

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

Countermeasures to Covert Access Methods

Edaptive Computing, Inc
Presenter : Dr. Praveen Chawla

July 23, 2013



Homeland
Security

Science and Technology



Company Profile

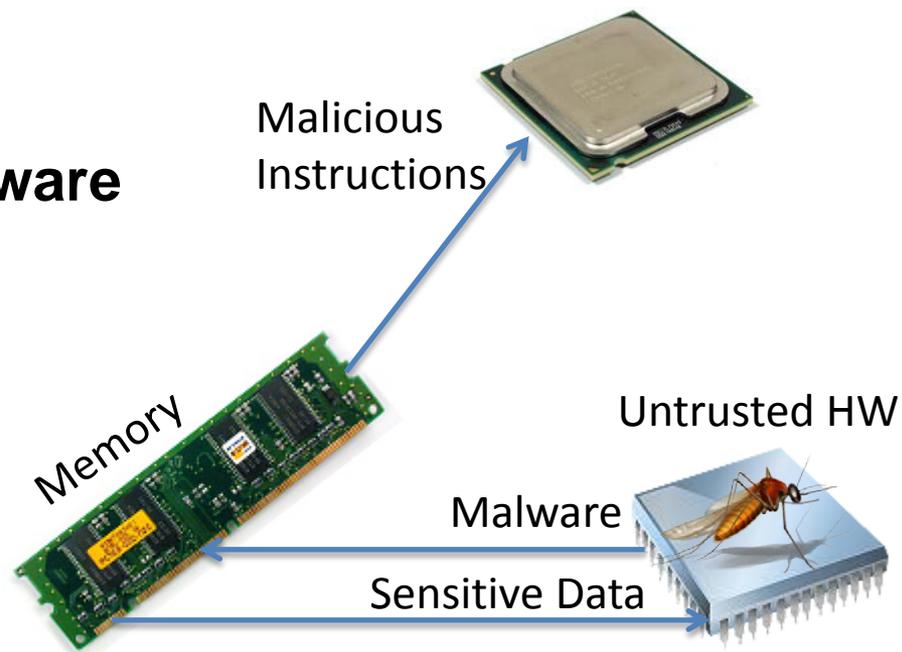
- **Record of SBIR Success**
 - **4 Phase III awards**
 - **Success Stories published by USAF, DARPA, NASA and USN**
- **Technology Transition**
 - **Successfully completed (3/05) Phase III contract from Air Force**
 - **Awarded (6/04) 10 year Phase III IDIQ contract from NAVAIR with over \$45+M ceiling; Awarded second Phase III (08/12) with \$10M ceiling**
 - **Received several delivery orders to apply and transition SBIR technologies**
 - **Awarded (9/10) 7 year Phase III IDIQ with AFRL/RYW with \$5 M ceiling**
 - **Scope: To assure design and documentation of hardware and software (AssuredWare)**
 - **First delivery order to assure FPGA designs**
 - **\$16+ million in Phase III sales and \$1 million in non-SBIR investments to-date;**
 - **Successfully applied analysis software to commercial applications**

Edaptive has successfully transitioned SBIR technologies to real-world solutions.

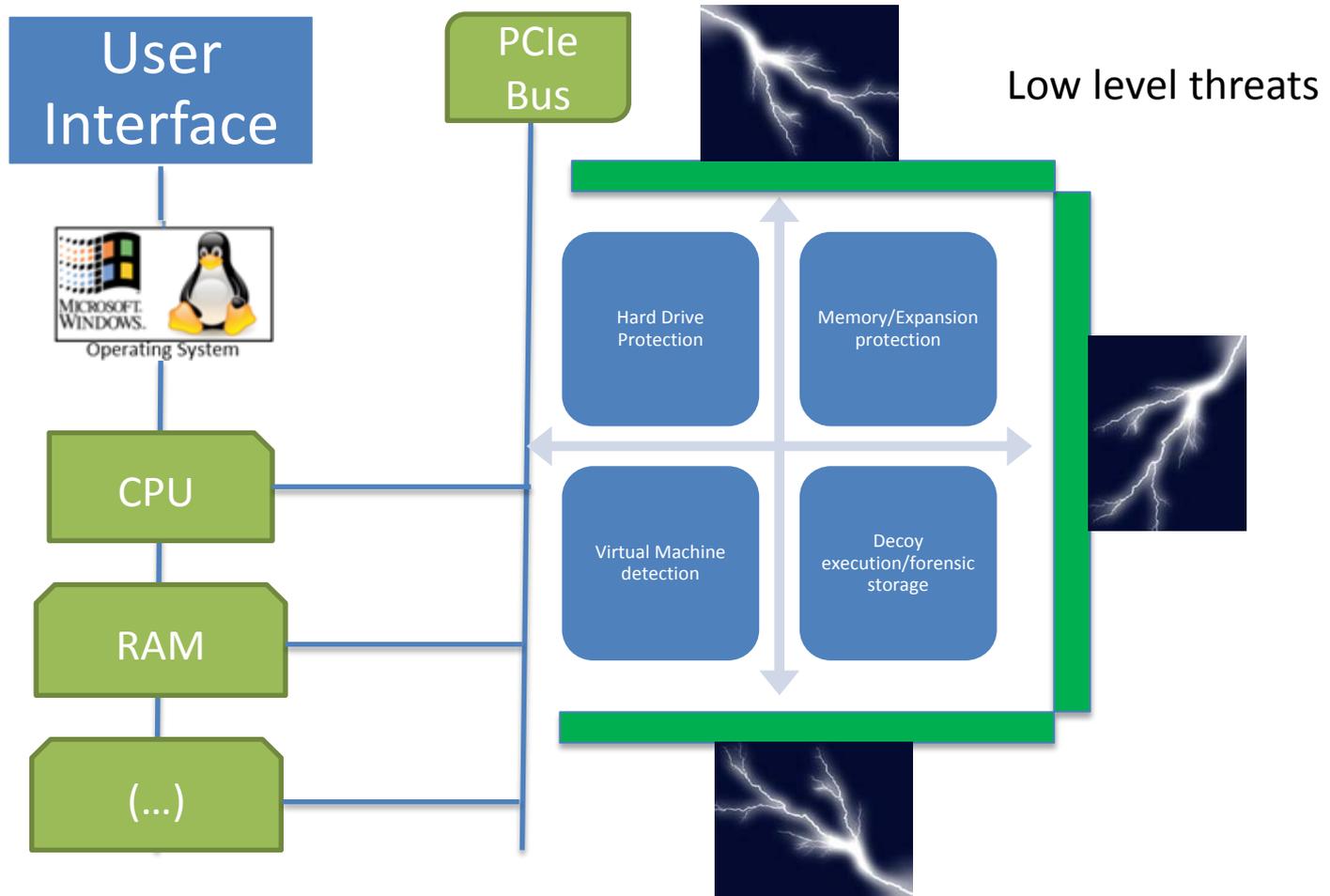
Customer Need

Hardware-based software attacks:

- are a real possibility (CIH virus, a.k.a. Chernobyl virus was first documented case)
- allow for read, write, execute access
- are difficult to detect
- are difficult to stop
- are able to re-infect software



Approach





Approach

- **Provide protection at the hardware level through a combination of software and hardware systems.**
- **Monitor low-level access to critical system devices including hard disks, memory, and peripherals**
- **Elicit and store information about attacks**



Benefits



- **Raise level of trust in computers**
- **Reduce attack susceptibility**
- **Enhanced level of visibility into hardware**
- **Tailor protection to particular computer system**
- **Collect and analyze information about attacks to learn more about adversary**



Current Status

- **Expansion ROM delivery**
- **Virtualization Detection and Protection**
- **Secure Hard Drive execution**
- **Memory Scanning for Malware**
- **Device Driver and GUI**
- **Decoy execution**
- **Forensic Storage**



Next Steps



- **Future tasks:**
 - Adding in Network Protection
 - Extensive Testing on Enterprise Systems
 - Reducing form factor to more efficient footprint
- **Asking for:**
 - Additional platforms for testing.
 - Expanded Test cases
 - Additional funding for expanded functionality and testing

Contact Information

Praveen Chawla, Ph.D.

CEO/CTO, Edaptive Computing, Inc.

1245 Lyons Road, Building G

Dayton OH 45458

Phone: (937) 433-0477 x101; (937) 369-4486 (Cell)

Fax: (937) 433-7366

Email: p.chawla@edaptive.com

URL: www.edaptive.com