression” as a string of instructions.

This functional analysis is made possible by a preprocessor that receives the suspect computer program and converts the program instructions into a standard form denoting their function. A detector reviews the standardized version of the suspect program against a library of standardized malicious code portions and indicates when malicious code is present in the suspect program.

Applications

- Detection of malicious software

Key Benefits

- Works with binary executables, the typical form in which infected programs are received
- Sensitive to the function of the malicious code, while largely indifferent to its expression
- Largely indifferent to code transposition and dead code insertion
- Can exploit conventional tools and techniques used for program analysis
- Provides a unique functional expression of code that may be used to provide effective functional analysis
- Shows decreased sensitivity to particular register or memory locations
- Provides a simple mechanism for generating a standardized version that can be readily supplemented as new functional equivalents or methods of obfuscation are discovered
- Easily implemented and augmented
- Easily added to other detection systems for further analysis of the identified malicious code portion

Additional Information

For More Information About the Inventors

- Somesh Jha

Tech Fields

- Information Technology : Computing methods, software & machine learning

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