



CENTER FOR INTERNET SECURITY BENCHMARKS

SUNY Technology Conference

June 20, 2013

Bill Kramp



AGENDA

- Why use the CIS benchmarks and toolkit
 - Risks
 - Vulnerabilities
 - 2012 Incident Statistics
 - Recent Higher-Ed Incidents
- Obtaining access to CIS resources
- How to use CIS-CAT to assess security settings
- Understanding the benchmark reports
- Develop a plan for using benchmarks
- Live demo



GOT RISK?

Se**r**vers

Personally **i**dentifiable information

Payment cards**S**

Des**k**tops, laptops, tablets



DO YOU HAVE ANY VULNERABILITIES?

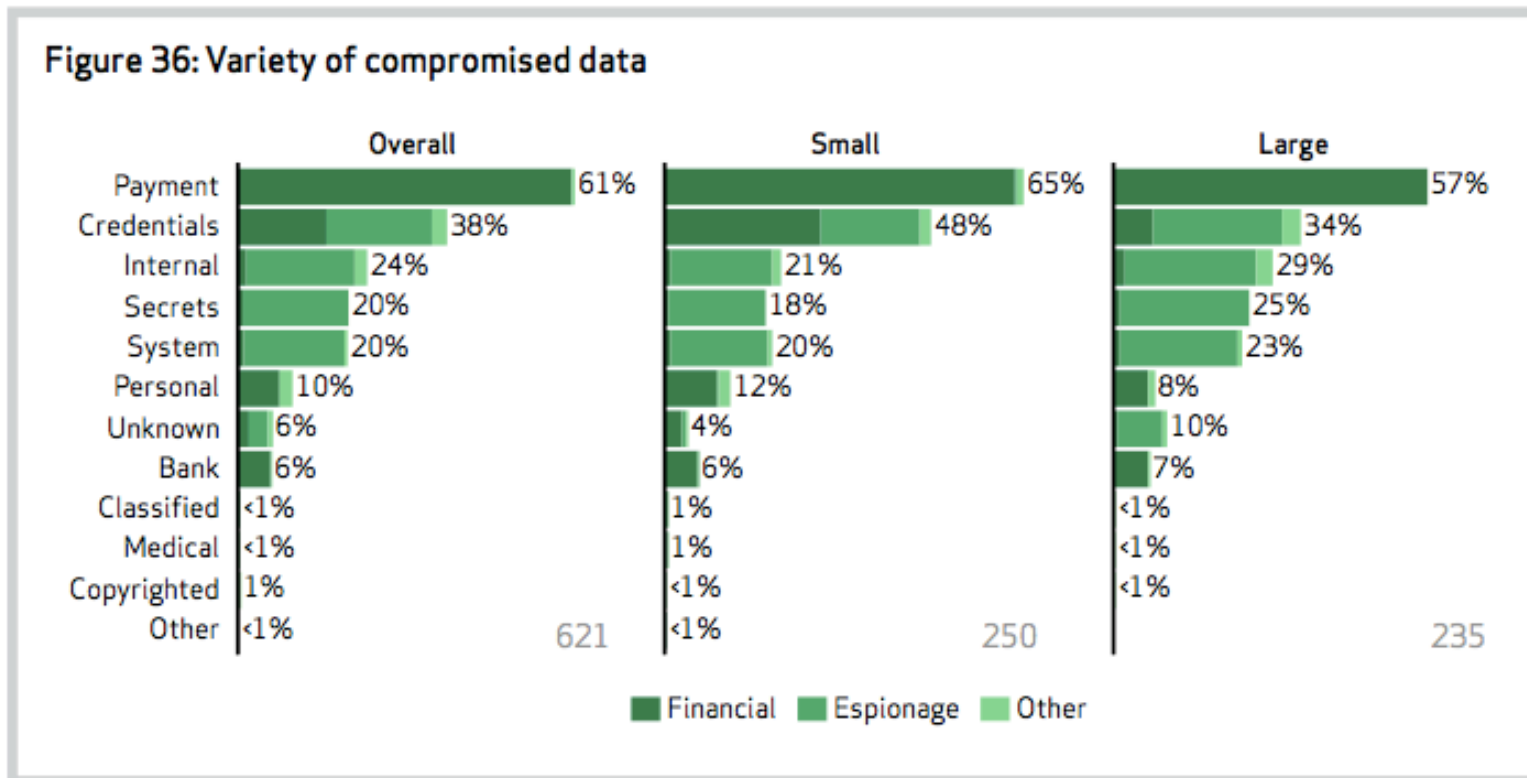
- No anti-virus?
- Not patching Operating Systems?
- Missing application updates?
- Insecure configurations (security controls)?



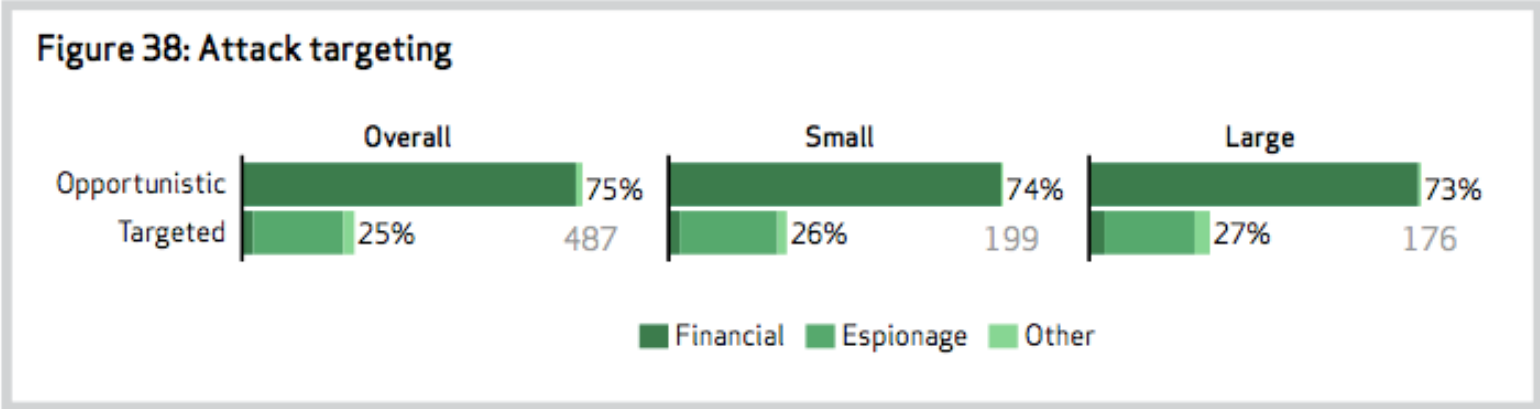
VERIZON 2013 BREACH REPORT



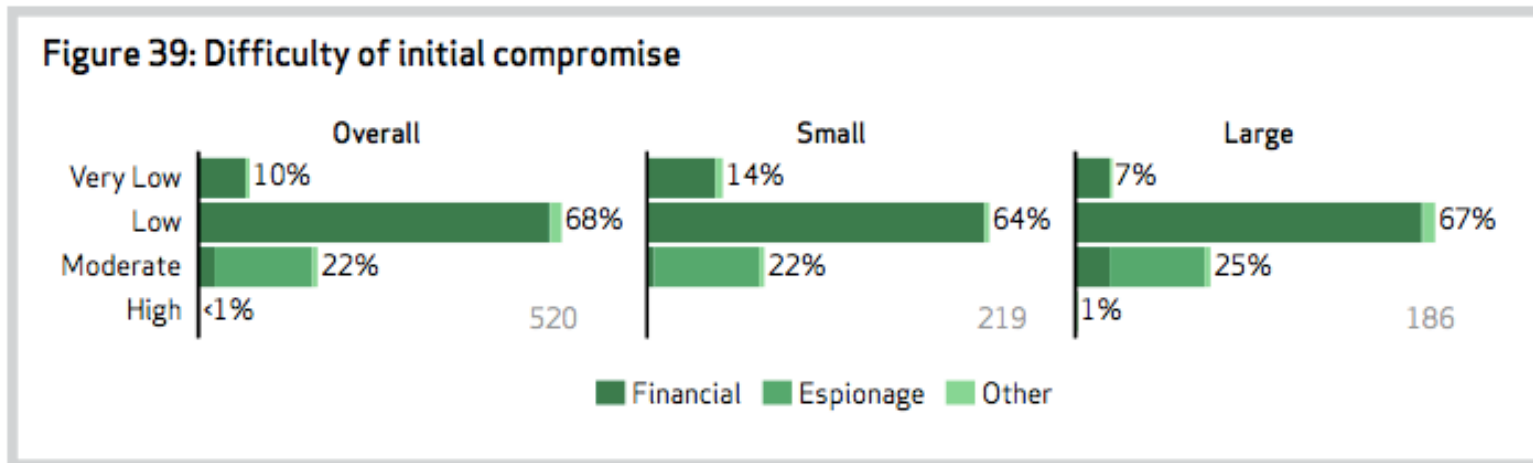
CREDIT AND DEBIT CARDS TOP TARGETS



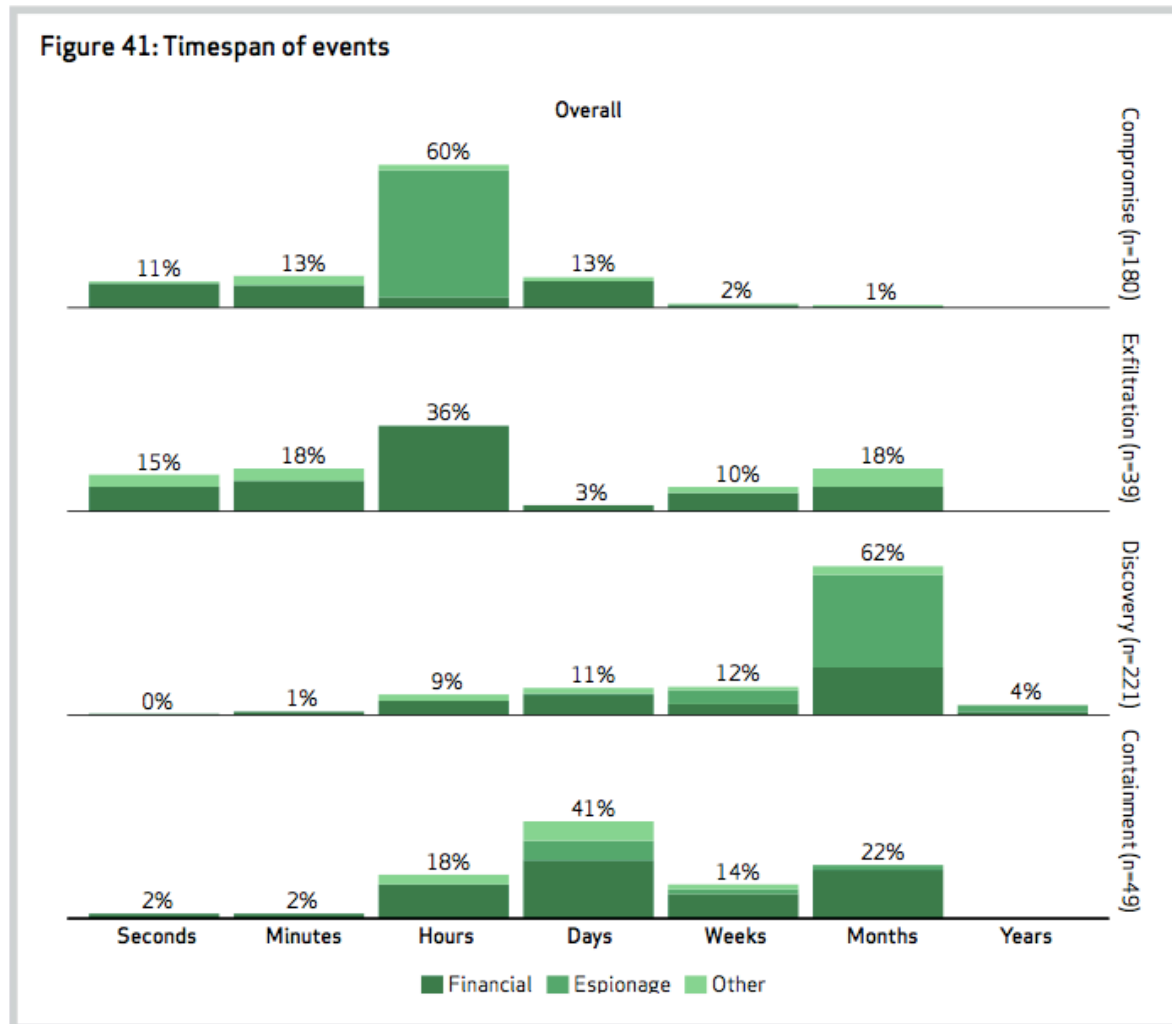
WRONG PLACE, WRONG TIME



LOW DIFFICULTY FOR MOST COMPROMISES

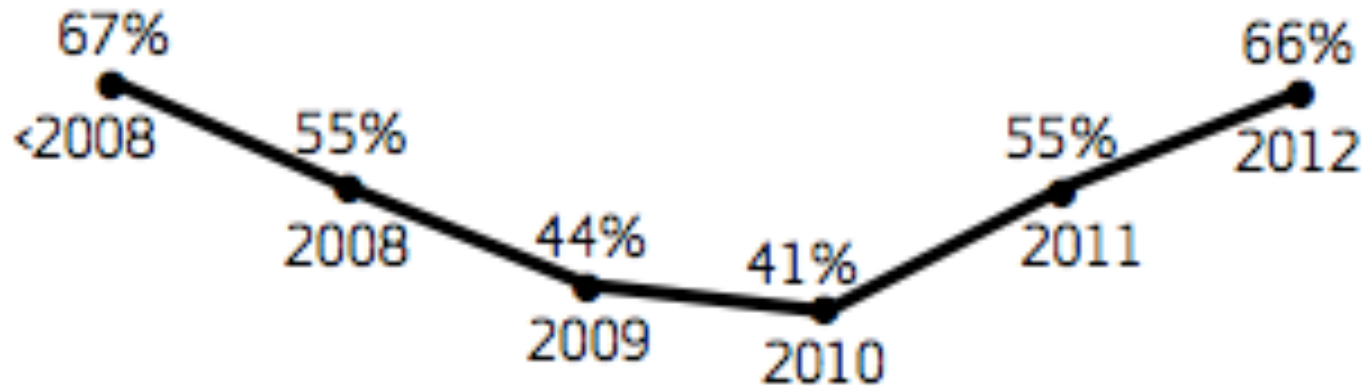


COMPROMISE TO CONTAINMENT TIMELINE



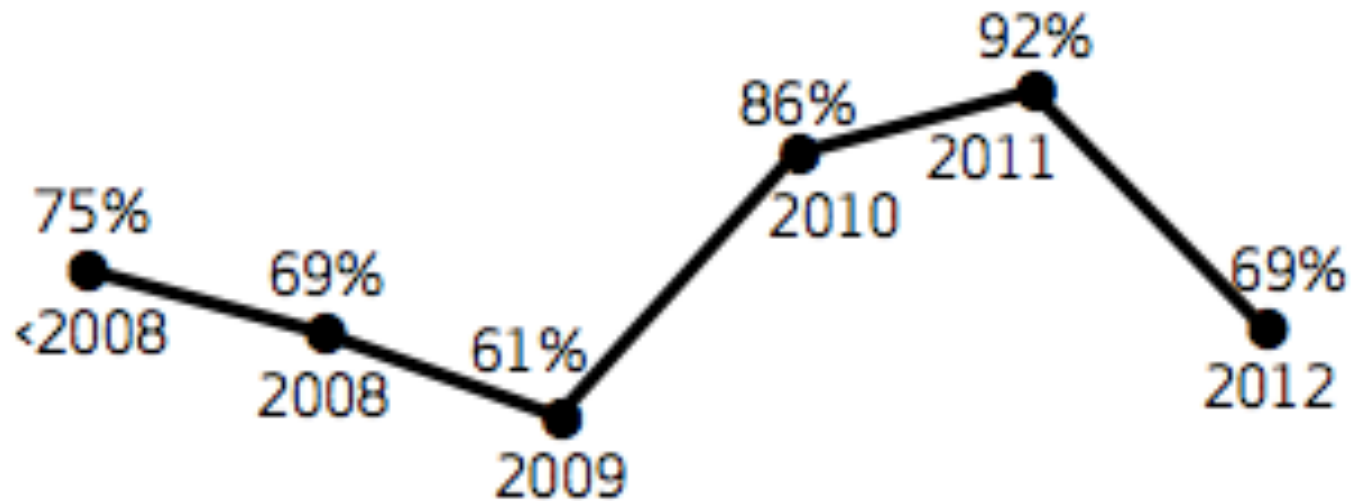
66% UNDETECTED FOR MONTHS (2012)

Figure 42: Percent of breaches that remain undiscovered for months or more



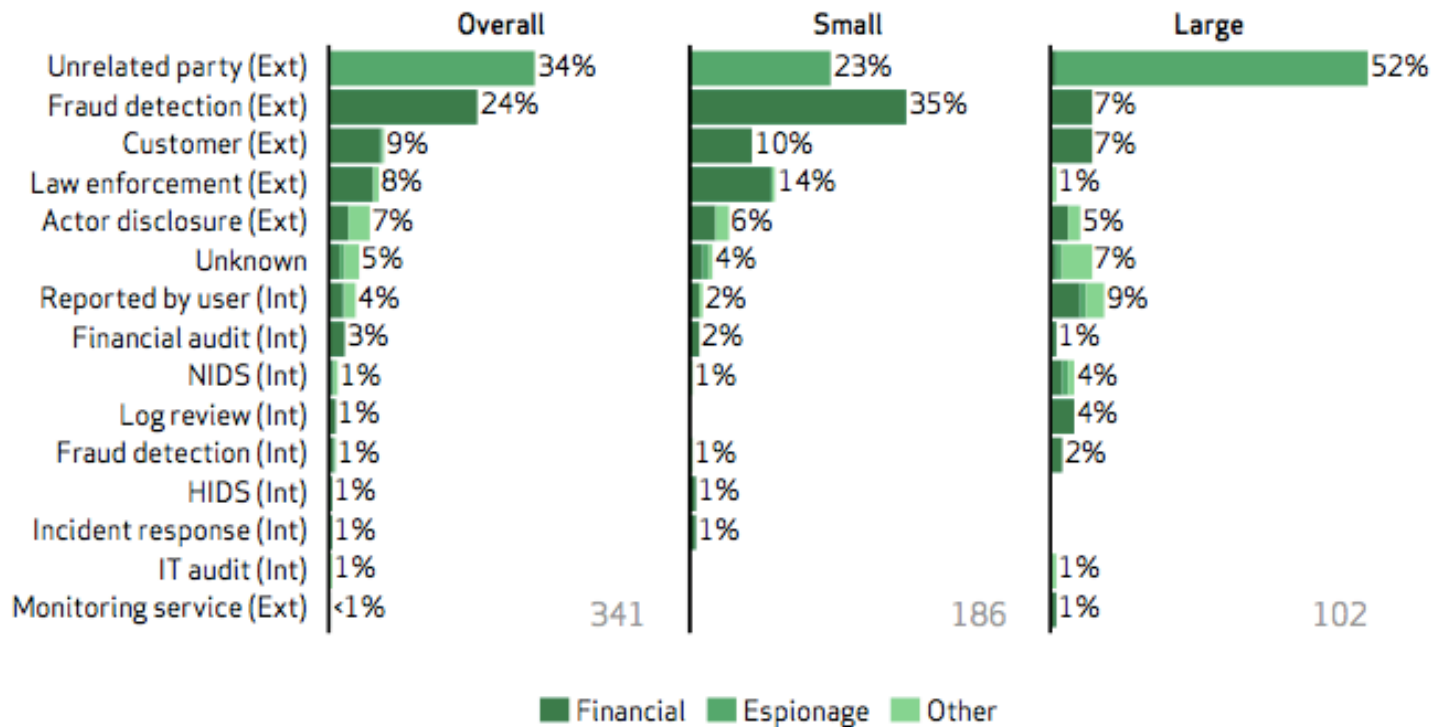
69% DETECTED BY OUTSIDERS (2012)

Figure 43: Percent of breaches discovered external to victim



DETECTION BY NIDS, HIDS, LOG REVIEWS OR IT AUDITS IN THE BOTTOM 10%

Figure 44: Discovery methods



RECENT HIGHER-ED INCIDENTS

- Kirkwood Community College (2013)
 - Website compromised
 - PII of 125,000 students stolen
 - Initial costs are \$350K for security consultant
- University of North Carolina-Charlotte (2012)
 - Student Information System Compromised
 - Misconfiguration and incorrect access settings
 - PII and banking exposed for 350,000 students



SOME REASONS FOR USING BENCHMARKS

- FERPA
- HIPAA
- PCI-DSS
- Financial losses
- Destruction of data
- Public Relations Issues
- Various state reporting rules for PII exposure



WHAT CAN WE DO BETTER?

○ Prevention

- Updating applications in a timely fashion
- Patching Operating Systems
- Anti-virus
- Good security controls (using CIS Benchmarks)

○ Detection

- Log analysis
 - Requires proper audit settings (using CIS Benchmarks)
 - Reviewing logs on a regular basis
 - Automatic alerts
- Paying attention for abnormal behavior of servers and applications



If a tree falls on your network
and it shows up in your syslog
and nobody is reading it -
you're still squished.

Marcus Ranum



BENCHMARKS/BEST PRACTICES

- National Institute of Standards and Technology (NIST) SP800 Guides
- SANS Institute Best Practices
- Center for Internet Security (CIS) Benchmarks



CENTER FOR INTERNET SECURITY (CIS)

- Provides information for improving security to reduce risk to the organization.
- Diverse membership:
 - Over 1500 subject matter experts
 - Experts are from various organizations:
 - Government
 - Higher Education
 - Corporations
- Several divisions:
 - Multi-State Information Sharing & Analysis Center
 - Trusted Purchasing Alliance
 - Security Benchmarks



WHAT CIS BENCHMARKS AREN'T



- A silver bullet
- A talisman
- A rabbits foot
- The Holy Grail




WHAT CIS BENCHMARKS ARE

- Consensus based development of:
 - Public and private contributors
 - Higher-Ed involvement
 - Best practices for security configurations
 - Tools for measuring security status
 - Resources for making informed security decisions
- Security Configuration Benchmarks
 - Can eliminate many of the known vulnerabilities
 - Enable auditing for tracking user/system activity



CIS WEB SITE



**CENTER FOR
INTERNET SECURITY**

Security BenchmarksSM MULTI-STATE Information Sharing & Analysis CenterSM Trusted Purchasing AllianceSM Info Inte Cer

in f t YouTube

Contact Us

ABOUT US | COMMUNITIES/MEMBERSHIP | RESOURCES & PUBLICATIONS | TRAINING & EVENTS

1 2 3 4 5 6 7 8

<< PREV NEXT >>



William Pelgrin offers three reasons why criminals exploit social networks (and tips to avoid getting scammed). [Read More](#)

Center for Internet Security

The Center for Internet Security (CIS) is a nonprofit organization focused on enhancing the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration. Through its four divisions--Security Benchmarks, Multi-State ISAC, Trusted Purchasing Alliance, and the Integrated Intelligence Center--CIS serves as a central resource in the development and delivery of high-quality, timely products and services to assist our partners in government, academia, the private sector and the general public in improving their cyber security posture.

[READ MORE ABOUT CIS](#)

Today's Cyber Security Tip: [Secure Your Laptop](#): Laptops are increasing in popularity for both business and personal use. The ... [Click here to read more](#)

<http://www.cisecurity.org/>



CIS SECURITY BENCHMARKS

SECURITY BENCHMARKS



The Security Benchmarks Division provides standards and metrics that dramatically raise the level of security to ensure the integrity of the public and private Internet-based functions on which society increasingly depends.

[Security Resources for Download](#)

[Security Benchmarks Membership](#)

[Join Consensus Team](#)



BENCHMARKS MEMBERSHIP BENEFITS

- Access CIS-CAT Benchmark tool
- Security benchmarks
- Rights to distribute benchmarks, tools and metrics within organization
- Redistribution of benchmark resources to enrolled students.
- Technical support



COST OF MEMBERSHIP

- NYS Office of Cyber Security (OCS)
- OCS purchased access to the Center for Internet Security Benchmarks
- Three year membership
- OCS sharing access with other NYS agencies and SUNY campuses
- Must use SUNY E-mail address when registering
- Cost to SUNY campuses = free



BENCHMARK CATEGORIES

Desktop: Office
Desktop: Web Browsers
Devices: Mobile
Devices: Network
Devices: Print
Logos
OS: Linux
OS: UNIX
OS: Virtualization
OS: Windows

Security Metrics
Servers: Authentication
Servers: Collaboration
Servers: Database
Servers: DNS
Servers: LDAP
Servers: Mail
Servers: Web
Tools: CIS-CAT
Tools: RAT



CIS-CAT BENCHMARK ASSESSMENT TOOL

- Java program to scan system security settings
- Works on many operating systems
- Generates reports in a variety of formats:
 - HTML
 - .csv
 - Text
- Dashboard
- Can be executed from external hard disks



CIS-CAT BENCHMARK ASSESSMENTS

- CIS_Apache_Tomcat_Benchmark_v1.0.0.xml
- CIS_Apple_OSX_10.6_Benchmark_v.1.0.0.xml
- CIS_Debian_Linux_Benchmark_v1.0.0.xml
- CIS_HP-UX_11i_Benchmark_v1.4.2.xml
- CIS_IBM_AIX_5.3-6.1_Benchmark_v1.1.0.xml
- CIS_Microsoft_Windows_2003_MS_DC_Benchmark_v2.0.0.xml
- CIS_Mozilla_Firefox_Benchmark_v1.0.0.xml
- CIS_Oracle_Database_11g_Benchmark_v1.0.1.xml
- CIS_Oracle_Database_9i-10g_Benchmark_v2.0.1.xml
- CIS_Oracle_Solaris_11_Benchmark_v1.0.0.xml
- CIS_Red_Hat_Enterprise_Linux_6_Benchmark_v1.1.0.xml
- CIS_Slackware_Linux_10.2_Benchmark_v1.1.0.xml
- CIS_Solaris_10_Benchmark_v5.0.0.xml
- CIS_SUSE_Linux_Enterprise_Server_10_Benchmark_v2.0.0.xml
- CIS_VMware_ESX_3.5_Benchmark_v1.2.0.xml
- CIS_VMware_ESX_4.1_Benchmark_v1.0.0.xml
- CIS_Windows_2008_Server_Benchmark_v1.2.0.xml (SCAP 1.1 Compliant)
- CIS_Windows_7_Benchmark_v1.2.0.xml (SCAP 1.1 Compliant)



RUNNING CIS-CAT BENCHMARK TOOL

Steps:

1. Download CIS-CAT
2. Install Java JRE
3. Configure script path to JRE (if needed)
4. Execute CIS-CAT script



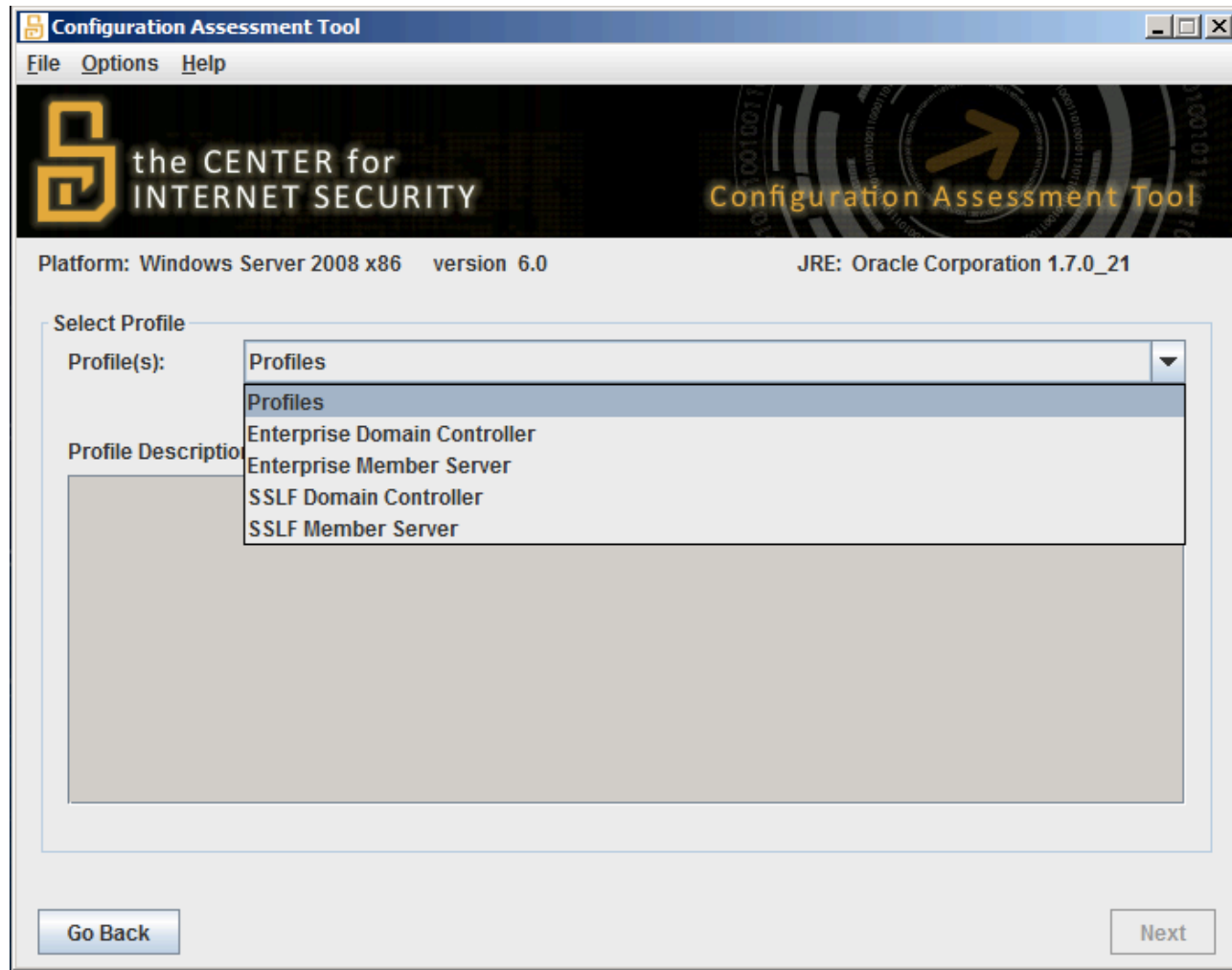
SELECT OS TO BENCHMARK



WINDOWS 2008 SERVER



VARIOUS TYPES OF SECURITY PROFILES



DOMAIN CONTROLLER PROFILE

Platform: Windows Server 2008 x86 version 6.0

JRE: Oracle Corporation 1.7.0_21

Select Profile

Profile(s):

Enterprise Domain Controller

Profile Description

This profile is used to define general settings that apply to both Domain Controller and Member server. Settings in this level are designed for systems operating in a managed environment where interoperability with legacy systems is not required. It assumes that all operating systems within the enterprise are Windows XP SP3 or later and Windows Server 2003 SP2 or later. In such environments, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended technical controls.



MEMBER SERVER PROFILE

Platform: Windows Server 2008 x86 version 6.0

JRE: Oracle Corporation 1.7.0_21

Select Profile

Profile(s):

Enterprise Member Server

Profile Description

The Member Server profile specifies configuration recommendations specific to Windows 2008 Server instances that are joined to a domain and are not domain controllers. Settings in this level are designed for systems operating in a managed environment where interoperability with legacy systems is not required. It assumes that all operating systems within the enterprise are Windows XP SP3 or later and Windows Server 2003 SP2 or later. In such environments, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended technical controls.



HIGH SECURITY DC PROFILE

Platform: Windows Server 2008 x86 version 6.0

JRE: Oracle Corporation 1.7.0_21

Select Profile

Profile(s):

SSLF Domain Controller

Profile Description

This profile is used to define general settings that apply to both Domain Controller and Member server. Settings in this level are designed for systems in which security and integrity are the highest priorities, even at the expense of functionality, performance, and interoperability. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment.



HIGH SECURITY MEMBER PROFILE

Platform: Windows Server 2008 x86 version 6.0

JRE: Oracle Corporation 1.7.0_21

Select Profile

Profile(s):

SSLF Member Server

Profile Description

The Member Server profile specifies configuration recommendations specific to Windows 2008 Server instances that are joined to a domain and are not domain controllers. Settings in this level are designed for systems in which security and integrity are the highest priorities, even at the expense of functionality, performance, and interoperability. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment.

CIS BENCHMARK REPORT

- Report Title Page
- Summary
- Profiles
- Assessment Results
- Assessment Details:
 - Description: what is this setting
 - Rational: why to use this security setting
 - Remediation: how to secure it
 - Audit: how to confirm the setting is correct
 - References: resources for security issue



REPORT TITLE PAGE

Security Configuration Assessment Report for WIN-LZH4J5HVE96

CIS Microsoft Windows Server 2008 Benchmark v1.2.0.11

Enterprise Member Server
Sunday, June 2 2013 16:59:20



REPORT SUMMARY PAGE

Summary

Description	Tests			Scoring		
	Pass	Fail	Error	Score	Max	Percent
1 Recommendations	72	93	0	720.0	1650.0	44%
1.1 Account Policies	6	3	0	60.0	90.0	67%
1.2 Audit Policies	1	1	0	10.0	20.0	50%
1.3 Detailed Audit Policy	12	8	0	120.0	200.0	60%
1.4 Event Log	0	6	0	0.0	60.0	0%
1.5 Windows Firewall	0	15	0	0.0	150.0	0%
1.6 Windows Components\Windows Update	0	3	0	0.0	30.0	0%
1.7 User Account Control	6	3	0	60.0	90.0	67%
1.8 User Rights	20	9	0	200.0	290.0	69%
1.9 Security Options	27	32	0	270.0	590.0	46%
1.10 Terminal Services	0	3	0	0.0	30.0	0%
1.11 Internet Communication	0	6	0	0.0	60.0	0%
1.12 Additional Security Settings	0	4	0	0.0	40.0	0%
Total	72	93	0	720.0	1650.0	44%

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.



ACTUAL REPORTS

- Windows 2008 Server
- Windows 7



COURT CASES TO THINK ABOUT

- Vaughan v. Menlove, (1837) 3 Bing. N.C. 467, 132 E.R. 490 (C.P.)
 - Standard of care under negligence is not based on the judgment of each individual, but a reasonable person.
 - Defendant was warned of risk, but ignored it.
- The T.J. Hooper, 53 F.2d 107 (S.D.N.Y. 1931)
 - A party is liable for not using technology that is widely used and an accepted standard.
 - The lack of any legal statutes does not absolve any liability for not using current technologies.



So lets flip some bits and lock those assets down, what could go wrong?



Breaking things tends to anger the users



REMEMBER

Security is a balance of
several competing forces

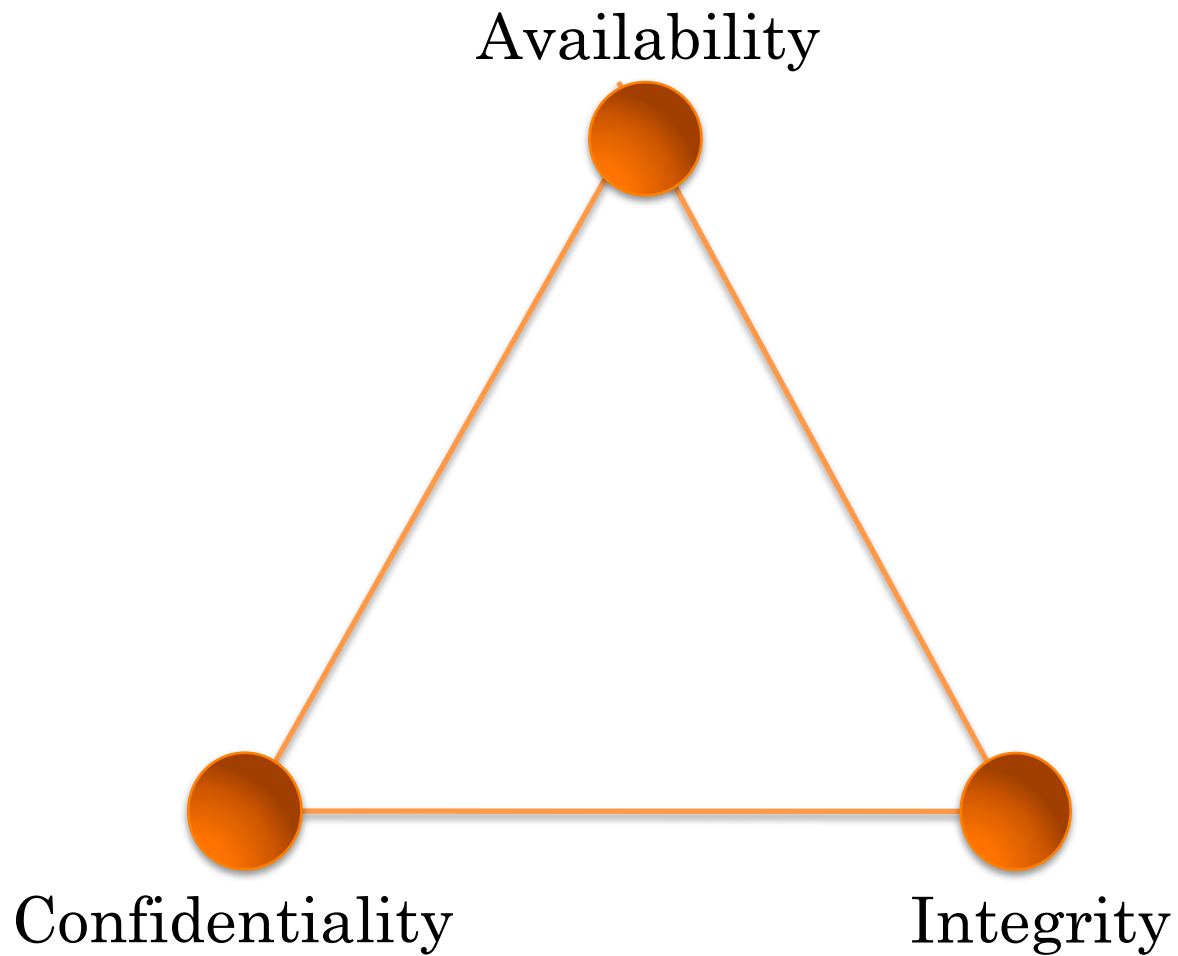


THREE MAIN SECURITY PRINCIPLES

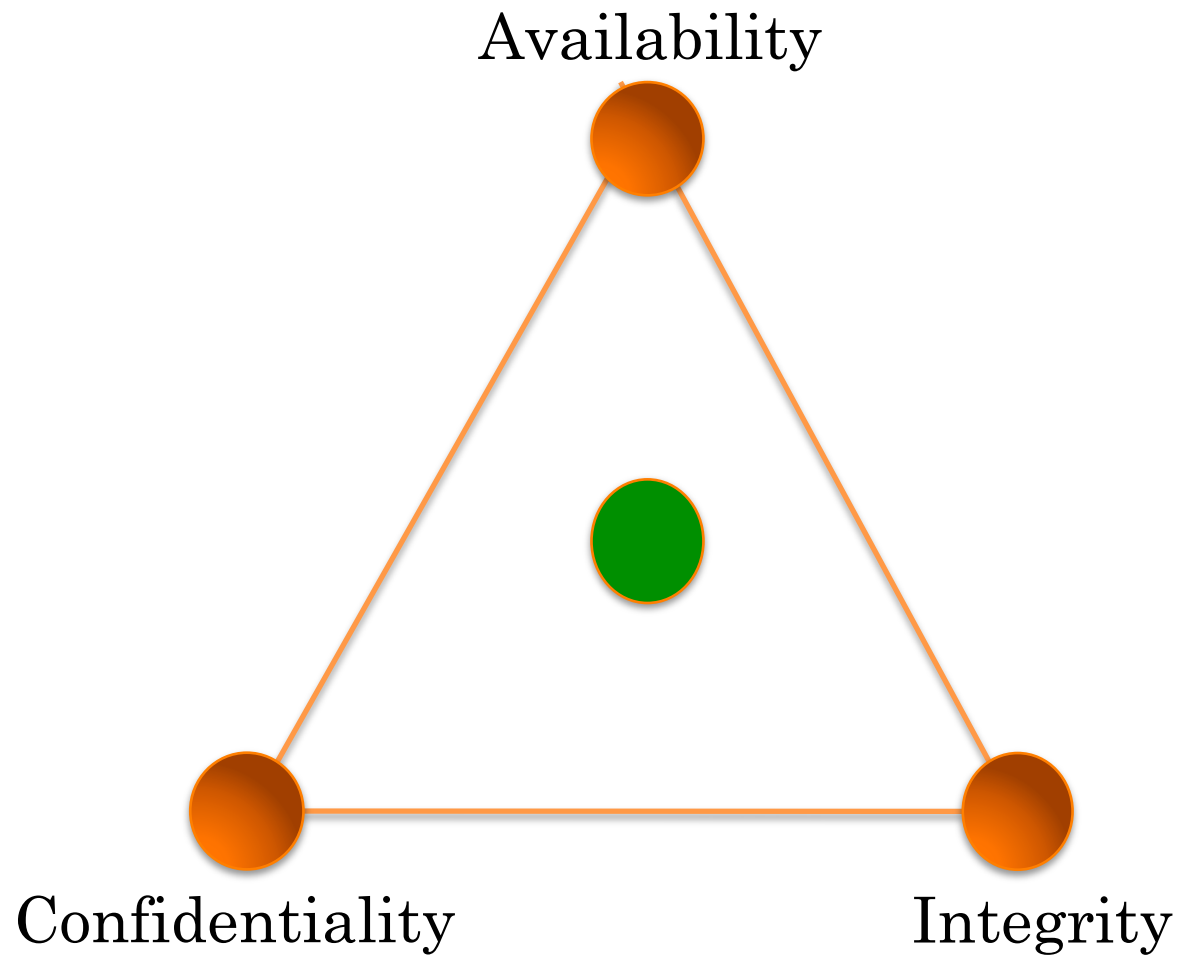
- Availability
- Integrity
- Confidentiality



SECURITY PRINCIPLE TRIANGLE



SECURITY SWEET SPOT DEPENDENT ON ORGANIZATIONS POLICIES



SECURITY TAKES PLANNING

- Allocate resources for using the CIS tools:
 - Time to research and understand benchmarks
 - Provide servers, desktops or vm's for testing
 - Time to implement security controls
- Develop a game plan to secure assets:
 - Secure the assets that are critical first?
 - Start with non-critical assets first as a pilot?
 - Secure new servers being deployed into production?
- Set a timeline:
 - It is important to get started, and not have it get pushed onto the back burner.
- Management needs to understand and support the initiative

