George Mason University,
Office of Technology Transfer
Seeks partners to license ...

ARTIFICIAL MALWARE SOFTWARE IMMUNIZATION

Tech ID # GMU 11-007 **Patent No. 8,806,640 & 9,483,637**

Description of Technology:

Inspired by the natural immune system, this technology can automatically immunize otherwise vulnerable programs such that the immunized programs can detect and stop, in real-time, the control flow hijacked by malware before permanent damage can be inflicted. The malware immunization is based on the sense of "self" dynamically generated by the kernel which is assigned to each system call of the immunized program at run-time. Such a dynamically generated sense of "self" enables the immunized (i.e., instrumented) program to distinguish in real time, malware actions (unmarked) from legitimate actions (marked), obviating the need for specific knowledge of the malware to make a positive identification.
A proof-of-concept prototype has been implemented in Linux.

Primary Investigator:

Dr. Xinyuan (Frank) Wang is an associate professor of computer science in the Volgenau School of Engineering at George Mason University.

Advantages:

- Real-time detection of malware attacks and live malware forensics
- Effective against known and unknown control flow malware
- Negligible run-time overhead
- Virtually no false positives detecting the non-self malware action have been achieved

George Mason University, Office of Technology Transfer

Contact

George Mason University
Office of Technology Transfer
4400 University Drive, MS 5G5
Fairfax, Virginia 22030
Phone: 703-993-8933
Fax: 703-993-9710
Email: hmehta4@gmu.edu