

Creating the Security Lab Environment

By: Jennifer Frazier

1

Outline

- Motivation
- Objective
- Methodologies
- Related Work
- JSS
- Security Tools
- Testing and Results
- Conclusion

2

Motivation

- SAIT Laboratory
 - Two Separate Projects With Common Goal
- Education
 - Labs With Classes
- Research
 - Testing Purposes
- Outreach
 - Relationships With Sponsors

3

Two Objectives

1. Create a Database of Security Tools
2. Create A Unix Environment on the Ultra V Workstations
 - Install Collected Security Tools
 - Protect Main Filesystem
 - Maintain Default State

4

Methodologies

Different Environments

- Cloning
- Proprietary
 - Deep Freeze, VMWare
- Non-proprietary Software
 - User Mode Linux, Chroot Jail

5

Related Work

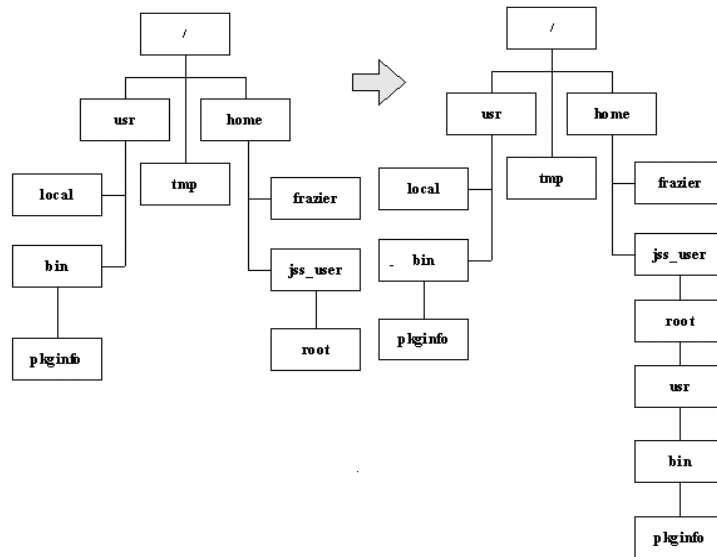
- Chroot Jail
 - Secure Environment
 - Copies Basic Commands
 - Chroot Command
- Improvements
 - Programs, Libraries and Directories
 - Network Usage
 - Restoring Environment

6

J's Secure Sandbox

- Filesystem inside Filesystem
- Maintains Tree Directory Structure
- Client – Server Design
- Restores Default Sandbox State

7

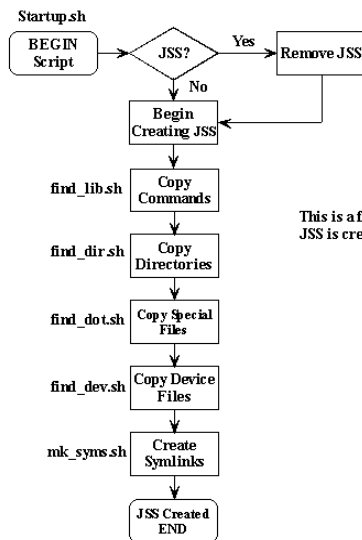


8

Server

- Contains Default JSS Filesystem
- Created Through Bash Scripts
- Synchronizes Sandbox With Client
- Sandbox Customizable

9

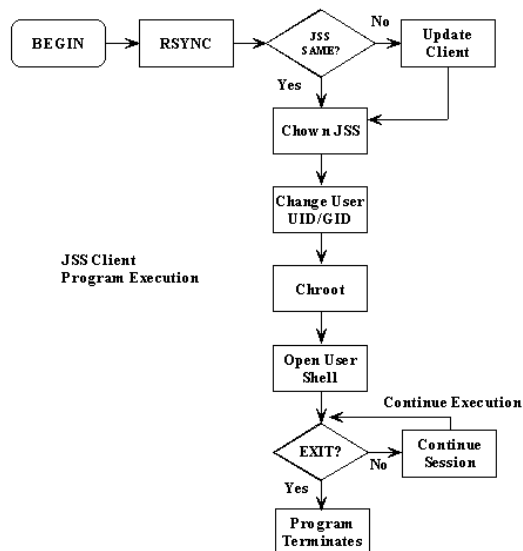


10

Main Client Program

- Restores Default Sandbox
- Gives jss_user Ownership of the Sandbox
- Launches User Environment
- Only Allows Single User to Execute Program

11

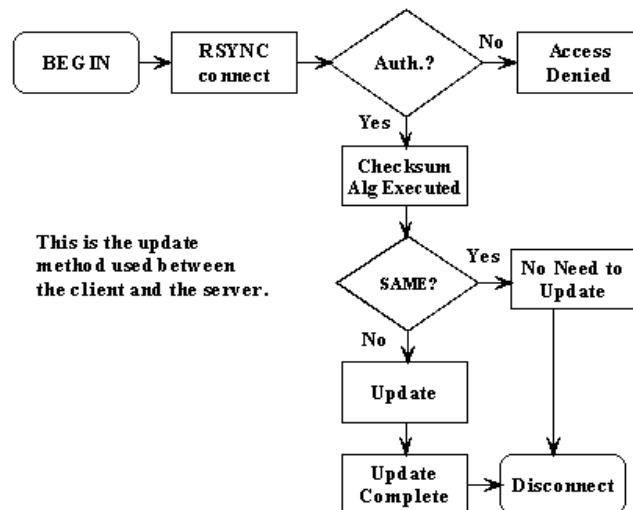


12

Rsync

- Allows Client to Update from Server
- Rsync Daemon
- Uses Rsync Algorithm
 - Utilizes Checksum Algorithm to Alleviate Need for Copying Entire Files

13



14

Security Tools

- Categories
 - Authentication & Encryption (5)
 - Hashes, PGP, Encryption/Decryption
 - Firewalls (2)
 - Intrusion Detection (16)
 - Sniffers, Host, Network, Hybrid, Real Time Auditing
 - Vulnerability Management (13)
 - PW Assess, Port & Assessment Scanners, Lockdown
 - Miscellaneous (4)
 - Front End, Testing, Media Prevention
- Installation & Testing Method

15

Testing and Results

- Size of the Sandbox
 - 280 MB, Solaris 1.5GB – 2GB
- Creation of Default JSS
 - 8 Minutes
- Rsync
 - 30 Seconds to 8 Minutes
- Testing Environment Re-creation
- Testing Tools in Sandbox

16

Conclusion

- Perform Security Studies on Ultra V
 - Accomplished through JSS Filesystem
- Bring Machines Back to Default State
 - Usage of Rsync Between Clients and Server
- Collect Database of Security Tools
 - Gathered and Tested 40 Security Tools

Through JSS & VMWare We Are One Step Closer in Transforming a Computer Laboratory into a Security Laboratory