Software attack protection and recovery via transactional application self-healing

Technology #m07-035

Lead Inventors: Angelos D. Keromytis, Ph.D.; Michael E. Locasto

Problem or Unmet Need: Although computer defense systems for detecting attacks on software applications exist, they are currently unable to take any remedial action once an executing application’s state is modified by an attack. In order to prevent exploitation of an attacked application, most defense systems terminate execution of the attacked application process. This mechanism reduces the availability of the application and risks losing ongoing work performed by the software at the time of the attack. Introducing self-healing mechanisms to software that would enable applications to safely continue execution after an attack could limit the extent to which attackers can interrupt normal application use without compromising system security.

Details of the Invention: The technology is a method for preventing a software application from crashing due to an external attack or internal fault. The technology supervises an executing application to detect attacks or faults and applies integrity repair policies via dynamic rewriting of the application’s executing routines to enable the application to continue normal execution after an attack or fault.

Applications: • The technology can reduce the likelihood of software crashes in high-availability and mission-critical scenarios.

Advantages: • The technology does not require that an application’s source code be modified in order to be protected. It therefore can be used with commercial or proprietary applications for which the source code is not readily available. Software vendors also do not need to modify their products in order to take advantage of the technology. • Unlike systems that can only detect and prevent attacks against software, the technology also provides self-healing features that can prevent software from crashing or being terminated in response to an attack; software protected by the technology therefore does not need to be restarted after an attack. • In order to reduce the performance penalty of supervised execution, the technology can be configured to selectively supervise specified portions of an application.

Patent Status: Patent Issued (7962798)

Licensing Status: Available for Licensing and Sponsored Research Support


Inventors

Angelos D. Keromytis