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

SYSTEM CALL REDUCTION FOR MALWARE PREVENTION

Tech ID # GMU 18-012 **Patent Pending**

Description of Technology:

Malware can compromise a user's system to perform malicious operations. Existing approaches to preventing malicious operations by malware target the system call used by malware. A system call is a programmatic way in which a computer program requests a service from a kernel of an operating system. Examples of such services include memory access, creation and execution of new processes, and integral kernel services such as project scheduling.

Our system can determine the operation state of an application. Operation states can include boot-up, execution, shut down etc. Based on the operation state, the application state can determine number of system calls allowable for use by the application. By defining which system calls are allowable on a per-application basis, it ensures that only the system calls necessary for a given application are allowed, thereby providing for a smaller attack vector. The attack vector can be further restricted by allowing only those system calls required for the operation state in which the application state is operating.

Primary Investigator:

Dr. Kun Sun is the Associate Professor of Information Sciences and Technology at George Mason University.

Advantages:

- Our Low-overhead, user-transparent containers enhance the security of cloud systems that deploy light-weight containers
- Enhances defensive capabilities against malicious attacks
- Significantly improves the trustworthiness and adaptation of the container based virtualization mechanisms in cloud systems.

Contact

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