Runtime detection and deactivation of malicious software

To detect malicious software behavior, this technology intercepts calls to operating system services and libraries and determines from what locations in memory the call originated. Calls made from regions of memory that store data rather than code are deemed to be potentially malicious and are halted before they can cause damage; other calls are deemed to be valid and are allowed to proceed. This technology also allows halted calls to be recorded by this mechanism for monitoring purposes.

Interceptor and halts calls that originate from suspicious regions in memory, thereby preventing damaging operations by malware

Many forms of malware exploit flaws in software applications by altering the flow of control in program execution and/or introducing malicious code into program memory. Since these methods of attack can often be detected by existing security software, some malware attempt to use existing operating system and library routines with its own parameters to achieve malicious ends; such attacks are harder to stave off as they do not introduce any executable code that can be detected. This technology can protect against this class of attacks even when confronted by unknown malware by intercepting and analyzing the origin of system and library calls made by executing software rather than searching for the signatures of specific recognized malware. The technology also affords the additional advantage of effectively neutralizing malicious code before it can do damage immediately upon detection.

Lead Inventor:

Alfred V. Aho, Ph.D.

Gaurav Kc
Applications:

- Real-time protection of sensitive computer systems from damage by malicious software.
- Detection of intrusion attempts by otherwise undetected or unknown malware.

Advantages:

- Prevents malicious code from damaging systems/data immediately upon detection.
- Can detect unknown malware based upon behavior rather than relying upon software signatures.

Patent information:

Patent Issued (US 7,971,255)

Tech Ventures Reference: IR M04-074

Inventors

Alfred V. Aho