

Trusted Computer Solutions – Welcome



Trusted Computer Solutions

presents:

Fast, Reliable, and Consistent Operating System (OS) Security Planning and Implementing Enterprise Compliance

This web seminar will begin promptly at 11:00 am ET

Thank you for joining us – please stand by.

Trusted Computer Solutions



- Founded in 1994, in Herndon, VA
- Approximately 125 employees in VA, TX, and IL
- Experience building security products that meet the most stringent security requirements mandated by the Intelligence Community & Federal government.
- Products Accredited and in Operational use today protecting our nation's most valuable digital assets
- Solutions include:
 - Cross Domain Solutions for DoD, Intelligence Community and Civilian Government
 - Operating System Automated Lock Down tools
 - Network Security solutions

Today's Presenter: Jamie Adams



- Senior Secure Systems Engineer at Trusted Computer Solutions for almost 2 years
- Lead developer on the Security Blanket product
- 20 years experience as a software developer and systems engineer for classified and unclassified systems
- Involved in the design, deployment, operation and accreditation of large scale, highly available mission critical systems in both the public and private sectors
- Performed 8 years of active duty as a Cryptologist/Submariner for the U.S. Navy





www.TrustedCS.com

Fast, Reliable, and Consistent OS Security
Planning and Implementing Enterprise Compliance



Jamie Adams
Senior Secure Systems Engineer
Trusted Computer Solutions

6/10/09



Planning and Implementing Enterprise Compliance



Discussion Topics:

- Information Categories and Security Objectives
- Operational, Technical, and Management Security Controls
- Deployment Scenarios
- Best practices for maintaining enterprise-wide OS security
- Security Blanket overview

Information Categories/Security Objectives



- Security Concepts recommended by the Federal Information Security Management Act (FISMA)
 - Information type or category¹
 - Availability, Integrity, Confidentiality²
 - 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 ³	Low	High	High

¹ NIST FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems

² NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems

³ 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



Security Controls – Best Practices



- 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

Security Controls: Operational & Management



→ Typically, operational and management controls are policy or procedure related, or dependent on physical infrastructure requirements

Examples:

→ Policy - background checks on personnel

→ Procedure - backup tapes are stored offsite

→ Physical infrastructure - card key/badge access systems installed

Security Controls: Technical Controls



- Password Aging
 - Maximum Time Between Password Changes
 - Expired Password Invalidation
 - Minimum Delay Between Password Changes
 - Password Expiration Warning
 - Limit Password reuse

- Password Length and Composition
 - Password Policy Length Minimum
 - No Empty Passwords
 - Password Policy Lowercase Minimum
 - Password Policy Numeric Minimum
 - Password Policy Special Characters
 - Password Policy Uppercase Minimum

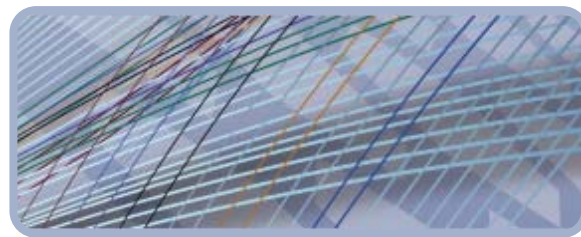
- Enforcing the Policy

Deployment Scenarios



- Lock down of master image
- Parent-to-child organization hand-off
- OEM or Integrators shipping to customers
 - Network Attended Storage (NAS)
- Virtual environments (continual turnover)
 - zSeries
 - ESX
 - VMWare

Deployment Challenges



- Determining the security policy for your organization
- Keeping systems locked down
- Knowing what has changed
- Ensuring updates are consistently deployed
- Easy, nimble repurposing of systems

Maintaining Operational Security



- Deployment scenarios should monitor and maintain security
 - Perform baseline when system is first built
 - Compare baselines to detect configuration drift
 - Patch management changes system configuration
 - Multiple System Administrators making changes
- Information Assurance
 - New guidelines and threats
 - Compliance evidence

Security Blanket



Security Blanket from Trusted Computer Solutions is the only enterprise platform that automatically configures your Linux and Solaris operating systems to meet industry standard and customized security requirements. Security Blanket consistently and predictably secures your enterprise-wide systems in a fraction of the time it takes to lock them down manually.

Security Blanket Workflow



**SECURITY
BLANKET**
BY TCS
TM

ENTERPRISE EDITION WORKFLOW

DEFINE THESE...

Clients

Profiles

Groups

NOW YOU CAN...

Associate a Profile
with a Group

Scan a Client
or Group

Run an Assessment
Report

Apply a Client or
Group Lock Down

OR

Undo a Client or
Group Lock Down

YOU CAN ALSO...

Run a Group
Baseline

View a
Baseline Report

Run a Baseline
Comparison Report

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

- Defense Information Systems Agency (DISA) UNIX Security Technical Implementation Guide (STIG)
- Center for Internet Security (CIS) RHEL and Solaris Benchmarks
- SysAdmin, Audit, Network, Security (SANS) Institute Top 20 Security Risks
- Payment Card Industry (PCI) Data Security Standard (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 Reporting and Change Control



- Reporting
 - Assessment Reports (standalone and group)
 - Baseline Reports and comparisons
 - XML used in reporting

- Change control support
 - Detailed Audit logs
 - Baseline Reports

Assessment Report



Security Module	Result	Severity Level
Audit		
▶ 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 Auth	Pass	Medium
Password Policy		
▶ Maximum Time Between Password Changes	Pass	High
▶ Password Policy Length Minimum	Pass	High
▶ Limit Password Reuse	Pass	High

Filter

Module Details

Cross Reference

Not Applicable
OS Not Applicable
Zone Not Applicable

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

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

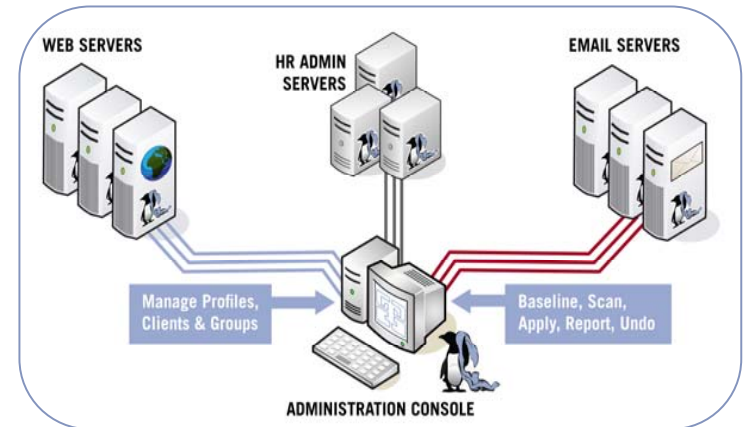
Baseline Comparison Report	
First Client Report: HRSvr1	2009-03-23 13:56:32
Second Client Report: HRSvr2	2009-03-23 13:02:07
Change Summary	
Hardware and Network Differences: 4	
File Differences: 4	
Software Differences: 882	
Hardware and Network	
IPtables	Changes detected
USB Buses and Devices	Changes 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

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
dmidcode-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 Blanket Enterprise Edition



- Administration Console is a web-based application
- Developed for organizations with a large number of Linux and/or Solaris servers that have common functionality and/or require the same security settings
- 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 5.2+)
 - ❖ Novell SUSE



Planning & Implementing Enterprise Compliance - Summary



- Categorization of information is critical for effective security implementation
- Choosing the right security controls to meet policy while not hindering system functionality
- Same security challenges apply to all deployment scenarios
- Security Blanket is the only enterprise solution that automatically configures the OS and creates the information assurance reports to meet industry standard guidelines



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."

*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*

"With Security Blanket I can lock down a Linux or Solaris system to DISA STIG compliance in under a minute. The ability to reverse the security implementation one security module at a time is a great feature in order to ensure the system is in a usable state and still sustain the highest level of security possible.

Before Security Blanket, I would have to maintain scripts and "hand jam" changes. The task of locking down a system was a long and drawn out process that could take days. Even then my systems were not as secure as they are with Security Blanket. Security Blanket can turn even the most novice Linux/Solaris administrators into System Security Professionals."

*Senior Engineer
Intelligence Community*



Best Security Product

TCS Contact Information



To take advantage of our FREE trial, go to:
www.TrustedCS.com/SecurityBlanket



To Buy Security Blanket:
Contact Tony Murphy
TMurphy@TrustedCS.com
703-537-4373



For more information
Contact Tony Murphy
TMurphy@TrustedCS.com
703-537-4373



Upcoming TCS Webinars



Coming soon: Additional webinars presented by Trusted Computer Solutions.
Save these dates!

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

“Does OS Security Frighten You?”
October 29, 2009 @ 11:00 am EST

**“The DISA UNIX STIGs - Supporting a
Defense in Depth Strategy”**
September 9, 2009 @ 11:00 am EST

“Security in the Virtual Environment”
November 14, 2009 @ 11:00 am EST

**“Critical Infrastructure Protection –
Maintaining Compliancy?”**
October 7, 2009 @ 11:00 am EST

