Utilizing Solaris 10 Security Features

Presented by:
Nate Rotschafer
Peter Kiewit Institute

Revised: August 8, 2005

Solaris 10 Security Features

- Outline
  - Solaris Development
  - Least Privilege
  - RBAC
  - Service Management Framework
  - Zones
  - Secure Networking
  - Logging and Auditing
  - Links and Discussion/Q&A

Solaris 10: One Source Tree

- All Solaris version now come from a single source tree
- Solaris source code is now available via www.opensolaris.org
- All versions get the advantages of work done with Trusted Solaris

Solaris 10 Security Goals

- Defending
  - Provide strong assurance of system integrity
  - Defend system from unauthorized access
- Enabling
  - Secure authentication of all active subjects
  - Protect communications between endpoints
- Deploying
  - Integratable stack architecture
  - Interoperable with other security architectures
  - Ease management and use of security features
  - Receive independent assessment of security

Hardening

- Secure Deployment
  - Minimal initial install
  - File integrity protection
  - Validated execution
- Breach Containment
  - MINIMAL process privileges
- Access Control
  - Role based
  - User based
  - File based
  - Packet based
- Auditing
  - Detailed audit trail
  - Centralized logging

Hardening Progress

- Solaris 8
  - Role based access controls
  - Tightened file permissions
- Solaris 9
  - More granular packages
  - Non-executable stack option
  - Flexible password encryption
  - SunScreen 3.2
  - OS/NE – Non-exec stack

Hardening Progress (con't)

- Solaris 10
  - Secure remote install
  - Service Management Framework
  - Granular process privs
  - File integrity checker
  - Zones
  - Minimal install option
  - Audit enhancements
  - Audit logging w/ syslog
  - Stateful packet filtering

Security

- Conservative Security Posture @ Install
  - Minimal install option
  - More services OFF by default
  - Service Manager for hardening
- Privileges
  - Decomposition of root privileges
  - Privileges can be inherited or relinquished
- Zones
  - Virtualization into application environments
  - Quarantine potentially risky software
  - Global zone can see into other zones (for IDS usage as an example)

Least Privilege

- UNIX is root or user
  - Kernel checks for explicitly for uid = 0 or object owner
- Solaris 10 privileges are evolved from common criteria evaluated implementation from Trust Solaris
- 48+ fine grained privileges instead of UID 0
  - Ppriv -lv shows privilege and what it protects
- Each process has 4 privilege sets
  - Inheritable set (I): set of privs child proc gets on exec
  - Permitted set (P): maximum set of privs for the proc
  - Effective set (E): subset of P that are currently needed
  - Limit set (L): upper bound a proc and its children can obtain

Basic Privileges

- New for Solaris 10
- These are things all normal users can normally do:
  - Proc_fork
  - Proc_exec
  - Proc_session
  - Proc_info
  - File_link_any
- Will expand in future releases
- Dropping proc_info means you can't even see other processes exist

Service Management Framework

- SMF: Dependency based service startup/recovery
- SMF service definitions contain security attributes
  - Assign uid/gid default and limit privileges for services
  - Provide a Solaris RBAC authorization that is required to administer the service
  - Provide a solaris RBAC authorization for reconfiguration of the service
- Provides distinction between configured and anabled
  - Service can be fully configured but disabled
  - Enables/disabled temporarily or permenantly
- Solaris 10 has two profiles
  - Generic.xml: most services enabled similar to Solaris 9
  - Generic_limited_net.xml: limited service set

Zones (Containers)

- Multiple virtualized application environments from single Solaris Kernel
- Works on all Solaris platforms from 1 CPU onwards
- Process containment
  - Resource usage and security isolation
- No direct access to hardware
- Zones appear as separate hosts from the outside
- Allows for separate uid/gid namespace per zone
  - Each zone has their own root user
  - Can be different nameservice domains
- Separate file systems space
- Services can be isolated from each other
  - Quaranteening potentially risky software
  - Isolating multiple distrusting parties
  - Containing damage by a breach
- Global zone can control all activities inside other zones
- Non-global zones run with less privileges

Secure Network Communications

- Solaris 8
  - IPSec Support (AH, ESP)
  - Smartcard Framework
  - Kerberos
  - GSS-API Exposed
- Solaris 9
  - TCP wrappers
  - 128-bit Cryptography
  - JDK 1.4
  - PAM modules
  - LDAP via SSL
  - Internet key exchange (IKE)
  - IPSEC
  - SSH
  - /dev/random

Secure Network Communications

- Solaris 10
  - User Crypto Framework
  - Kernel Crypto Framework
  - SASL Framework
  - PAM enhancements
  - Apache SSL
  - Mozilla GSS/Kerberos
  - Java JCE
  - LDAP via kerberos
  - SSH use of GSS-API
  - Apache GSS

Password Enhancements

- Failed login can now lock account
- Can now unlock an account preserving the old password
- Password history
- Improved control over password sanity checks
  - Includes cracklib support
- Support for pluggable crypt interface

Solaris 10 Packet Filter

- Based on Open Source IP Filter 4.x
- Stateful and stateless packet inspection
- Text based config
  - /etc/ipf/ipf.conf
  - /etc/ipf/ipnat.conf
  - Filter by: ip addr (src, dst), port, interface, direction, ipsec
  - Enforces: block, pass, r logging of packet
- Built-in NAT and port address translation

Cryptographic Framework

- Standards based pluggable framework
- Userland & kernel
- Adminstrative policy
- End user commands
  - Encrypt
  - Digest
  - Mac
  - Pktool
- Java JCE utilizes the userland tools
- OpenSSL engine for the userland tools
  - Apache mod_ssl uses this by default

Kerberos Integration

- Bundled kerberos-aware apps
  - telnet
  - ftp
  - Rsh
  - rlogin
  - Rdist
  - KDC
  - Mozilla
  - Apache
  - SSH
- Enhanced interoperability and security
  - TCP and IPv6 support

Auditing and Reporting

- Remote logging via syslog
- Audit trail xml translation
- Audit trail noise reduction
- Audit event reclassification

Solaris 10 Security Information

- Solaris 10 Home
  - www.sun.com/software/solaris/10/
- Solaris 10 Security Article
  - www.securityfocus.com/infocus/1776
- Solaris 10 Documentation
  - docs.sun.com/db/prod/solaris.10#hic
- Solaris 10 Security Blogs
  - Blogs.sun.com/gbrunett
  - Blogs.sun.com/casper
  - Blogs.sun.com/arunpn

Thanks To:

- Sun Microsystems for excellent online info
- NebraskaCERT 2005
- ConAgra Foods

- Contact Info:
  - E-Mail: nate.rotschafer@conagrafoods.com
  - Phone: 402-577-3567
- Slides available on Portal

Discussion/Q&A