

# **Hardening and the Trusted Computer Base Open Source Security Tools for Information Technology Professionals**

**School of Professional Studies (SPS)**

**The City University of New York (CUNY)**

Aron Trauring  
Adjunct Professor  
CEO, Zoteca

Class 2 September 19th, 2005

# Trusted Computer Base

- Need a base computer to run security tools
- Heart of the security operation must itself be as secure as possible
- Entire list of elements that provide security: OS, programs, hardware, physical protection, procedures
- Critical that the OS, which underlies everything, be totally secure

# Problem

- Modern OSes violate the minimalist principle in the extreme
- Operating systems are extremely complex and getting more so
- Tons of other software installed on top of the OS
- Vendors tendency to make things “easy to use”
- Standard installations add to much software and services

# TCB Dangers

- Vulnerable to attack by intruders who e.g. can shut off your IDS
- Intruders can alter data to deceive you into feeling secure
- Commandeered security box makes intruders' job easier
- Ensuring your base system is secure is the first task of security administration

# Why GNU/Linux?

- Unix modularity — minimalist principle
- Unix layered approach to security — defense in depth
- FOSS review — vigilance

## TCSEC standard (“Orange Book”)

- TCSEC is the Trusted Computer System Evaluation Criteria (“Orange Book”) for single computer systems with terminal access
- first standard definition of a trusted computer system and how to evaluate and ensure them (original spec Aug 83, revised Dec 85)
- National Computer Security Center (NCSC) of the National Security Agency (NSA)
- Must have an explicit, enforced security policy
- Access to information must be controlled by rights of subjects vs class of information
- Audit trails must be kept

- System must contain mechanisms which can be independently evaluated to provide sufficient assurance that they enforce the stated requirements

## **TCSEC Rainbow Series**

- “Red Book” — Trusted Network Interpretation
- “Yellow Book” — Methodology for Security Risk Assessment
- “Lavendar Book” — Database Security Evaluation

## Evaluation Criteria Classes

- D — Minimal Protection
- C1 — Discretionary Security Protection
- C2 — Controlled Access Protection
- B1 — Labelled Security Protection
- B2 — Structured Protection
- B3 — Security Domains
- A1 — Verified Design

## Other Government Baselines and Standards

- Information Technology Security Evaluation Criteria (ITSEC) is the harmonized European trusted evaluation standard
- Common Criteria is being developed as an ISO standard (JTC1.SC27), based on existing TCSEC, ITSEC, CTCPEC (Canadian), Federal (US) standards

# Minimalism and Hardening

- Only what is needed should be made available.
- Only permit access to what you really need.
- Unless explicitly permitted, access is strictly forbidden.
- Hardening means applying minimalist principles to your system.

# Linux Options

- Bastille Linux
- grsecurity — kernel modifications and patches
- LIDS — Linux Intrusion Defense System
- RSBAC — full-featured kernel security tool-kit
- SELinux — NSA initiative
- CIS Guidelines/Scoring Tools <http://cisecurity.org/> — for all OSes

# General Hardening Tasks

1. Disable or remove all unneeded services
2. Run latest version of services that are required
3. Disable or remove all unused user accounts
4. Keep up-to-date with security patches
5. Check and maintain system logs
6. Restrict access to special services (e.g. cron) to root
7. Review and fix file permissions on critical system files
8. Review and fix general system file permissions (e.g. no world write)

9. Remove development tools if you can
10. Limit the number of daemon processes permitted
11. Run local firewalls and not just perimeter firewalls
12. Run a system hardening script
13. Use sudo

# Securing Network Services

1. Only use the secure version of a service (SSH, SFTP)
2. Disable insecure protocols (r\*, FTP, Telenet)
3. Prevent service processes from having access to data they don't need through virtualization
4. Specify logging and access control for all services giving them only the minimal rights necessary
5. Services should have special users and not run as root (if possible)
6. Drop packets at the router firewall so they never reach server (prevent DoS)
7. Harden network infrastructure

## 8. Address wireless issues