



[www.TrustedCS.com](http://www.TrustedCS.com)

## **Security Compliance Made Easy**

*Jamie Adams*  
*Senior Secure Systems Engineer*  
*Trusted Computer Solutions*

4/23/09



# What is the motivation for compliancy?



- Mandates by:
  - organization
  - management
  - industry
  
- Manage your own recognized risk
  
- All standards, mandated or implemented by choice, are based on lessons learned



## Security Compliance Made Easy – Goals



- Security Concepts
  - Security objectives: Confidentiality, Integrity, Availability
  
- Security Controls
  - Operational and Technical
  - Baselineing
  
- Security Blanket
  - Introduction to Security Blanket product
  - Implementing Security Blanket to ensure compliance within your enterprise

# Security Compliance



- Security Concepts recommended by the Federal Information Security Management Act (FISMA)
  - Information type or category<sup>1</sup>
  - Availability, Integrity, Confidentiality<sup>2</sup>
  - Potential impact to an organization's mission
- Mission Impact
  - Low – “...effect on organizational operations, organizational assets, or individuals”
  - Moderate – “...serious...”
  - High – “...severe or catastrophic...”
- Information Types
  - Public, investigative, administrative, and sensor information
- Security Categorization Applied to Information Systems

Information Systems	Confidentiality	Integrity	Availability
Public	N/A	Moderate	Moderate
Investigative	High	Moderate	Moderate
SCADA <sup>3</sup>	Low	High	High

<sup>1</sup> NIST FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems

<sup>2</sup> NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems

<sup>3</sup> SCADA: Supervisory Control and Data Acquisition

# Security Controls



- Security Controls as defined by FISMA
  - Operational:
    - System and Information Integrity (SI)
  - Technical:
    - Identification and Authentication (IA)
    - Access Control (AC)
    - Audit and Accountability (AU)
    - System and Communications Protection (SC)
  - Management
    - Policy and Procedure



# Reducing the Attack Surface



- Minimizing system services is crucial
- If a service or application must be used:
  - run as few features as possible
  - restrict access and tighten authentication as much as possible
  - divulge as little about the service as possible (i.e., do not disclose version)
- Identify system resource utilizations

# Industry Standard Security Guidelines



## → Government Guidelines

- U.S. Defense Information Systems Agency (DISA) UNIX Secure Technical Implementation Guidelines (STIGs), Release 1.16
- U.S. Joint Air Force Army Navy (JAFAN 6/3)
- U.S. Director Central Intelligence Directive (DCID 6/3)

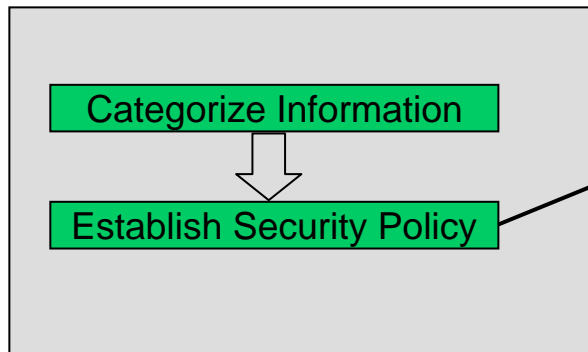
## → Industry Guidelines

- Center for Internet Security (CIS) Linux Benchmarks, v1.0.5/v1.1 and Solaris 10 Benchmark, v4.0
- SysAdmin, Audit, Network, Security (SANS) Institute
- Payment Card Industry Data Security Standard (PCI DSS), v1.1
- Critical Infrastructure Protection (CIP) from North American Electric Reliability Corporation (NERC)

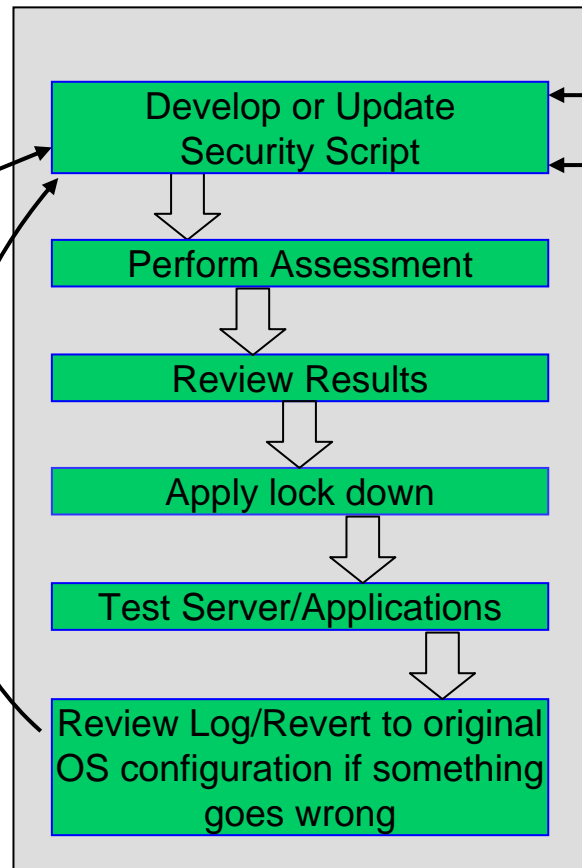
# Security Implementation Life Cycle



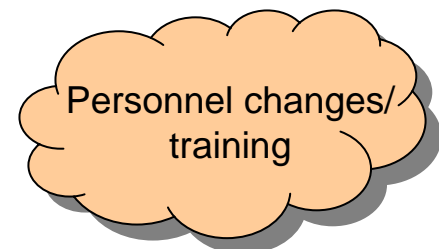
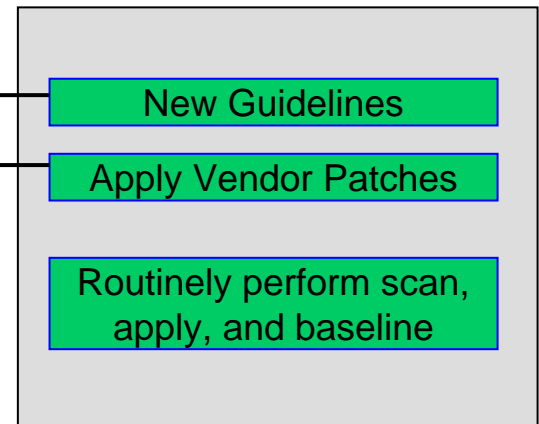
## Plan



## Implement



## Maintain



Green = Manual processes

# Security Access Controls



## → Access Controls: Password Policy

### Password Policy

#### Aging

Specify when users must change their passwords and how often they can change them.

Expiration  days

Expiration warning  days

Max days between changes  days

Min days between changes  days

Set Aging on Active Accounts

Expired Password Invalidation

#### Composition

Require newly chosen passwords to adhere to the following rules:

No Empty Passwords

Minimum Length  characters

At least two lowercase letters

At least two uppercase letters

At least two numbers

At least two special characters

Limit Password Reuse

No Plus Entries in Password Files

# Security Access Controls



## → Access Controls: System File and Directory Permissions

### **Directory and File Permissions**

#### **System Directories and Files**

*Ensure vital system files and directories are secure; in most cases these modules are just enforcing the operating system defaults.*

- Password Repository Permissions (e.g., `/etc/shadow`)
- System Configuration File Permissions (e.g., `/etc/*`)
- Sysctl.conf Permissions
- System Command File Permissions (e.g., `/sbin/*`)
- Secure Shell Binaries (e.g., `/usr/bin/bash`)
- System Library File Permissions (e.g., `/lib/*`)
- System Log File Permissions (e.g., `/var/log/*`)
- System Device Directory Ownership (e.g., `/dev/*`)
- System Run Control Script Permissions (e.g., `/etc/init.d/*`)
- Secure SUID/SGID Executables
- Crontab Perms
- Restrict Write-Access on Man Pages

#### **Other**

- Secure World Writable Files
- Secure World Writable Directories
- Secure Unowned Files
- Correct Uneven File Permissions
  
- Secure Audio Devices (`/dev/audio*`)
- InterNetNews Config File Perms

#### **Rules for new files (creation masks)**

- Default umask
- Set FTP Umask (gssftp)
- Daemon Umask

#### **Account Specific**

- Root Home Directory Permissions
- Home Directory Permissions
- Home Directory Ownership
- Home Directory Contents
- User Dot File Perms (e.g., `$/HOME/profile`)
- Secure Netrc Files (`$/HOME/netrc`)

# The Challenge of Compliance

(Do you have a headache yet?)



I know that consultants are an option but they're expensive. What happens when we make changes after they leave?

My background is in Windows. How am I going to secure all of these Linux and Solaris servers?

I don't have time to take classes on this stuff.

Uh oh. Joe's on vacation. Now how did he lock down that new server?

Yikes, they just released new STIGs. I'll have to update my scripts AGAIN!

Scripts are available but they don't support the policy.

I don't have the time to read books on OS lock down and if I did, what if I make a mistake?

Whew! It took me all week to lock down one box. Only 25 more boxes to go ☹

50 new servers just arrived and you want them locked down by when?

# Security Blanket



Security Blanket lock down software from TCS can automatically assess, configure & measure your Linux and Solaris systems for the level of security you decide they should have.

Security Blanket supports lock down guidelines published by some of the most respected security industry leaders in the World.

- Defense Information Systems Agency (DISA) UNIX Secure Technical Implementation Guidelines (STIGs)
- Center for Internet Security (CIS)
- SysAdmin, Audit, Network, Security (SANS) Institute
- Payment Card Industry Data Security Standard (PCI DSS)
- Critical Infrastructure Protection (CIP)
- Joint Air Force Army Navy (JAFAN)
- Director of Central Intelligence Directive (DCID) 6/3

# Security Blanket Life Cycle



## Plan

Establish Security Policy

## Implement

Install or Update Security Blanket

Review Modules Guide

Create/Modify Profile

Perform Scan

Review Assessment Report

Apply the Profile

Test Server/Applications

Review Log and perform Undo (if applicable)

## Maintain

New Guidelines

Apply Vendor Patches

Routinely perform scan, apply, and baseline

Personnel changes/  
training

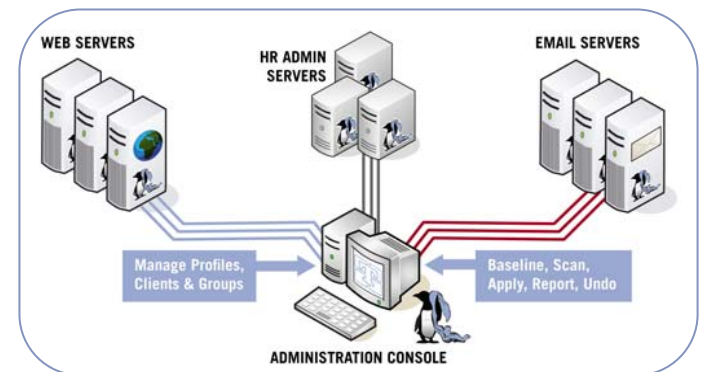
Green = manual processes

Blue = Security Blanket automation

# Security Blanket Enterprise Edition



- Administration Console is a web-based application
- Developed for organizations with a large number of Linux and/or Solaris servers that need to be functionally grouped and managed as groups
- Lock down is consistently applied to all servers within the defined group
- Supported Operating Systems:
  - Red Hat Enterprise Linux (RHEL) 4 and 5
  - CentOS 4 and 5
  - Oracle Enterprise Linux (OEL) 4 and 5
  - Solaris 10 (SPARC & x86)
  - Console requires RHEL 5, CentOS 5, or OEL 5
- ❖ Additional OS support for 2009:
  - ❖ Fedora 10
  - ❖ zSeries (RHEL, CentOS, or OEL 5.2+)
  - ❖ Novell SUSE



# Security Blanket Benefits



- Consistency - Automatic OS configuration ensures consistent lock down of all servers in a group or an enterprise. Groups can contain both Linux and Solaris servers in the same group.
- Reliability - Ensures system compliancy even when the application of patches changes the system configuration resulting in compromised security.
- Assurance – Regularly assessing security posture, baselining systems, and comparing baselines establishes audit trails to track changes to server environment.
- Manageability – centralized administration via the Console.
- Flexibility – Web based console allowing network access from any location.

**Enormous Time & Cost Savings!**

# Security Blanket Profiles



- Way of implementing an organization's security policy
- High-level policies are implemented across multiple operating systems
- Profiles allow full compliancy or adjustments to policy areas to address mission requirements
- Mix and match compliancy models to obtain the optimal policy for your organization

# Security Modules



- Auditing and Logging
  - Enabling auditing subsystem and setting audit rules
- System and User Account Protections
  - Password aging, unused accounts, misconfigured system accounts, duplicate uids, etc.
- Networking
  - Disable IP forwarding, enable reverse path source validation, ignoring ICMP ECHO and TIMESTAMP requests
- Web and Database Servers
  - Strengthening PHP settings, disabling or enabling web and database services.
- Other
  - Restricting the use of certain tools such as compilers or ping

## Sample Modules

Cron Logging	<input type="checkbox"/>		<a href="#">Help</a>
Enable vsftpd Additional Logging	<input type="checkbox"/>		<a href="#">Help</a>
Secure Authpriv Logging	<input type="checkbox"/>		<a href="#">Help</a>
Maximum Time Between Password Changes	<input type="checkbox"/>	<input type="text" value="60"/> days	<a href="#">Help</a>
Password Policy Length Minimum	<input type="checkbox"/>	<input type="text" value="9"/> characters	<a href="#">Help</a>
Limit Password Reuse	<input type="checkbox"/>	<input type="text" value="5"/> times	<a href="#">Help</a>
No Empty Passwords	<input type="checkbox"/>		<a href="#">Help</a>
Minimum Delay Between Password Changes	<input type="checkbox"/>	<input type="text" value="1"/> days	<a href="#">Help</a>
Password Policy Lowercase Minimum	<input type="checkbox"/>		<a href="#">Help</a>

# Security Blanket Life Cycle



## Plan

Establish Security Policy

## Implement

Install or Update Security Blanket

Review Modules Guide

Create/Modify Profile

Perform Scan

Review Assessment Report

Apply the Profile

Test Server/Applications

Review Log and perform Undo (if applicable)

## Maintain

New Guidelines

Apply Vendor Patches

Routinely perform scan, apply, and baseline

Personnel changes/  
training

Green = manual processes

Blue = Security Blanket automation

# Security Reporting and Change Control



- Reporting
  - Assessments (standalone and group)
  - Baseline reports and comparisons
  - XML used in reporting
  
- Change control support
  - Detailed Audit logs
  - Baseline reports

# Assessment Report



Filter

Module Details

Cross Reference


Not Applicable  
OS Not Applicable  
Zone Not Applicable

Security Module	Result	Severity Level
<b>Audit</b>		
▶ Enable the Audit Subsystem	Pass	High
▶ Audit Log Rotation	Pass	Medium
▼ Audit Rules Configures the audit subsystem to record security-relevant events such as file access, file deletions, login, logouts, session initiations, discretionary access control changes, and administrative actions.	Pass	Medium
UNIX STIG GEN002820 GEN002720 GEN002740 GEN002760 GEN002800 GEN002820		
DCID 4.B.1.b(2)(d)(1) 4.B.1.b(2)(d)(2) 4.B.1.b(2)(d)(3) 4.B.1.b(2)(a) 4.B.2.a(5)(a) 4.B.3.a(8)(a)		
JAFAN 4.B.1.b(2)(d)(1) 4.B.1.b(2)(d)(2) 4.B.1.b(2)(d)(3) 4.B.1.b(2)(a) 4.B.2.a(5)(a) 4.B.3.a(8)(a)		
NERC/FERC CIP-005-1-R3 CIP-007-1-R5.1.2 PCI DSS 10.2.2 10.3		
▶ Cron Logging	Pass	Medium
▶ Enable vsftpd Additional Logging	Not Applicable	High
▶ Secure Shell	Pass	Medium
<b>Password Policy</b>		
▶ Maximum Time Between Password Changes	Pass	High
▶ Password Policy Length Minimum	Pass	High
▶ Limit Password Reuse	Pass	High


# Automatic Lock Down (Remediate to Compliance)



## Initial Scan Results

Group Assessment Report			
Creation Date: 2008-11-24 11:05:49			
Group Name: HRAdmin			
Module	Severity Level	Result	
<b>Audit</b>			
▶ Enable the Audit Subsystem	High	HR Svr1	<b>FAIL</b>
		HR Svr2	<b>FAIL</b>
▶ Audit Log Rotation	Medium	HR Svr1	Pass
		HR Svr2	Pass
▶ Audit Rules	Medium	HR Svr1	Pass
		HR Svr2	Pass
▶ System Accounting	Medium	HR Svr1	Not Applicable
		HR Svr2	Not Applicable
▶ Cron Logging	Medium	HR Svr1	<b>FAIL</b>
		HR Svr2	<b>FAIL</b>
▶ Enable vsftpd Additional Logging	High	HR Svr1	Not Applicable
		HR Svr2	Not Applicable
▶ Secure Authpriv Logging	Medium	HR Svr1	<b>FAIL</b>
		HR Svr2	<b>FAIL</b>
<b>Password Policy</b>			
▶ Maximum Time Between Password Changes	High	HR Svr1	Pass
		HR Svr2	Pass
▶ Password Policy Length Minimum	High	HR Svr1	<b>FAIL</b>
		HR Svr2	<b>FAIL</b>

## Post Apply Scan Results

Group Assessment Report			
Creation Date: 2008-11-24 11:14:51			
Group Name: HRAdmin			
Module	Severity Level	Result	
<b>Audit</b>			
▶ Enable the Audit Subsystem	High	HR Svr1	Pass
		HR Svr2	Pass
▶ Audit Log Rotation	Medium	HR Svr1	Pass
		HR Svr2	Pass
▶ Audit Rules	Medium	HR Svr1	Pass
		HR Svr2	Pass
▶ System Accounting	Medium	HR Svr1	Not Applicable
		HR Svr2	Not Applicable
▶ Cron Logging	Medium	HR Svr1	Pass
		HR Svr2	Pass
▶ Enable vsftpd Additional Logging	High	HR Svr1	Not Applicable
		HR Svr2	Not Applicable
▶ Secure Authpriv Logging	Medium	HR Svr1	Pass
		HR Svr2	Pass
<b>Password Policy</b>			
▶ Maximum Time Between Password Changes	High	HR Svr1	Pass
		HR Svr2	Pass
▶ Password Policy Length Minimum	High	HR Svr1	Pass
		HR Svr2	Pass

# Audit Logs



## → Security Blanket Audit Log

Logs are plain text and access is restricted to root. They can be remotely retrieved by the Enterprise Console over TLS.

```
2009 Apr 03 11:29:53 [CrontabPerms] INFO: ----- Initiating Scan -----
2009 Apr 03 11:29:53 [CrontabPerms] NOTICE: Scan Failed: /etc/crontab has permissions of 644 instead of 400
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /var/spool/cron with permissions of 700, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.daily with permissions of 700, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.daily/makewhatis.cron with permissions of 700, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.hourly with permissions of 700, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.hourly/inn-cron-rnews with permissions of 700, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.hourly/mcelog.cron with permissions of 700, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.hourly/inn-cron-nntpsend with permissions of 700, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.deny with permissions of 600, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.d with permissions of 700, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.d/sa-update with permissions of 600, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.monthly with permissions of 700, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.monthly/0anacron with permissions of 700, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] DEBUG: Found /etc/cron.allow with permissions of 600, owner 'root', and group 'root'
2009 Apr 03 11:29:53 [CrontabPerms] NOTICE: Scan Failed.
2009 Apr 03 11:29:53 [CrontabPerms] INFO: ----- Initiating apply change -----
2009 Apr 03 11:29:53 [CrontabPerms] NOTICE: Apply Performed: /etc/crontab : Set owner to 'root', group to 'root', and permissions to 400
2009 Apr 03 11:29:53 [CrontabPerms] NOTICE: Apply Performed: Permissions and ownership of crontab files changed.
2009 Apr 03 11:29:53 [CrontabPerms] INFO: ----- Initiating undo change -----
2009 Apr 03 11:29:53 [CrontabPerms] NOTICE: Undo Performed: /etc/crontab : Owner reset to 'root', group reset to 'root', and permissions reset to 644
2009 Apr 03 11:29:53 [CrontabPerms] NOTICE: Undo Performed: Permissions and ownership of crontab files restored.
```

# Baselines



## → Baseline Reports

- All installed packages
- Cryptographic checksums (SHA1) of /bin, /lib, /etc, and more
- PCI Devices
- USB Buses and Devices
- BIOS Memory and Known Entry End Points
- DMI/SMBIOS Table
- IPTables and Network Interfaces and Routing

## → Baseline Comparison Reports

- Same machine from two points in time
- Two different machines
- XML Format

# Client Baseline Report



Baseline Report	
HRSvr1 System Information	
Creation Date: 2008-11-18 21:13:38	Client name: HRSvr1
Kernel: 2.6.18-92.el5	
Report Summary	
4 Hardware Reports 2 Network Reports 4 File Reports 811 Software Package Reports	
Hardware	
PCI Devices	<pre>00:00.0 Host bridge: Intel Corporation 82G33/G31/P35/P31 Express DRAM Controller (rev 02) 00:01.0 PCI bridge: Intel Corporation 82G33/G31/P35/P31 Express PCI Express Root Port (rev 02) 00:02.0 VGA compatible controller: Intel Corporation 82G33/G31 Express Integrated Graphics Controller (rev 02) 00:19.0 Ethernet controller: Intel Corporation 82562V-2 10/100 Network Connection (rev 02) 00:1a.0 USB Controller: Intel Corporation 82801I (ICH9 Family) USB UHCI Controller #4 (rev 02) 00:1a.1 USB Controller: Intel Corporation 82801I (ICH9 Family) USB UHCI Controller #5 (rev 02) 00:1a.2 USB Controller: Intel Corporation 82801I (ICH9 Family) USB UHCI Controller #6 (rev 02) 00:1a.7 USB Controller: Intel Corporation 82801I (ICH9 Family) USB2 EHCI Controller #2 (rev 02) 00:1b.0 Audio device: Intel Corporation 82801I (ICH9 Family) HD Audio Controller (rev 02) 00:1d.0 USB Controller: Intel Corporation 82801I (ICH9 Family) USB UHCI Controller #1 (rev 02) 00:1d.1 USB Controller: Intel Corporation 82801I (ICH9 Family) USB UHCI Controller #2 (rev 02) 00:1d.2 USB Controller: Intel Corporation 82801I (ICH9 Family) USB UHCI Controller #3 (rev 02) 00:1d.7 USB Controller: Intel Corporation 82801I (ICH9 Family) USB2 EHCI Controller #1 (rev 02) 00:1e.0 PCI bridge: Intel Corporation 82801 PCI Bridge (rev 92) 00:1f.0 ISA bridge: Intel Corporation 82801IR (ICH9R) LPC Interface Controller (rev 02) 00:1f.2 RAID bus controller: Intel Corporation 82801 SATA RAID Controller (rev 02) 00:1f.3 SMBus: Intel Corporation 82801I (ICH9 Family) SMBus Controller (rev 02)</pre>
	<pre>Bus 002 Device 001: ID 0000:0000 Device Descriptor:   bLength           18   bDescriptorType   1   bcdUSB            2.00   bDeviceClass      9  Hub   bDeviceSubClass   0  Unused   bDeviceProtocol   1  Single TT   bMaxPacketSize0  64   idVendor          0x0000   idProduct         0x0000   bcdDevice         2.06   iManufacturer     3  Linux 2.6.18-92.el5 ehci hcd</pre>



# Baseline Comparison



## Baseline Comparison Report



First Client Report: HRSvr1 2009-03-23 13:56:32

Second Client Report: HRSvr2 2009-03-23 13:02:07

### Change Summary

Hardware and Network Differences: 4

File Differences: 4

Software Differences: 882

### Hardware and Network

IPtables	Changes detected
USB Buses and Devices	Changes detected
DMI/SMBIOS Table	Changes detected
PCI Devices	No changes
Routing	No changes
BIOS Memory and Known Entry Points	Changes detected

### Files

System Libraries	Changes detected
System Binaries	Changes detected
Devices - /dev	Changes detected
System Configuration Files - /etc, /usr/local/etc	Changes detected

### Software

#### Additions - Found in first report but not in the second

automake-1.9.6	A GNU tool for automatically creating Makefiles.
libuser-devel-0.54.7	Files needed for developing applications which use libuser.
kudzu-devel-1.2.57.1.17	Development files needed for hardware probing using kudzu.
newt-devel-0.52.2	Newt windowing toolkit development files.
compat-libstdc++-296-2.96	Compatibility 2.96-RH standard C++ libraries
rpm-build-4.4.2	Scripts and executable programs used to build packages.
xmlsec1-devel-1.2.9	Libraries, includes, etc. to develop applications with XML Digital Signatures and XML Encryption support.
boost-1.33.1	The Boost C++ Libraries
ecryptfs-utils-41	The eCryptfs mount helper and support libraries
frysk-0.0.1.2008.03.19.rh1	Frysk execution analysis tool
dbus-devel-1.0.0	Libraries and headers for D-BUS

## Baseline Comparison

Compare two baselines for the same server or compare the baselines from two different servers to see what differences exist

Changes - Found in both reports but versions are different	
xorg-x11-xfs-1.0.2	X.Org X11 xfs font server
libXfixes-4.0.1	X.Org X11 libXfixes runtime library
dmidecode-2.7	Tool to analyse BIOS DMI data.
bitstream-vera-fonts-1.10	Bitstream Vera Fonts
sendmail-8.13.8	A widely used Mail Transport Agent (MTA).
eog-2.16.0.1	Eye of GNOME image viewer
atk-1.12.2	Interfaces for accessibility support
PyQt-3.16	Python bindings for Qt
parted-1.8.1	The GNU disk partition manipulation program.
cpuspeed-1.2.1	CPU Frequency adjusting daemon.
conman-0.1.9.2	ConMan - The Console Manager
isdn4k-utils-3.2	Utilities for configuring an ISDN subsystem.
kernel-headers-2.6.18	Header files for the Linux kernel for use by glibc
pam_ccreds-3	Pam module to cache login credentials
minicom-2.1	A text-based modem control and terminal emulation program.
procps-3.2.7	System and process monitoring utilities.
lrzsz-0.12.20	The lrz and lsz modem communications programs.
mkbootdisk-1.5.3	Creates a boot floppy disk for booting a system.
mutt-1.4.2.2	A text mode mail user agent.
libXrandr-1.1.1	X.Org X11 libXrandr runtime library
liboil-0.3.8	Library of Optimized Inner Loops, CPU optimized functions
xorg-x11-drv-vmouse-12.4.0	Xorg X11 vmouse input driver
gtksourceview-1.8.0	A library for viewing source files
xorg-x11-drv-tseng-1.1.0	Xorg X11 tseng video driver
pango-1.14.9	System for layout and rendering of internationalized text
rhythmbox-0.9.5	Music Management Application
cyrus-sasl-2.1.22	The Cyrus SASL library.
gnome-python2-canvas-2.16.0	Python bindings for the GNOME Canvas.

## Security Compliance Made Easy - Summary



- Compliance can be mandated by an organization, management or industry, or is a way to manage your own recognized risk
- Understanding security concepts is crucial to developing a solid security strategy
- Managing security controls is key to reducing risk
- Regularly validating security posture via assessments and baselines provides compliance assurance or identifies changes to the security posture
- Security Blanket is the only enterprise platform that automatically configures your OS to meet industry standards - - consistently, and predictably, in a fraction of the time that it takes to lock down manually.



# Testimonials



*"I have been buttoning down secure UNIX OS's for over a decade. I always considered it a black art and a major pain. No more. It is all over. I am not joking when I say that Security Blanket demystified the whole process. It is easy to use, extremely flexible and should be used by anyone who really is interested in securing their machine and keeping it that way. The other key point is its ability to automatically on a scheduled basis check to see that all is still in order. I am amazed it could be this simple. Thank you."*

*Daniel Halstead, Engineer  
Department of Defense*

*"Thanks to Security Blanket, I was able to lock down all 18 of my classified servers in one day. Prior to using Security Blanket, locking down one server would have taken an entire week. It was so easy to create a custom profile by modifying the default DISA STIG profile for our specific site needs. Now I have a custom security profile that I can use for all of my servers. Having the ability to automatically run weekly baseline reports is also a big time saver! Now that I am using Security Blanket, I have more time to focus on mission critical tasks and projects".*

*Principal Field Support Engineer  
National Test Range*



Voted "Best Security Product"

# TCS Contact Information



To take advantage of our FREE trial, go to:

[www.TrustedCS.com/SecurityBlanket/SecurityBlanket-Try-Out](http://www.TrustedCS.com/SecurityBlanket/SecurityBlanket-Try-Out)



To Buy Security Blanket:

Contact Ryan Stowell

[ryan.stowell@carahsoft.com](mailto:ryan.stowell@carahsoft.com)

703-871-8529



For more information

Contact Ryan Stowell

Carahsoft

[ryan.stowell@Carahsoft.com](mailto:ryan.stowell@Carahsoft.com)

703-871-8529



# Upcoming TCS Webinars



**Coming soon:** Additional webinars are scheduled to provide further guidance for planning and implementing OS Security and maintaining OS compliance as environments change. These webinars will be presented by Trusted Computer Solutions, and hosted by Carahsoft. **Save these dates!**

**“Planning and Implementing OS Security”**  
June 25, 2009 @ 11:00 am EST

**“Maintaining OS Security”**  
August 20, 2009 @ 11:00 am EST

