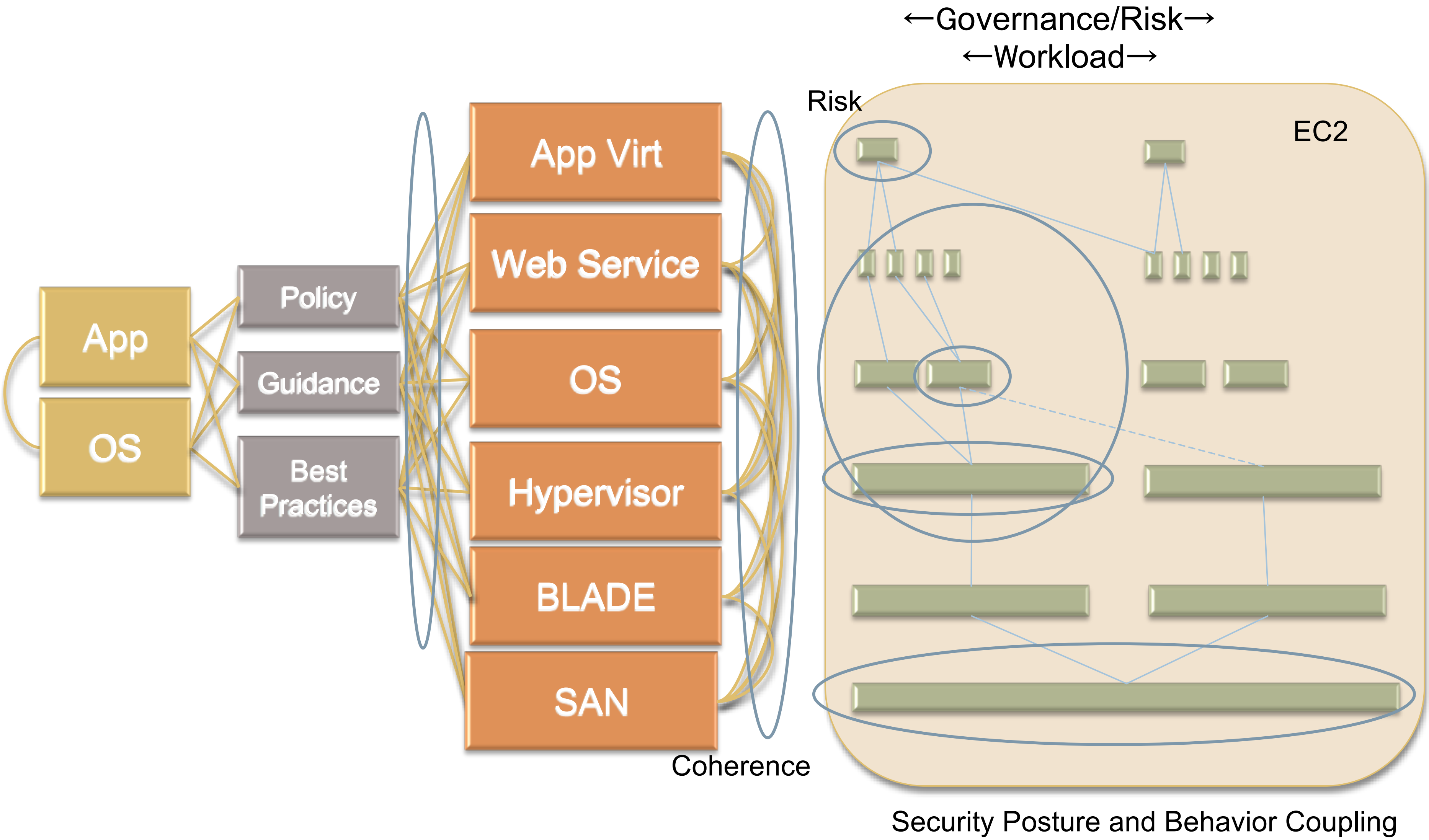
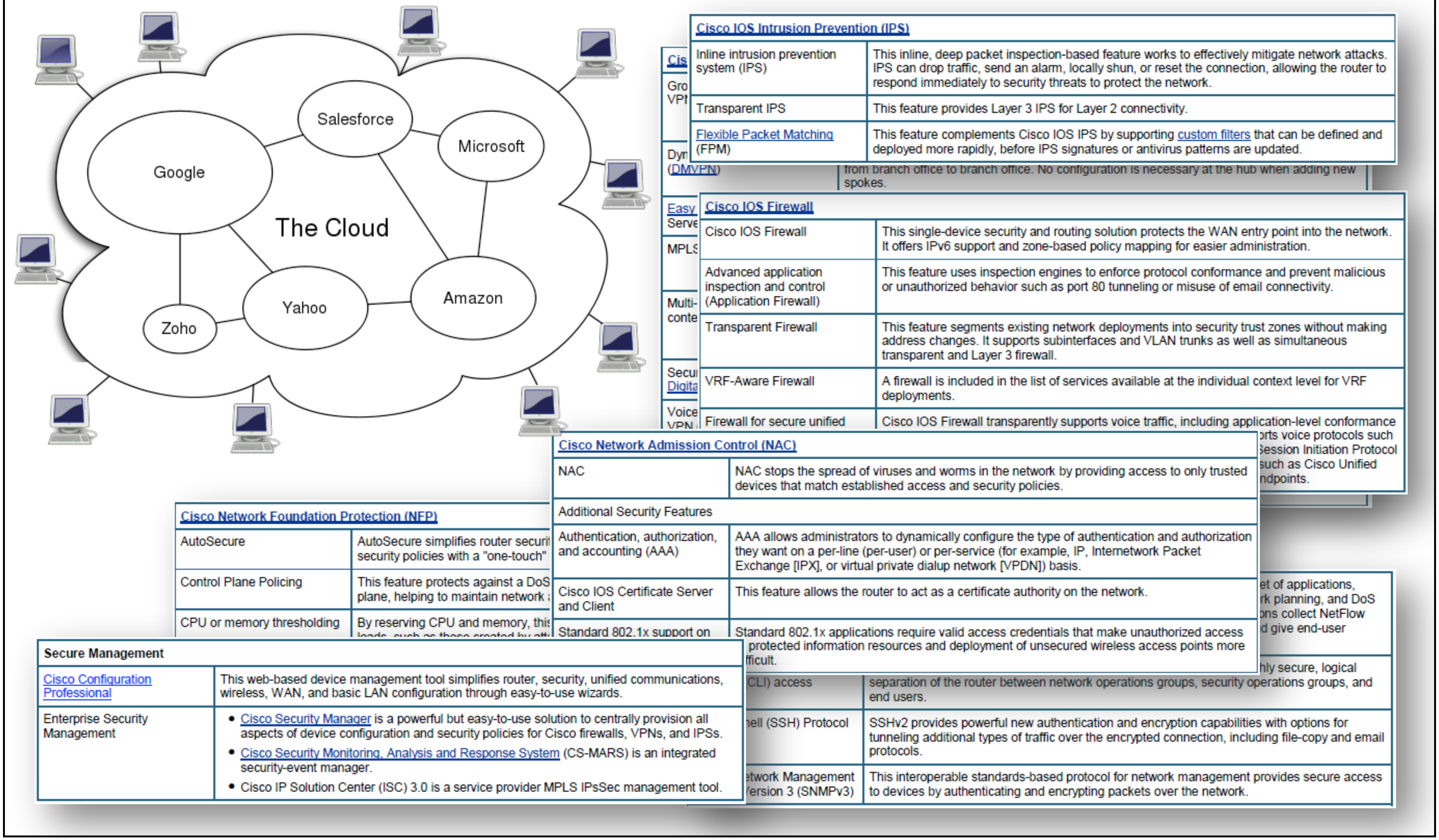
Complexity in the Cloud



Fabric: Lots of Configuration!



Cisco IOS Intrusion Prevention (IPS)	
Inline intrusion prevention system (IPS)	This inline, deep packet inspection-based feature works to effectively mitigate network attacks. IPS can drop traffic, send an alarm, locally shun, or reset the connection, allowing the router to respond immediately to security threats to protect the network.
Transparent IPS	This feature provides Layer 3 IPS for Layer 2 connectivity.
Flexible Packet Matching (FPM)	This feature complements Cisco IOS IPS by supporting custom filters that can be defined and deployed more rapidly, before IPS signatures or antivirus patterns are updated.

Cis	
Gro VPN	
Dyn (DMVPN)	from branch office to branch office. No configuration is necessary at the hub when adding new spokes.
Easy Serve	
MPLS	
Multi- conte	
Secu Digita	
Voice VPN	

Cisco IOS Firewall	
Cisco IOS Firewall	This single-device security and routing solution protects the WAN entry point into the network. It offers IPv6 support and zone-based policy mapping for easier administration.
Advanced application inspection and control (Application Firewall)	This feature uses inspection engines to enforce protocol conformance and prevent malicious or unauthorized behavior such as port 80 tunneling or misuse of email connectivity.
Transparent Firewall	This feature segments existing network deployments into security trust zones without making address changes. It supports subinterfaces and VLAN trunks as well as simultaneous transparent and Layer 3 firewall.
VRF-Aware Firewall	A firewall is included in the list of services available at the individual context level for VRF deployments.
Firewall for secure unified	Cisco IOS Firewall transparently supports voice traffic, including application-level conformance orts voice protocols such Session Initiation Protocol such as Cisco Unified ndpoints.

Cisco Network Admission Control (NAC)	
NAC	NAC stops the spread of viruses and worms in the network by providing access to only trusted devices that match established access and security policies.
Additional Security Features	
Authentication, authorization, and accounting (AAA)	AAA allows administrators to dynamically configure the type of authentication and authorization they want on a per-line (per-user) or per-service (for example, IP, Internetwork Packet Exchange [IPX], or virtual private dialup network [VPDN]) basis.
Cisco IOS Certificate Server and Client	This feature allows the router to act as a certificate authority on the network.
Standard 802.1x support on	Standard 802.1x applications require valid access credentials that make unauthorized access protected information resources and deployment of unsecured wireless access points more fficult.

Cisco Network Foundation Protection (NFP)	
AutoSecure	AutoSecure simplifies router securit security policies with a "one-touch"
Control Plane Policing	This feature protects against a DoS plane, helping to maintain network a
CPU or memory thresholding	By reserving CPU and memory, this loads, such as those created by att

	et of applications, rk planning, and DoS ons collect NetFlow d give end-user
(CLI) access	hly secure, logical separation of the router between network operations groups, security operations groups, and end users.
hell (SSH) Protocol	SSHv2 provides powerful new authentication and encryption capabilities with options for tunneling additional types of traffic over the encrypted connection, including file-copy and email protocols.
etwork Management Version 3 (SNMPv3)	This interoperable standards-based protocol for network management provides secure access to devices by authenticating and encrypting packets over the network.

Secure Management	
Cisco Configuration Professional	This web-based device management tool simplifies router, security, unified communications, wireless, WAN, and basic LAN configuration through easy-to-use wizards.
Enterprise Security Management	• Cisco Security Manager is a powerful but easy-to-use solution to centrally provision all aspects of device configuration and security policies for Cisco firewalls, VPNs, and IPSs. • Cisco Security Monitoring, Analysis and Response System (CS-MARS) is an integrated security-event manager. • Cisco IP Solution Center (ISC) 3.0 is a service provider MPLS IPsSec management tool.

The cloud is very different

- Deeper stacks
- … each layer has its own vulnerabilities
- More intimately coupled
- More dynamic workloads
- Multi-tenant
- … each with different (evolving) governance
- … under potentially different (evolving) regulatory domains
- … accountable for different (evolving) due care

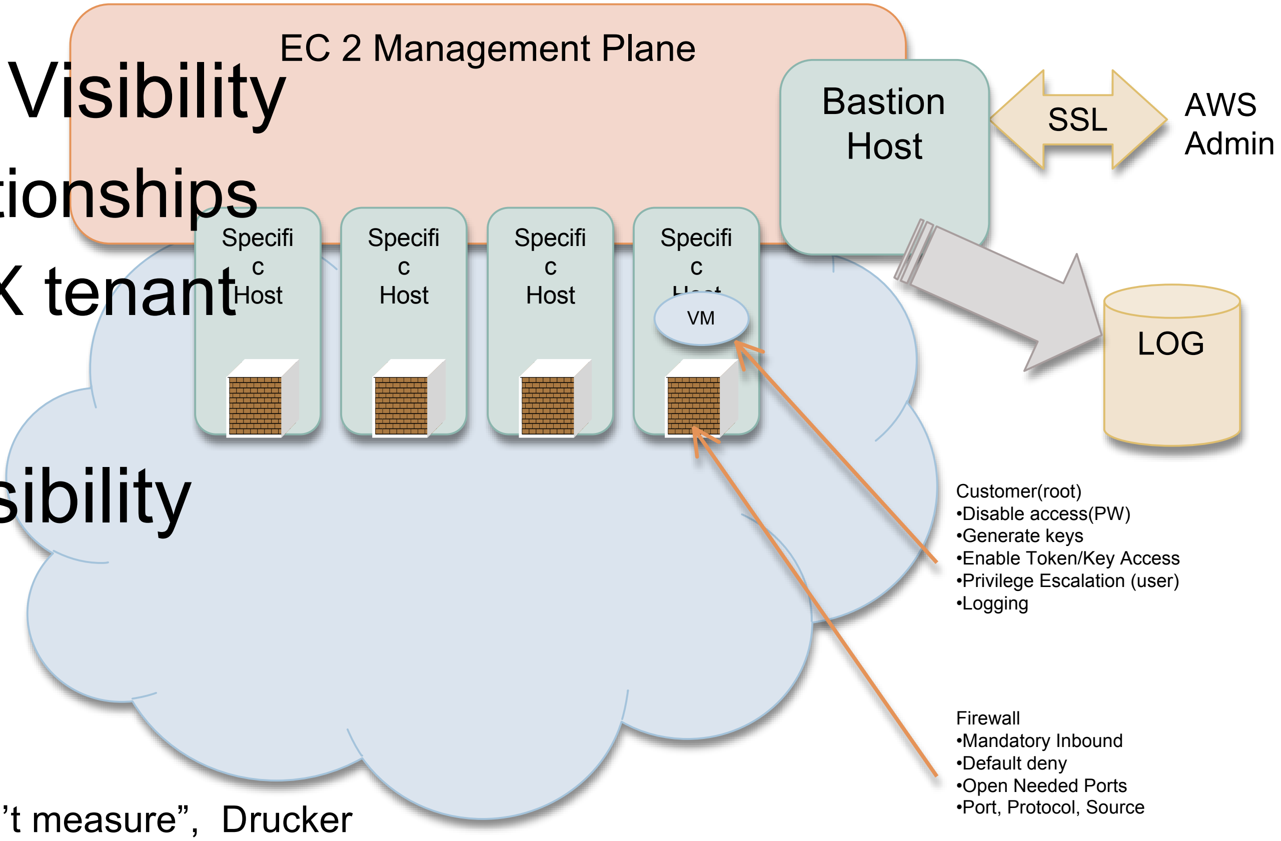
But… (Variation on the Gartner 7)

- Am I compliant? (at every level in any state)
- Trust Stack: Physical or Logical or…..
- What is shared? (coupling)
- Where is the problem? (context via connect the dots)
- How well is my deployment working? (at all levels)
- How should I re-provision? (next desired state)
- How can I improve? (good citizens vs. problem children)

- Issue: Black Box Abstraction of Complex Activity:
  - Can’t Manage what you can’t measure. Drucker
  - Can’t Measure what you can’t see. Deming
  - => Automation, of any kind, without feedback inevitably does the wrong thing very efficiently.

Solution Direction: Visibility

- Visibility vs. Transparency
- Configuration Visibility
  - Sec/Op Relationships
  - Trust/health X tenant
  - Root Cause
- Behavioral Visibility
  - Root/Cause
  - Alignment
  - Improvement



Customer(root)
•Disable access(PW)
•Generate keys
•Enable Token/Key Access
•Privilege Escalation (user)
•Logging

Firewall
•Mandatory Inbound
•Default deny
•Open Needed Ports
•Port, Protocol, Source

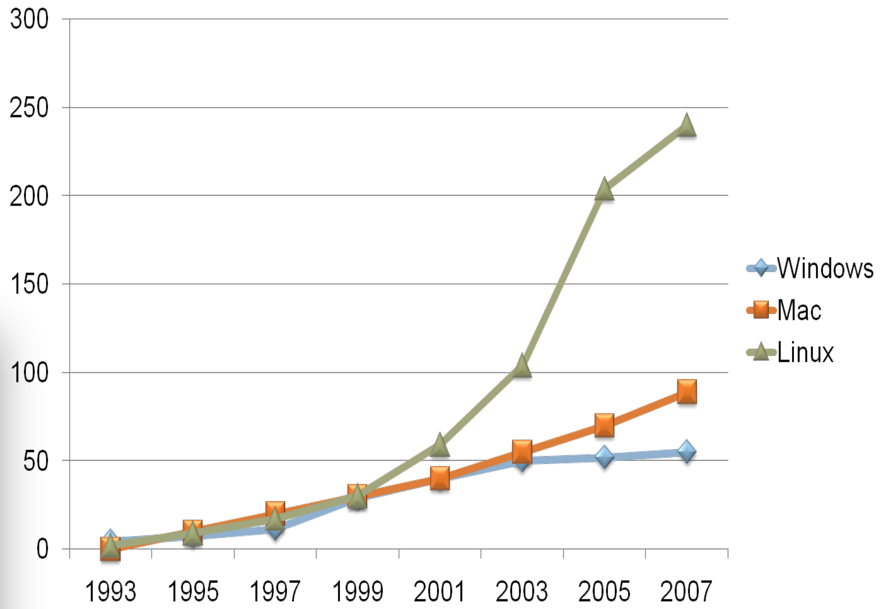
"You can't manage what you can't measure", Drucker
"You can't measure what you can't see", Deming

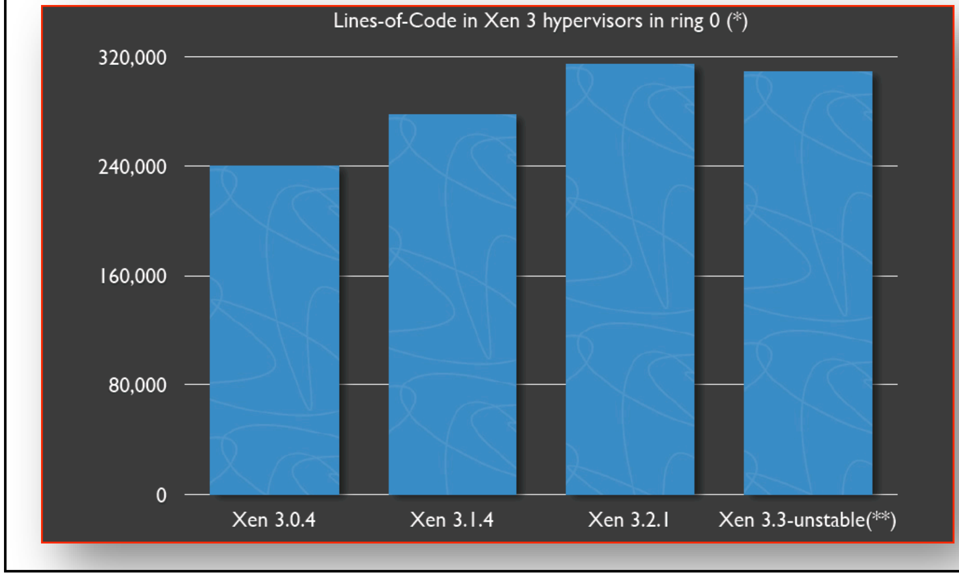
Solution Direction: Models

- Model-based controls (SML, OVF, OSLO, SDM, UCA …)
  - Tie constraints to intentional relationships
  - Service lifecycle: design – de-provisioning
  - Dynamics (autonomics)
  - Inform “next desired state” (design impact of change)
  - XCCDF – OVAL, … but in model vocabulary

Solution Direction: Small is Good

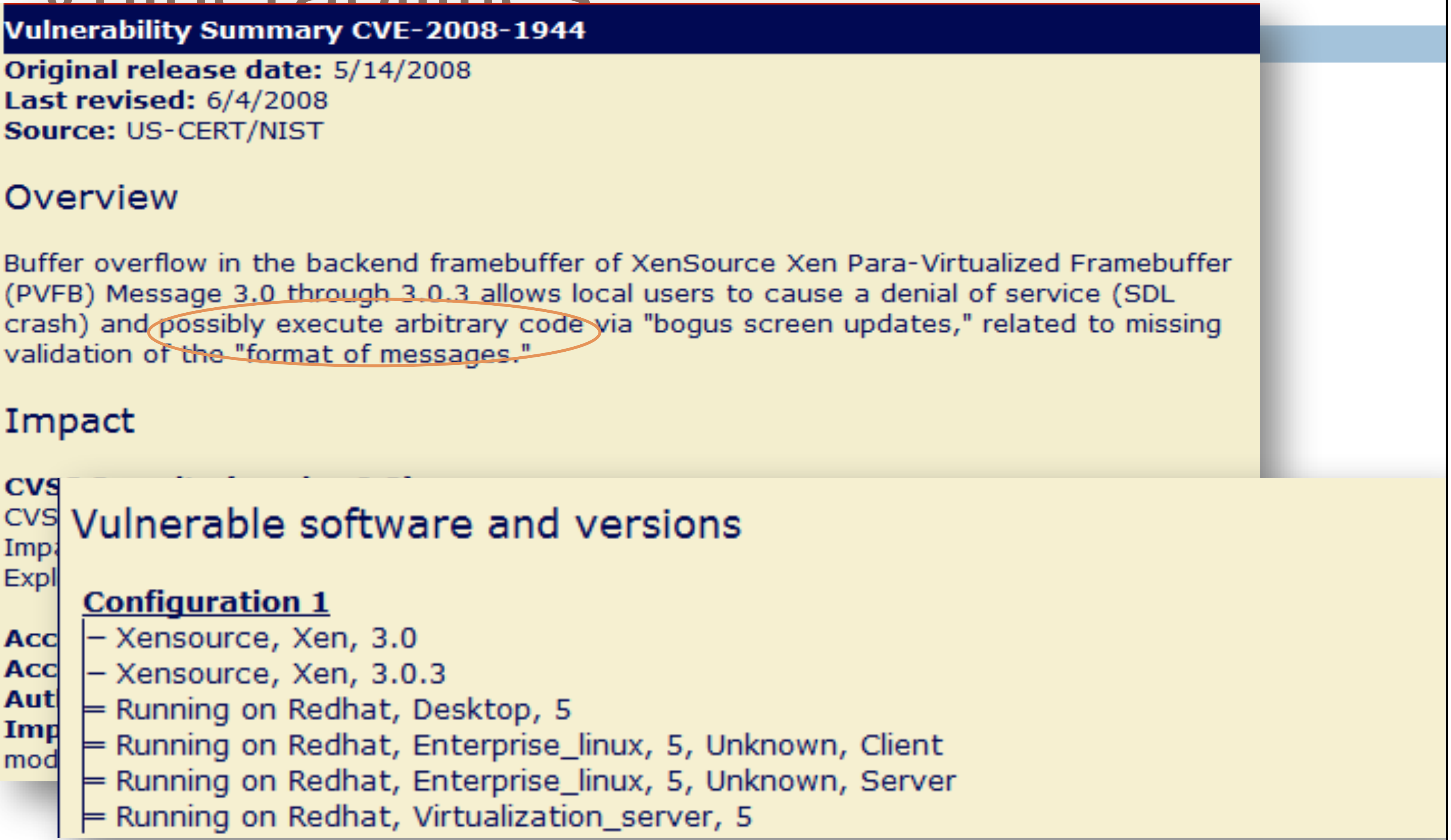
- (much) Smaller Virtualization Kernels
  - Hyper Guard, sHype, Flask, …





Appendix

Virtualization Specific Vulnerabilities



Vulnerability Summary CVE-2008-1944

Original release date: 5/14/2008
Last revised: 6/4/2008
Source: US-CERT/NIST

Overview

Buffer overflow in the backend framebuffer of XenSource Xen Para-Virtualized Framebuffer (PVFB) Message 3.0 through 3.0.3 allows local users to cause a denial of service (SDL crash) and possibly execute arbitrary code via "bogus screen updates," related to missing validation of the "format of messages."

Impact

CVS
CVS
Imp
Expl

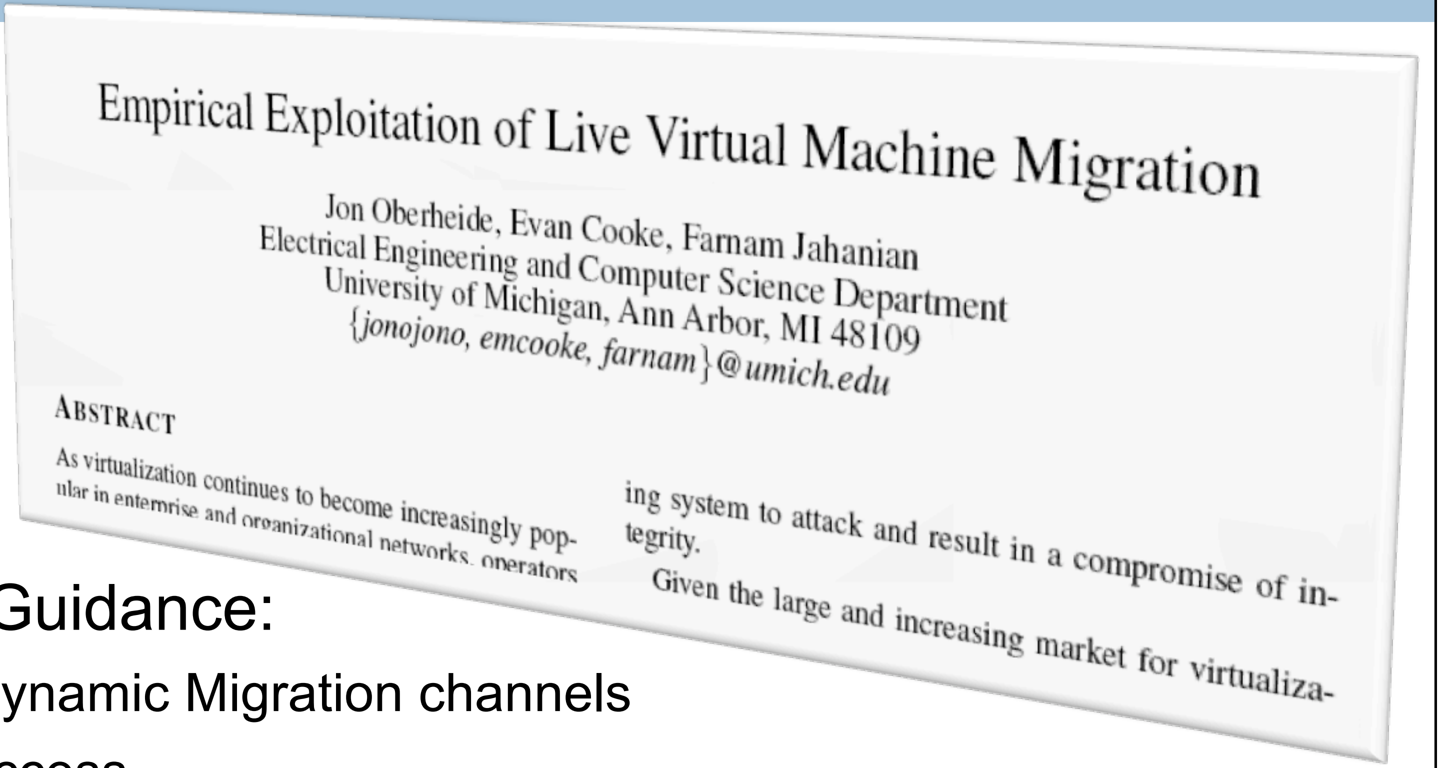
Acc
Acc
Aut
Imp
mod

Vulnerable software and versions

Configuration 1

- Xensource, Xen, 3.0
- Xensource, Xen, 3.0.3
- Running on Redhat, Desktop, 5
- Running on Redhat, Enterprise_linux, 5, Unknown, Client
- Running on Redhat, Enterprise_linux, 5, Unknown, Server
- Running on Redhat, Virtualization_server, 5

Virtualization Specific Vulnerabilities XenSploit



Empirical Exploitation of Live Virtual Machine Migration

Jon Oberheide, Evan Cooke, Farnam Jahanian
Electrical Engineering and Computer Science Department
University of Michigan, Ann Arbor, MI 48109
{*jonojono, emcooke, farnam*}@*umich.edu*

ABSTRACT

As virtualization continues to become increasingly popular in enterprise and organizational networks, operators

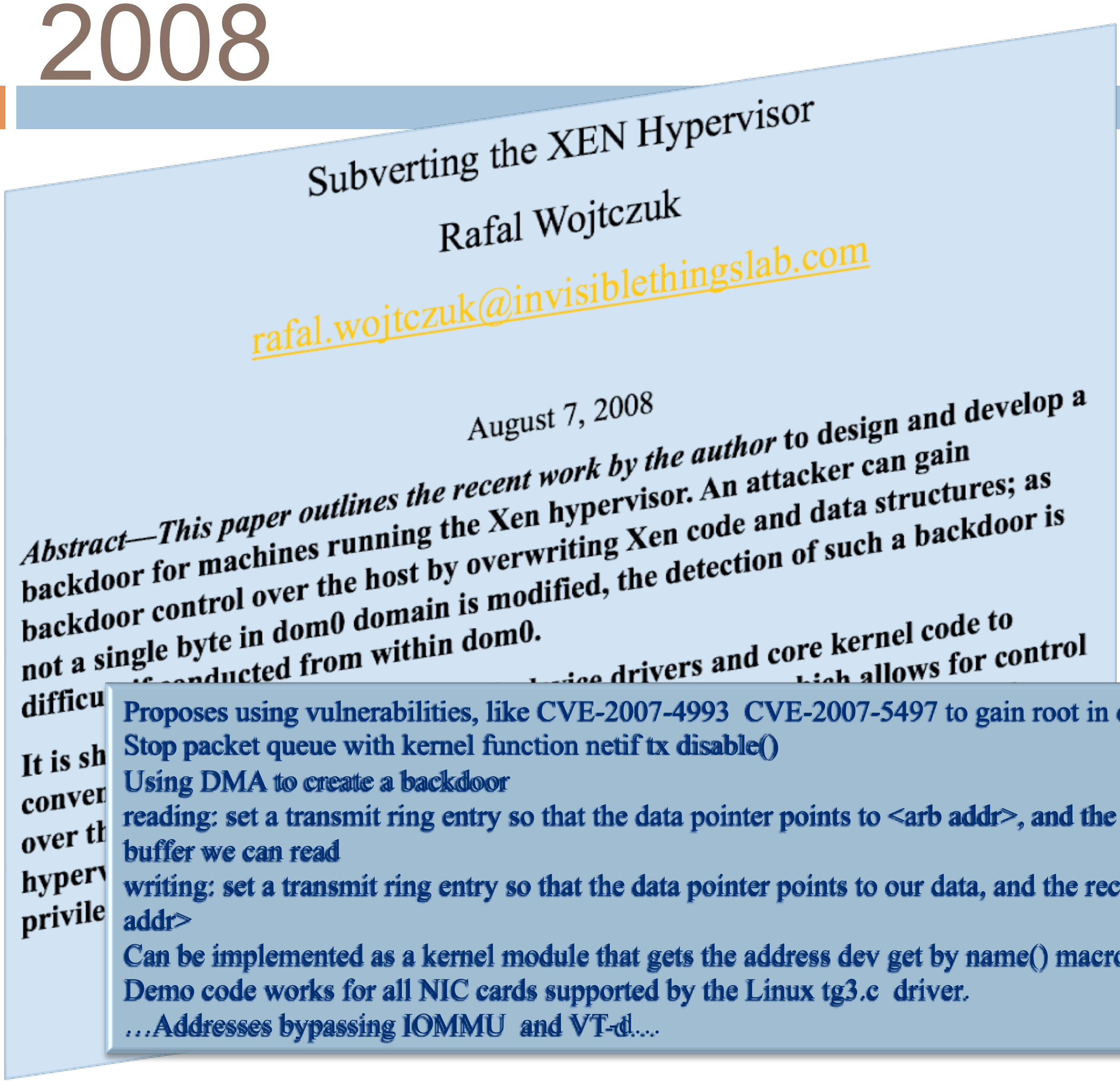
ing system to attack and result in a compromise of integrity.

Given the large and increasing market for virtualiza-

- Resulting Guidance:
  - Encrypt Dynamic Migration channels
  - Restrict access
  - Tightly control vNIC configuration
  - Isolate LANs (Management, Transactional, Dynamic Migration)

http://www.eecs.umich.edu/techreports/cse/2007/CSE-TR-539-07.pdf

“Owning Xen”: ITL, BlackHat 2008



Subverting the XEN Hypervisor

Rafal Wojtczuk

rafal.wojtczuk@invisiblethingslab.com

August 7, 2008

Abstract—*This paper outlines the recent work by the author* to design and develop a backdoor for machines running the Xen hypervisor. An attacker can gain backdoor control over the host by overwriting Xen code and data structures; as not a single byte in dom0 domain is modified, the detection of such a backdoor is
difficu
if conducted from within dom0.
device drivers and core kernel code to
hich allows for control

It is sh
conver
over th
hyperv
privile

Proposes using vulnerabilities, like CVE-2007-4993 CVE-2007-5497 to gain root in dom0 from unprivileged dom.

Stop packet queue with kernel function netif tx disable()

Using DMA to create a backdoor

reading: set a transmit ring entry so that the data pointer points to <arb addr>, and the receive ring entry data pointer points to buffer we can read

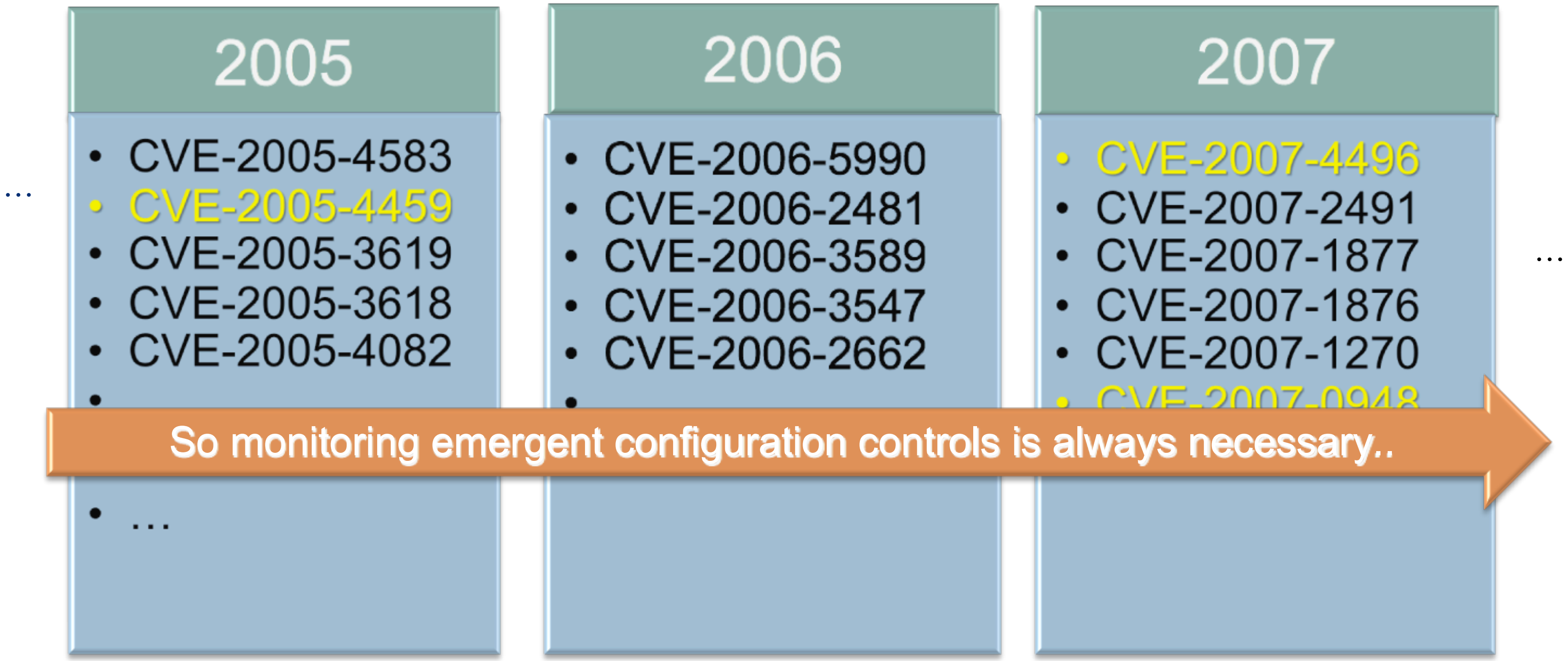
writing: set a transmit ring entry so that the data pointer points to our data, and the receive ring entry data pointer points to <arb addr>

Can be implemented as a kernel module that gets the address dev get by name() macro

Demo code works for all NIC cards supported by the Linux tg3.c driver.

…Addresses bypassing IOMMU and VT-d….

Server Virtualization Vulnerabilities



…

2005

- CVE-2005-4583
- CVE-2005-4459
- CVE-2005-3619
- CVE-2005-3618
- CVE-2005-4082
-
- …

2006

- CVE-2006-5990
- CVE-2006-2481
- CVE-2006-3589
- CVE-2006-3547
- CVE-2006-2662
-

2007

- CVE-2007-4496
- CVE-2007-2491
- CVE-2007-1877
- CVE-2007-1876
- CVE-2007-1270
- CVE-2007-0948

…

So monitoring emergent configuration controls is always necessary..

Reference: NIST National Vulnerability Database, http://nvd.nist.gov/ <needs update>