Security Test and Evaluation: ARSC Experiences with Cray and SGI Systems

Cray Users Group: May 25,1999

Virginia Bedford
Arctic Region Supercomputing Center
PO Box 756020
Fairbanks, Alaska 99775-6020
907-474-5426
virginia.bedford@arsc.edu

Overview

- What is an ST&E?
- ARSC's environment
- Mechanics of Reviews
- Policy questions
- Individual Accountability
- Root Access
- Authentication
- setuid and setgid executables
- (Un)necessary services
- SWS's et al.
- OS vulnerabilities
- Systems Management
- Tools and Software
- Impacts to Users
- Preparation and Maintenance
- Suggestions
- References

What is an ST&E?

- Formal review and process of security disciplines
  - Procedures and configuration management
  - Operating System vulnerabilities
  - Network probes and tests
- Based on Policy and Law
- Findings and observations

ARSC's Environment

- Relationships
  - Department of Defense
  - University of Alaska
- Networks
  - Internet
  - Defense Research Engineering Network
  - UA WAN
- Minimal MLS

- The Systems
  - J90 (Unicos 10.0)
  - T3E (Unicos/mk 2.0.3.x)
  - SGIs (Irix 6.2, 6.3, 6.4, 6.5)
  - SWS (Sun)
  - OWS (Sun)
  - MWS (Sun)
  - Silo workstation (Sun)
  - Network monitoring (Suns)

Individual Accountability

- Group Accounts
- Initial File Permissions
- File Ownership
- Dot (Environment) Files
- Crontabs
- World writable files
- Dot in Path
- Xhost and xauth
- Distributed processing
- Root access
- Authentication
- Kerberos/SecurID

Dot File Checker

- Unsafe permissions.
- Ownership of file by someone other than owner of home directory
- Links, hard or symbolic or to nonexisting files
- Contents of .netrc
- Contents of .shosts and .rhosts

IRIX Set-UID and Set-GID files

- Full review of Irix 6.2, 6.3, 6.4 files
  - Unknown – reason for permissions is unknown; ramifications of removal are unknown
  - Not used – binaries never used; permissions can be changed without ramification
  - Only run by root – permissions can be changed
  - Can run with lesser privileges if group is changed
  - Must run with privileges –> wrappers
- Will Irix 6.5 make all our problems go away?

Root Access

- Critical element
- Care and feeding
- Alternatives
  - full root access
  - zup
  - super
  - sudo
  - sudo w/SecurID

Authentication

- Passwords
- Ssh
- Kerberos with SecurID

(Un)necessary Services

- What's gone?
- What's changed?
- What's left?

- SWS's
- Silo workstation
- SGIs
- Crays

Network Issues

- Ipforwarding
- SNMP
- Tcpwrappers
- Restricting information
- Access control lists
- Email

SWS's (and OWS's and MWS's)

- Services
- Accounts
- Permissions
- Rhosts, hosts.equiv and mainframe relationships
- Solaris
- Upgrades and regression

Other changes and considerations

- /etc/ftpusers
- Tcpwrappers
- Accounts with no shells
- Webservers

Operating System Vulnerabilities

- How to find what they are?
- How to keep up?
- SWS's (Suns)
- Irix
- Unicos

Systems Management

- Configuration Management
- Logging and Auditing
- Impacts to Users

Tools

- Secure Shell – ssh
- Kerberos
- Kerberos/SecurID
- Tcpwrappers
- Sudo
- Swatch
- Tiger

- ARSC “sanity checker”
- ARSC “perm checker”
- ARSC “dotfile checker”
- John the Ripper
- ISS – Internet Security Scanner
- Tripwire

Conclusions and Recommendations

- A security review is an enlightening experience. Do it.
- The myth that “a secure system is harder to use” is false. It doesn’t have to be harder to use.
- When a system is secure it gets easier to pay attention to High Performance Computing.
- Impacts to users as well as security should be evaluated prior to each change.
- Vendor support is needed for software such as Secure Shell and kerberos.