2013 DHS S&T/DoD ASD (R&E)
CYBER SECURITY SBIR WORKSHOP

Frontiers in Cyber Security: Beyond the OS

Clear Hat Consulting, Inc.
Sherri Sparks

7/23/13

Homeland Security
Science and Technology

Company Profile

- CHC was founded in 2007 by S. Sparks and S. Embleton
- Small R&D Based Cyber Security Company
- Located in downtown Orlando, FL
- Mission Statement
  - “To research and develop proactive, innovative solutions to cutting edge cyber security problems”

Customer Need (1)

- High value systems such as those used by government, banks, communications carriers, and SCADA systems may be subject to highly sophisticated, targeted attacks
  - Sensitive data or intellectual property can be lost!
  - Remediation is expensive!

- While the “defense in depth” approach to cyber security is given lip-service, existing technology leaves the deepest part of the attack surface (chipset interface) wide open!

Customer Need (2)

- It is time for cyber security to move beyond the OS…
  - Chipset level attacks are defined by their interactions with the processor and chipset hardware not the OS
  - An attack is likely to go unnoticed if it doesn’t make detectable changes to OS kernel code or data structures
  - Existing Kernel based protections are not capable of monitoring low level CPU and chipset accesses
  - Kernel protections are vulnerable to malicious tampering by malicious kernel code
  - Kernel protections are limited in their ability to detect and respond to advanced threats in “real-time”

Background:
Exploitation Vectors Beyond The OS

- Virtual Memory Configuration
- System Management Mode (SMM)
- Active Management Technology (AMT)
- Advanced Configuration & Power Interface (ACPI)
- Direct Memory Access (DMA)
- Peripheral Hardware (Disk, Video, Network, etc.)

- Processor Caches
- Virtualization Extensions
- PCI Expansion ROMs

- BIOS
- CPU Microcode
- Local & I/O APICs

SBIR Projects

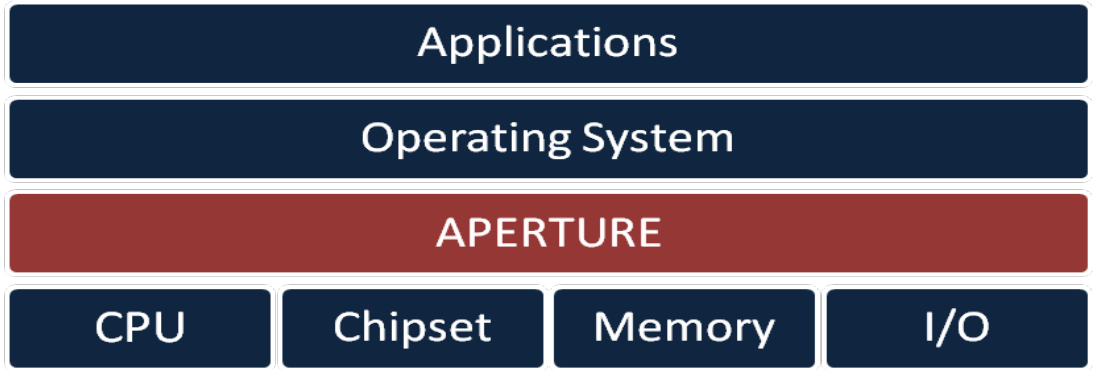
- **OSD09-IA1:** Real-time Adversarial Characterization and Adaptive Protection Countermeasures (Phase 2)

- **OSD09-IA2** : Countermeasures to Covert Access Methods to Reduce Attack Susceptibility and Ensure Trust (Phase 2)

- **OSD10-IA1:** Countermeasures to Malicious Hardware to Improve Software Protection Systems (Phase 2)

Approach: OSD09-IA1 & OSD09-IA2 Introducing APERTURE

- A Chipset Level Firewall
  - Takes security beyond the OS by using hardware virtualization to provide a window or “aperture” into low level CPU and chipset behaviors
  - Combines a user defined access control policy with *real-time* threat assessment and response capabilities to guard against sophisticated chipset and kernel level attacks
  - Protection runs in an isolated memory space that provides security against malicious tampering



Benefits: OSD09-IA1 & OSD09-IA2

Real-time monitoring and access control

- Capable of controlling access to many different types of system resources targeted by advanced persistent malware
  - ✓ CPU Registers (Model Specific Registers (MSRs), Control Registers, Debug Registers)
  - ✓ Sensitive Instructions
  - ✓ I/O Ports
  - ✓ PCI Configuration Space
  - ✓ Architectural, OS, and Device Memory Ranges

Benefits: OSD09-IA1 & OSD09-IA2
Dynamic, real-time memory forensic platform

- Capable of automated threat assessment and response including real-time forensic data acquisition
  - ✓ Policy Violation Information
  - ✓ CPU State
  - ✓ Chipset State
  - ✓ Kernel Object Data
  - ✓ Kernel Memory Dumps
- Can record information at multiple points during an attack
- Can improve incident response by providing the ability to see the progression of system state changes during an advanced cyber attack

Applications: OSD09-IA1 & OSD09-IA2

- Advanced malware detection
  - Early detection of sophisticated attacks or zero-day attacks that target low-level CPU and chipset resources
- Advanced incident response and reverse engineering
  - Provide a sequential trace of policy violations relating to low level CPU and chipset resource interactions
  - Captures valuable information about sophisticated attack vectors:
    - Attack origin
    - Resource types targeted by the attack

Customer Need: OSD10-IA1

- The work under this effort is focused at detecting and preventing chipset level / firmware attacks on desktop peripheral components (with an emphasis on protecting the hard disk drive)
- Compromised COTS desktop peripheral hardware & firmware pose serious security risks to government and high value commercial customers…
  - Desktop computers are routinely used to operate on and store sensitive classified data.
  - Desktop computers may be used to interface with other types of sensitive systems (e.g. weapons system hardware)
  - Some peripherals, like hard disks, are not limited to desktop or laptop computers, but may be found in all manner of military and industrial systems requiring persistent data storage!
- There are currently few security tools capable of preventing, detecting, or mitigating peripheral device firmware compromises!

Note: This presentation is subject to SBIR data rights

Project Scope: OSD10-IA1

- Because of the size and diversity of the COTS desktop peripheral attack surface, CHC has limited the scope of their effort primarily to researching and securing the hard disk firmware attack surface
- Hard disk security is extremely important because, aside from the BIOS, it is the only device that has the direct responsibility of storing and providing access to system code and data (including the boot sector)
- A compromise of the disk drive's hardware or firmware implies a compromise of the entire computer system!

Note: This presentation is subject to SBIR data rights

Background: Phase 1 Results

- At the conclusion of our Phase 1 effort, we were successful in:
  - Dumping and disassembling a significant number of firmware routines in a popular COTS hard drive
  - Locating critical data structures in the drive firmware
  - Identifying the firmware ATA command handling routines
  - Identifying where the drive's data buffers are stored
  - Developing a proof of concept disk malware test case
  - Identifying countermeasures for disk based threats

Approach: OSD10-IA1

- **Phase II: A Dual Focused Approach**
- Facilitate a greater understanding of the COTS peripheral component attack surface
- Research and develop a host oriented protection to improve the ability of critical software systems to carry out their missions even when they are operating in hostile hardware environments.

Approach: OSD10-IA1

- **COTS Peripheral Attack Surface Research**
  - Examine both platter and SSD drives across the HDD market space
  - Ongoing research concludes that most commercial HDDs are vulnerable to firmware exploitation!
  - Current security products do not address these vulnerabilities!

Approach: OSD10-IA1

- **Implement Disk Oriented Host Peripheral Protection Capabilities**
  - Utilize bare metal hypervisor to…
    - Enforce peripheral device isolation via Intel Vt-D I/O virtualization technology
    - Monitor and enforce ATA Interface specification for all HDD disk devices
    - Provide secure, hypervisor level disk encryption interface
    - Provide user configurable ATA Command Access Control Policy for disk devices

Current Status

- **OSD09-IA1 and OSD09-IA2**
  - Finished Phase II Effort ~1 month ago
  - Implementation of an operational Advanced Prototype Is Complete

- **OSD10-IA1**
  - Recently Finished Year 1 of Phase II Effort

Next Steps

- **OSD09-IA1 and OSD09-IA2**
  - Meet with primes, govt agencies, and commercial software security companies interested in acquisition of and / or investment in CHC's APERTURE technology
  - Participate in cyber security conferences to promote capabilities of CHC's APERTURE technology
- **OSD10-IA1**
  - Complete Phase II Research & Development

Contact Information

Clear Hat Consulting

Security beyond the OS…

407.841.8320

www.clearhatconsulting.com