Software And Hardware Methods For Multi-Variant Parallel Program Execution To Detect, Quarantine And Repair Malicious Code Injection

Tech ID: 20813 / UC Case 2007-624-0

CONTACT

Ben Chu
ben.chu@uci.edu
tel: .

OTHER INFORMATION

CATEGORIZED AS

- **Computer**
  - Hardware
  - Security
  - Software

RELATED CASES

2007-624-0

BRIEF DESCRIPTION

In its simplest form this invention consists of a novel software-only approach to malicious code detection and repair in real time. However by including a minute extra component (< 0.001% total transistor count) to a standard commercial processor this process can enable fully automatic repair of malicious code injections.

FULL DESCRIPTION

Researcher's at UCI Department of Computer Science's Secure Systems and Software Laboratory have developed a fundamentally new software and hardware approach to security called "multi-variant code execution". Instead of endlessly attempting to eliminate vulnerabilities (having accepted that inevitability) they merely ensure that these vulnerabilities can never be exploited.

The principal idea is to run several slightly different instances of the same program that are otherwise identical, in lockstep, on multiple disjoint processing elements. A monitoring layer compares the states of the different computations at regular intervals or checkpoints and flags an error if they differ. A malicious intruder would need to devise a different attack vector for each of the program instances running concurrently and would need to corrupt all of the concurrent processes between checkpoints to avoid detection. An attack vector that is designed to corrupt one of the processes will cause "collateral" data modifications in the other processes and if the variable layout differs between the two program variants, which it will, it becomes extremely difficult to devise an absolutely symmetric attack that corrupts both (or many) program instances while simultaneously producing semantically identical collateral effects.

Multi-variant code execution is a disruptive technology that eliminates a wide range of malware threats such as "zero-day" attacks and sophisticated polymorphic and metamorphic viruses and worms.

SUGGESTED USES

Computer security

ADVANTAGES

More secure, faster, inexpensive, zero cost to end user

STATE OF DEVELOPMENT

Patent pending

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	8,239,836	08/07/2012	2007-624

UCI Beall Applied Innovation

5270 California Avenue / Irvine,CA 92697-7700 / Tel: 949.824.2683