



**Process Control Systems
Industry Conference**

A Hybrid Virtualization Environment for Process Control System Security

**David Kleidermacher, CTO
Green Hills Software, Inc.**

Agenda

- ◆ **Exposure of Control Systems to Insecure Computing Infrastructure**
- ◆ **Current IT Security Posture**
- ◆ **Development in High Assurance IT Security**
- ◆ ***Virtsec* for Control Systems**

Nuclear Power Plant Shutdown

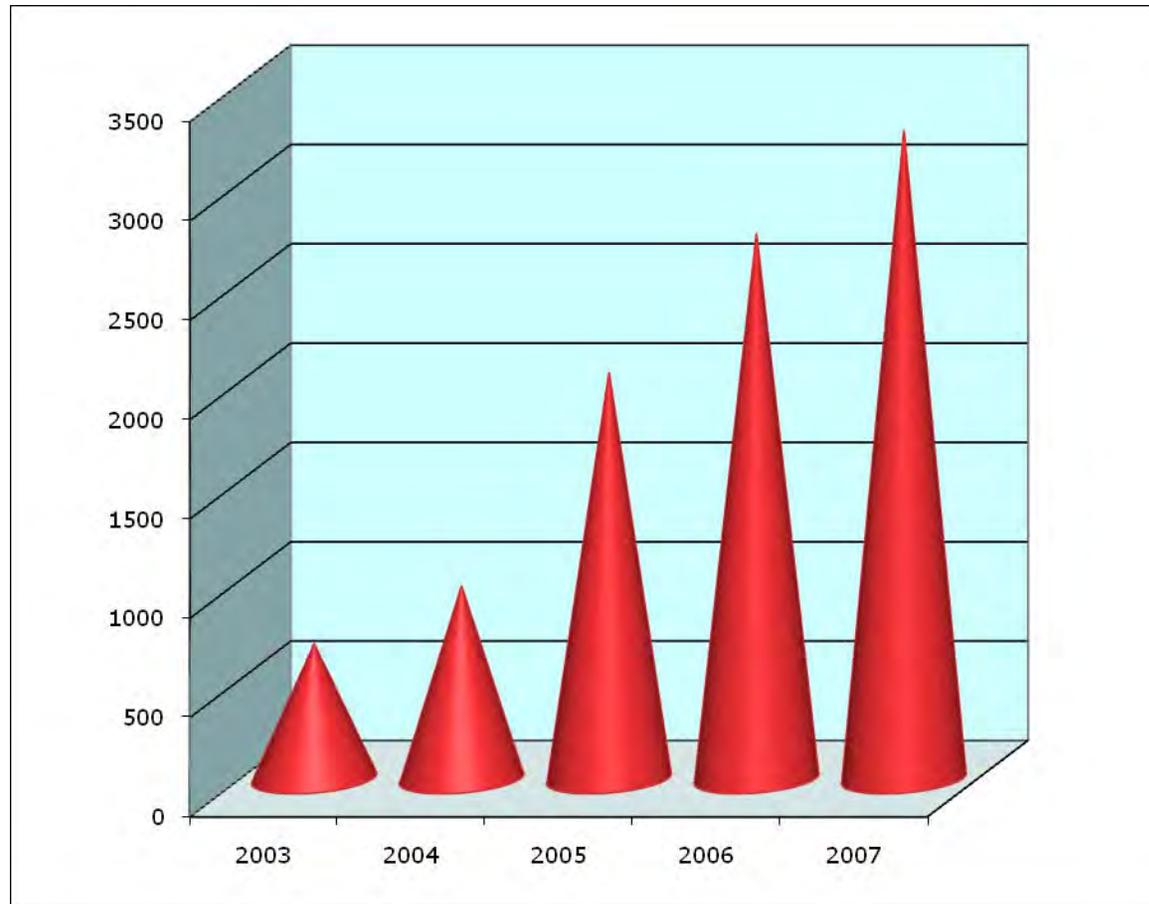
“Technicians were aware that there was full two-way communication between certain computers on the plant's corporate and control networks.”

“Computer security experts say the Hatch plant incident is the latest reminder of problems that can occur when corporate computer systems at the nation's most critical networks are connected to sensitive control systems that were never designed with security in mind.”



IT Security Trends

High Severity Software Vulnerabilities



Source: Common Vulnerabilities and Exposures (CVE) – cve.mitre.org

Common Criteria Primer

◆ Common Criteria (ISO/IEC 15408)

- International standard for evaluating security
- Classes of products based on functional and assurance requirements
 - Firewalls, operating systems, etc.

Common Criteria Level	EAL Description
<i>N/A</i>	N/A
<i>EAL 1</i>	Functionally tested
<i>EAL 2</i>	Structurally tested
<i>EAL 3</i>	Methodically tested and checked
<i>EAL 4</i>	Methodically designed, tested, and reviewed
<i>EAL 5</i>	Semiformally designed and tested
<i>EAL 6</i>	Semiformally verified, designed, and tested
<i>EAL 7</i>	Formally verified, designed, and tested

Public and Government Mislead

- ◆ VMware's recent EAL 4 security certification
 - “The EAL4+ rating is the ***highest assurance level*** that is recognized by all signatories under the Common Criteria Certificates (CCRA).”
 - “It can be used ... for ***sensitive, government computing environments that demand the strictest security.***”
 - Delivers “***unmatched levels of reliability and security***”
- ◆ ***Trusted*** Solaris – also EAL 4
 - “***The Most Secure Operating System*** on the Planet”
- ◆ Symantec Enterprise Firewall – also EAL 4
 - “This certification highlights Symantec's commitment ... to offer customers the ***highest level of security*** in today's market”

What Does EAL 4 Really Mean?

- ◆ Note that Windows and Linux have also met EAL 4
- ◆ Protection Profile:
 - *“Protection against ...inadvertent or casual attempts to breach the system security”*
 - Not appropriate *“against determined attempts by hostile and well funded attackers to breach system security”*

http://www.niap-ccevs.org/cc-scheme/pp/pp_os_ca_v1.d.pdf

What Does EAL 4 Really Mean?

- ◆ *“It’s secure as long as nothing is connected to it”* – NSA security evaluator

- ◆ *“Security experts have been saying the security of the Windows family of products is hopelessly inadequate. Now there is a rigorous government certification confirming this.”* – Jonathan Shapiro, Johns Hopkins computer security expert

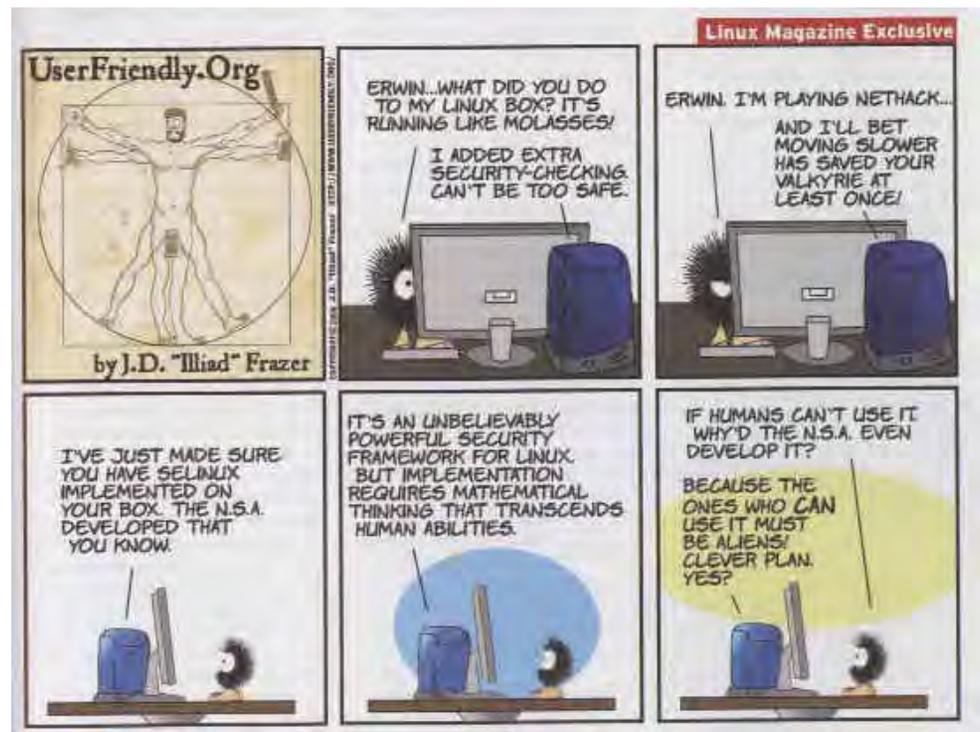
What Does EAL 4 Really Mean?

◆ How about SELinux?

- Like Trusted Solaris, adds security controls on top of a low assurance foundation
- Putting a padlock on a screen door

◆ SELinux website

- *“There has been no work focused upon increasing the assurance of Linux”*
- *“Security-enhanced Linux is ... very unlikely by itself to meet any interesting definition of secure system.”*



What Does EAL 4 Really Mean?

◆ But we can make it secure, can't we?

- *EAL 4 “is the highest level at which it is likely to be economically feasible to retrofit an existing product line.”* – Common Criteria v2.1

◆ EAL 4 means: ***certified hackable***

EAL 4 – Certified Hackable

◆ Numerous security vulnerabilities in Windows, Linux, Solaris, VMware, Cisco, & Symantec

National Vulnerability Database
automating vulnerability management, assessment, and compliance checking

There are 1868 matching records. Displaying matches 1 through 20.

CVE-2007-3902
Summary: Security flaw in a certain Red Hat patch, applied to kernel 2.6.9 on Red Hat Enterprise Linux (RHEL), 5 and Fedora 9 through 8, and on Foresight Linux and other appliances, allows remote attackers to cause a denial of service (memory consumption) via a large number of CWD commands, as demonstrated by an attack on a daemon with the file, the configuration error, and the CVE-2007-3902.

CVE-2008-2145
Summary: The net-snmpd tool on Ubuntu Linux 7.04, 7.10, and 8.04 LTS does not recognize authorized keys lines that contain options, which make it easier for remote attackers to exploit the net-snmpd daemon to cause a denial of service (DoS) via a large number of CWD commands, as demonstrated by an attack on a daemon with the file, the configuration error, and the CVE-2008-2145.

National Vulnerability Database
automating vulnerability management, assessment, and compliance checking

There are 1788 matching records. Displaying matches 1 through 20.

CVE-2008-2400
Summary: Unspecified vulnerability in the services before 4.2.3, when running as a service on Windows, allows local users to gain privileges via unknown attack vectors.

CVE-2008-1838
Summary: Unspecified vulnerability in Microsoft Exchange Protection Engine (Exchange.D) 1.3.072.0 and 1.0.1.0, as used in multiple Microsoft Exchange servers, allows remote attackers to cause a denial of service (link space exhaustion) via a file with "bad" data structured that trigger the creation of large temporary files, a different vulnerability than CVE-2008-1337.

National Vulnerability Database
automating vulnerability management, assessment, and compliance checking

There are 584 matching records. Displaying matches 1 through 20.

CVE-2008-2141
Summary: Race condition in the STRENGTH Administrative Driver (ASD) in Sun Solaris 10 allows local users to cause a denial of service (panic) via unknown vectors.

CVE-2008-2144
Summary: Multiple unspecified vulnerabilities in Solaris 10 patch sets for Sun Cluster 3.5 and 3.0 allow remote attackers to cause a denial of service or execute arbitrary code via compliance (e.g. FPM).

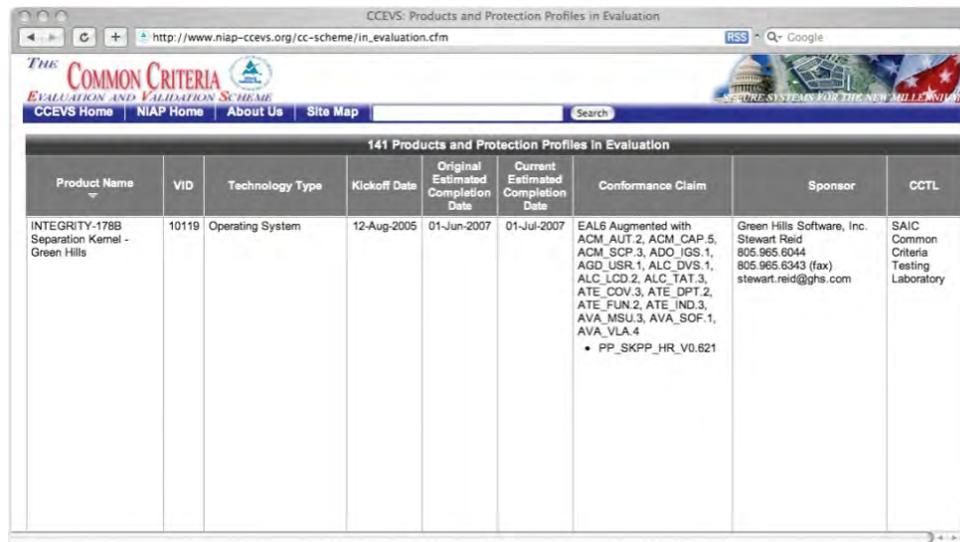
CVE-2008-2121
Summary: Unspecified vulnerability in Symantec's Altru Deployment Solution 6.8.0 and 6.9.0 before 6.9.176 allows remote attackers to retrieve weakly encrypted domain credentials via unknown attack vectors related to a missing file.

EAL 4 for Process Control Systems

“The vulnerabilities are endemic because we have whole networks and infrastructures built on software that’s insecure. Once an outsider gains root access, he could do anything. Any given day, some new vulnerability pops up.” – Michael Vatis, executive director of the Task Force on National Security in the Information Age

High Assurance – Achievable?

- High assurance Common Criteria evaluation
 - http://www.niap-ccevs.org/cc-scheme/in_evaluation.cfm (VID 10119)
 - NSA penetration testing



The screenshot shows a web browser window displaying the NIAP CCEVS website. The page title is "CCEVS: Products and Protection Profiles in Evaluation". The URL in the address bar is "http://www.niap-ccevs.org/cc-scheme/in_evaluation.cfm". The page features a navigation menu with links for "CCEVS Home", "NIAP Home", "About Us", and "Site Map". A search bar is also present. The main content area is titled "141 Products and Protection Profiles In Evaluation" and contains a table with the following data:

Product Name	VID	Technology Type	Kickoff Date	Original Estimated Completion Date	Current Estimated Completion Date	Conformance Claim	Sponsor	CCTL
INTEGRITY-178B Separation Kernel - Green Hills	10119	Operating System	12-Aug-2005	01-Jun-2007	01-Jul-2007	EAL6 Augmented with ACM_AUT.2, ACM_CAP.5, ACM_SCP.3, ADD_IGS.1, AGD_USR.1, ALC_DVS.1, ALC_LCD.2, ALC_TAT.3, ATE_COV.3, ATE_DPT.2, ATE_FUN.2, ATE_IND.3, AVA_MSU.3, AVA_SOF.1, AVA_VLA.4 • PP_SKPP_HR_V0.621	Green Hills Software, Inc. Stewart Reid 805.965.6044 805.965.6343 (fax) stewart.reid@ghs.com	SAIC Common Criteria Testing Laboratory

EAL 7 Operating System in F-35

- ◆ Mission systems
- ◆ Display systems
- ◆ Communication/Navigation/Identification Systems (CNI)
- ◆ Crypto Engine
- ◆ Lead program for certification
 - “**high robustness**”: the most valuable information exposed to the most determined and resourceful attackers
 - ***This is the level of security we need***



High Robustness Operating Systems

◆ Designed for security

- Guaranteed resource availability and Deterministic operation
 - Other operating systems susceptible to DoS
- Least privilege model for security using object capabilities
 - Other operating systems have weak access control
 - Anatomy of a buffer overflow
 - » Stack segment with execute privilege
 - » Program launch privilege
 - » File system access privilege
 - » File modification privilege
- Minimal microkernel architecture
 - Other operating systems are hopelessly complex and riddled with bugs (vulnerabilities)

High Robustness Operating Systems

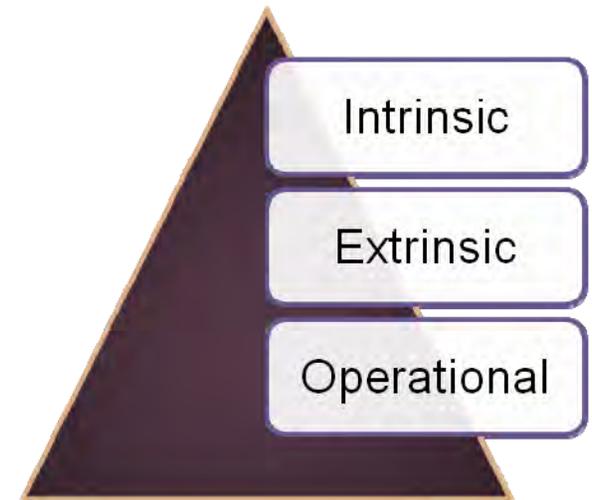
◆ Assurance artifacts

- Formal methods (done right)
- Plans / design / documentation for every single line
- MCDC testing
- Secure configuration management and delivery
- Much more

High Robustness Software

◆ Independent Evaluation/Certification

- DO-178B Level A
- IEC-61508 SIL 3
- CMMI Level 3
- NSA EAL6+
- Type I/II FDA/CDRH Medical
- NSA Type 1



◆ Proven in Use in Critical Systems

- Medical/Industrial/Avionics/Automotive/Financial/Consumer
- At least 10 years of use in demanding applications
- *"It's easier to prove something when it is already correct"* – Rockwell Collins Formal Methods Center of Excellence

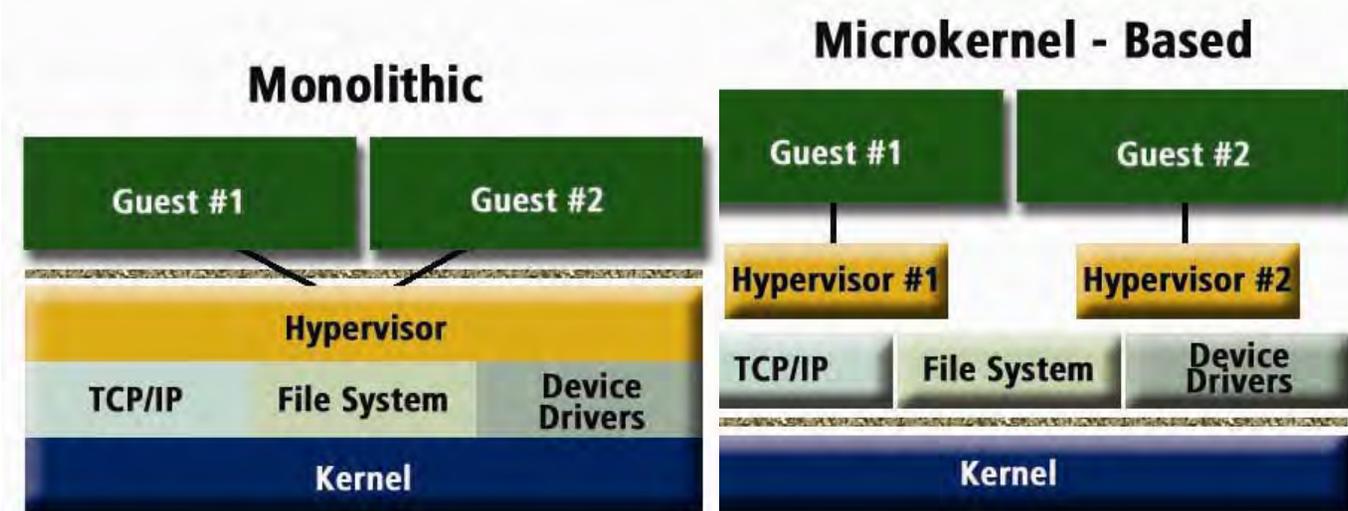
Virtualization Security (*virtsec*)

- Virtualization does not imply security
- Security experts recognize that virtualization can *increase* attack surface
 - King, et al (SubVirt, Blue Pill) – UMich, MSFT research
 - Tavis Ormandy – Empirical Study of Security Exposure in Virtualized Environments (QEMU, VMware, etc.) – *“Virtualization is no security panacea”*



Virtualization Security

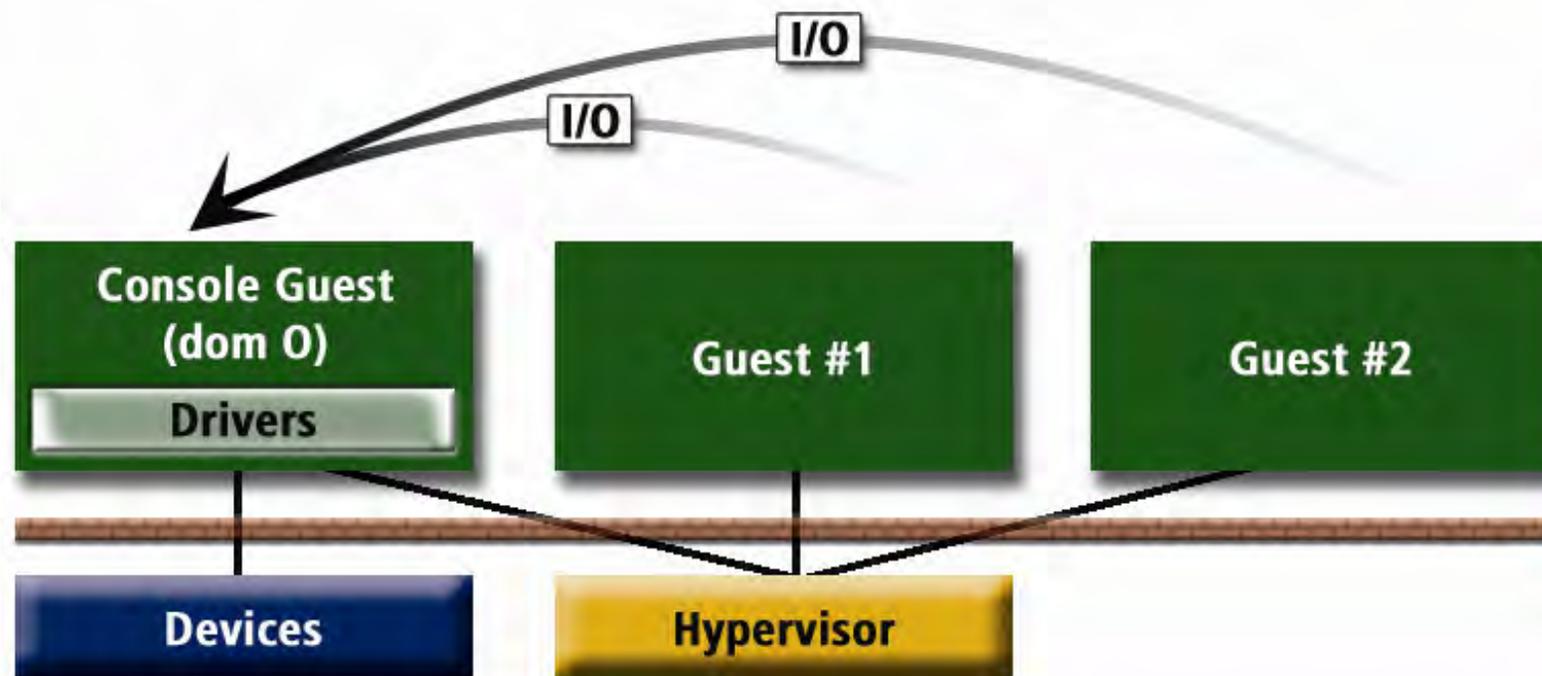
- ◆ Hypervisor architecture – legacy vs. secure



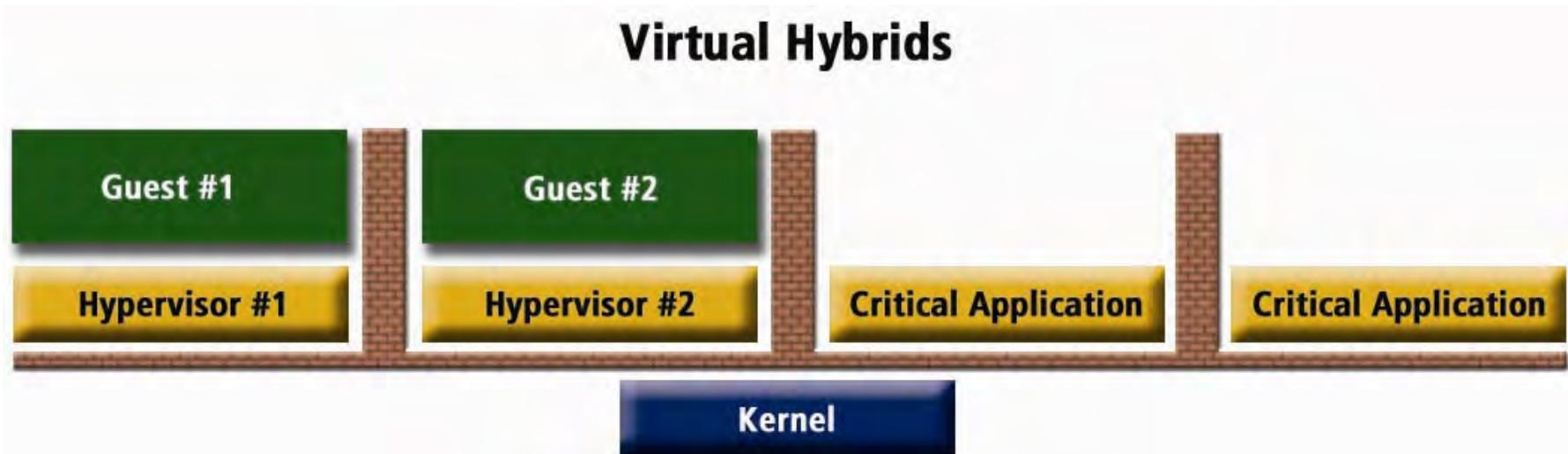
- ◆ INTEGRITY, with Padded Cell technology is an example of the microkernel approach

Virtualization Security

- ◆ Hypervisor architecture – beware console OS (large TCB)

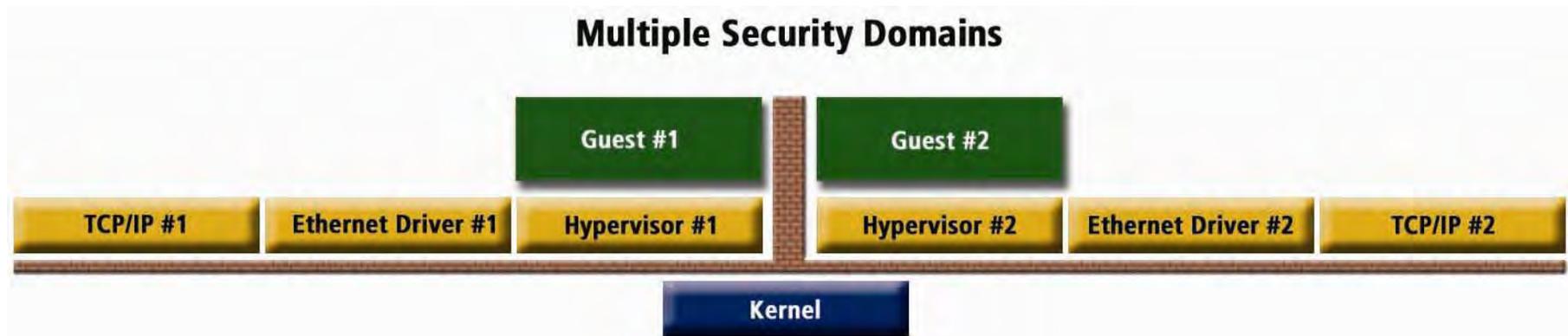


Virtualization Security



- ◆ Critical applications hosted by high assurance kernel
- ◆ Brick wall partitioning between guests and critical apps

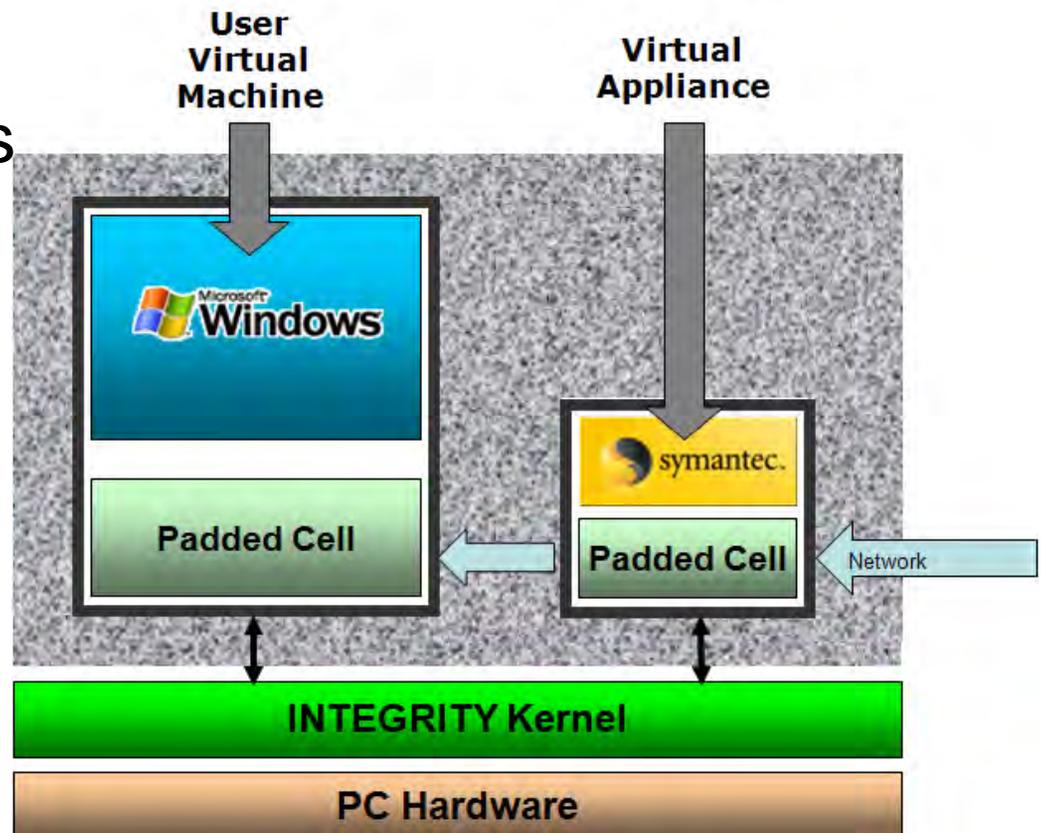
Virtualization Security



- ◆ Guest 1: Control system environment
- ◆ Guest 2: Corporate network / quality-of-life environment
 - Browse the Internet safely!
- ◆ Choices for sharing a display

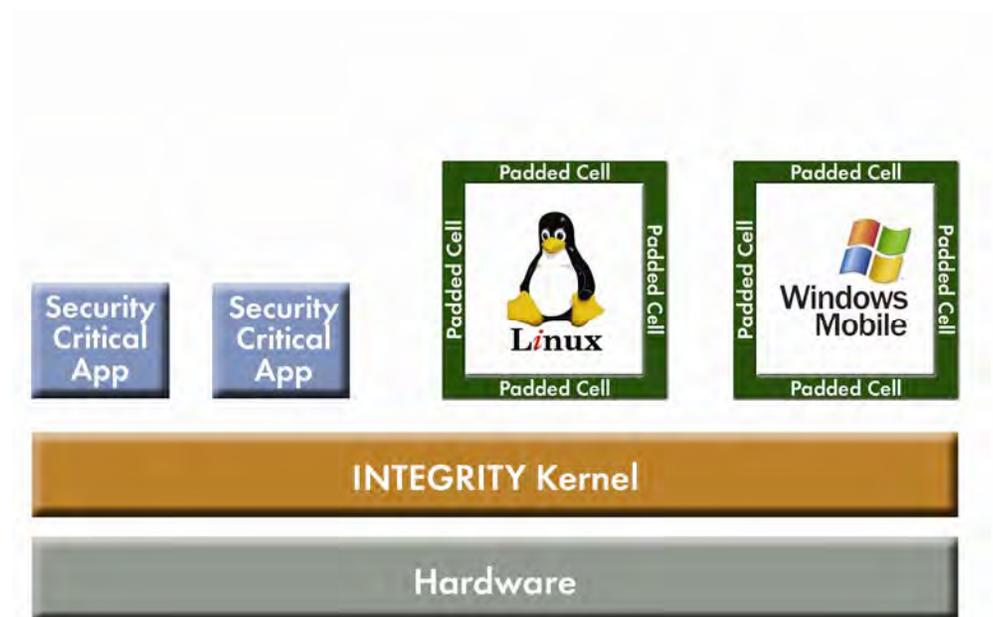
Virtualization Security

- Secure virtual appliances
 - Access control
 - Policy managers
 - Firewalls
 - Anti-virus



Virtualization Security

- ◆ Not just desktops and servers
 - ◆ Laptops
 - ◆ Mobile Devices
 - ◆ Digital keys
 - ◆ In-person proofing



Virtualization Security

- ◆ Beyond the security kernel
 - ◆ Rogue peripherals
 - ◆ Commandeered platform software – BIOS, security kernel
 - ◆ Performance problems due to virtualization

Virtualization Security

- ◆ Intel to the rescue
 - ◆ Rogue peripherals: *VT-d*
 - ◆ Commandeered platform software: *TXT*
 - ◆ Performance problems due to virtualization: *VT-x*, *VT-d*, and follow-on generations of both

Summary

- ◆ Risk of compromised process control systems
- ◆ Current security posture of IT infrastructure
- ◆ High assurance is here
- ◆ *Virtsec* is a key enabling technology
 - ◆ Security where you need it
 - ◆ Even if the control and corporate networks meet
 - ◆ While retaining use of common operating environments