Enhanced Information Security Monitoring Using Analog Signals

A measurement framework to capture and catalog program-dependent signals at specific frequencies to prevent attackers from obtaining sensitive/secret information within a computer

Georgia Tech inventors have developed a measurement framework that uses micro-benchmarks to capture and catalog program-dependent signals at specific frequencies. The end-goal of these inventions lies in preventing potential attackers from penetrating and obtaining sensitive/secret information within the computer. The first invention comprises of a methodology to rapidly discover activity-modulated signals using specially designed micro-benchmarks. It utilizes recognizable spectral patterns that can identify those signals exhibiting a particular type of behavior such as amplitude modulation. The second invention, called CAMELIA, provides accurate and precise security monitoring of embedded, mission-specific, and traditional computing devices and software while keeping the monitoring and computing systems separate. CAMELIA uses the previous invention's capability of measuring small signal emanations as the basis of security monitoring activity. This approach is revolutionary in that the monitoring is occurring outside the computing device or system versus current monitoring systems that reside within the computing device. Consequently, no modifications need to be made to the computing device to enable this security mechanism.

Summary Bullets

- Accurately and precisely perform security monitoring of information and data being used by computer devices and systems
- Eliminates the need for the security mechanism to be incorporated into the device/system being monitored
- Capable of functioning without using resources of the device or system being monitored

Solution Advantages

- Accurately and precisely perform security monitoring of information and data being used by computer devices and systems
- Eliminates the need for the security mechanism to be incorporated into the device/system being monitored
- Capable of functioning without using resources of the device or system being monitored
- Can be used as a means to benchmark and compare the performance of different computing devices used to handle sensitive data

Potential Commercial Applications

- Security monitoring
- Software profiling
- Code debugging
- Security enhancements
- Embedded and mission-critical devices or systems

Background and More Information

Computer security is a key element in current IT systems and infrastructure. All computers and computing systems tend to leak information through unintentional conduits called side channels. Side channels refer to involuntary analog signals that emanate due to small variations in power consumption by the computing elements. These emanations can be used by a hacker or other malevolent to decipher secret information such as encryption keys being used by the computer for computing or communication purposes. This issue has been known for around 50 years but a comprehensive methodology that identifies the side channels and effectively characterizes differences in leaked energy from different program codes has been lacking.

Inventors

- Milos Prvulovic
  Professor - Georgia Tech School of Computer Science, College of Computing
- Dr. Alenka Zajic
  Professor - Georgia Tech School of Electrical and Computer Engineering

IP Status

:

Publications

, -

Images

Visit the Technology here:
Enhanced Information Security Monitoring Using Analog Signals