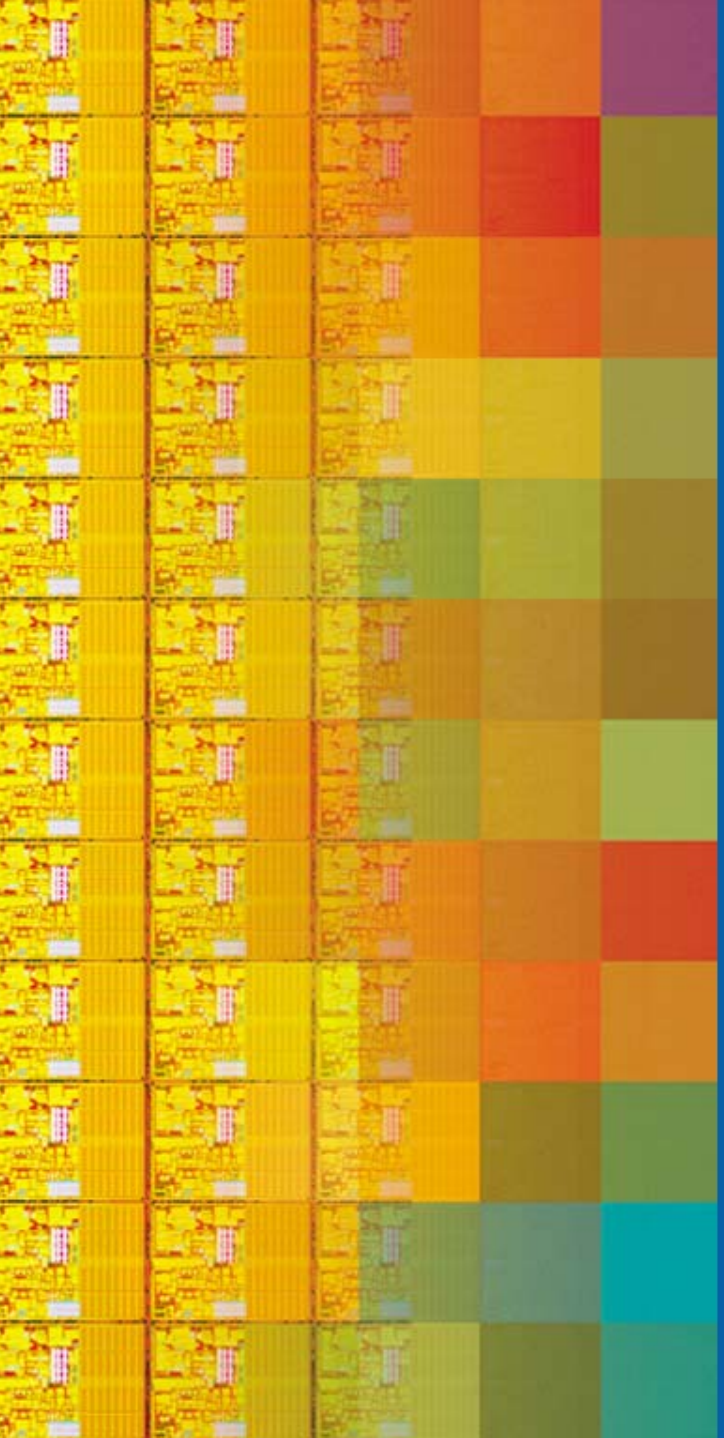


intel Leap ahead™

Intel Developer FORUM

VT Integrity Services for Networking

Uri Blumenthal
Security Architect
Corporate Technology Labs

Intel Developer FORUM

Agenda

- Research motivation
- VISN research
  - Integrity Measurement
  - Memory Protections
- Potential Applications

Virus Attacks Cost $14.2B+

W32.Kiman.A worm

Discovered on: February 02, 2006
Symantec* SecurityResponse*

Checks for the presence of a debugger and terminates itself if one is found on the compromised computer. The same action is taken if it detects that it's running in a virtual machine.

… CD Copy Protection Relies on Hacker Rootkit

Techweb* Nov 2, 2005

Security researchers have identified a rootkit … within the copy protection scheme … to prevent music CDs from being copied to computers

Walker' Pushes or Stealth Rootkits

.com* July 28, 2005
l program capable of es and elevating process xplore the idea of memory ide the rootkit in memory mance impact.

l "raise the bar" for a memory hook the kernel memory oncept driver

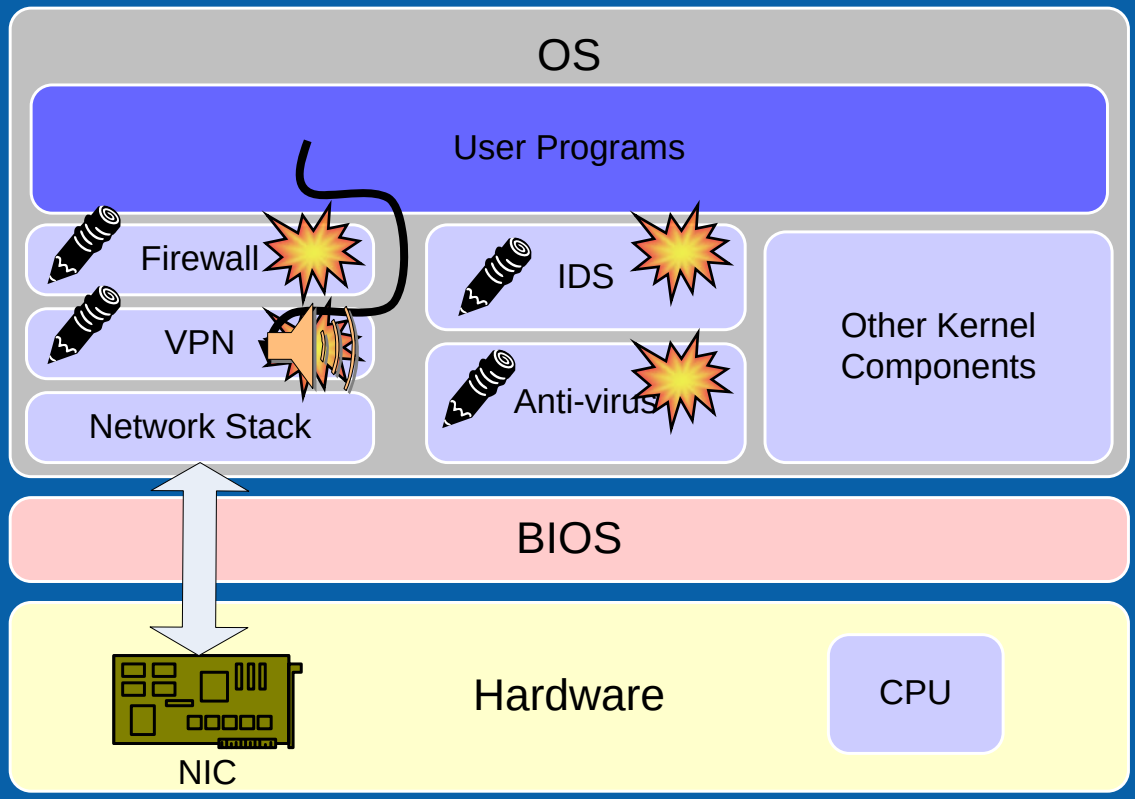
+Computer Economics - 2005 Malware Report

Some Malware Examples

- 3 of the top 10 malicious code samples reported to Symantec* disable security applications+
  - Tooso.F (Trojan), Tooso.B (Trojan), KillAV (Trojan)
- Other well known malware
  - W32.Witty.Worm: Attacks firewall, destroys data
  - W32.Beagle.DN@mm : Attempts to disable security apps
  - W32.IRCBot.I : Attempts to end security processes
  - W32.Aizu.G : Attempts to modify firewall settings
  - W32.Bugbear.b@mm: Attempts to shut down popular antivirus and firewall apps

+Symantec Internet Security. Threat Report. Trends for January 05–June 05. Volume VIII, Published September 2005

Effects Of Memory Based Attacks



- Disable
- Circumvent
- Eavesdrop
- Modify

New Attacks Require New Approach

- Sophistication of attacks increasing cleanup costs
- Attacks target software security applications
- Memory based attacks not completely addressed by today's solutions
- Time between publication and exploit decreasing

New attacks target software integrity and presence

Agenda

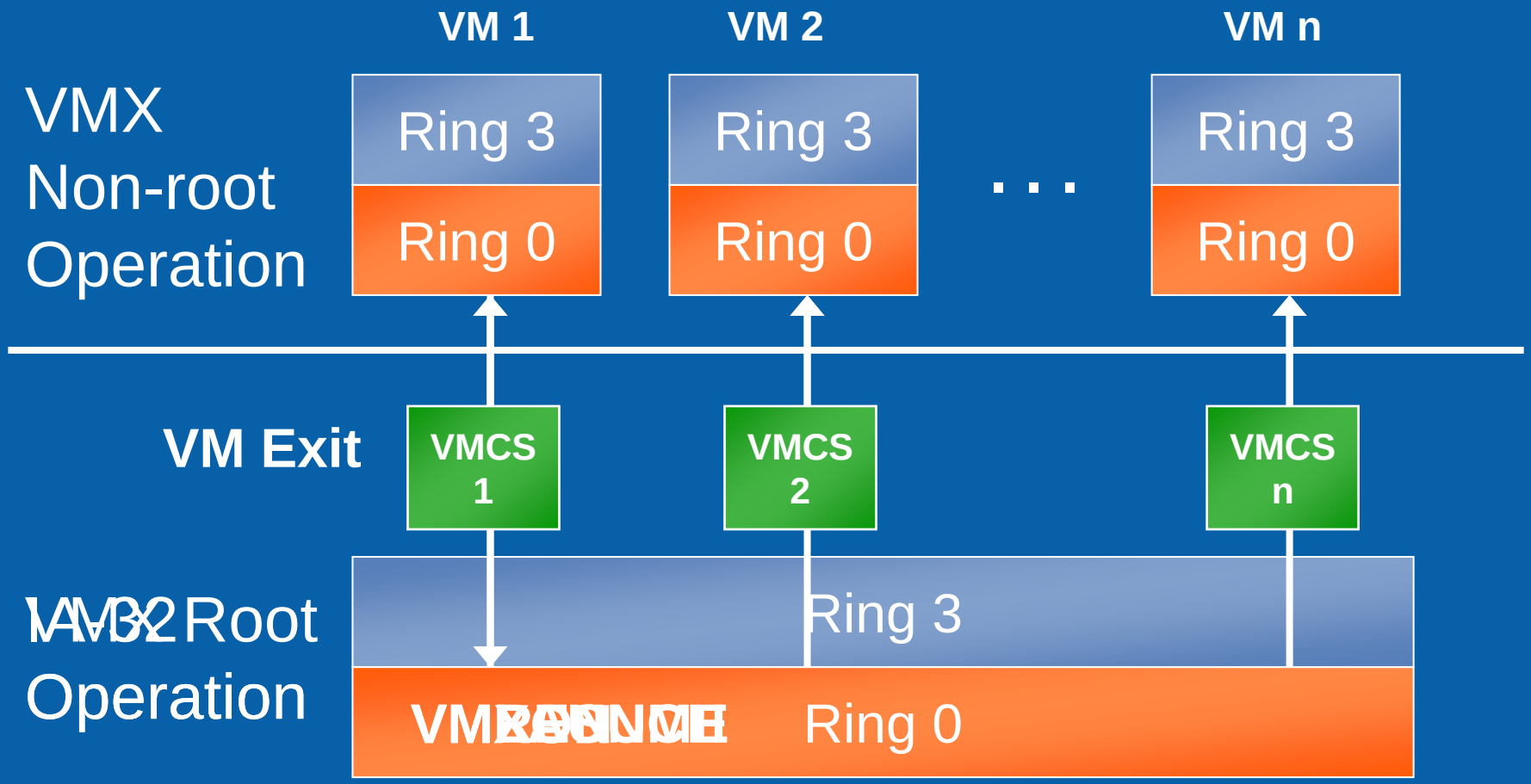
- Research motivation
- VISN research
  - VISN Integrity Measurement
  - VISN Memory Protections
- Potential Applications

VISN Approach

- What it is:
  - Recognize the valid software agents on the platform and aid in protecting them
  - Aid in mitigating memory based attacks

- What it is *not*:
  - A reactive system that tracks known attacks using signatures
  - Example - A signature based host intrusion detection system or an anti-virus program

VT-x Overview



Some Causes of VMEXIT

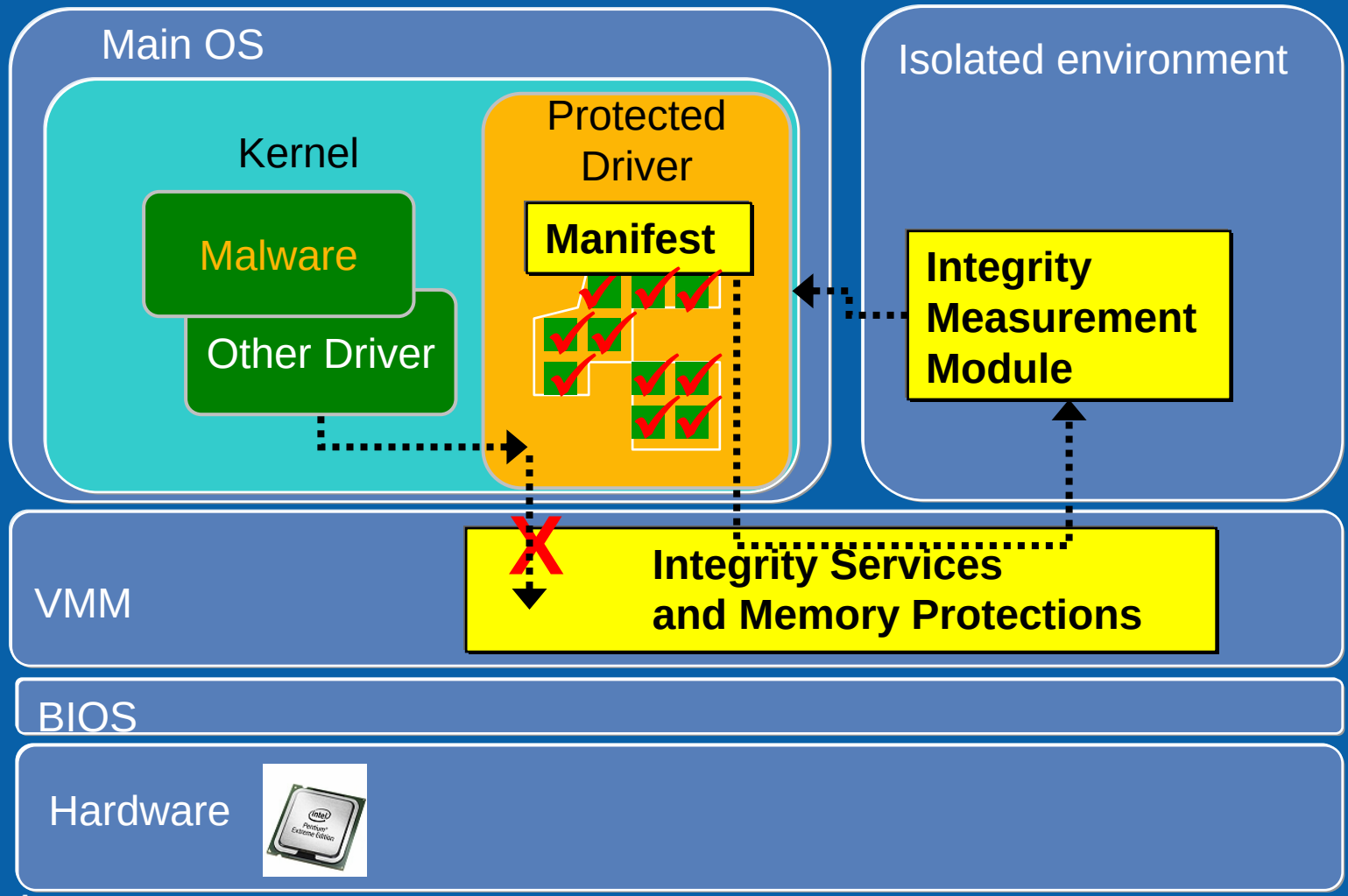
- Paging state exits allow page-table control
  - Control Register 3 (CR3) accesses
  - INVLPG cause exits
  - Selectively exit on page faults
  - CR0/CR4 controls allow exiting on changes to selected bits

- Controls provided for asynchronous events
  - Host interrupt control allows delivery to VMM even when guest blocking interrupts

VISN Components

- Software agent
  - Integrity Manifest
- Isolated OS
  - Integrity Measurement Module
- Virtual Machine Monitor (VMM)
  - Memory Protection Module

VISN Research Prototype



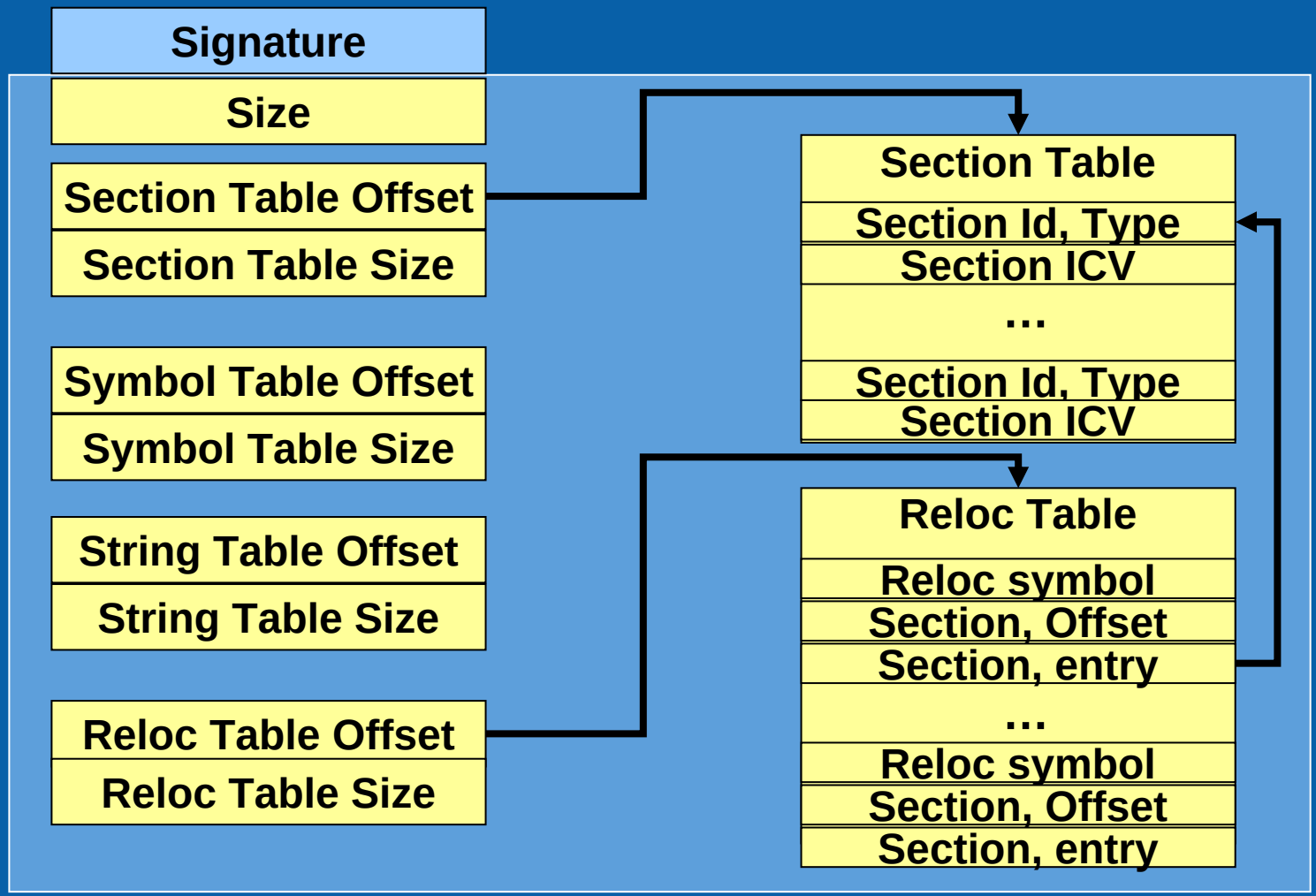
VISN components

Integrity Measurement Module

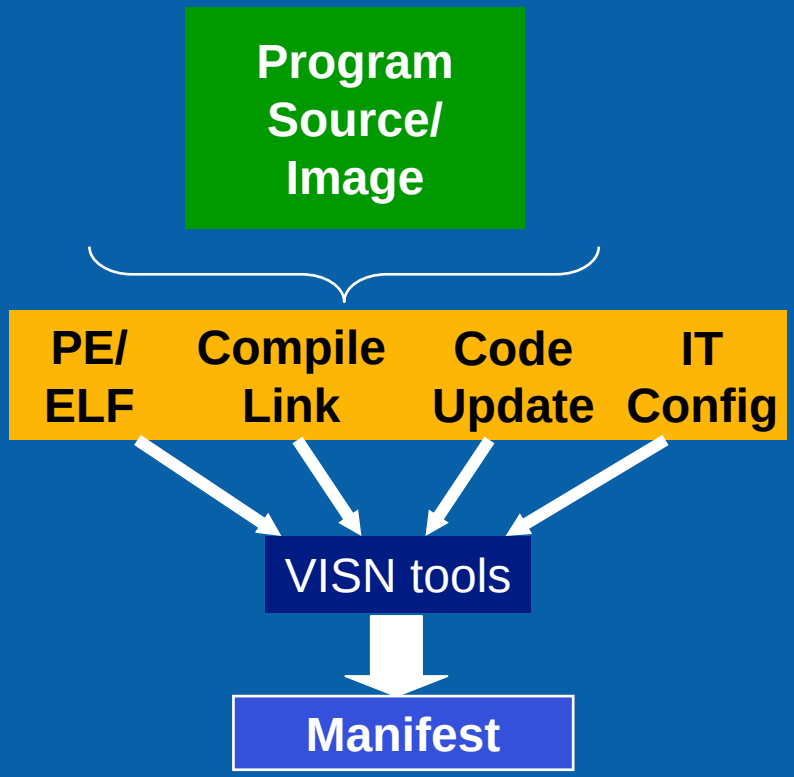
- *Purpose 1*: Identify, locate and validate programs
- *Purpose 2:* Detect modifications of registered programs

- IMM is located in an isolated partition
  - Protection offered by VT
  - Uses VMM services for locating the agent
- Integrity Manifest
  - In memory cryptographically supported identity
  - Binary format independent

VISN Integrity Manifest



Integrity Manifest Creation



Requirements

-*Runtime information*
- *Relocations*
- *External symbols*

-*Cryptographic Signature*

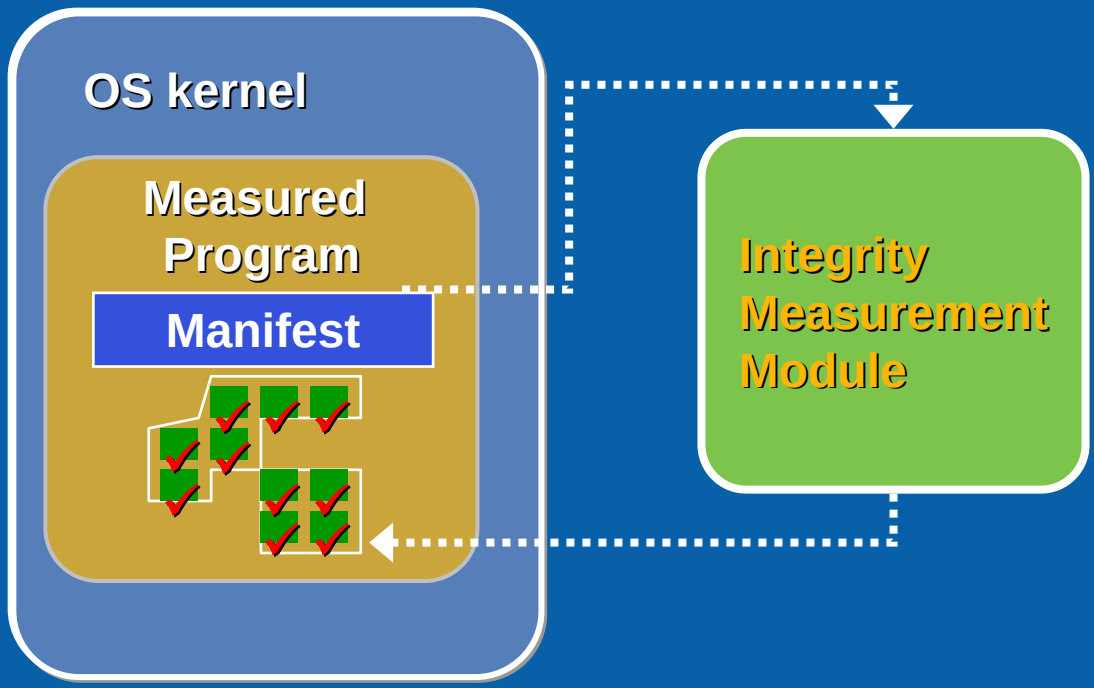
-*Code and Data Sections*

-*Code Entry points*

-*Minimal to no* program change

-Creation by Vendor or IT

Integrity Measurement



- From isolated VT partition
- Unspoofable access to memory
- Establishes programs location in memory

Definitively finds and validates platform agents

Agenda

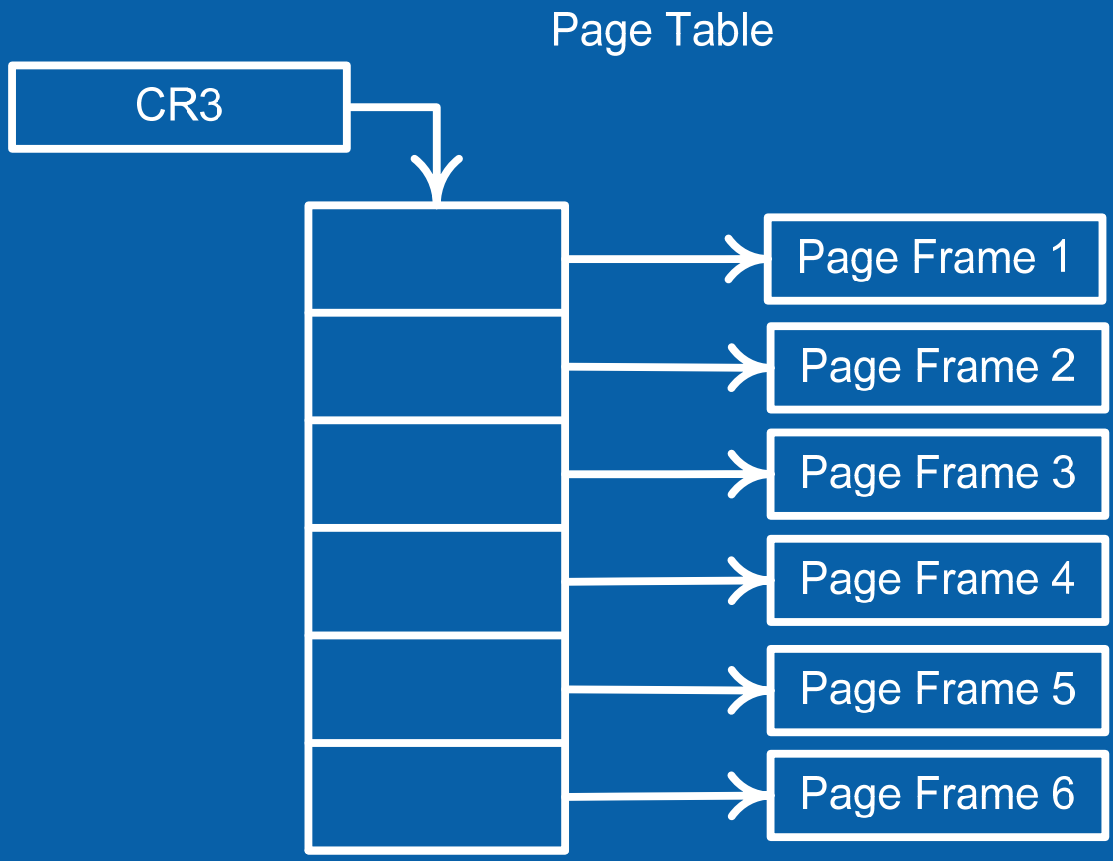
- Research motivation
- VISN research
  - VISN Integrity Measurement
  - VISN Memory Protections
- Potential Applications

VISN Memory Protections

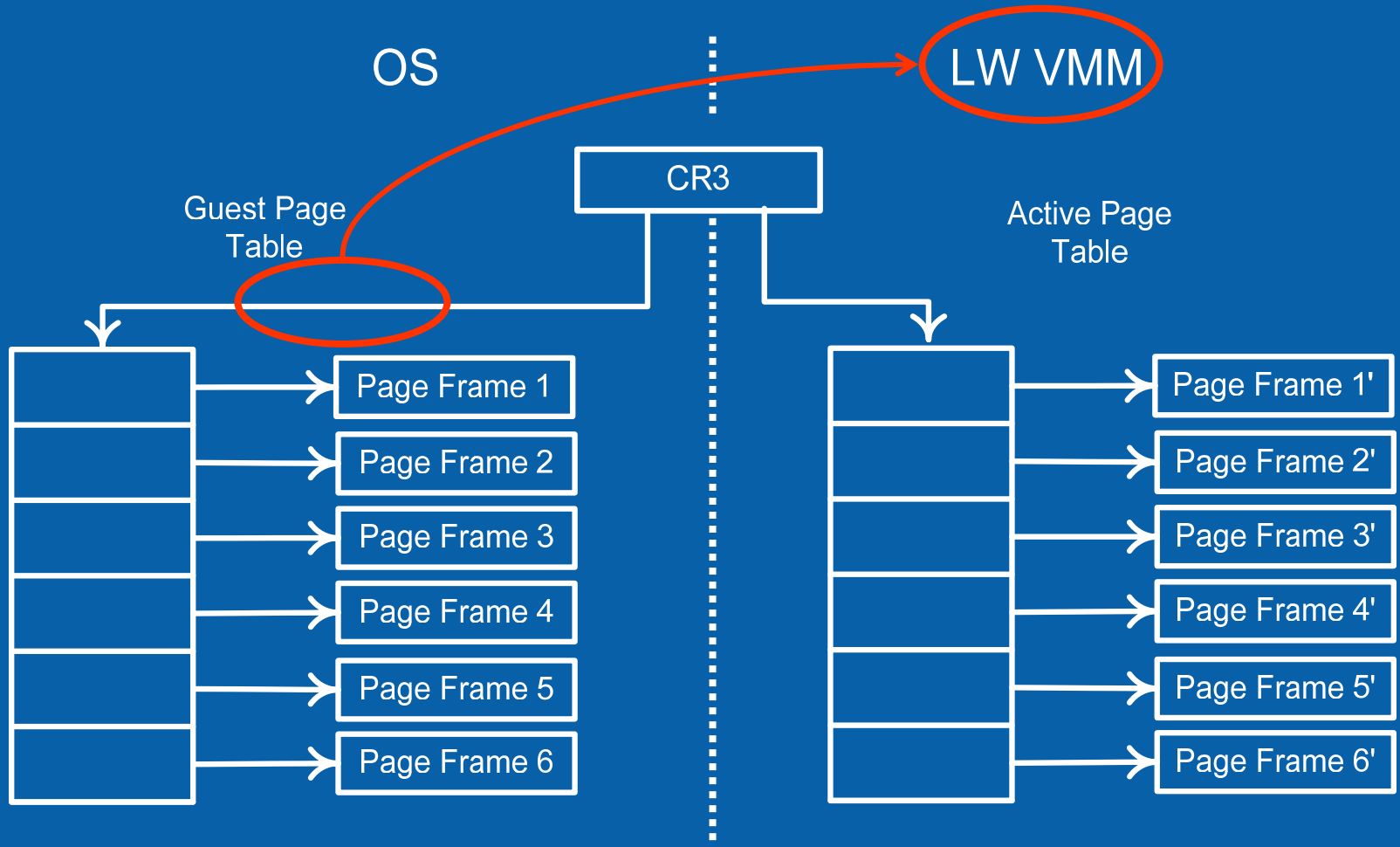
- *Purpose 1*: Aid in preserving the integrity of valid software agents
- *Purpose 2*: Help ensure valid software agents are used the right way
  - Program Entry points
  - Dynamic data protection

- Resides in the VMM
- Monitors memory accesses
  - Uses VT capabilities for efficiency

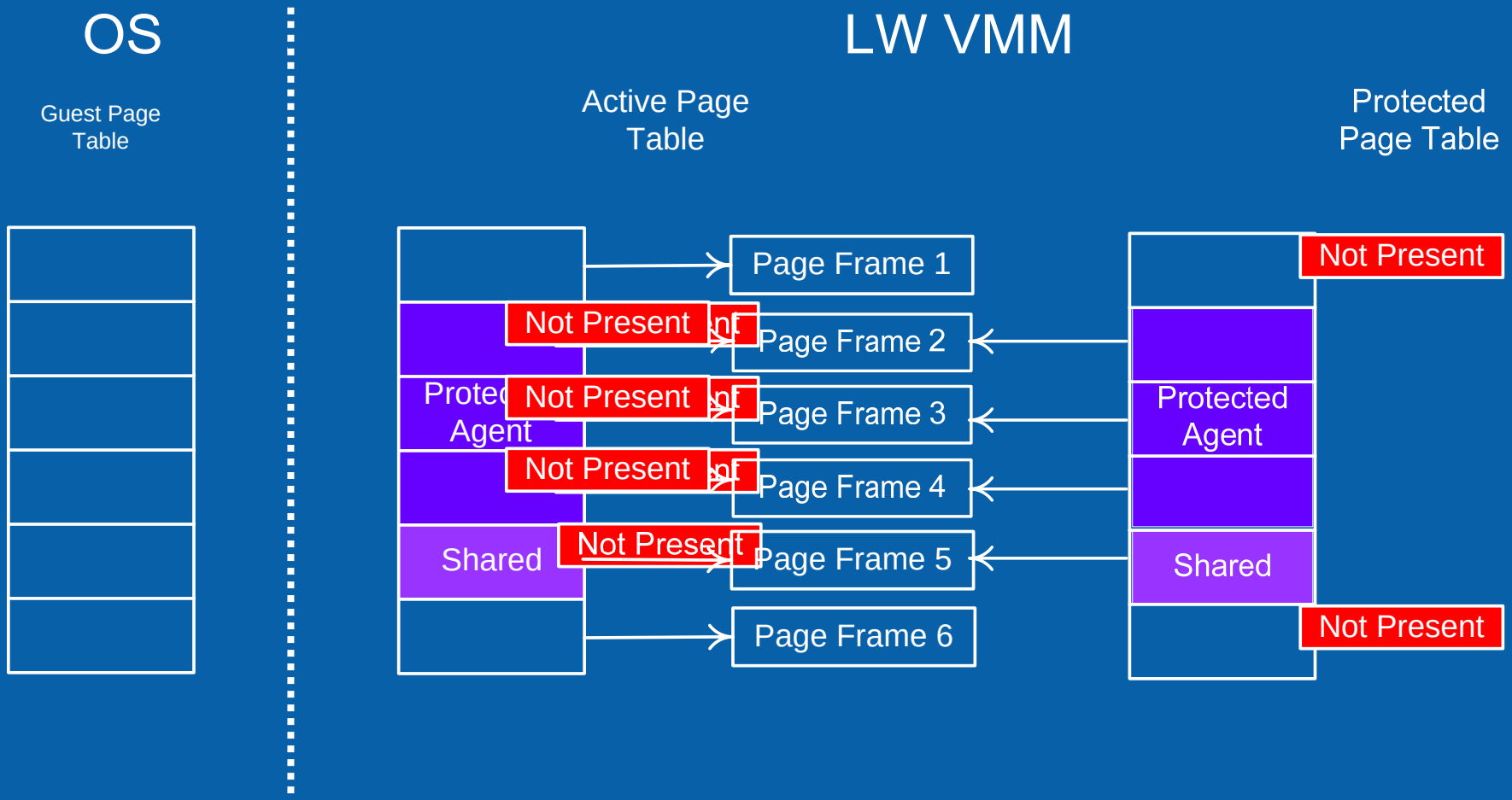
IA-32 Virtual Memory (Simplified)



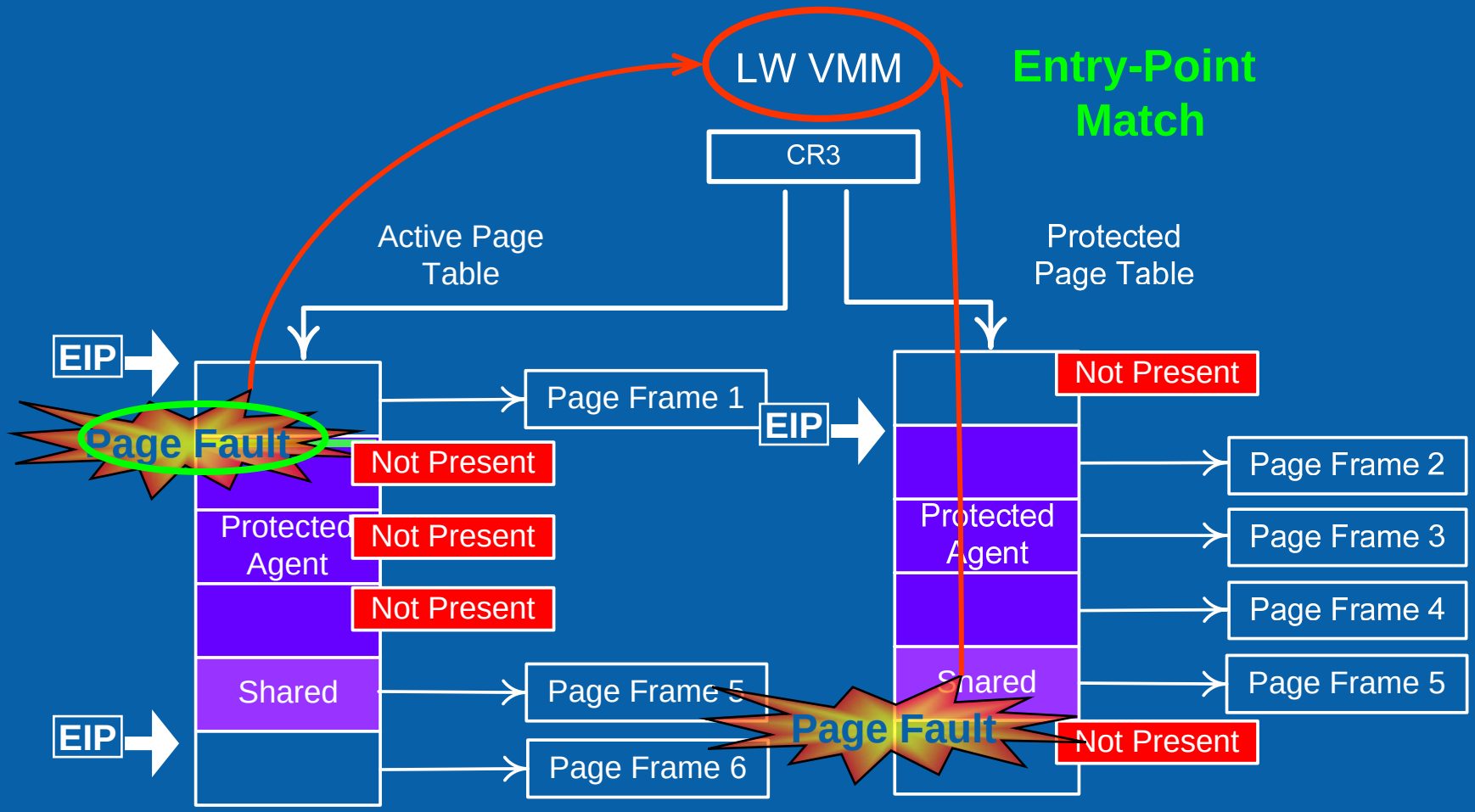
VT Virtual Memory (Simplified)



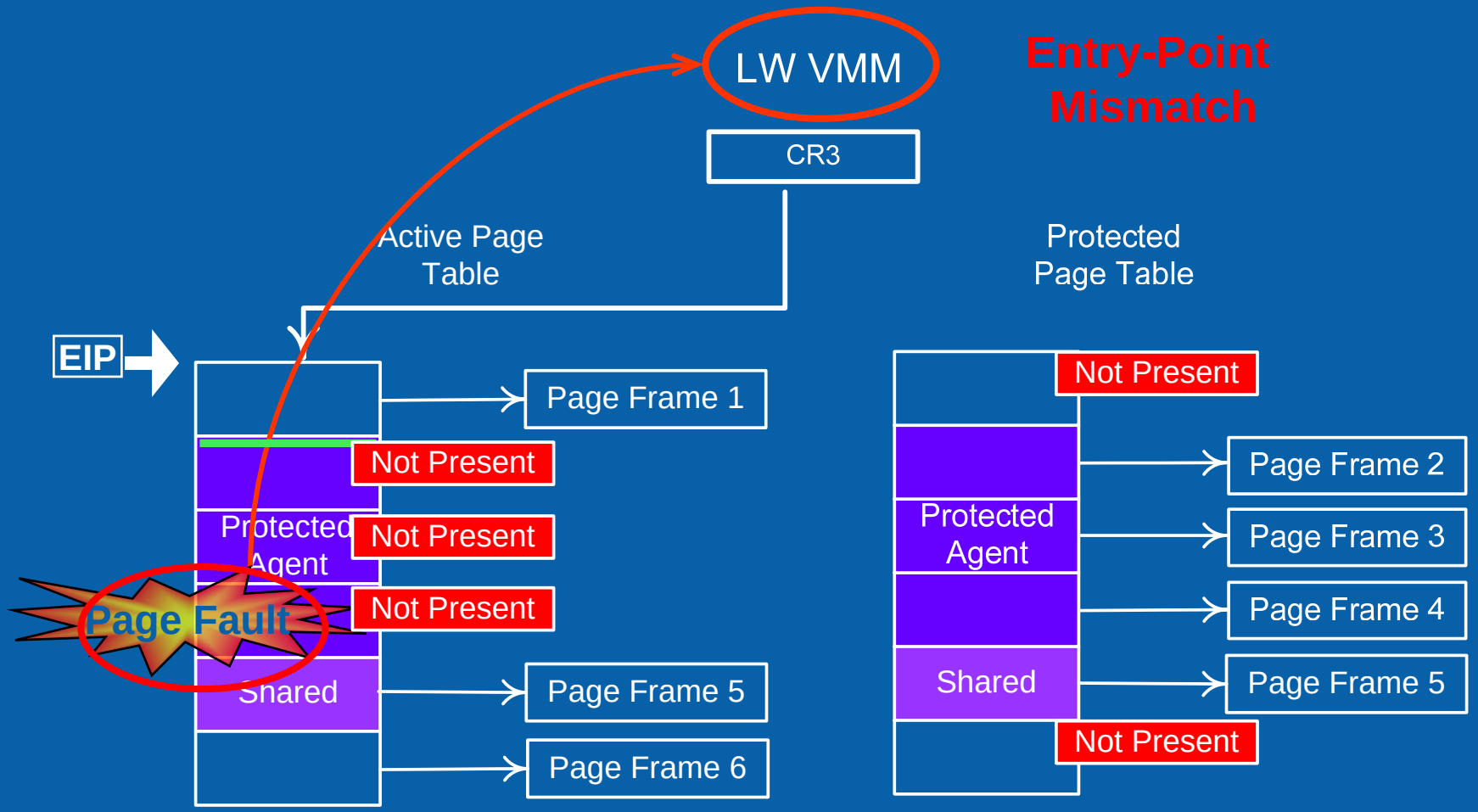
VISN Memory Protection - Setup



VISN Memory Protection - Operation



VISN Memory Protection - Operation



VISN Features Review

- Program integrity verified in memory from isolated partition
- Program integrity preserved using memory protections – *attacks mitigated*
- Program dynamic data and entry points honored – *program use enforced*

Prevention of memory attacks and invalid invocation

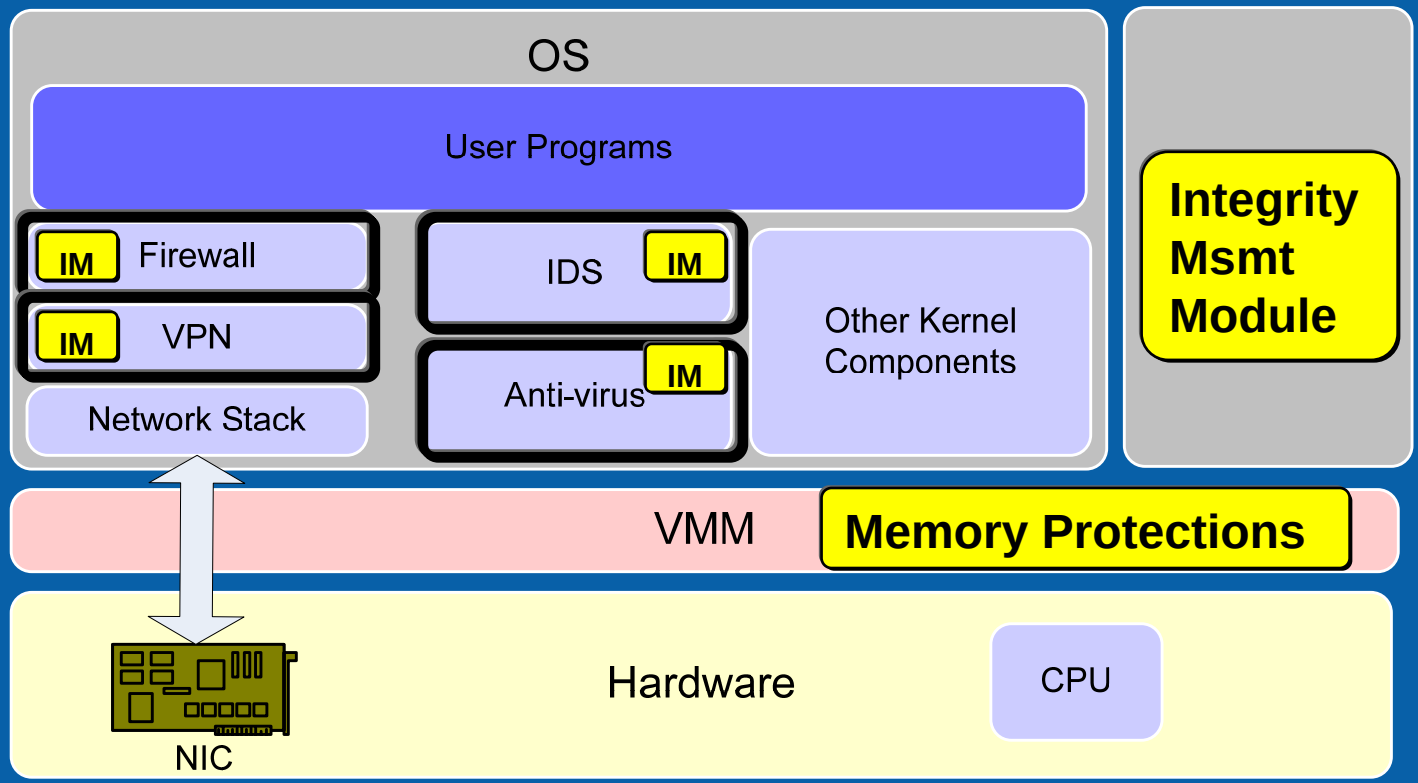
Agenda

- Research motivation
- VISN research
  - VISN Integrity Measurement
  - VISN Memory Protections
- Potential Applications

Potential Applications

- Security Software
- Device drivers
- Critical OS components

Thwarting Memory Based Attacks



~~Disable, Circumvent, Eavesdrop, Modify~~

Summary

- New attacks target software integrity and presence
- VISN aids in definitively finding and validating software agents
- VISN mitigates runtime memory attacks and ensures correct usage of agents
- Several applications can benefit from VISN

Q / A

- Additional details at http://www.intel.com/technology/magazine/research/runtime-integrity-1205.htm
- Please fill out the session evaluation form
- Visit the VISN demonstration in the Tech Showcase, Booth 1003
- Please join us for the VISN chalk talk
  - 3:30 – 4:20 in room 2001A

Thank you!


intel
Leap ahead™