IBM T J Watson Research Center

# Toward Trusted Virtual Domains

*hypervisor security architecture –*
*foundation for secure distributed services*

Thomas Rueter
Systems Architect Northeast Europe.
trueter@de.ibm.com

February, 2007

© 2007 IBM Corporation

# Links to the IBM Research Resources for sHype

- Trusted Virtual Data Center
  - http://domino.research.ibm.com/comm/research_projects.nsf/pages/ssd_trustedvirtualdatacenter.index.html
- Trusted Virtual Domains
  - http://domino.research.ibm.com/comm/research_projects.nsf/pages/ssd_tvd.index.html
- Secure Hypervisor
  - http://domino.research.ibm.com/comm/research_projects.nsf/pages/ssd_shype.index.html
- Integrity Measurement Architecture
  - http://domino.research.ibm.com/comm/research_projects.nsf/pages/ssd_ima.index.html
- Secure Systems Department
  - http://domino.research.ibm.com/comm/research_teams.nsf/pages/secure_systems_department.index.html

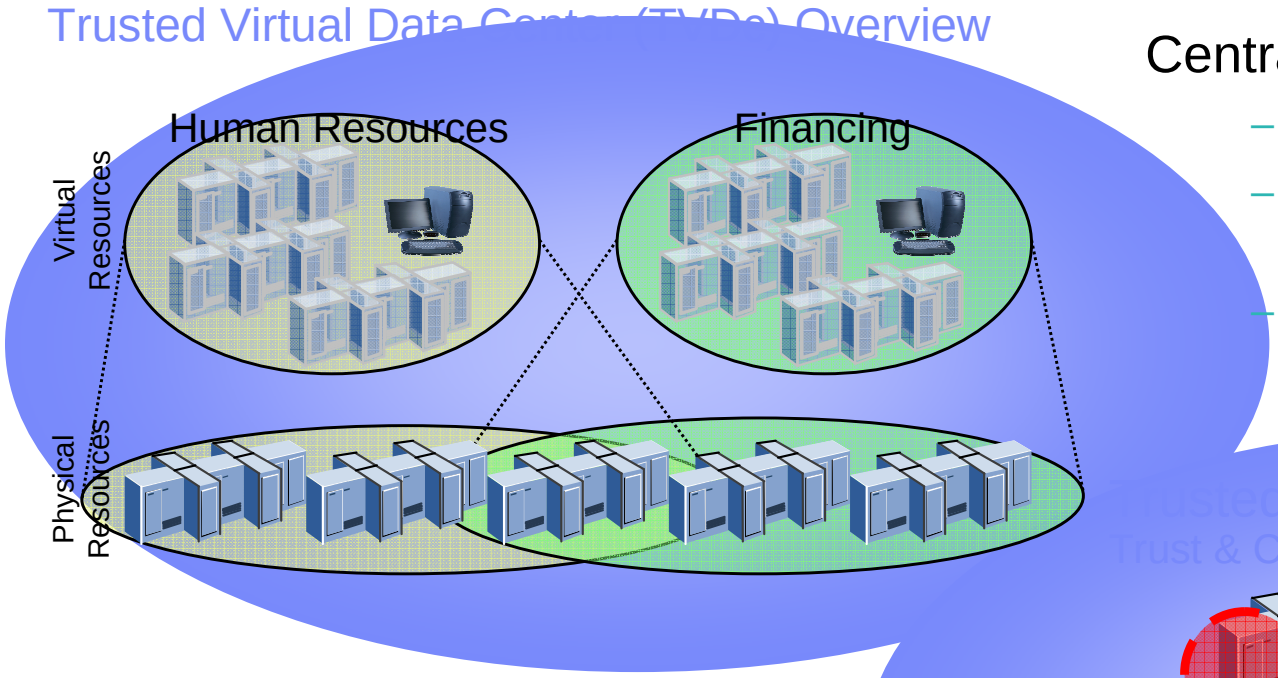

© 2007 IBM Corporation

# Prologue

- Significant Challenges
  - Status quo approach to IT and business security is too complex, is not measurable, will not scale
  - Lack of secure foundation for on demand, secure operating systems not economically viable
- Synergistic Strategy
  - Leverage emerging *trusted computing* technologies (TCG) and commoditization of virtualization (Intel / AMD, EMC, Microsoft, IBM)
  - Near-term: strong guarantees position security as an enabler
  - Longer-term: measurability, radically simplified IT security management

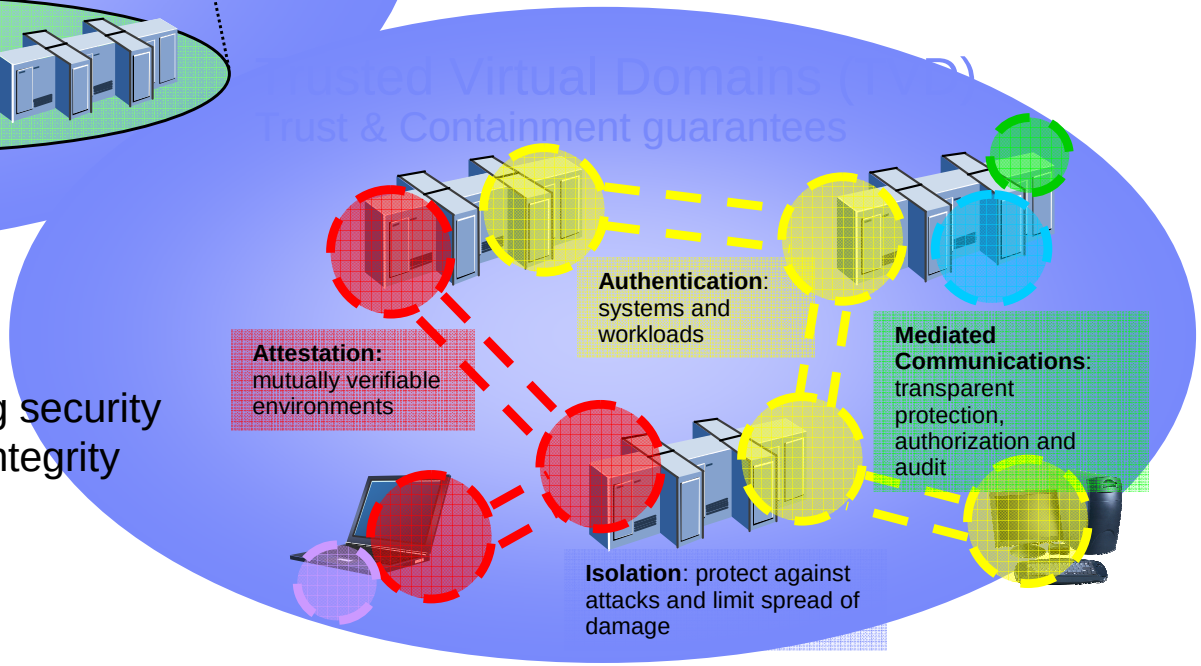

© 2007 IBM Corporation

# Virtualization-based Security & Systems Management




## Centralized IT Security management

- Abstracting the physical infrastructure
- Policy-driven configuration and management
- Flexible distributed workload and resource-based access controls




## Distributed Enforcement

- Coarse-grain but extremely strong security guarantees – e.g., confinement, integrity
- Transparent data protection
- Audit and resource control


© 2007 IBM Corporation

# Discussion Outline

- Virtualization Background
  - Industry Trends and the Security Opportunity
- Hypervisor Security Architecture (*sHype*)
  - Access Control and Integrity Measurement
- Distributed Trusted Computing Base
  - Unified policy enforcement at the virtualization layer across platforms
- Trusted Virtual Domains
  - Concepts, prototype, realization


© 2007 IBM Corporation

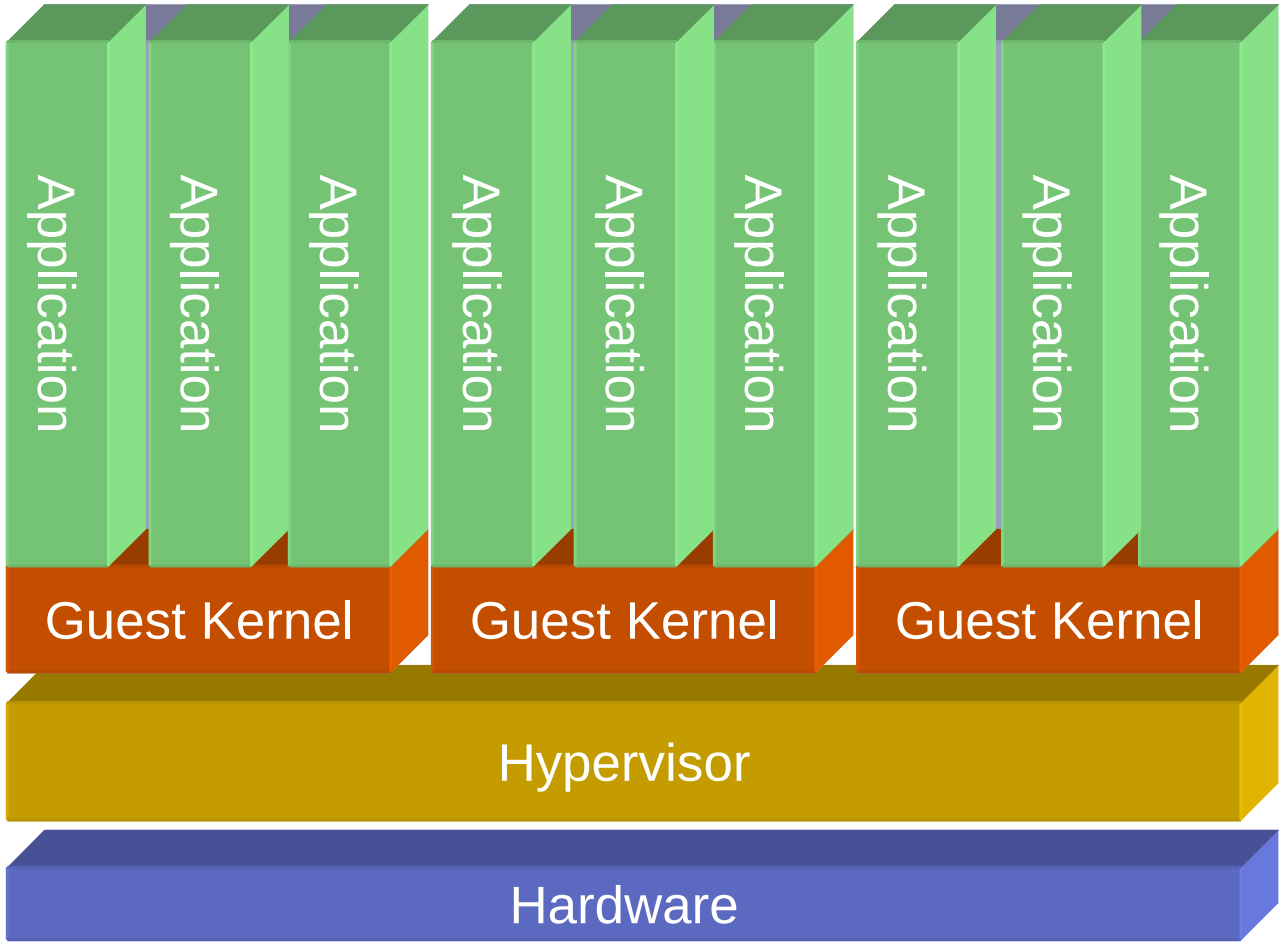
# Virtualization Landscape at a Glance

Broad term with many meanings, e.g., from emulation to modeling

- Application-level (or middleware-level) virtualization
  - E.g., Java Virtual Machine, Softricity (Microsoft SoftGrid), Thinstall
  - Potentially including the emerging field of application streaming
- Operating system-level virtualization
  - E.g., Linux VServers, Solaris Containers / Zones, Virtuozzo (SWsoft)
- Hypervisor-based virtualization
  - Type 1: VMware ESX, Microsoft Viridian, Xen
  - Type 2: VMware Workstation, Microsoft Virtual PC


© 2007 IBM Corporation

# Classic Type 1 Hypervisor




Virtual Machines

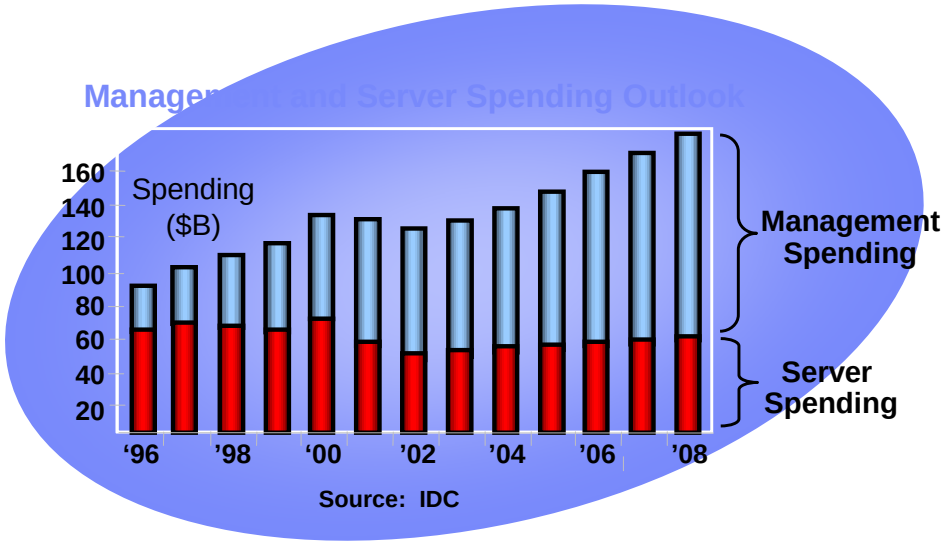
Virtualizes hardware

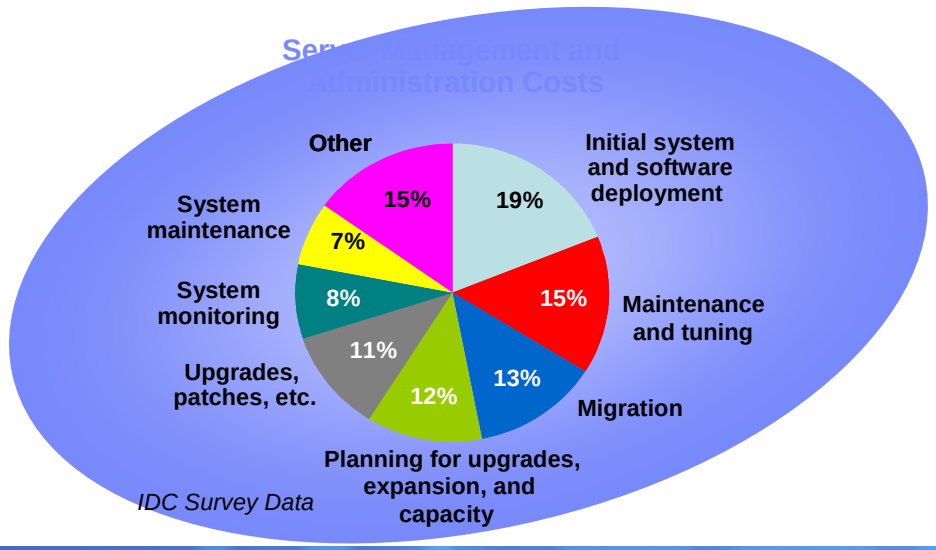
CPU and I/O devices


© 2007 IBM Corporation

# Economics Driving Renewed Interest in Virtualization

- Primarily a server consolidation story today
  - Space, electricity, cooling can account for 50% cost of operating a data center
  - Less than 10% utilization rates can be typical for commodity systems
- Promises to radically simplify Systems Management
  - Redistributing workloads to further optimize utilization as well as performance (e.g., transaction latency), availability, power, and even security
- Basis for new IT delivery and provisioning paradigm (licensing?)
  - New systems provisioned using pre-built images (e.g., appliances)





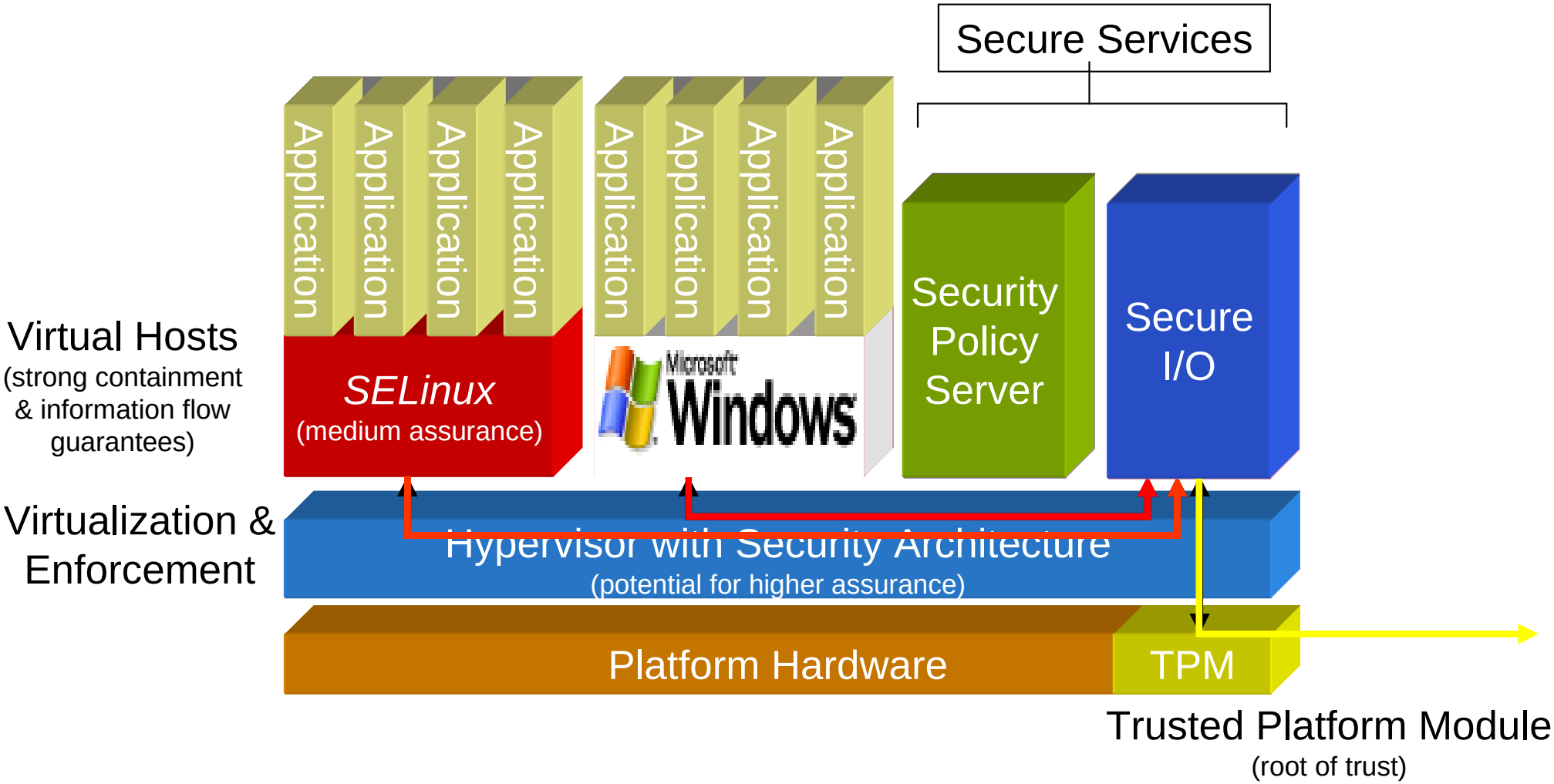
© 2007 IBM Corporation

# Case for Virtualization-based Systems Security

- Type 1 hypervisor solutions becoming pervasive
  e.g., IBM server families
  - *System z (mainframe)*: z/VM, Processor Resource / Systems Manager (PR/SM)
  - *Systems p & i (RISC)*: PHYP (converged platform hypervisor)
  - *System x* (Intel/AMD): VMware, Microsoft Viridian, Xen
  - Hypervisors becoming part of the firmware / BIOS
- Isolation on shared platforms has always been an advantage
  - Emergence of self-virtualizing I/O adaptors, network and storage virtualization
- Reduced size, complexity of hypervisor vs. operating system
  - Potential for greater degree of reliability / higher assurance
- Layered system security model emerging
  - hardware → ***hypervisor*** → OS → middleware / applications


© 2007 IBM Corporation

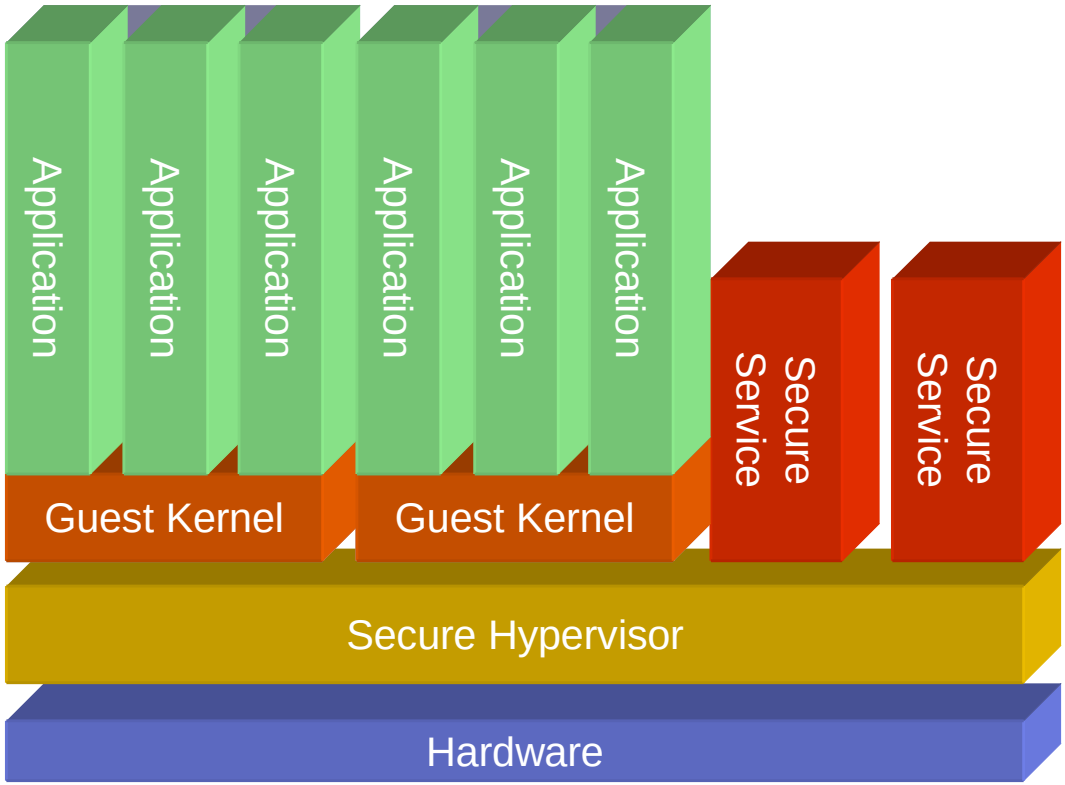
# Hypervisor Security Architecture complements OSes with strong isolation, controlled sharing, & verifiable / attestable environments





© 2007 IBM Corporation

# sHype Architecture Goals

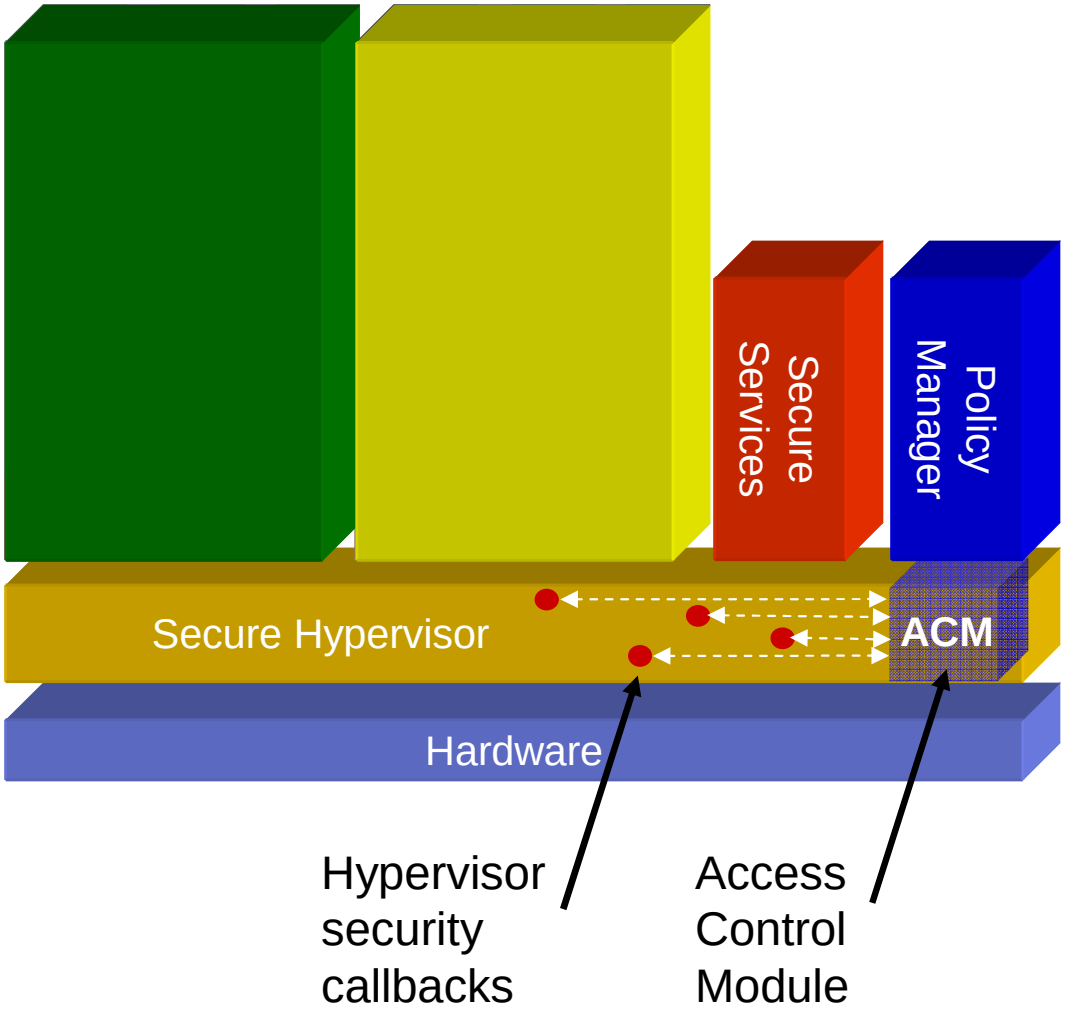



- Strong isolation guarantees between virtual machines
- Mediated resource sharing and communications
- Platform and virtual machine content integrity guarantees
- Platform and virtual machine content attestation
- Resource control and metering
- Secure services – e.g., audit, monitor, I/O, …


© 2007 IBM Corporation

# Access Control – *Mediation & Isolation*

- Flexible framework required
  - One access control policy does not fit all – e.g., Biba (Integrity), Bell-LaPadula (Confidentiality), Clark-Wilson, …
- Access Control Module (ACM)
  - May vary depending on policy requirements
- Core hypervisor instrumented with callbacks into ACM
  - Mediate all inter-virtual machine communication / resource sharing
  - Callback evaluation at resource binding time (low overhead)
- Implemented
  - Xen & PHYP





© 2007 IBM Corporation

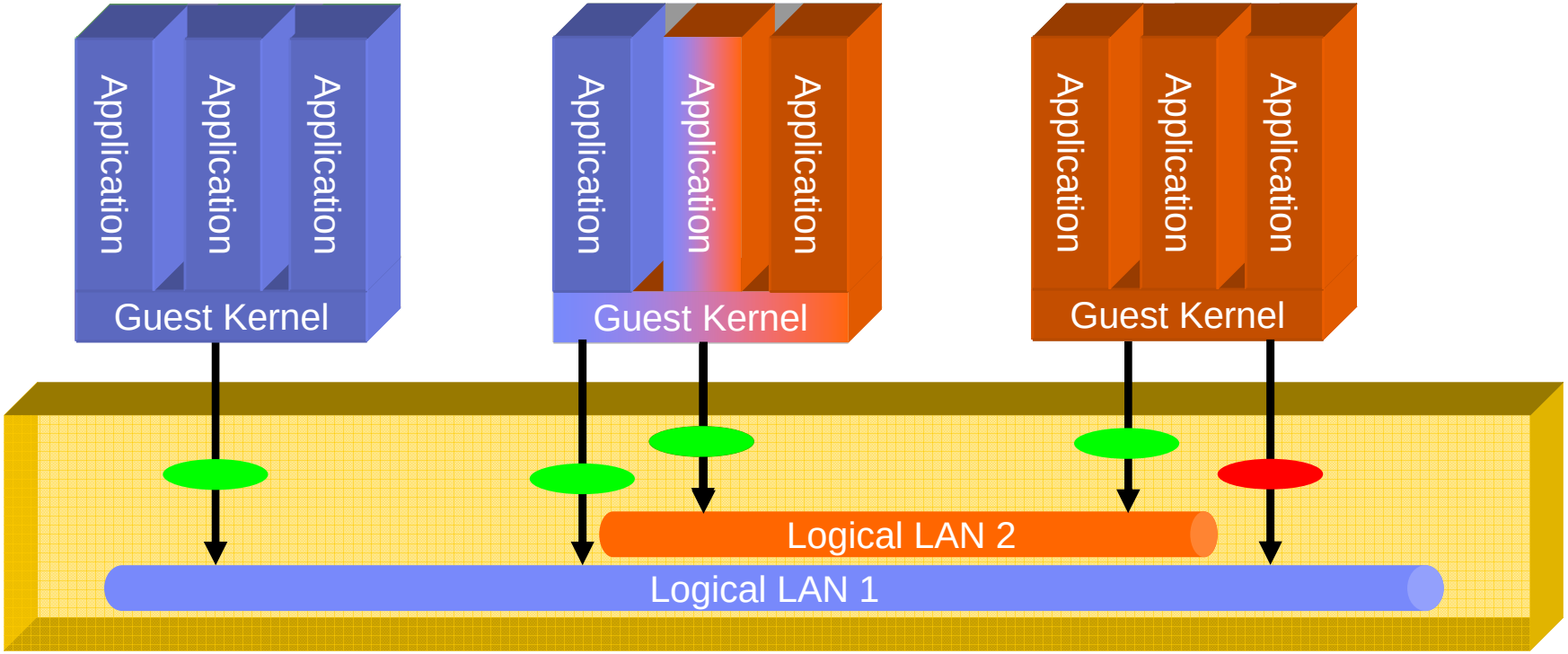
# Access Control Policies

- Policy-based information flow control for virtual machines (VMs)
  - *Mandatory* Access Control (MAC), enabled by defining security / confinement domains specific to VMs and their resources
- All resources conceptually assigned *colors* [Rushby81]
  - Exampe1: Red = IBM Accounting, Blue = IBM HR, Green = IBM Sales
  - Example2: Magenta = Avis, Gold = Hertz, Kelly = National
  - Virtual machines with like colors define *coalitions*
  - Only virtual machines belonging to the same coalition can share resources freely
- Exemplification policies
  - *Simple Type Enforcement*:
    enforces isolation of coalitions and sharing through multi-colored VMs
  - *Chinese Wall*:
    defines *conflict sets* – enforces that no conflicting VMs run at the same time on the same platform – e.g., {Hertz, Avis}


© 2007 IBM Corporation

# Multi-Level Secure Logical LAN

## Simple Type Enforcement example

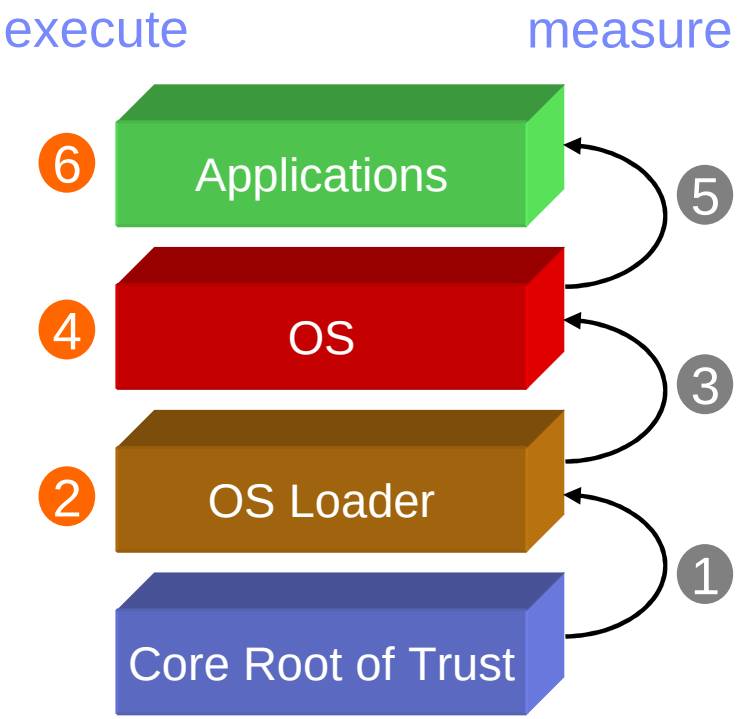



Security policy enforced at time of resource binding


© 2007 IBM Corporation

# Integrity Measurement – *Integrity & Attestation*

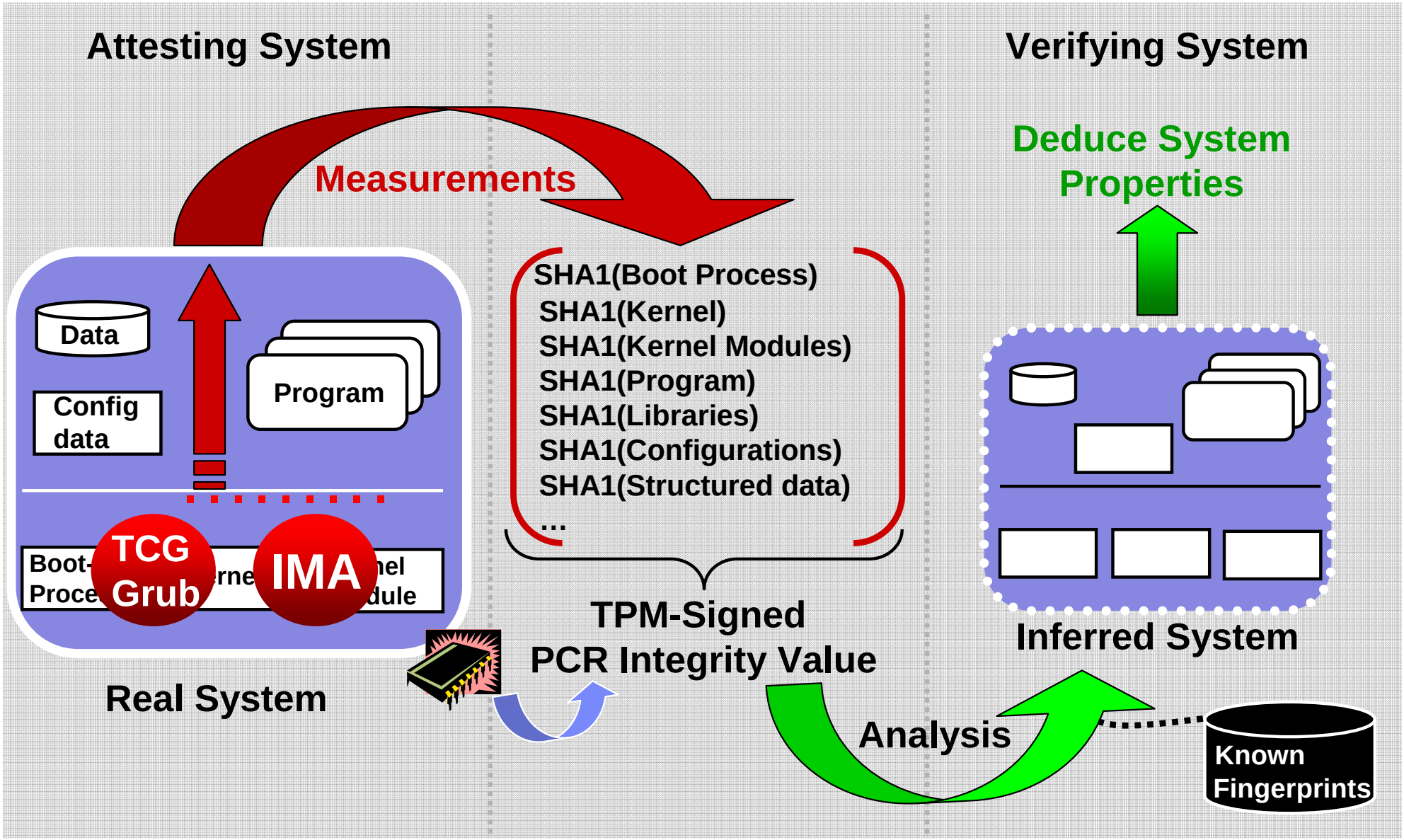
- Provide runtime integrity guarantees upon which to base trust
  - Certificates provide static endpoint identity only (and secure communications SSL / IPSec)
  - Does the system currently satisfy security-related requirements / SLAs?
- Leverage Trusted Platform Module (TPM) / Core Root of Trust for Measurement
  - Remotely attest system configuration (software-stack measurement)
  - Detect cheating / compromise (load guarantees)
  - Protect sensitive data (binding data)
  - Non-intrusive / negligible overhead
- Implemented for Linux in 2004





© 2007 IBM Corporation

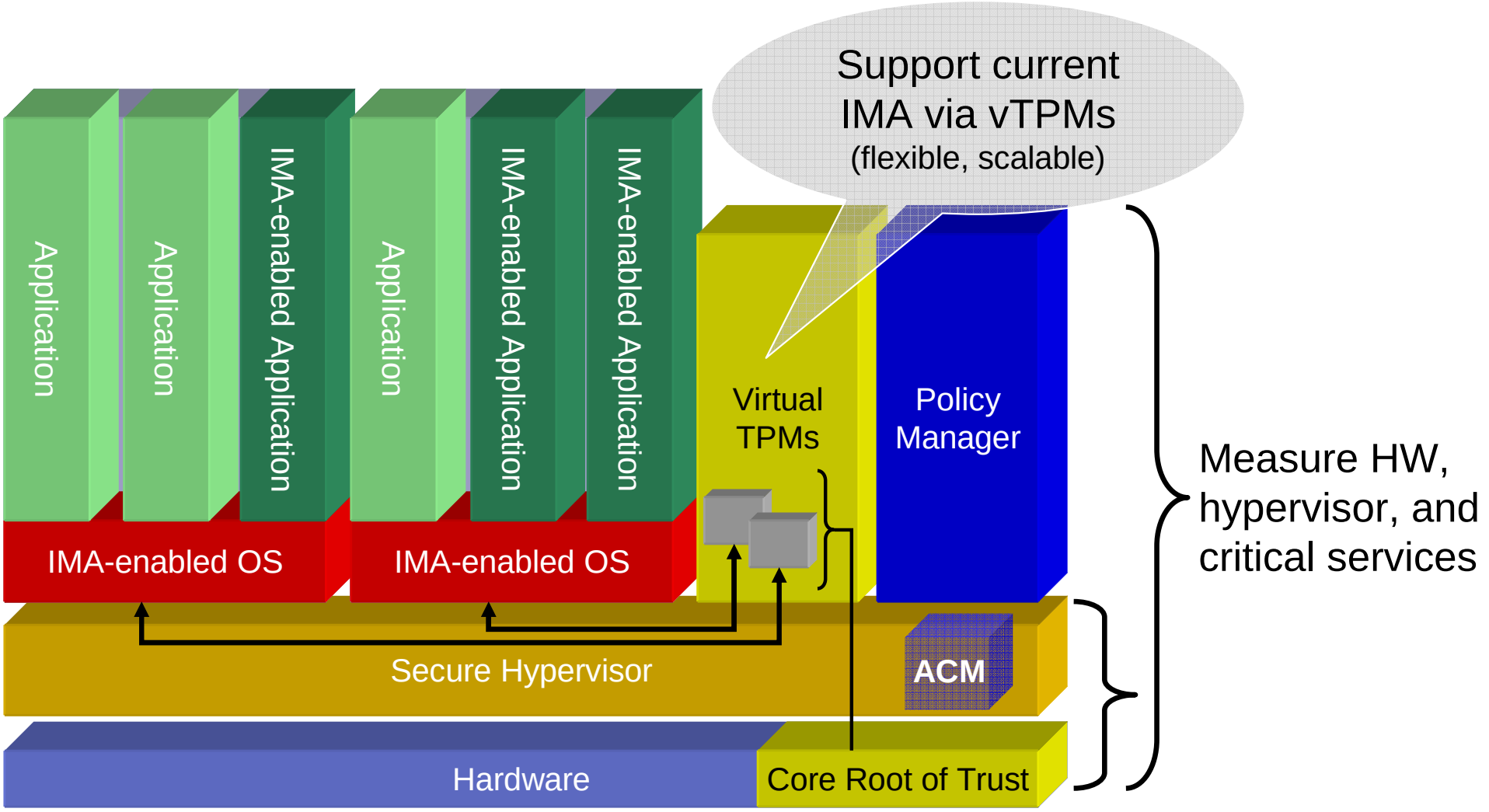
# Integrity Measurement Architecture (IMA)






© 2007 IBM Corporation

# Extending Integrity Measurement in sHype



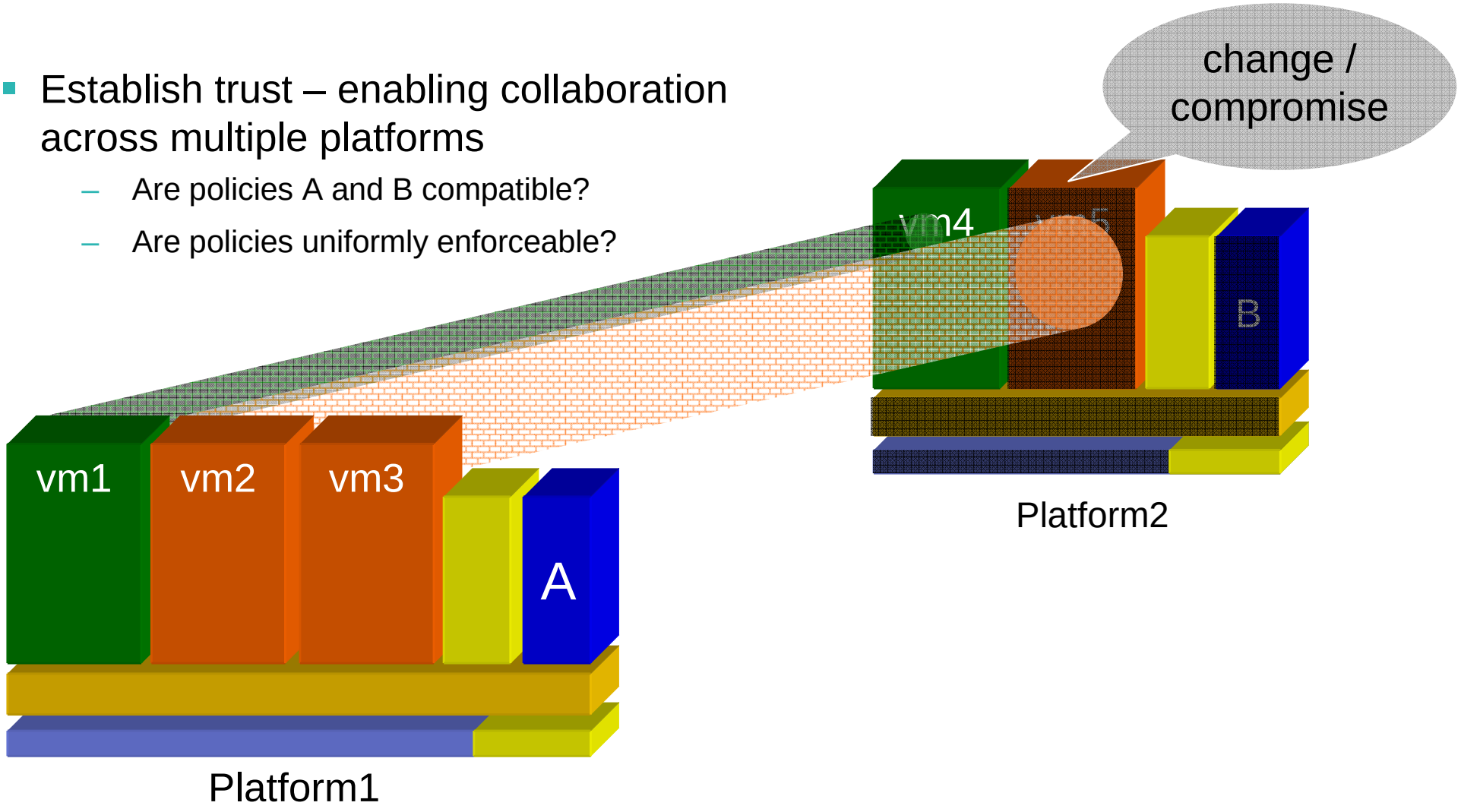


© 2007 IBM Corporation

# Distributed Trusted Computing Base

## Putting Access Control and Integrity Measurement together

- Establish trust – enabling collaboration across multiple platforms
  - Are policies A and B compatible?
  - Are policies uniformly enforceable?

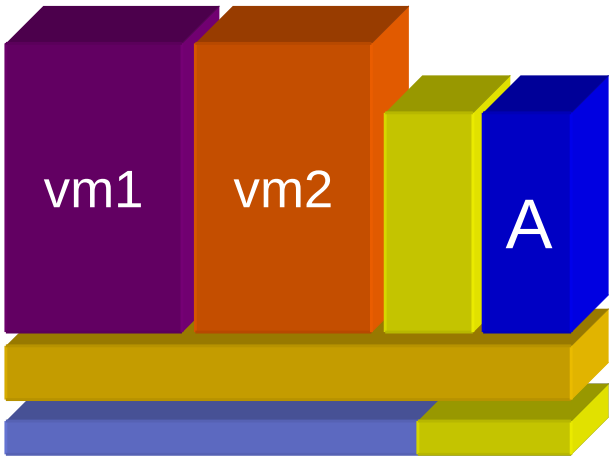




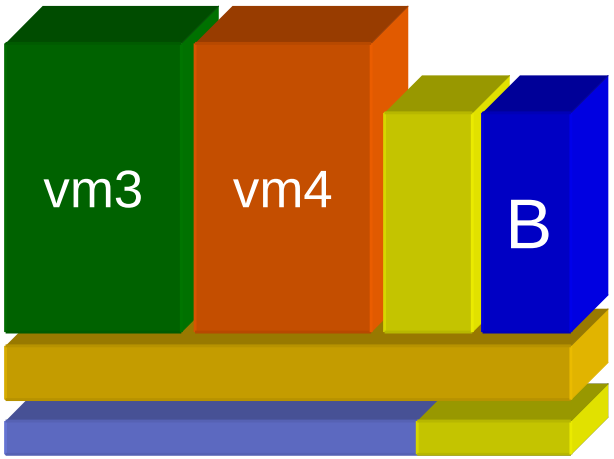
© 2007 IBM Corporation

# Remaining Design / Implementation Challenges

- Efficient mutual verification of remote system integrity
  - coalitions, policies, hypervisor, and HW
- Runtime detection of changes / compromises
- Support for workload save / restore / migration
  - changes to the trust chain, don't want to remeasure running programs




Platform1




Platform2

© 2007 IBM Corporation

# Virtualization isn't all positive for security

- Virtual Machine images handled with the ease of files
  - Create, copy, save, read and modify, share, migrate, rollback
- Virtual Machine images proliferate and become more transient
  - Because it's easy, everyone will do it
  - May appear and/or disappear sporadically
- Problems for security
  - Management complexity due to explosive growth in number of virtual machines
  - Exposure of sensitive data in stored images
  - Cryptographic and other protocols which rely on freshness or randomness
  - Reactivate previously patched vulnerabilities via rollback capability


© 2007 IBM Corporation

# Trusted Virtual Domains

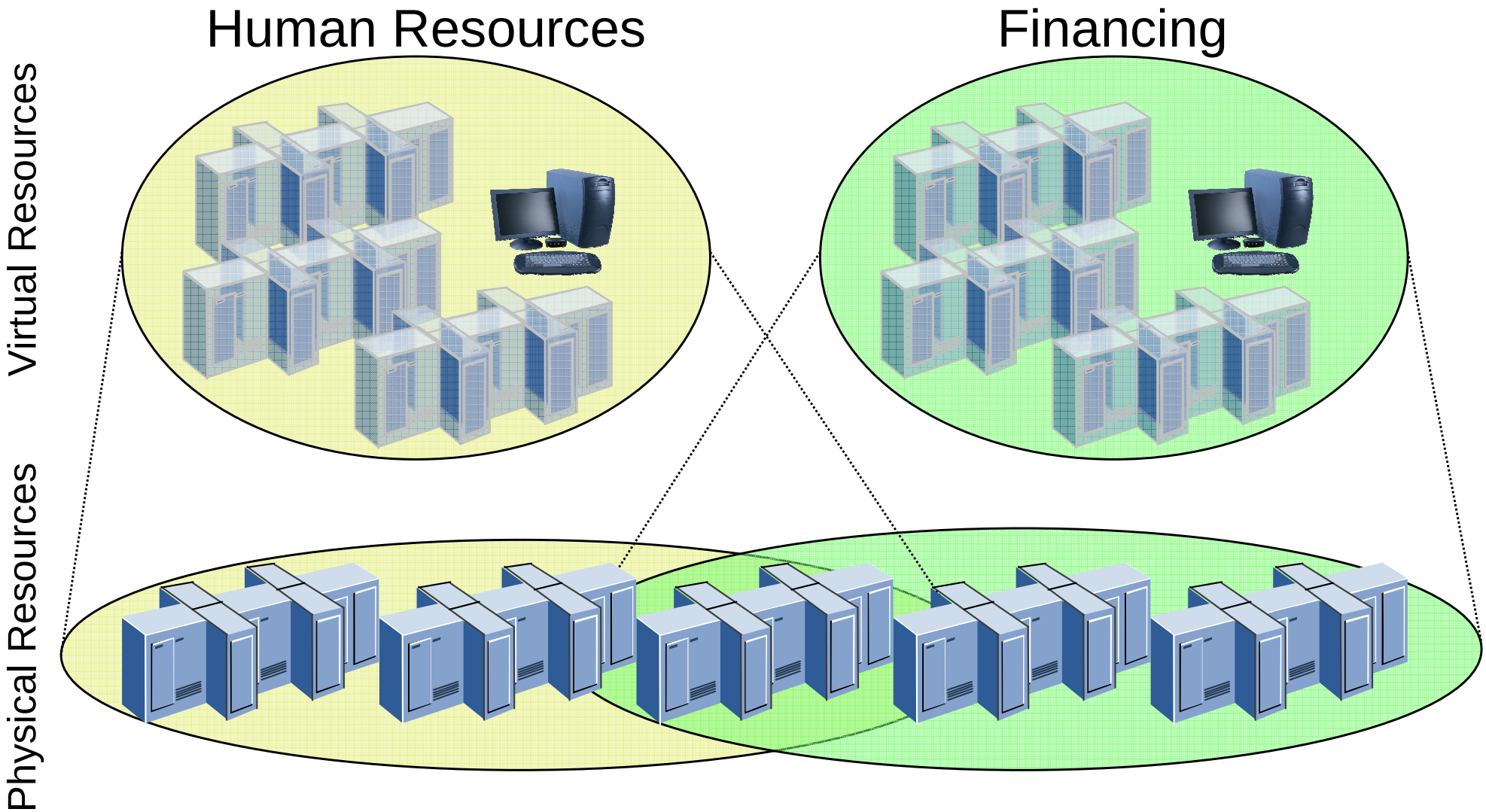
- Operational risk dramatically rising
  - Increase in threats, vulnerabilities being exploited faster, management cost / complexity of current approach unsustainable
- Managing compliance risk
  - HIPAA, SOX, EU AP & US privacy regulations…
- Risk is multiplied by increase of heterogeneous interconnected systems and sharing of resources on a global scale

Thesis:

- A fundamentally new approach is needed
  - Dynamically establish trust in relationships and guarantee protection of sensitive data in a shared business environment


© 2007 IBM Corporation

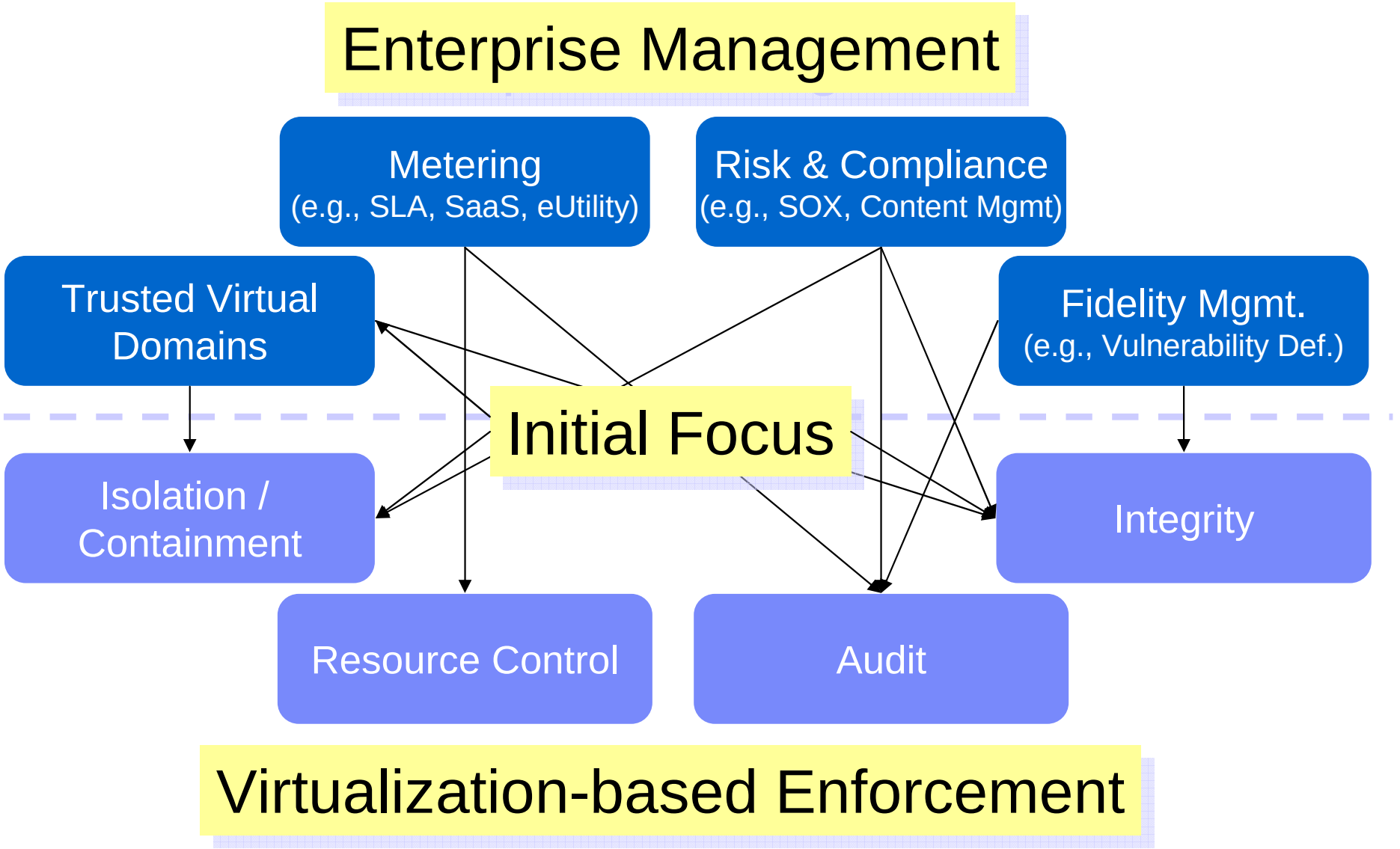
# Trusted Virtual Data Center (TVDc) Overview





© 2007 IBM Corporation

# Management and Enforcement Capability Areas

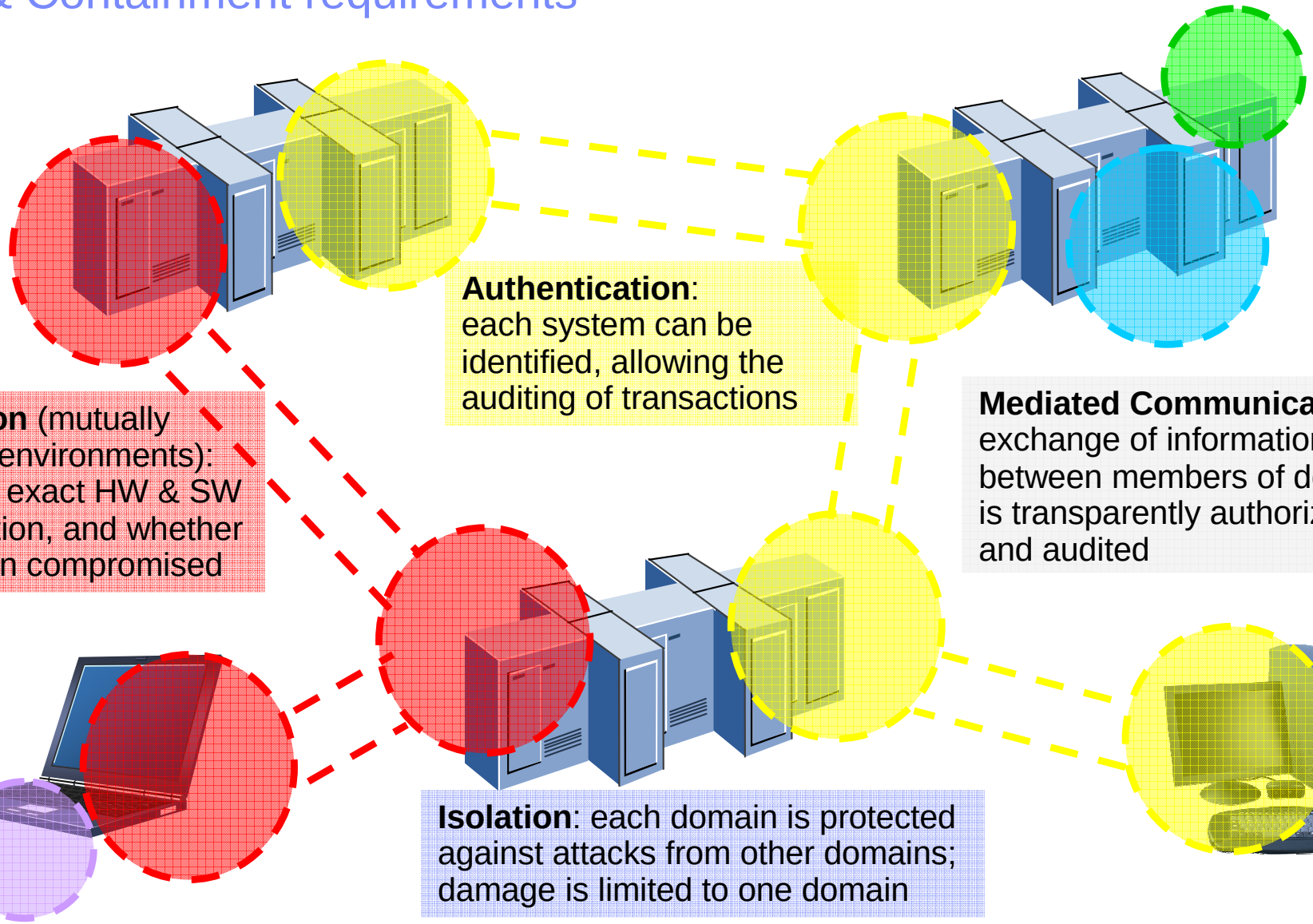




© 2007 IBM Corporation

# Trusted Virtual Domains (TVD)

## Trust & Containment requirements



**Authentication**: each system can be identified, allowing the auditing of transactions

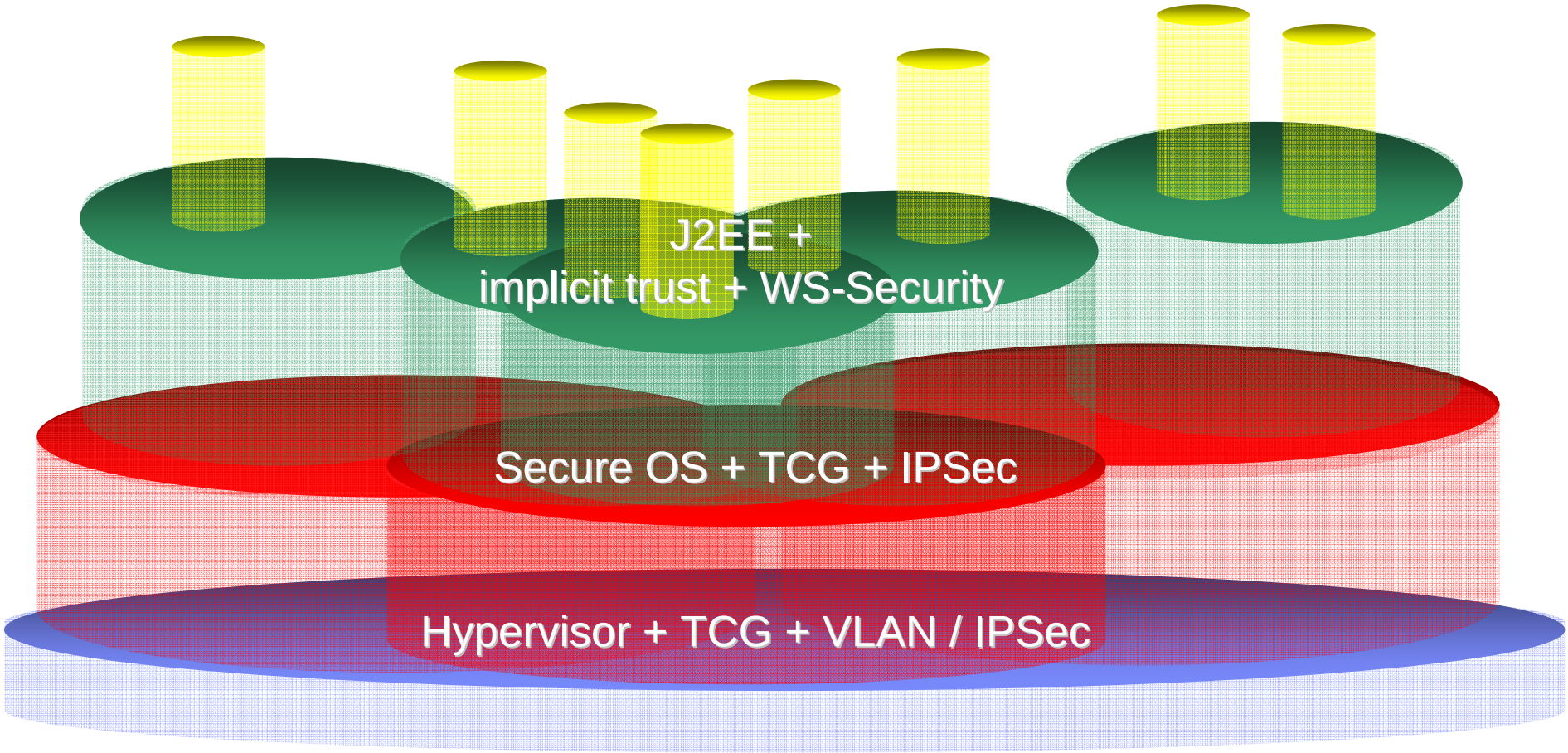
**Attestation** (mutually verifiable environments): can verify exact HW & SW configuration, and whether it has been compromised

**Mediated Communications**: exchange of information between members of domains is transparently authorized and audited

**Isolation**: each domain is protected against attacks from other domains; damage is limited to one domain


© 2007 IBM Corporation

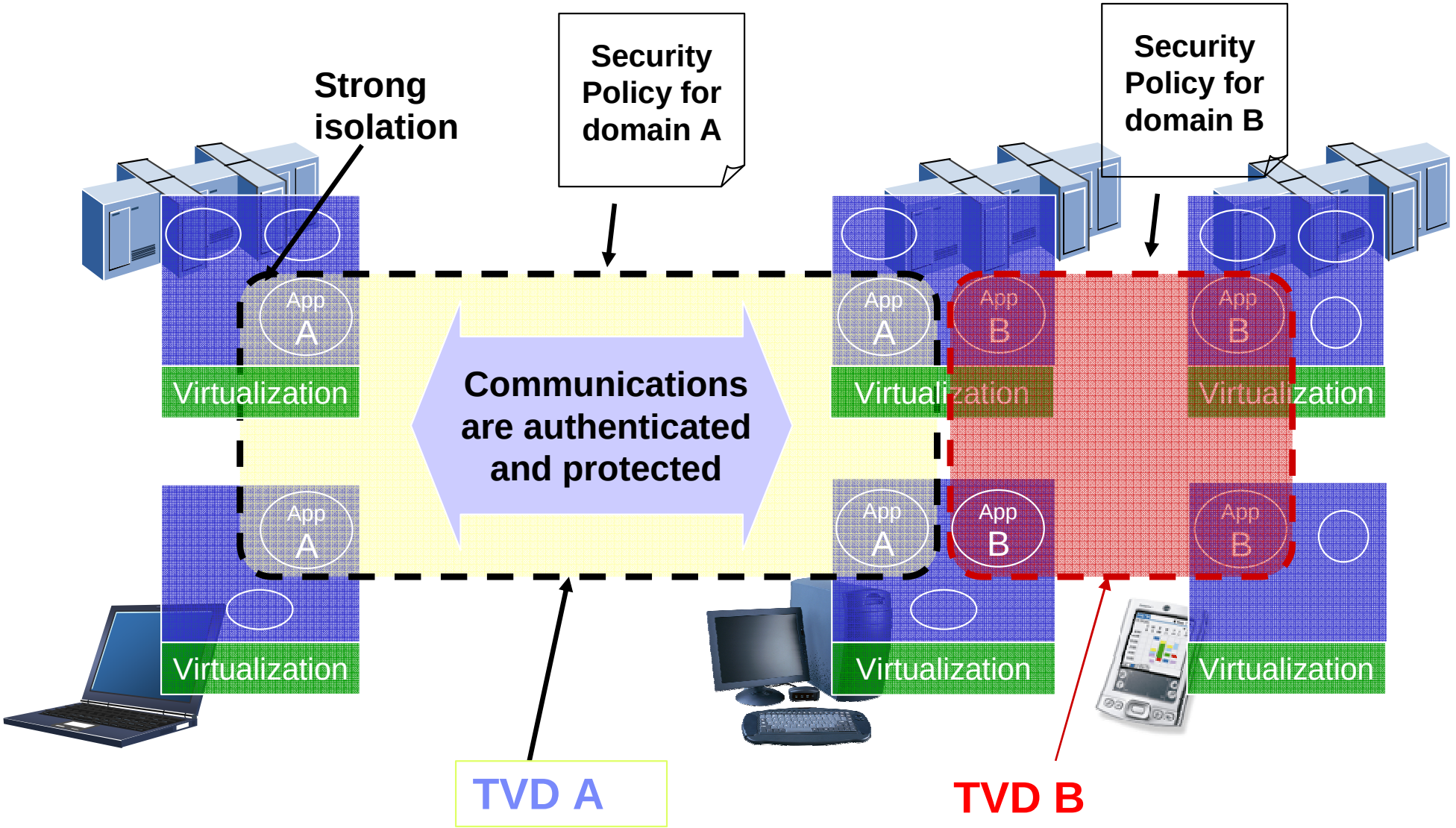
# Realizing TVDs with Multiple Technologies





© 2007 IBM Corporation

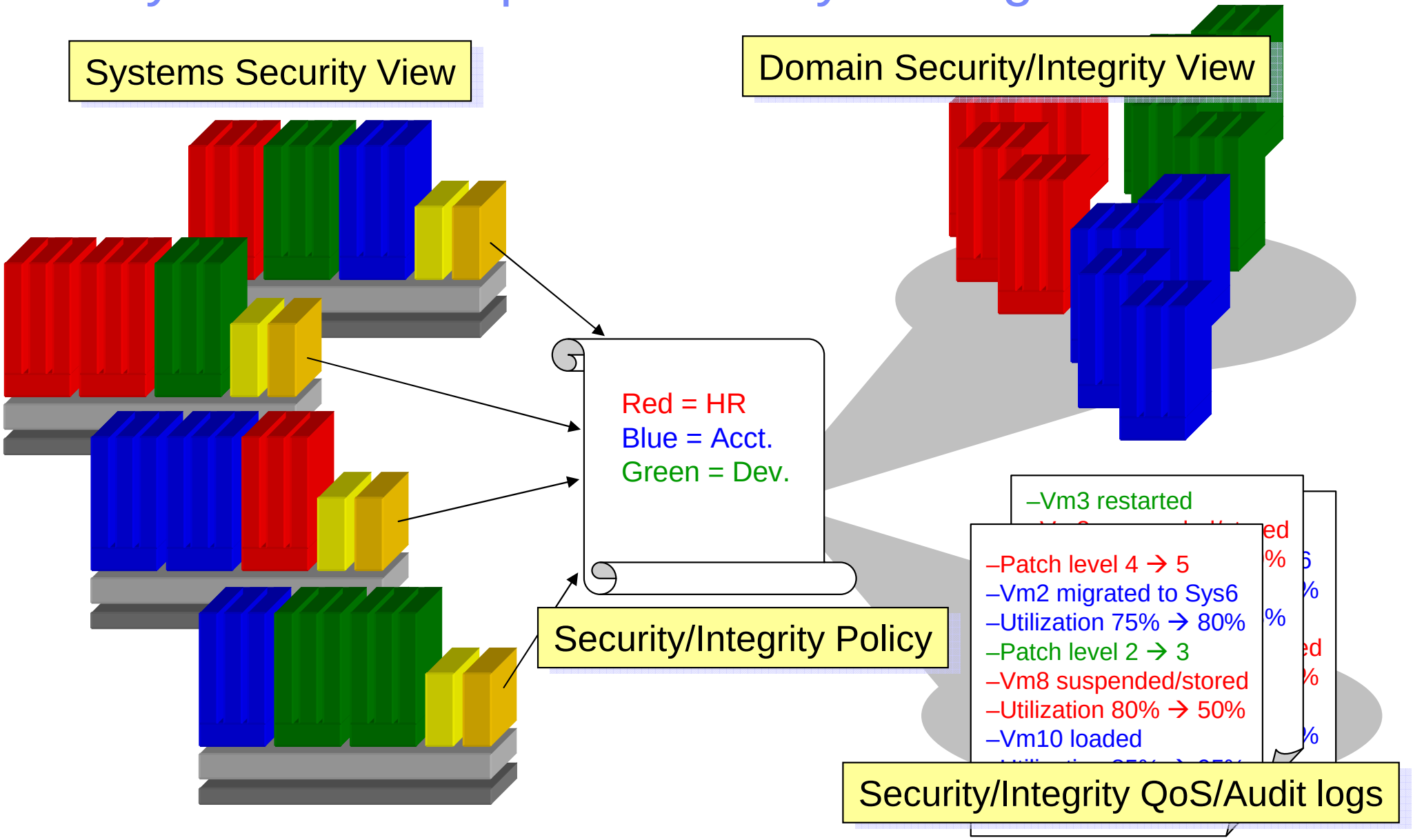
# Overlay of Trust Domains on to Multiple Platforms





© 2007 IBM Corporation

# Policy-driven Enterprise Security Management

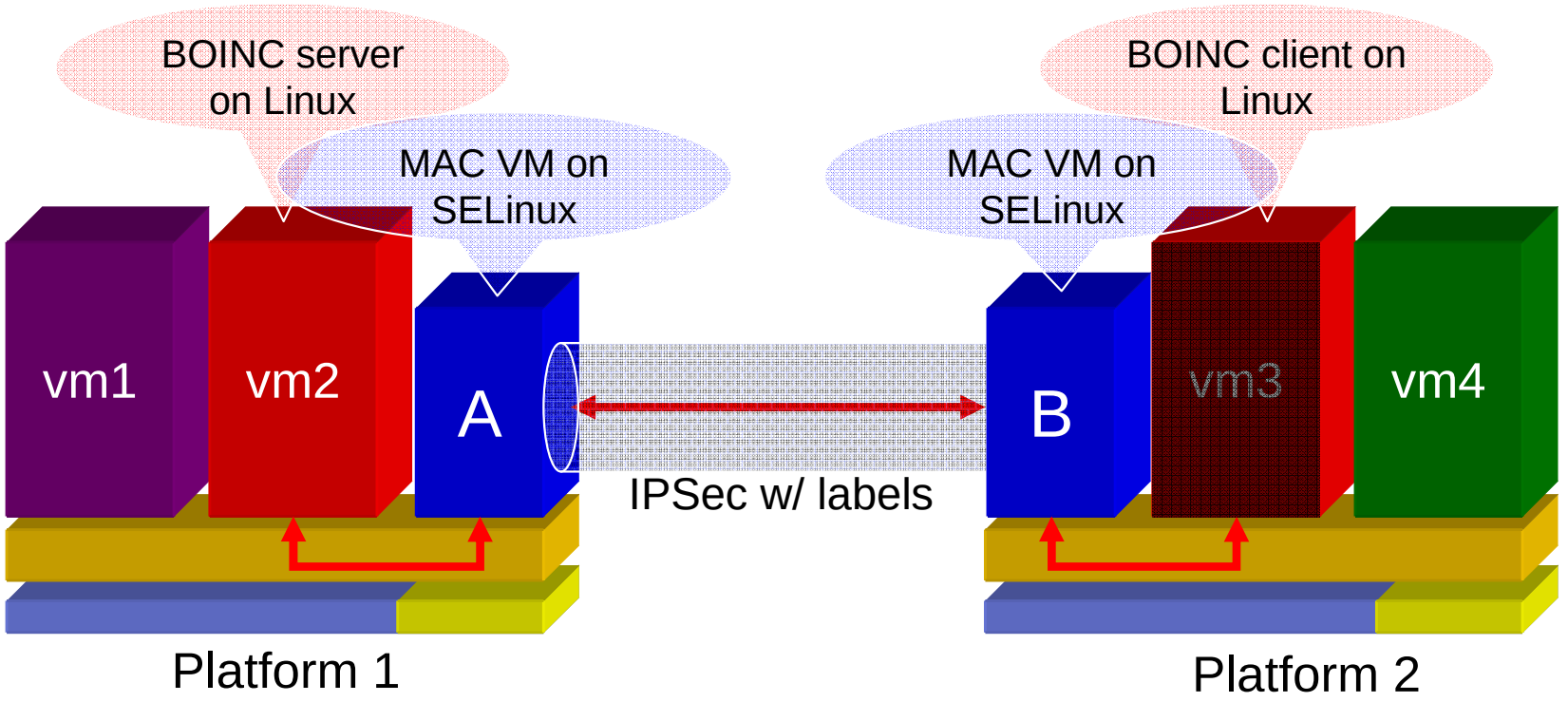




© 2007 IBM Corporation

# Prototype TVD Implementation

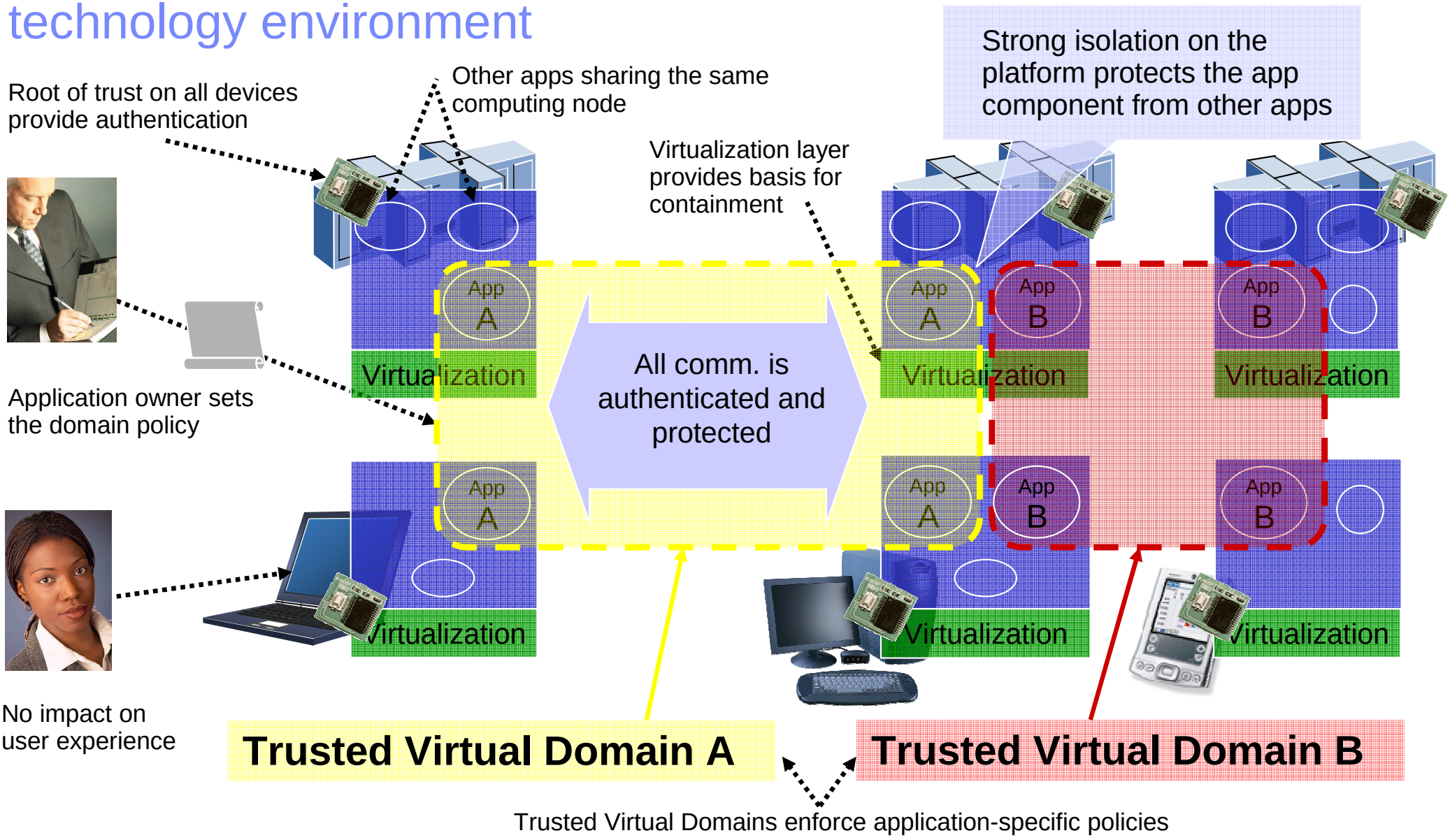
- Application Scenario:
  - Berkeley Open Infrastructure for Network Computing (BOINC)
  - Widely used for SETI@home, IBM's World Community Grid and many other distributed computation projects
  - Unaware of security constraints in our configuration





© 2007 IBM Corporation

# Vision: Dynamically establish trust relationships with strong security guarantees in a shared business information technology environment





© 2007 IBM Corporation

# Summary

- Current and future challenges will not be met with existing solutions and approaches alone
- A fundamentally new approach is required
  - Dynamic trust establishment and strong containment guarantees
- Trusted Virtual Domains promise …
  - Satisfy on demand requirements and radically simplify IT security management
  - Significant challenges / risk / opportunity
    - Theory, scalability, composition / decomposition of policies
    - Broad IBM Research-wide effort
- sHype Hypervisor Security Architecture
  - A logical first step for foundational security and distributed Trusted Computing Base
  - Significant progress on Access Control framework and on extending the Integrity Measurement Architecture

http://www.research.ibm.com/secure_systems_department


© 2007 IBM Corporation

Thank you for your audience!

*Thomas Rueter*
*trueter@de.ibm.com*

© 2007 IBM Corporation