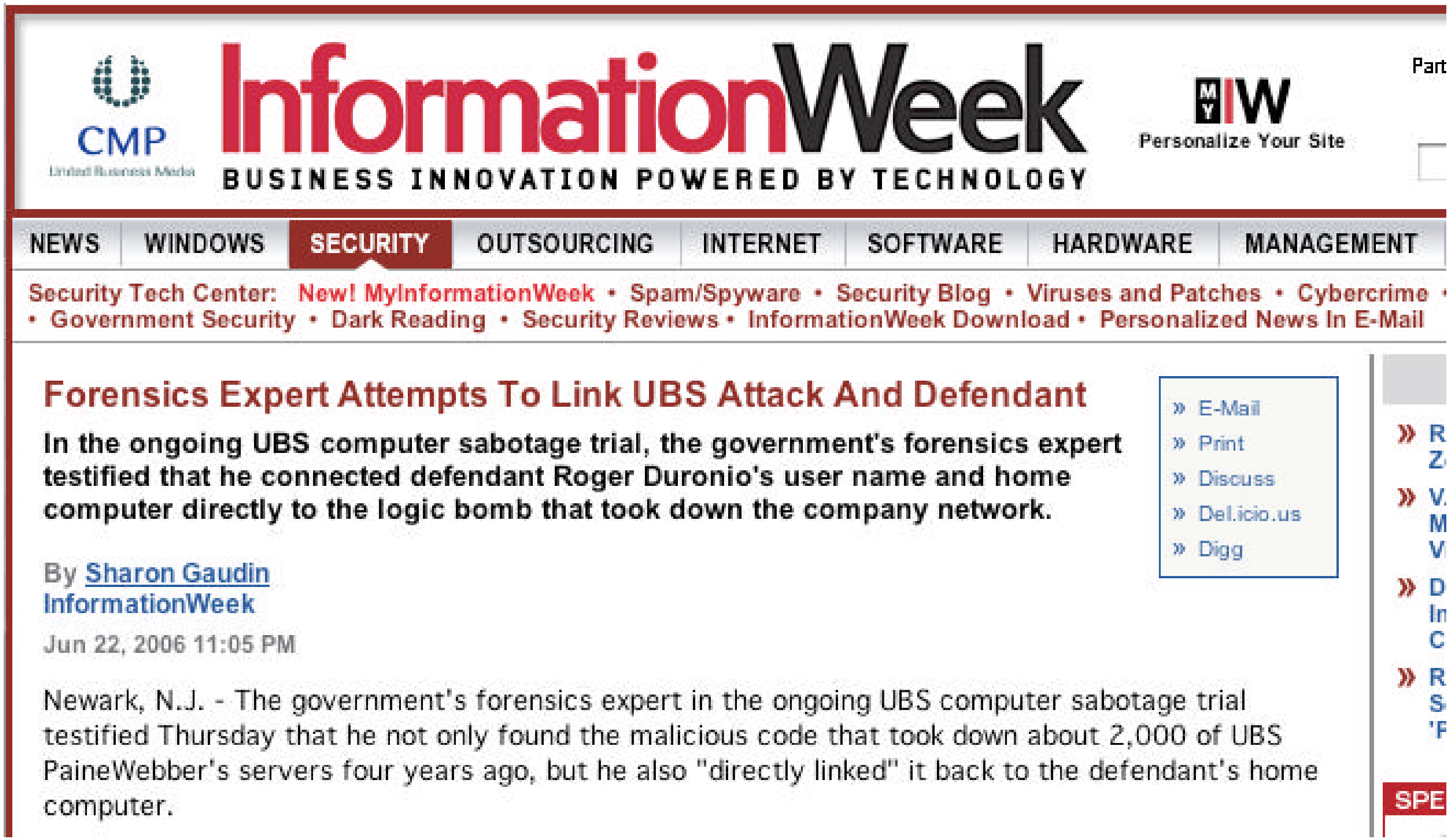
Critical Infrastructure Protection

Security in an HPC-Environment

Peter Streibelt

caster@skarabaeus.de

Critical Infrastructure Protection


CMP
United Business Media
InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY
MYIW
Personalize Your Site
Part
NEWS
WINDOWS
SECURITY
OUTSOURCING
INTERNET
SOFTWARE
HARDWARE
MANAGEMENT
Security Tech Center: New! MyInformationWeek • Spam/Spyware • Security Blog • Viruses and Patches • Cybercrime • Government Security • Dark Reading • Security Reviews • InformationWeek Download • Personalized News In E-Mail
» E-Mail
» Print
» Discuss
» Del.icio.us
» Digg
SPE

Forensics Expert Attempts To Link UBS Attack And Defendant

In the ongoing UBS computer sabotage trial, the government's forensics expert testified that he connected defendant Roger Duronio's user name and home computer directly to the logic bomb that took down the company network.

By Sharon Gaudin
InformationWeek

Jun 22, 2006 11:05 PM

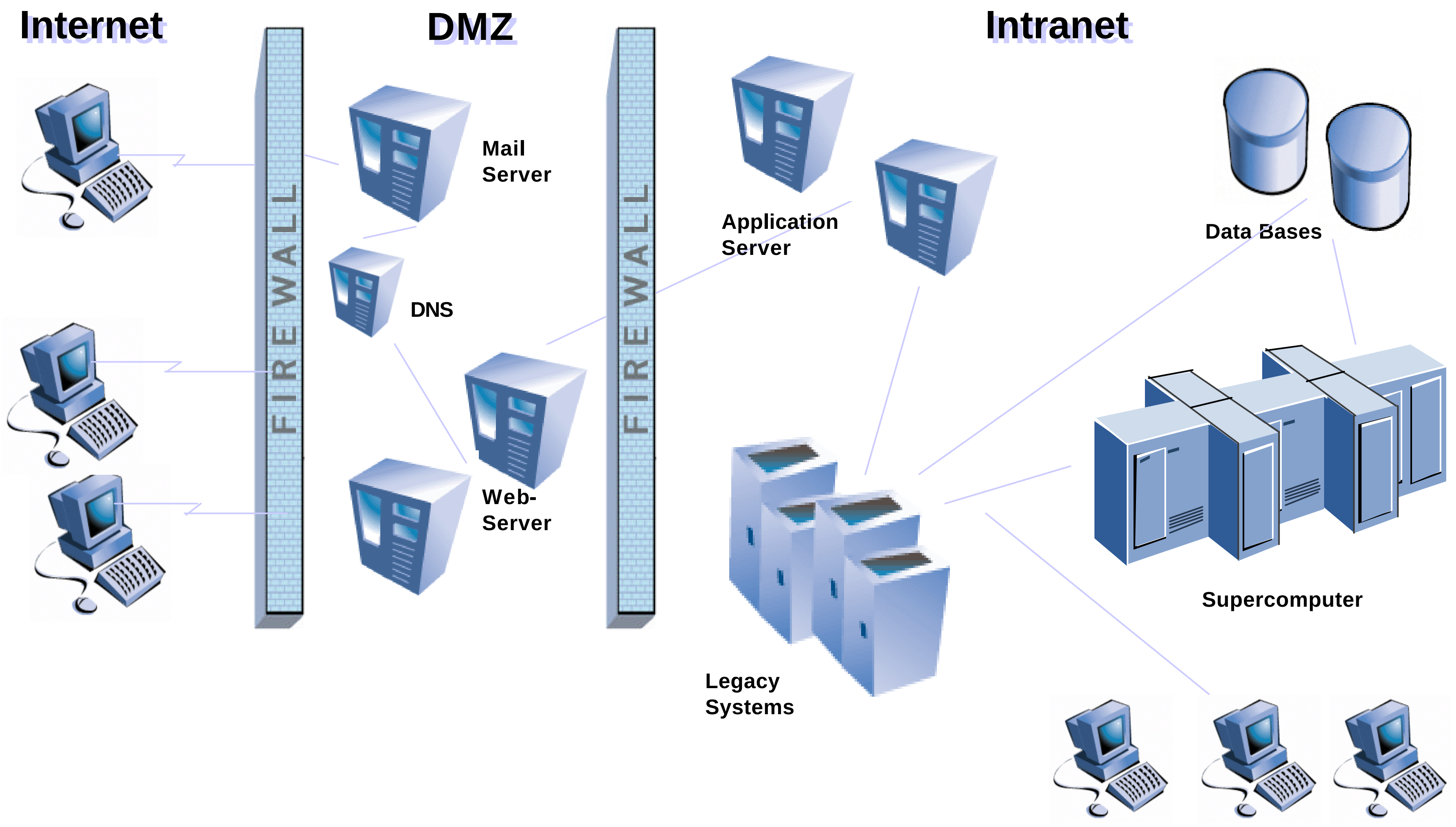
Newark, N.J. - The government's forensics expert in the ongoing UBS computer sabotage trial testified Thursday that he not only found the malicious code that took down about 2,000 of UBS PaineWebber's servers four years ago, but he also "directly linked" it back to the defendant's home computer.

http://www.informationweek.com/showArticle.jhtml?articleID=189600779

Intentional Security Threats

- Malware
  - Viruses
  - Worms
  - Trojans
  - Spyware
- Insider
  - Disgruntled worker
  - Bored or inquisitive operator
- Hacker
- Terrorist

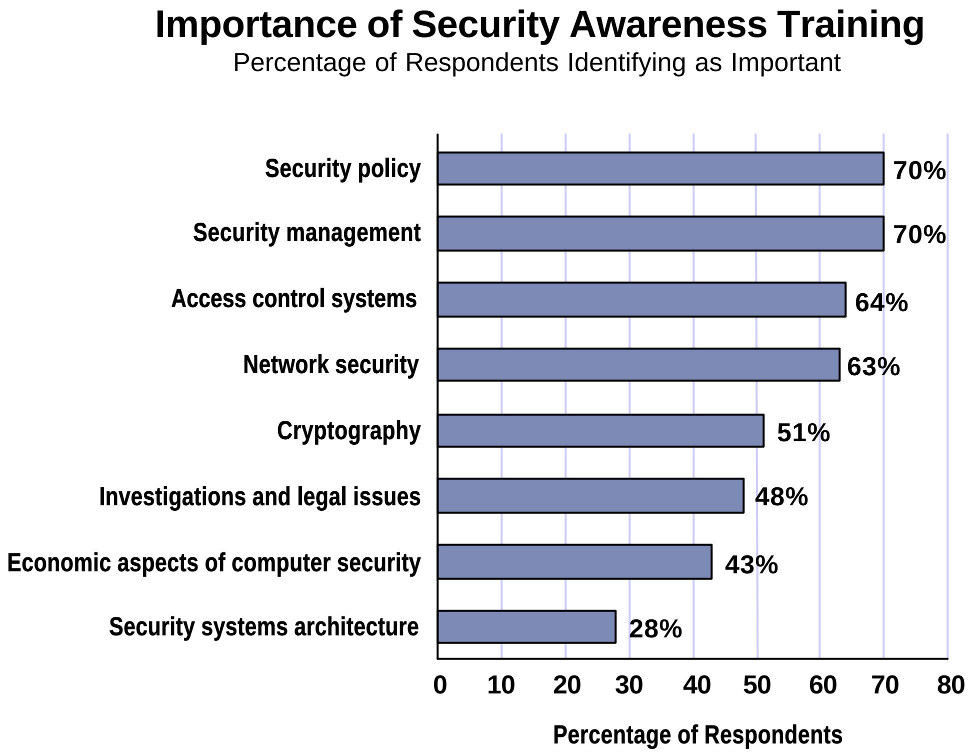
A typical Networking Infrastructure



Difficulties and Problems

- Massive inflow of vulnerabilities
  - Time to exploitation is shrinking
  - Increasing sophistication of attacks vs. automation of malware
- Poorly designed software
  - Poor engineering
  - Poor usability
- Minimal outflow
  - Well-known vulnerabilities do not get fixed
- Complexity of security management
  - Complex set-up and administration
  - Standard passwords and settings/profiles not changed
  - Social security attacks
- Operating systems (OS), routers, application monocultures
  - Write once, attack everywhere

Security is on almost everyone's agenda

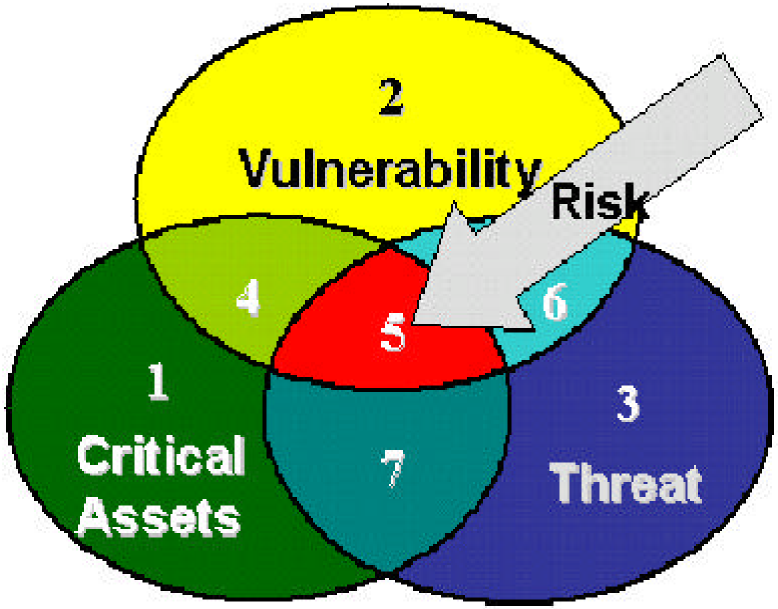


Source: 2005 CSI/FBI Computer Crime and Security Survey, Computer Security Institute

2005: 694 Respondents

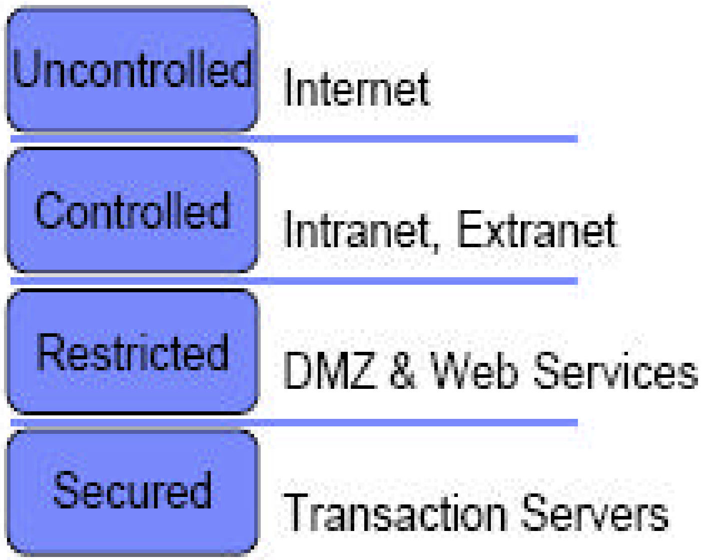
- In a recent CSI/FBI study, 87 percent of organizations surveyed reported that they conduct security audits.
- "Vast majority" of these organizations view security training as important.
- Most believe that their companies don't make security enough of a priority.

Risk Determination

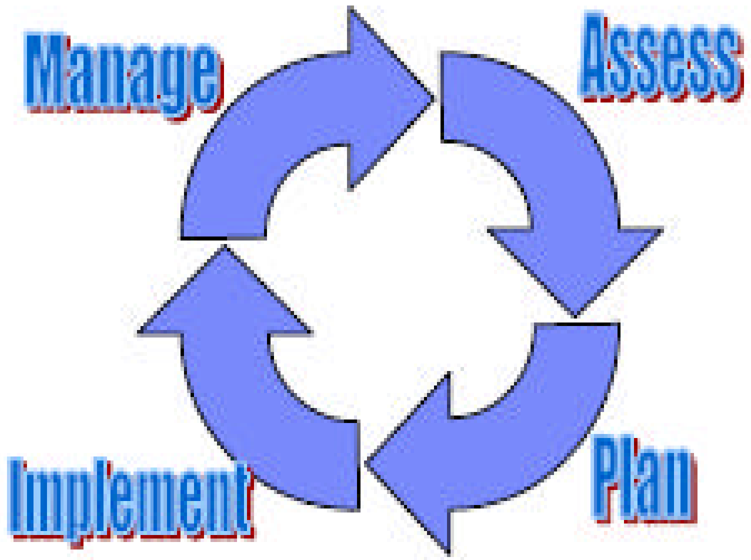


1 - Critical Assets without known vulnerabilities and known threats
2 - Vulnerabilities without known threats and no harm to critical assets
3 - Threats without known vulnerabilities and no harm to critical assets
4 - Critical assets with known vulnerabilities, but no known threats
5 - Critical assets with known vulnerabilities and known threats
6 - Threats which require in depth knowledge to be exploited, but don’t harm critical assets
7 - Critical assets without vulnerabilities, but known threats

Defense in Depth



Uncontrolled	Internet
Controlled	Intranet, Extranet
Restricted	DMZ & Web Services
Secured	Transaction Servers



Manage

Assess

Implement

Plan

On-going Defense in Depth

Understand Risks
Identify Assets
Set Requirements for Data and Assets
Identify Owners

Plan

- Policy and Standards Definition
- Enterprise Architecture
- Internet Architecture
- Secure Solution Design
- Process Design
- Privacy Strategy and Implementation

Select Technology
Set Management Process

Implement

- Product Selection
- Product Implementation
- Vault Registry Services

Educate Users
Operate Secure Infrastructure
Set Procedures to minimize Risks

Manage

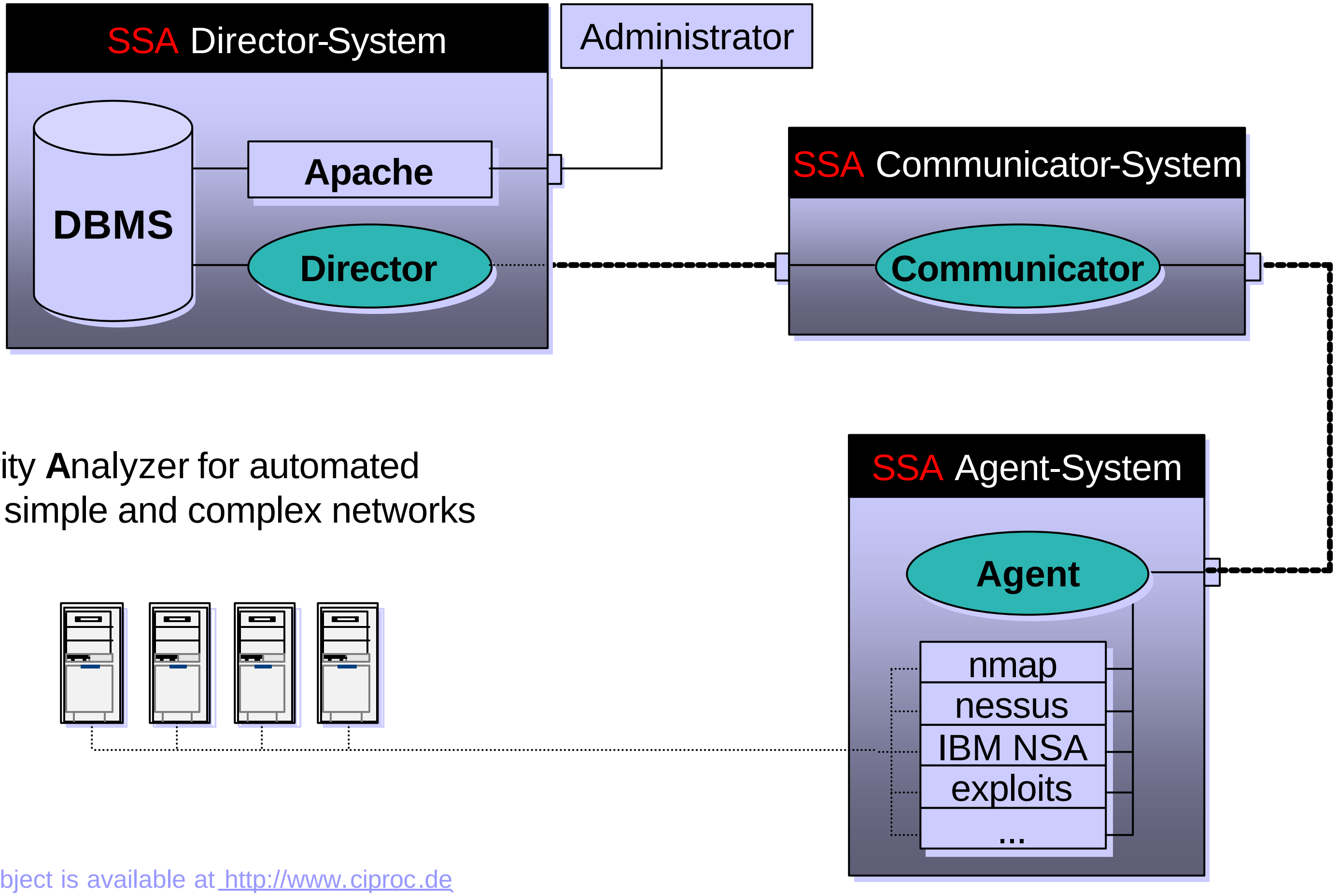
- Firewall Operations
- Logfile Analysis
- Intrusion Detection
- Disaster Recovery
- Compliance
- Change Management

Self-assessments
Internal Audits
External Audits

Assess

- Health-Check
- Ethical Hacking
- Security Policy
- Networking Assessment
    - ✓ Site
    - ✓ Process
    - ✓ Application
    - ✓ System
    - ✓ Network
    - ✓ Internet

Supporting Technology - Penetration Tools

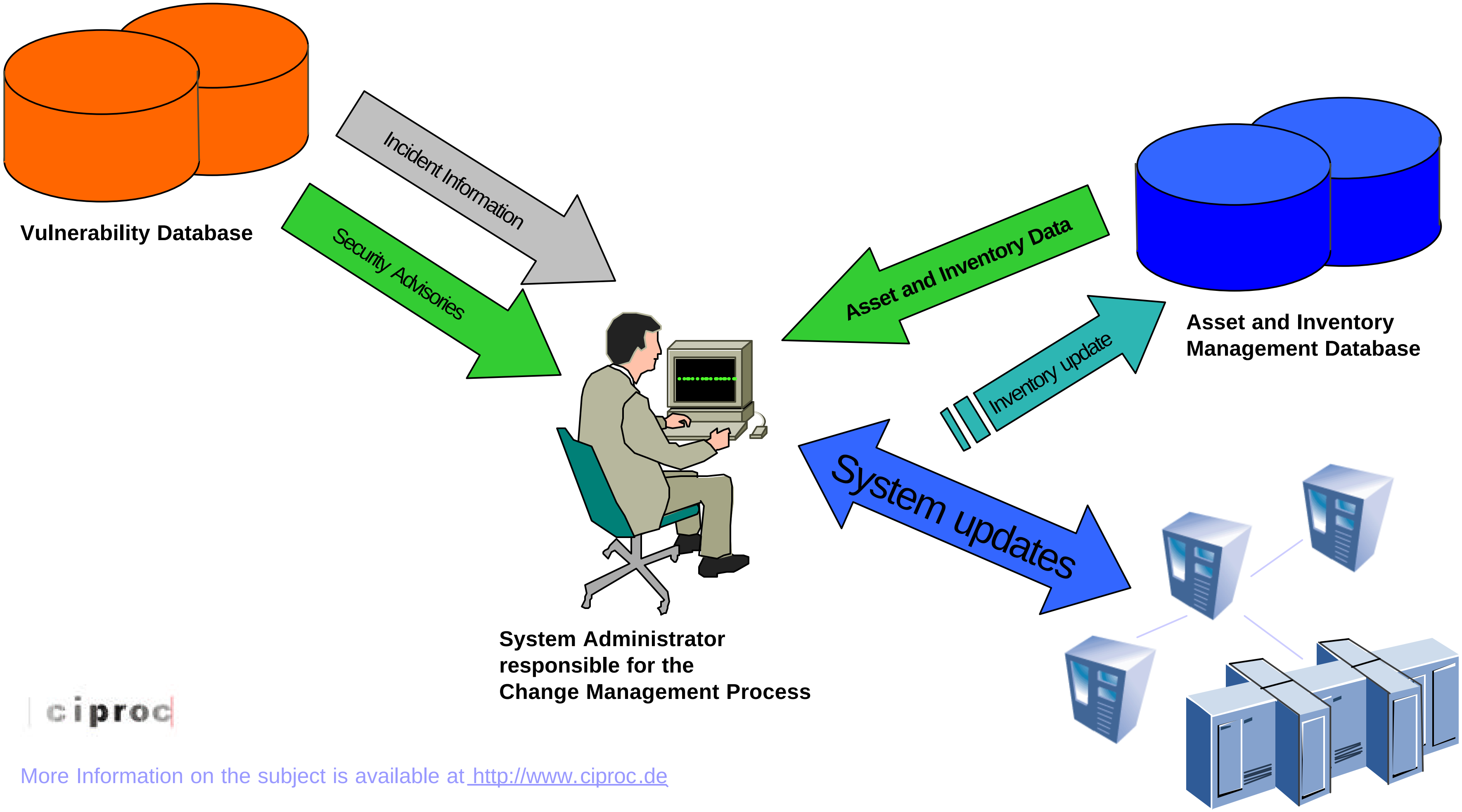


Skarab@eus **S**ecurity **A**nalyzer for automated penetration-tests of simple and complex networks

ciproc

More Information on the subject is available at http://www.ciproc.de

Supporting Technology - Customized Vulnerability Management System



Vulnerability Database

Asset and Inventory
Management Database

System Administrator
responsible for the
Change Management Process

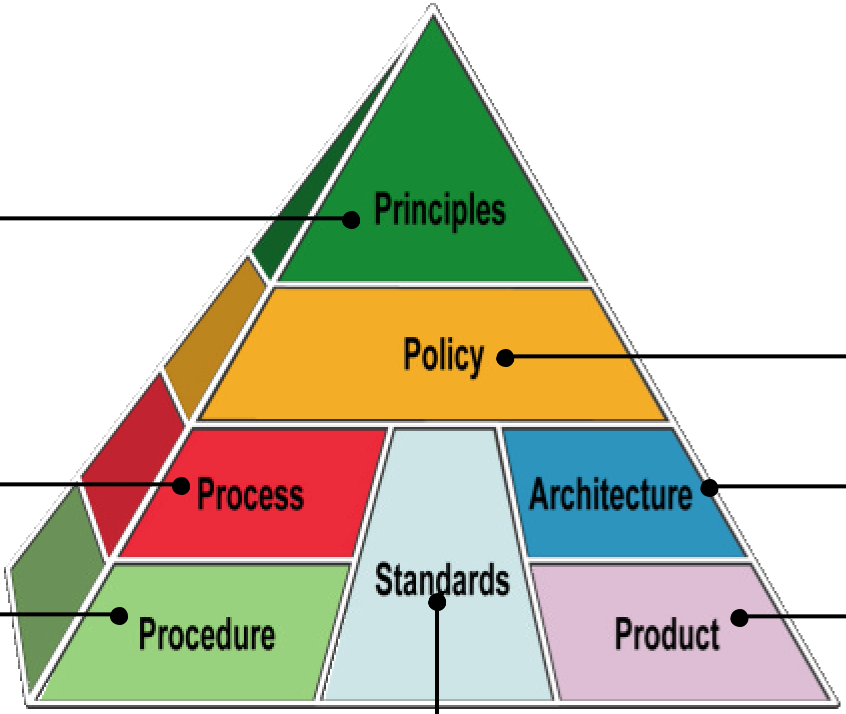
ciproc

More Information on the subject is available at http://www.ciproc.de

Security Themes

- Governance
- Privacy
- Threat mitigation
- Transaction and data integrity
- Identity and access management
- Application security
- Physical security
- Personnel security

IBM Enterprise Security Model



Security principles:
Value statements that the business requires for the delivery of security (including trust model, asset profile)

Security processes:
Activities typically performed across multiple organizations to implement company policies and standards

Security procedures:
Specific operational steps that individuals must take to achieve goals, which are often stated in policies

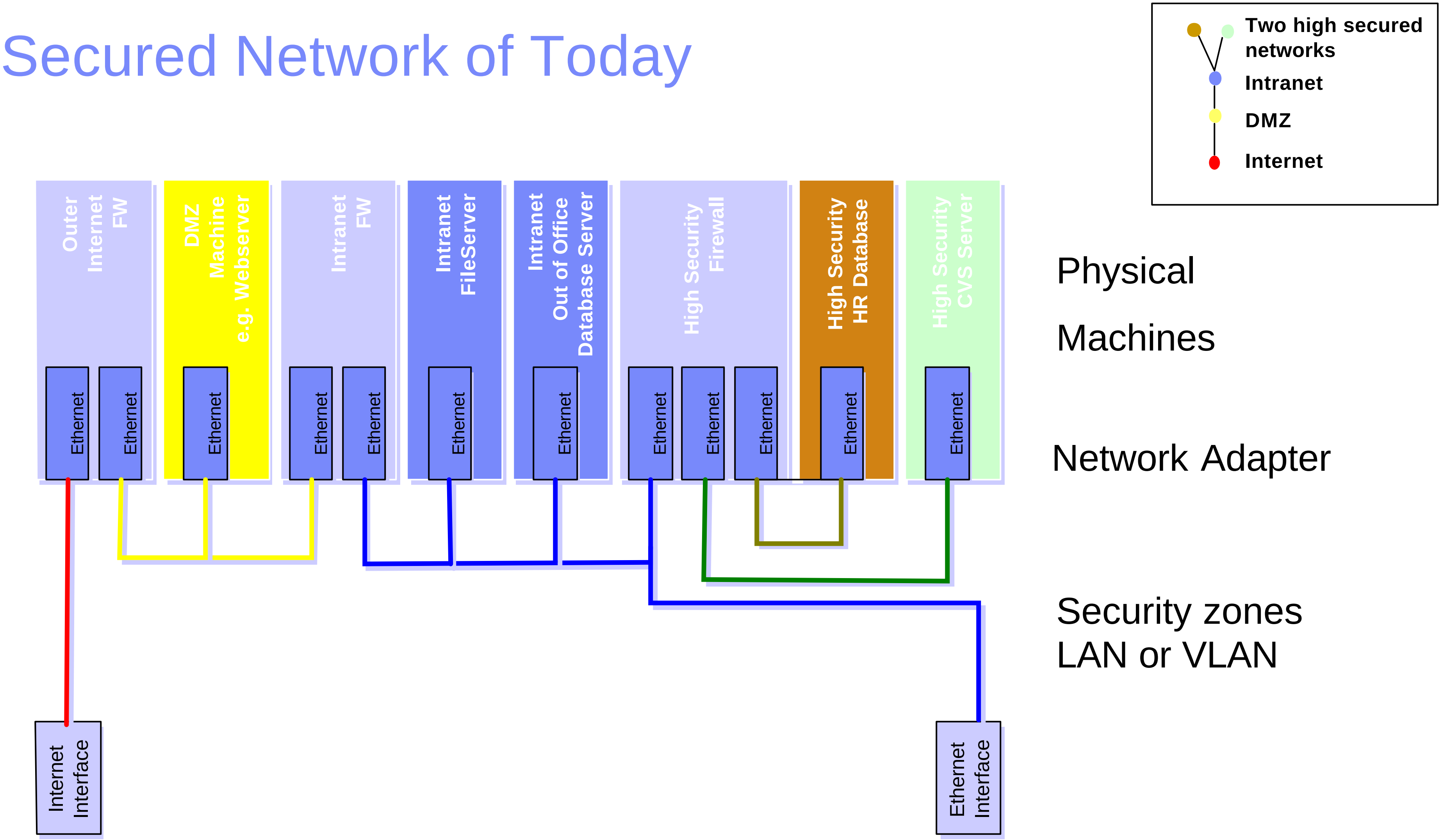
Security policy:
The security rules that must be followed (including risk management, threat/risk analysis)

Security architecture:
Details how all the technologies fit together (including trust model, asset profile)

Security products:
Specific products and tools offered by the security organization

Security standards:
Set of rules for implementation policy; standards make specific mention of technologies, methodologies, implementation procedures and other details factors

Secured Network of Today

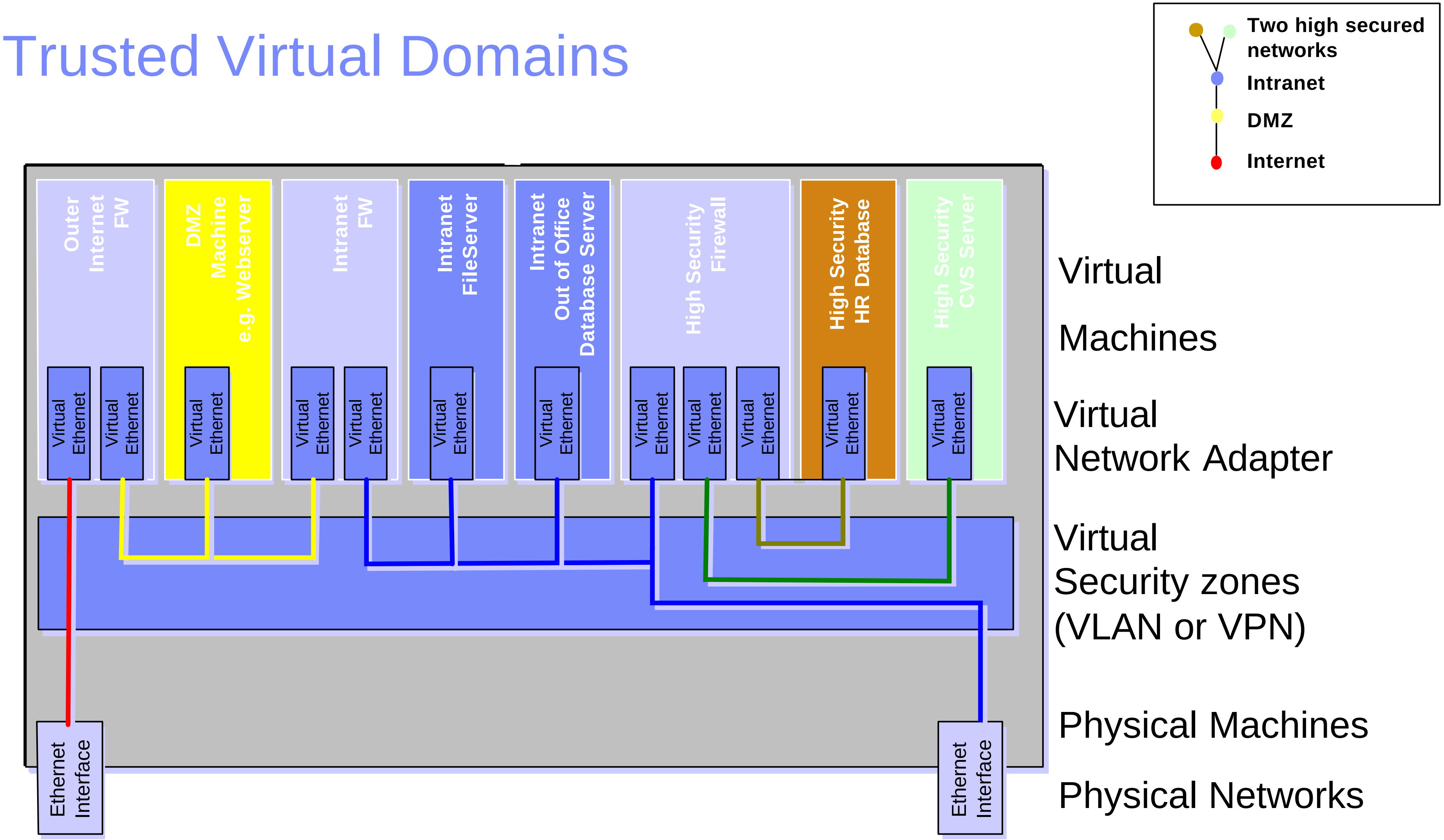


Physical Machines

Network Adapter

Security zones LAN or VLAN

Trusted Virtual Domains



Two high secured networks

Intranet

DMZ

Internet

Outer Internet FW

DMZ Machine e.g. Webserver

Intranet FW

Intranet FileServer

Intranet Out of Office Database Server

High Security Firewall

High Security HR Database

High Security CVS Server

Virtual Ethernet

Ethernet Interface

Virtual Machines

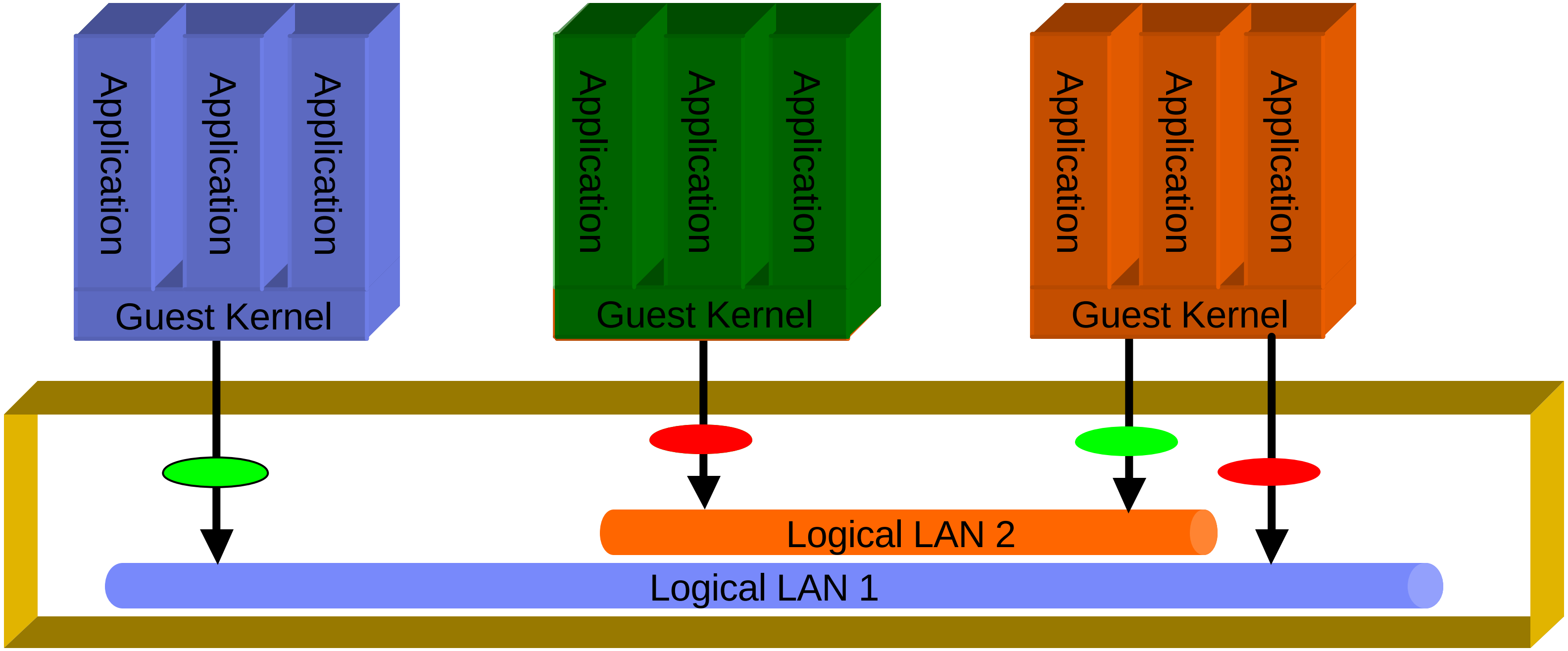
Virtual Network Adapter

Virtual Security zones (VLAN or VPN)

Physical Machines

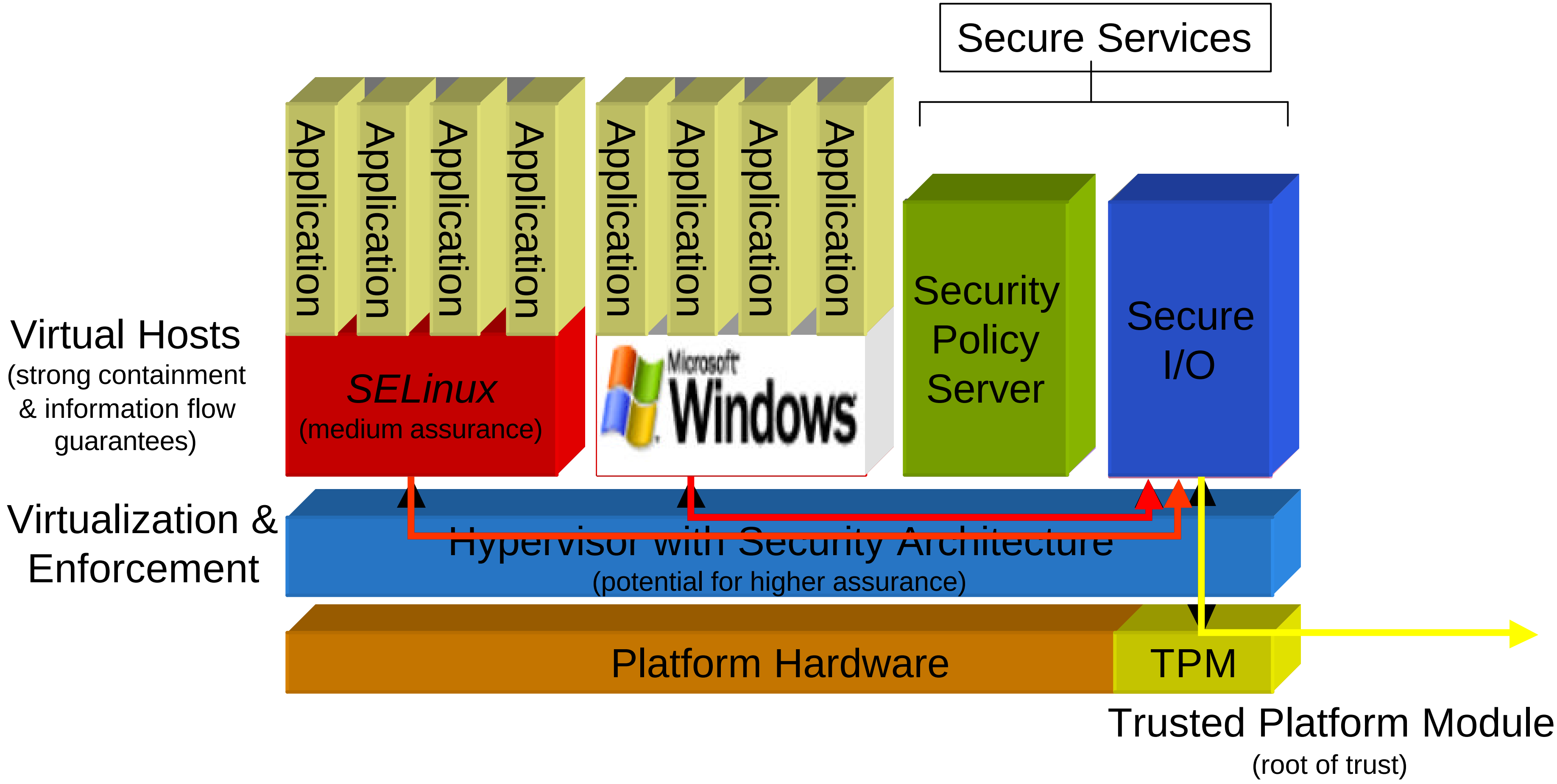
Physical Networks

Multi-Level Secure LAN

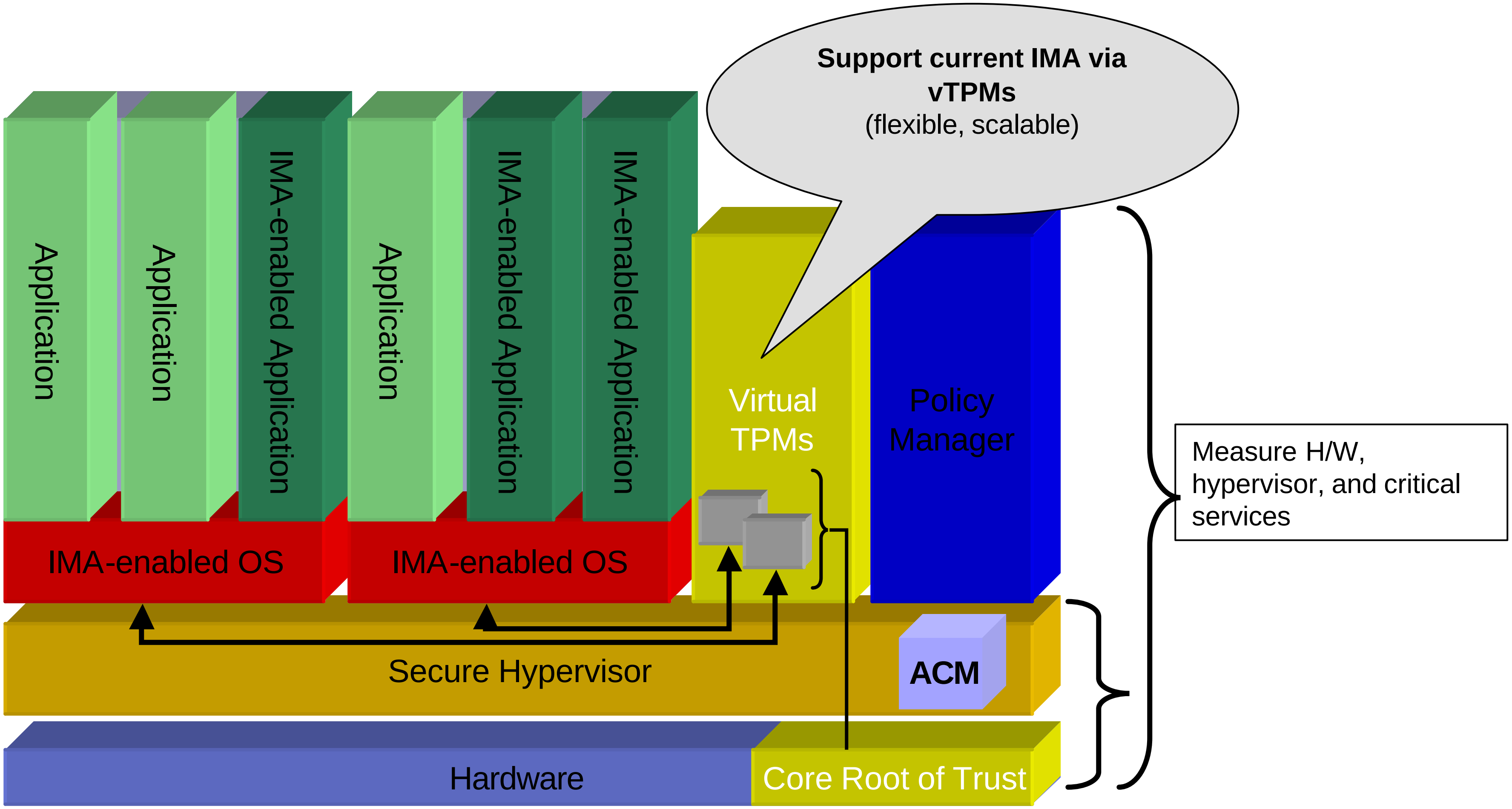


🟢🔴 Security policy enforced at time of resource binding

Secure Hypervisor Architecture



Integrity Measurement Architecture

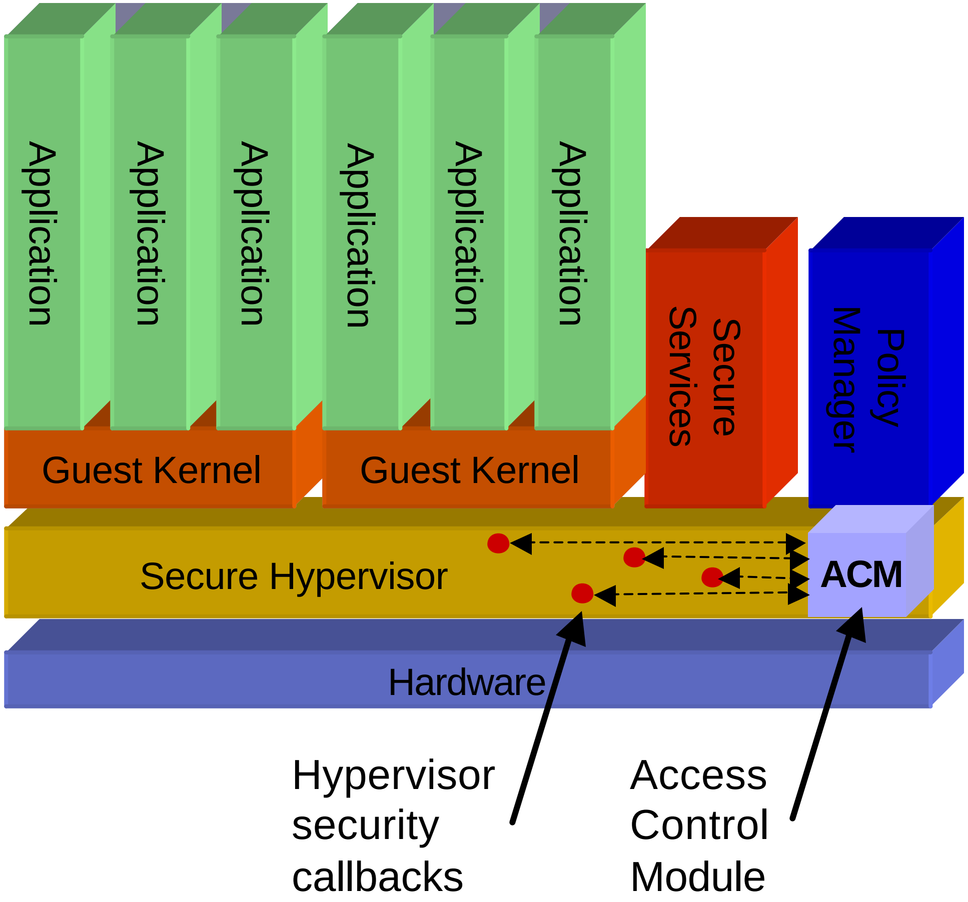


Multi-Level Security vs. Trusted Virtual Domains

- Multi-Level Security
  - “Fixed” classification of data and systems
  - Focus on basic security
  - Inflexible, not scaleable and expensive from today’s perspective

- Trusted Virtual Domains
  - Virtualized logical zones
  - Content-based security
  - Policy enablement
  - Separation of high and medium assurance

sHype/Xen Implementation



http://www.xensource.com/products/download

- Flexible Framework
  - supports multiple policies
- Access Control Module
  - may vary, depending on policy requirements
- Hypervisor Security Hooks
  - ✓ mediate all inter-virtual machine communication
  - ✓ interact with ACM for access decision
- Implemented for Xen, PHYP, rHype in various stages
- Availability: Xen 3.0 (Open-Source, GNU Public License)

Questions???

References

- Information about the author is available at
  - http://www.caster.xhost.de
  - http://www.roots-of-the-net.de

- Special thanks to my friends from IBM Research
  - Dr. Matthias Schunter
  - Andreas Wespi