Information Security Overview

CIA Model, Policies and Standards, Cryptography, VPN and PKI

Security Solutions for different technologies:

Cisco Systems and Sun Microsystems

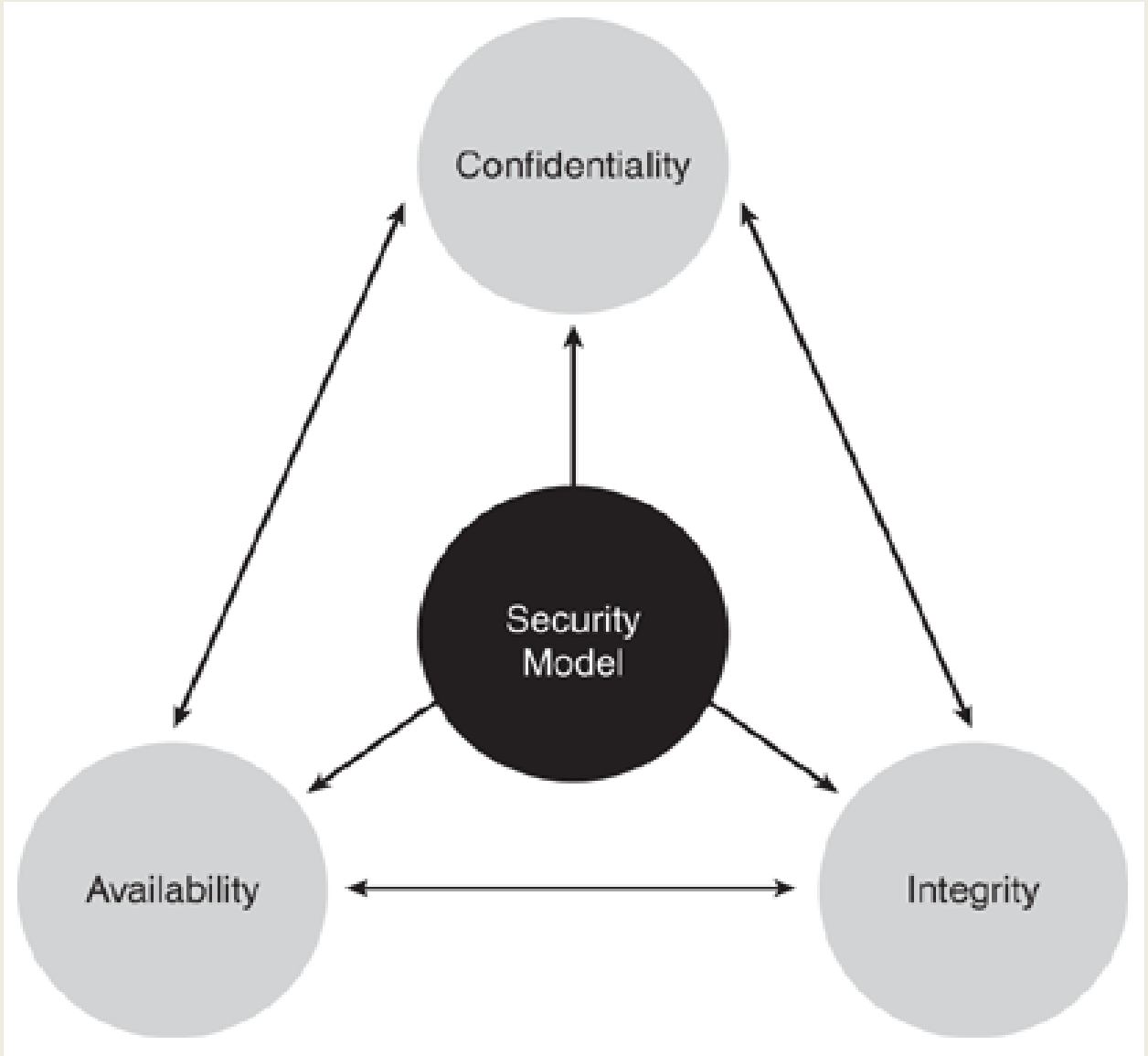
By Norik Simonyan

Objectives

Hardware and Software Security solutions
- **Hardening Cisco Devices**
- **Cisco IOS Firewall**

Securing Solaris 10
- **Role-based access control (RBAC).**
- **Basic Audit Reporting Tool (BART).**
- **Solaris Security Toolkit (SST)**
- **Some Useful Links**

The CIA Model



Confidentiality

Confidentiality (Cryptography and encryption, VPN …)

Confidentiality Attacks

Packet capture
Ping sweep and port scan
Dumpster diving
Electromagnetic interference (EMI) interception
Wiretapping
Social engineering
Sending information over overt channels
Sending information over covert channels

Integrity

Integrity (md5, certificates…**)**

Integrity Attacks

Salami attack: This is a collection of small attacks that result in a larger attack when combined.
Data diddling: The process of data diddling changes data before it is stored in a computing system.
Trust relationship exploitation: Different devices in a network might have a trust relationship between themselves.
Password attack(Trojan horse, Packet capture, Keylogger, Brute force, Dictionary attack, Botnet, Hijacking a session)

Availability

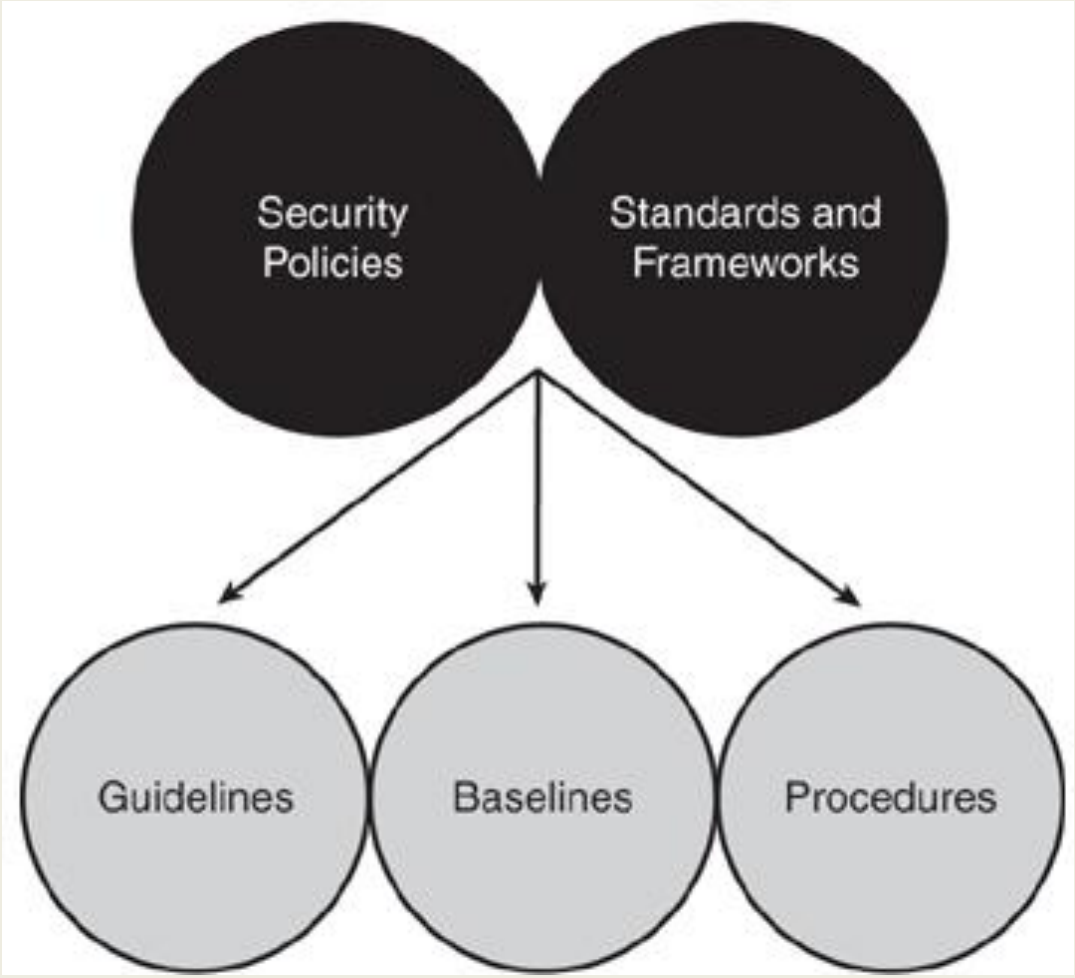
Availability (failover, backups…**)**

Availability Attacks

Denial of service (DoS)
Distributed denial of service (DDoS)
TCP SYN flood
ICMP attacks
Electrical disturbances (Power spike, Electrical surge, Power fault, Blackout, Power sag, Brownout)
Attacks on a system's physical environment (Temperature, Humidity, Gas)

Security Policy

Policies, Standards, Procedures, Baselines, Guidelines:



Security Implementation

Security Wheel:

- Secure
- Monitor and respond
- Test
- Manage and Improve

Main parts of network security

- Risk Analysis, Management, and Avoidance
- Factors Contributing to a Secure Network Design
- User Awareness and Training

Security Policy Responsibilities in a company

- Chief Security Officer (CSO)
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)

Some Security Product Vendors

ThreatGuard

TENABLE Network Security

secure elements

McAfee

symantec.

ManTech International Corporation

Premier Data Services

G2

Cryptography

Cryptographic Algorithms

- **Symmetric key cryptography** (also known as secret key or preshared key cryptography):
- **Asymmetric key Cryptography** (also known as public Key cryptography):
- **Hash algorithm** (or hash function):

Symmetric and Asymmetric Key Cryptography

Symmetric Key Cryptography

Data Encryption Standard (DES):

Triple-DES (3DES):

Advanced Encryption Standard (AES):

Asymmetric Key Cryptography

RSA:

Diffie-Hellman (DH):

Digital Signature Algorithm (DSA):

Public-Key Cryptography Standards (PKCS):

Hash Algorithm

Hash Algorithm

Message Digest (MD) algorithms:
MD2 (see RFC 1319):
MD4 (see RFC 1320):
MD5 (see RFC 1321):
Secure Hash Algorithm (SHA):
SHA-1 (see RFC 3174): (Transport Layer Security (TLS), Secure Sockets Layer (SSL), Pretty Good Privacy (PGP), Secure Shell (SSH), Secure Multipurpose Internet Mail Extension (S/MIME), and IPSec)

Virtual Private Network

Cryptographic VPN technologies include

IP Security (IPsec)

Layer 2 Tunneling Protocol (L2TP): (Protected by IPsec)

Generic Routing Encapsulation (GRE): (Protected by IPsec)

Point-to-Point Tunneling Protocol (PPTP): (Protected by MPPE: Microsoft Point-to-Point Encryption Protocol, see RFC 3078)

Public Key Infrastructure

PKI Components

Digital certificate (also known as identity certificate):

Certificate Authority (CA):

Registration Authority (RA)

Directory service:

Certificate Revocation List (CRL):

Simple Certificate Enrollment Protocol (SCEP):

Security Solutions for different technologies:


CISCO

Hardware and Software Security solutions

Detecting, Preventing, and Responding to Attacks and Intrusions

Cisco Security Monitoring, Analysis, and Response System (CS-MARS)
Cisco IPS solutions
Cisco Security Agent (CSA)
Cisco Security Manager
Host-based Intrusion Prevention System (HIPS)
Network-based Intrusion Detection System (NIDS),

Integrated Security Products

Cisco IOS router
Cisco ASA 5500 series security appliance
Cisco PIX 500 series security appliance
Cisco 4200 series IPS appliances
Cisco Security Agent (CSA)
Cisco Secure Access Control Server (ACS)
Cisco Catalyst 6500 series switch and Cisco 7600 series router modules
Cisco Router and Security Device Manager (SDM)

Cisco ASA 5500 Series Security Appliances

Cisco PIX 535 Security Appliance

Cisco 4200 Series IPS Appliances

Hardening Cisco Devices

Physical Security (locks, CCTV, guards**)**
Creating Strong Passwords
Pass-Phrase Technique
Password Encryption (service password-encryption**)**
ROMMON Security (no service password-recovery**)**
User Accounts
Privilege Levels (1 through 15**)**
Interactive Access Methods (Console Port, VTY Ports, VTY Access Using Telnet, VTY Access Using SSH, Auxiliary Port**)**
Banner Messages (MOTD, Login banner, EXEC banner, Incoming banner, SLIP-PPP banner message**)**
Cisco Discovery Protocol (CDP)
TCP/UDP Small-Servers

continued…

Hardening Cisco Devices

Finger
Identification (auth) Protocol
DHCP and BOOTP Service
Trivial File Transfer Protocol (TFTP) Server
File Transfer Protocol (FTP) Server
Autoloading Device Configuration (no service config, no boot network)
PAD (no service pad)
IP Source Routing (no ip source-route)
Proxy Address Resolution Protocol (ARP)(no ip proxy-arp)
Gratuitous ARP (no ip gratuitous-arps)
IP Directed Broadcast (no ip directed-broadcast, no ip directed-broadcast)

continued…

Hardening Cisco Devices

IP Mask Reply (no ip mask-reply)
IP Redirects (no ip redirects)
ICMP Unreachable (ip unreachables)
HTTP (no ip http server)
Network Time Protocol (NTP)
Simple Network Management Protocol (SNMP)
Auto-Secure Feature

Cisco IOS Firewall

Cisco IOS Firewall stateful packet inspection (SPI)
Context-Based Access Control (CBAC)
(CU-SeeMe, FTP, H.323 (such as NetMeeting), HTTP (Java blocking), ICMP, Microsoft, NetShow, RealAudio,RTSP (Real-Time Streaming Protocol),RPC (Sun RPC, not DCE RPC), SMTP (Simple Mail Transport Protocol), ESMTP (Extended Simple Mail Transport, Protocol), SQL*Net, StreamWorks, TFTP, UNIX R-commands (such as rlogin, rexec, and rsh), VDOLive)
Intrusion Prevention System (IOS IPS) (formerly known as IOS IDS)
Authentication proxy
Port-to-Application Mapping (PAM)
Network Address Translation (NAT)
Zone-Based Policy Firewall (ZFW)


Sun
microsystems

Sun Microsystems, Securing Solaris 10

Process Rights Management

Role-based access control (RBAC)

Solaris Zones

Basic Audit Reporting Tool (BART)
(Audit and Integrity Control)

Solaris Security Toolkit (SST)

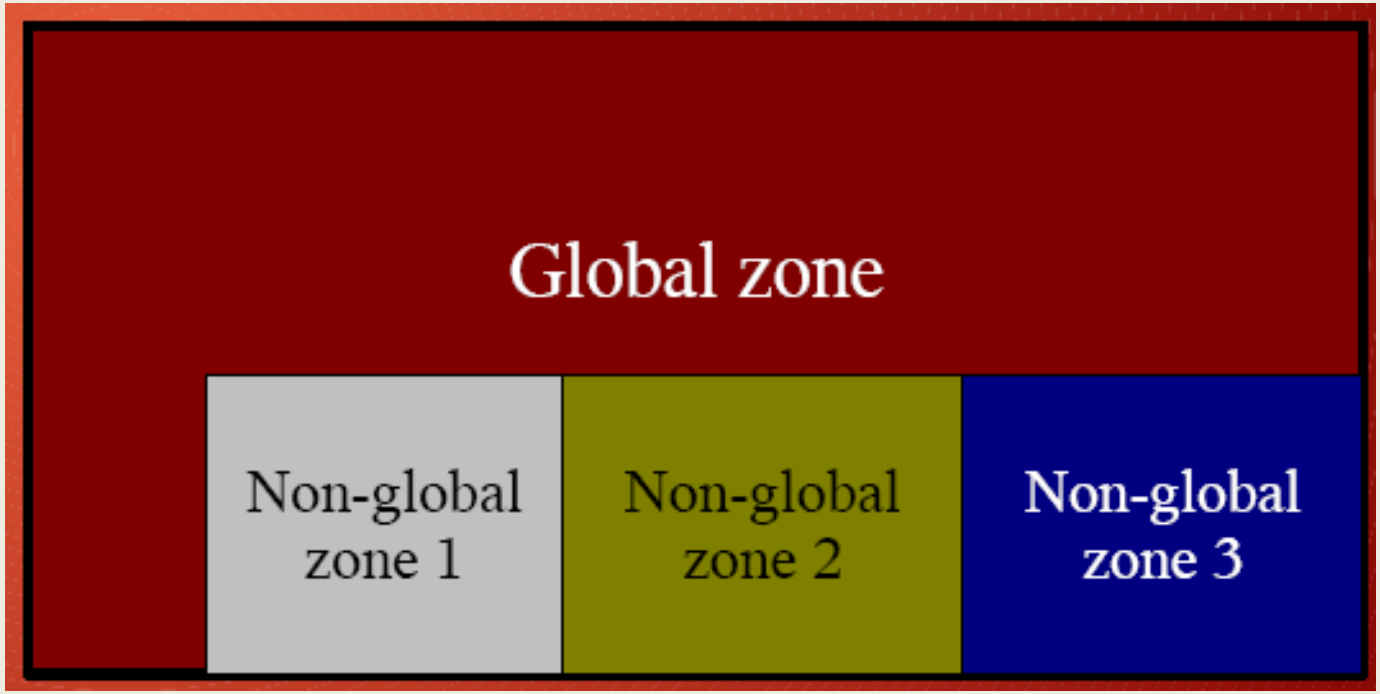
Solaris 10 security mechanisms

Process Rights Management;
Unlimited access for user Root and limited right for processes

RBAC (Role Based Access Control)
Role,
Authorization,
Right profiles (Primary Administrator, System Administrator, and Operator)

Zones (Visualization, Isolation, Security)

Solaris Zones



Role-based access control and rights profile

Primary Administrator rights profile – Provides the capabilities of superuser in one profile.

System Administrator rights profile – Provides a profile that can do most tasks that are not connected with security. This profile includes several other profiles to create a powerful role.

Operator rights profile – Provides limited capabilities to manage files and offline media. This profile includes supplementary rights profiles to create a simple role.

Printer Management rights profile – Provides a limited number of commands and authorizations to handle printing. This profile is one of several profiles that cover a single area of administration.

Basic Solaris User rights profile – Enables users to use the system within the bounds of security policy. This profile is listed by default in the *policy.conf* file.

Basic Audit Reporting Tool

Basic Audit Reporting Tool (BART) as a solution for Integrity.

- Easy and flexible syntax
- Control over installed OS
- Control over File System changes

BART enables you to determine what file-level changes have occurred on a system, relative to a known **baseline**. You use BART to create a baseline or **control manifest** from a fully installed and configured system. You can then compare this baseline with a snapshot of the system at a later time, generating a report that lists file-level changes that have occurred on the system since it was installed.

Basic Audit Reporting Tool

BART's main components

BART Manifest
BART Report
BART Rules File

Additional benefits and uses of BART

- Provides an efficient and easy method for cataloging a system that is running the Solaris software at the file level.
- Enables you to define which files to monitor and gives you the ability to modify profiles when necessary. This flexibility allows you to monitor local customizations and enables you to reconfigure software easily and efficiently.
- Ensures that systems are running reliable software.
- Allows you to monitor file-level changes of a system over time, which can help you locate corrupted or unusual files.
- Helps you troubleshoot system performance issues.

Solaris Security Toolkit (SST)

Solaris Security Toolkit software

OR

JumpStart Architecture and Security Scripts (JASS**) toolkit**

SST main components

Hardening – Modifying Solaris OS configurations to improve a system's security.

Auditing – Determining if a system's configuration is in compliance with a predefined security profile.

Scoring – Counting the number of failures uncovered during an audit run. If no failures (of any kind) are found, then the resulting score is 0. The Solaris Security Toolkit increments the score (also known as a vulnerability value) by 1 whenever a failure is detected.

An Example

```
# ./jass-execute -d secure.driver

[NOTE] The following prompt can be disabled by setting
JASS_NOVICE_USER to 0.
[WARN] Depending on how the Solaris Security Toolkit is configured,
it is both possible and likely that by default all remote shell
and file transfer access to this system will be disabled upon
reboot effectively locking out any user without console access to
the system.

Are you sure that you want to continue? (YES/NO) [NO]
y

[NOTE] Executing driver, secure.driver

============================================================
secure.driver: Driver started.
============================================================

============================================================
Solaris Security Toolkit Version: 4.2.0
Node name:                        ufudu
Zone name:                        global
Host ID:                          8085816e
Host address:                     10.8.31.115
MAC address:                      8:0:20:85:81:6e
OS version:                       5.10
Date:                             Tue Jul 5 16:28:24 EST 2008
============================================================
[...]
```

Download and Try

You can download the software distribution file (SUNWjass-n.n.pkg.tar.Z) from http://www.sun.com/security/jass

Then

```
# uncompress SUNWjass-4.2.pkg.tar.Z
# tar -xf SUNWjass-4.2.pkg.tar
# pkgadd -d . SUNjass
```

Some Useful Links

Some Useful Links

GENERAL SOURCES OF VULNERABILITY INFORMATION

- http://cve.mitre.org
- http://xforce.issnet
- http://seclab.cs.ucdavis.edu/projects/vulnerabilities/#databases/
- http://www.cs.purdue.edu/coast/projects/vdb.html
- http://www.rootshell.com/

Some Useful Links

VENDOR-SPECIFIC SECURITY PATCHES

BSDI ftp://ftp.bsdi.com/bsdi/patches
Caldera OpenLinux ftp://ftp.caldera.com/pub/OpenLinux/security/
Debian Linux ftp://ftp.usdebian.org/debian
Compaq http://www3.compaq.com/support/files
FreeBSD ftp://ftp.FreeBSD.org/pub/FreeBSD/
Hewlett Packard http://us-support.external.hp.com/
IBM http://service.software.ibm.com/support/rs6000
NT http://www.microsoft.com/security/
OpenBSD http://openbsd.com/security.html
RedHat Linux http://www.redhat.com/corp/support/
SCO ftp://ftp.sco.com/SSE
SGI ftp://ftp.sgi.com/patches/
Sun http://sunsolve.sun.com/

Some Useful Links

For investigating potential vulnerabilities within network services:

SecurityFocus (*http://www.securityfocus.com*)
milw0rm (*http://www.milw0rm.com*)
Packet Storm (*http://www.packetstormsecurity.org*)
FrSIRT (*http://www.frsirt.com*)
MITRE Corporation CVE (*http://cve.mitre.org*)
NIST National Vulnerability Database (*http://nvd.nist.gov*)
ISS X-Force (*http://xforce.iss.net*)
CERT vulnerability notes (*http://www.kb.cert.org/vuls*)

IA Policy Web Sites

Some Useful Links

- Electronic Frontier Foundation (EFF): http://www.eff.org/pub/CAF/policies
- Georgia Institute of Technology Computer and Network Usage Policy: http://www.gatech.edu/itis/policy/usage/contents.html
- General Services Agency (GSA) Policies: http://www.itpolicy.gsa.gov
- SANS Institute Information Security Reading Room: http://www.sans.org/infosecFAQ
- Information Systems Security (Infosyssec) Portal: http://www.infosyssec.com
- IA Support Environment (IASE) Policy & Guidelines: http://www.iase.disa.mil/policy.html
- National Institute of Standards & Technology (NIST) Computer Security Resource Center (CSRC): http://www.csrc.nist.gov
- Information Systems Audit and Control Association (ISACA) Standards: http://www.isaca.org/down.htm

Thank You

Any Questions ?