Ranjan Raut, CSCI 5593

Review#1, 04-FEB-2019

Paper Review on "**A computer architecture with hardware-based malware detection**"

This paper has proposed a way to nullify attacks of Malware type-I and II using specific architecture in Hardware. Attacks such as Malware type-0 can be easily blocked by software utilities. But, attacks of type I and II are difficult to trace. These attacks take advantage of vulnerability of architectures that share same memory for instruction and data (e.g. von-Neumann-architecture). Sequence of instructions can be executed from data segment too. These attacks load the code with malicious functionality into memory camouflaging as data loading and then change instructions of actual processes to put malicious segment into the execution in the reference of the host process.

As a solution, authors proposed to use Harvard Architecture. In this architecture, two physically separate memories are used: Instruction and Data, each connected to processor via separate bus. Instruction memory will be always read only to processor shielding type I and II attacks. A special security processor can be used in order to modify instructions in memory. In order to execute instructions stored in data memory, a transfer must be made by security processor. Security processor puts check on such transport, blocking harmful code. This security is enforced by implementation of 'AddressGuard'. Data memory has function pointers which contain addresses of instruction memory. Modification in such addresses can reference to different code. AddressGuard checks if referenced instruction adheres to specific segment of memory. If not, then same is reported to security core and necessary actions are taken. AddressGuard also logs and analyze data at run time, which also helps in recognizing unauthorized access.

This architecture not only separates user and application memory space from OS space, but also has user core and security core as two separate cores for security. Security applications and OS are hosted on security core, which only refers to read-only instruction memory. Security core loads programs into user memory with the help of OS and it is user core who deals with address violations. User core can execute non-modified program. It does use AddressGuard and report suspicious jumps from loaded segments of instruction to the security core.

This architecture compromises performance for security and future work is likely to achieve both performance and security.

Reference

Klaus Hildebrandt, Igor Podebrad, Bernd Klauer, "A Computer Architecture with Hardwarebased Malware Detection", Published in: 2010 International Conference on Availability, Reliability and Security, 15-18 Feb 2010, Krakow, Poland, DOI: 10.1109/ARES.2010.39