A Silicon Anti-Virus Engine
Adrian Tang, John Demme, Simha Sethumadhavan, Salvatore Stolfo
Columbia University
{atang, jdd, simha, sal}@cs.columbia.edu

AV systems today rely on correct functioning of not only the AV software but also the underlying OS and VMM. Thus, proper functioning of software AV requires millions of lines of complex code which houses thousands of bugs to work correctly. As evidenced in numerous software AV attacks, effective software AV systems have been difficult to build. At the same time, malware incidents are increasing and there is strong demand for good anti-virus solutions; the software anti-virus market is estimated at close to 8 B dollars annually. Coming at this from a different angle, we developed a new class of robust AV systems called Silicon anti-virus systems (SAV). Unlike software AV systems, SAVs are lean and mostly implemented in hardware to avoid reliance on complex software, but, like software AV systems, are updatable in the field when new malware is encountered. We describe the first generation of Silicon AV that uses simple machine learning techniques with existing performance counter infrastructure. Our published works show that common malware such as viruses and adware, and even zero day exploits can be detected accurately (eg. Android malware 82.3% and Linux rootkit 60% accuracy) [1, 2]. These systems form an effective first-line, energy-efficient defense against malware.

References
Problem Statement and Goals

• Proliferation of malware – stealthier and increasing in number
• Complex software implementation (many lines of code) - High bug density
• Software-level detection mechanisms have limited effectiveness

Rethinking malware detection with hardware approach and low-level features

Approach

• Detect malware based on runtime micro-architectural profiles of programs
• Micro-architectural profiles can be efficiently audited using hardware performance counters
• Build signature-based and anomaly-based machine learning models

Key Insight: Programs (and malware) exhibit unique micro-architectural signatures

Results

Signature-based

- Android malware
  - 82.3% accuracy
- Linux rootkit
  - 60% accuracy
  - Difficult problem; rootkits are tiny slices of execution
- Side-channel attack
  - 100% accuracy; No false positive

Accuracy of Android malware classifiers

Anomaly-based

- 99.5% AUC score for AM-1 event set (STORE, LOAD, MISP_RET, CALL_ID) for detection of Stage1 shellcode
  - 1.5% slowdown with sampling rate of 512k insn.
  - 100% true positive with 1.1% false positive rate
