Practical Solaris 10 Security

Glenn Brunette
Distinguished Engineer
Sun Microsystems, Inc.

Agenda

- Attacker Goals
- Attack Scenario Background
- Attack Defense Scenario
- Attack Detection Scenario

Attacker Goals

- Local System Access
- Administrative Privileges
- Access Privileged Information
- Conceal Attack and Avoid Detection
- Inject, Modify or Destroy Local Content
- Staging Platform for Further Attacks

Attack Scenario Background

- While operating from the network:
  - Attack originates from a local or remote network.
  - Attacker does not have local system access.
- While operating from the local system:
  - Attacker has obtained command line access (unprivileged account).
- In Both Cases:
  - Attack takes place against a Solaris 10 non-global zone.
  - Solaris 10 global zone == “service processor”

Attack Defense Scenario

- IP Filter, TCP Wrappers, IPsec, etc.
- Service Management Facility (SMF)
- Process Rights Management
- Non-Executable Stack
- Pluggable Authentication Mechanism (PAM)
- Reduced Installation Profile
- Solaris Zones
- Solaris Cryptographic Framework
- User Rights Management

Attack Defense Scenario

- IP Filter, TCP Wrappers, IPsec, etc.

Attack Defense Scenario

- IP Filter, TCP Wrappers, IPsec, etc.
- Service Management Facility (SMF)

Service Management Facility

- Provide a uniform mechanism to disable/manage services.
  - e.g., `svcadm [disable|enable] telnet`
- Support alternative service profiles
  - e.g., “Secure by Default” profile (in Solaris 10 11/06)
- Leverage authorizations to manage/configure services.
- Define context to permit services to be started as a specific user and group and with specific privileges.
- Support automatic service dependency resolution.
  - e.g., `svcadm enable -r nfs/client`
- Facilitate delegated service restarts.

Solaris Secure By Default

- Only Secure Shell is reachable by default.
  - `root` use of Secure Shell is not permitted by default.
- Existing services are configured in SMF to either be:
  - Disabled by default
  - Listening for local (e.g., loopback) connections only
- Configuration can be selected using CLI or JumpStart:
  - `netservices`: `open` (traditional) or `limited` (SBD)
  - `service_profile`: `open` or `limited_net`
- Default installation method in Nevada/OpenSolaris:
  - Solaris upgrades are not changed or impacted.
  - Solaris 10 initial (fresh) installations can select SBD mode.

Solaris Secure By Default Example #1

```
# netservices
netservices: usage: netservices [ open | limited ]

# netservices limited
restarting syslogd
restarting sendmail
dtlogin needs to be restarted. Restart now? [Y] y
restarting dtlogin

# netstat -af inet -P tcp | grep LISTEN
[...]
*.sunrpc                 *.*    0      0 49152      0 LISTEN
*.ssh                    *.*    0      0 49152      0 LISTEN
localhost.smtp           *.*    0      0 49152      0 LISTEN
localhost.submission     *.*    0      0 49152      0 LISTEN
```

SMF Execution Context

- `exec` methods can be forced to run as a given user:
  - `{start, stop, etc.}/user`
- `exec` methods can be forced to run as a given group:
  - `{start, stop, etc.}/group`
- `exec` methods can be forced to use specific privileges:
  - `{start, stop, etc.}/privileges`
  - `{start, stop, etc.}/limit_privileges`
- Other `exec` context can also be defined:
  - default project and resource pool, supplemental groups, etc.

SMF Execution Context Example

```
# svcprop -v -p start apache2
start/exec astring /lib/svc/method/http-apache2\ start
start/timeout_seconds count 60
start/type astring method
start/user astring webservd
start/group astring webservd
start/privileges astring
basic,!proc_session,!proc_info,!file_link_any,net_privaddr
start/limit_privileges astring :default
start/use_profile boolean false
start/supp_groups astring :default
start/working_directory astring :default
start/project astring :default
start/resource_pool astring :default
```

Example taken from the Sun BluePrint: Limiting Service Privileges in the Solaris 10 Operating System, http://www.sun.com/blueprints/0505/819-2680.pdf

Attack Defense Scenario

- IP Filter, TCP Wrappers, IPsec, etc.
- Service Management Facility (SMF)
- Process Rights Management

Process Rights Management

- Solaris kernel checks for privileges and not just `UID == 0`!
  - Division of `root` authority into discrete privileges (67 and counting)
  - Privileges can be granted to processes based on need.
  - Privileges can be disabled or dropped when not needed.
  - Child processes can have different (fewer) privileges than the parent.
- Completely backward compatible and extensible.
  - No changes required to use existing code.
- Privilege bracketing helps to mitigate effects of future flaws.
  - e.g., `proc_fork` and `proc_exec`
  - e.g., `proc_info`

Process Privileges Example #1

```
$ ppriv $$
28983:  bash
flags = <none>
        E: basic
        I: basic
        P: basic
        L: all
```

```
$ ppriv -l basic
file_link_any
proc_exec
proc_fork
proc_info
proc_session
```

```
$ ppriv -De cat /etc/shadow
cat[3988]: missing privilege "file_dac_read" (euid =
101, syscall = 225) needed at ufs_iaccess+0xc9
cat: cannot open /etc/shadow
```

```
$ ppriv -s -proc_fork,-proc_exec -De /bin/vi
[attempt to run a command/escape to a shell]
vi[4180]: missing privilege "proc_fork" (euid = 101,
syscall = 143) needed at cfork+0x3b
```

Process Privileges Example #2

```
# ppriv -S `pgrep rpcbind`
933:    /usr/sbin/rpcbind
flags = PRIV_AWARE
        E: net_bindmlp,net_privaddr,proc_fork,sys_nfs
        I: none
        P: net_bindmlp,net_privaddr,proc_fork,sys_nfs
        L: none

# ppriv -S `pgrep statd`
5139:   /usr/lib/nfs/statd
flags = PRIV_AWARE
        E: net_bindmlp,proc_fork
        I: none
        P: net_bindmlp,proc_fork
        L: none
```

Process Privilege Debugging

```
web_svc zone:   # svcadm disable apache2
global zone:    # privdebug -v -f -n httpd
web_svc zone:   # svcadm enable apache2
global zone:    [output of privdebug command]
```

STAT	TIMESTAMP	PPID	PID	PRIV	CMD
USED	273414882013890	4642	4647	net_privaddr	httpd
USED	273415726182812	4642	4647	proc_fork	httpd
USED	273416683669622	1	4648	proc_fork	httpd
USED	273416689205882	1	4648	proc_fork	httpd
USED	273416694002223	1	4648	proc_fork	httpd
USED	273416698814788	1	4648	proc_fork	httpd
USED	273416703377226	1	4648	proc_fork	httpd

privdebug is available from the OpenSolaris Security Community:
http://www.opensolaris.org/os/community/security/projects/privdebug/

Attack Defense Scenario

- IP Filter, TCP Wrappers, IPsec, etc.
- Service Management Facility (SMF)
- Process Rights Management
- Non-Executable Stack

Non-Executable Stack Example

```
$ cc -o shell-exstk shell.c
$ cc -o shell-noexstk -M /usr/lib/ld/map.noexst shell.c

$ ./shell-exstk
Attempting to start a shell...
$ exit

$ ./shell-noexstk
Attempting to start a shell...
Segmentation Fault(coredump)

Sep 16 15:06:06 kilroy genunix: [ID 533030 kern.notice]
NOTICE: shell-noexstk[23132] attempt to execute code on
stack by uid 101
```

Attack Defense Scenario

- IP Filter, TCP Wrappers, IPsec, etc.
- Service Management Facility (SMF)
- Process Rights Management
- Non-Executable Stack
- Pluggable Authentication Mechanism (PAM)

Attack Defense Scenario

- IP Filter, TCP Wrappers, IPsec, etc.
- Service Management Facility (SMF)
- Process Rights Management
- Non-Executable Stack
- Pluggable Authentication Mechanism (PAM)
- Reduced Installation Profile

Reduced Networking Metacluster

Meta Cluster	Size (MB)	# Pkgs	# Set-UID	# Set-GID
Reduced Networking SUNWCrnet	191	92	28	11
Core SUNWCreq	219	139	34	13
End User SUNWCuser	2100	604	57	21
Developer SUNWCprog	2900	844	59	21
Entire SUNWCall	3000	908	72	22
Entire + OEM SUNWCXall	3000	988	80	22

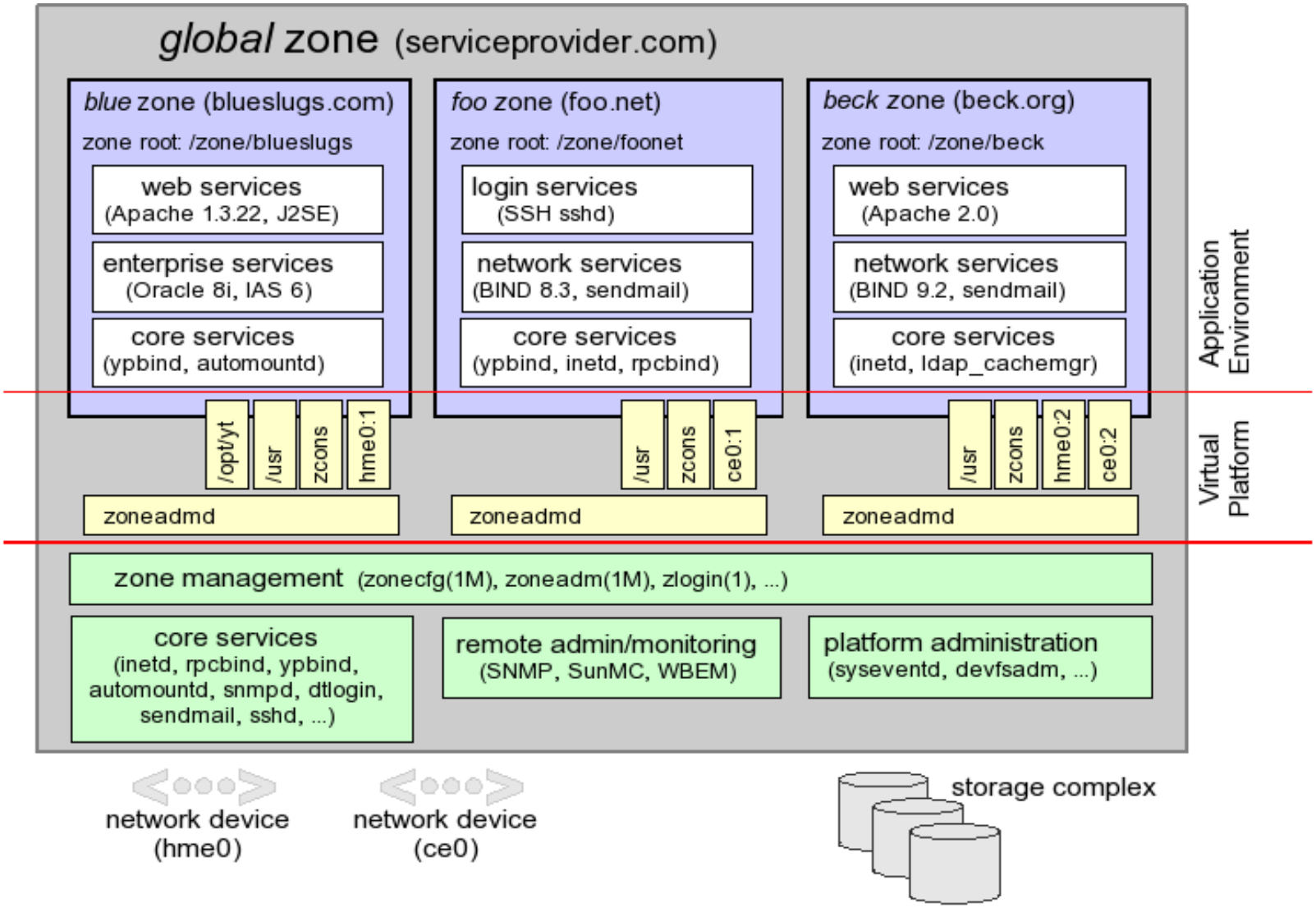
Attack Defense Scenario

- IP Filter, TCP Wrappers, IPsec, etc.
- Service Management Facility (SMF)
- Process Rights Management
- Non-Executable Stack
- Pluggable Authentication Mechanism (PAM)
- Reduced Installation Profile
- Solaris Zones

Zones

- Zones are virtualized application environments.
  - No direct access to hardware.
- Zones have security boundaries around them.
- Zones have their own:
  - root directory, naming service configuration, process containment, resource controls, devices, etc.
- Zones communicate via network only (default).
- Zones operate with fewer privileges (default).

Zones



Zones Security Example #1

```
# modload autofs
Insufficient privileges to load a module

# modunload -i 101
Insufficient privileges to unload a module

# snoop
snoop: No network interface devices found

# mdb -k
mdb: failed to open /dev/ksyms: No such file or directory

# dtrace -l
   ID   PROVIDER            MODULE                    FUNCTION NAME

# ppriv -D -e route add net default 10.1.2.3
route[4676]: missing privilege "sys_net_config"
(euid = 0, syscall = 4) needed at ip_rts_request+0x138
add net default: gateway 10.1.2.3: insufficient privileges
```

Zones Security Example #2

```
# mount -p
/          -   /          zfs    - no
                                    rw,devices,setuid,exec,atime
/dev       -   /dev       lofs   - no zonedevfs
/lib       -   /lib       lofs   - no ro,nodevices,nosub
/platform  -   /platform  lofs   - no ro,nodevices,nosub
/sbin      -   /sbin      lofs   - no ro,nodevices,nosub
/usr       -   /usr       lofs   - no ro,nodevices,nosub
[...]

# mv /usr/bin/login /usr/bin/login.foo
mv: cannot rename /usr/bin/login to /usr/bin/login.foo:
Read-only file system
```

Zones Security Example #3

```
# zonecfg -z myzone info limitpriv
limitpriv: default,sys_time

# zlogin myzone ppriv -l zone | grep sys_time
sys_time

# zlogin myzone svcs -v ntp
STATE          NSTATE          STIME    CTID   FMRI
online         -               10:17:58    214
svc:/network/ntp:default

# zlogin myzone ntpq -c peers
     remote           refid      st t when poll reach   [...]
==============================================================[...]
*blackhole 129.146.228.54   3 u   48   64   77    [...]

# ssh blackhole date ; date ; zlogin myzone date
Thu Jun 15 10:25:25 EDT 2006
Thu Jun 15 10:25:25 EDT 2006
Thu Jun 15 10:25:25 EDT 2006
```

Attack Defense Scenario

- IP Filter, TCP Wrappers, IPsec, etc.
- Service Management Facility (SMF)
- Process Rights Management
- Non-Executable Stack
- Pluggable Authentication Mechanism (PAM)
- Reduced Installation Profile
- Solaris Zones
- Solaris Cryptographic Framework

Cryptographic Framework

- Standards-based, pluggable framework
  - Kernel support as well as user-land (PKCS#11)
  - Supports administrative policies (e.g., FIPS 140 algorithms only)
- By default, supports major algorithms.
  - Encryption : AES, Blowfish, RC4, DES, 3DES, RSA
  - Digest : MD5, SHA-1, SHA-256, SHA-384, SHA-512
  - MAC : DES MAC, MD5 HMAC, SHA-1 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC
  - Optimized for both SPARC, Intel and AMD
- Framework supports pluggable hardware/software providers:
  - e.g., UltraSPARC T1 and the Sun CryptoAccelerator 6000

Attack Defense Scenario

- IP Filter, TCP Wrappers, IPsec, etc.
- Service Management Facility (SMF)
- Process Rights Management
- Non-Executable Stack
- Pluggable Authentication Mechanism (PAM)
- Reduced Installation Profile
- Solaris Zones
- Solaris Cryptographic Framework
- User Rights Management

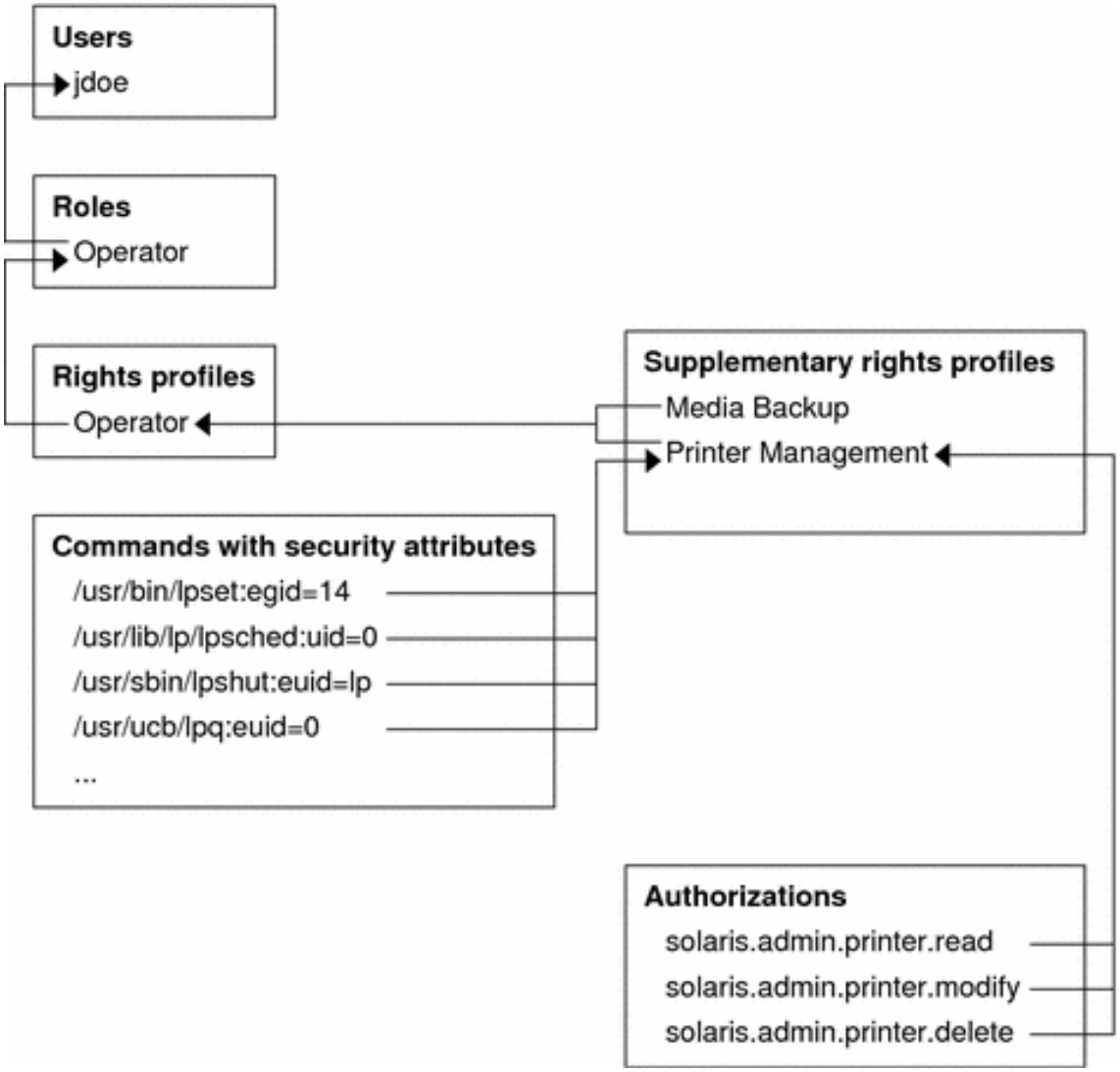
User Rights Management (Roles)

Solaris Users versus Roles

- Roles can only be accessed by users already logged in.
- Users cannot assume a role unless authorized.

```
$ id -a
uid=80(webservd) gid=80(webservd)

$ roles
No roles

$ su - root
Password:
Roles can only be assumed by authorized users
su: Sorry
```

User Rights Management (Rights)



User Rights Management Example

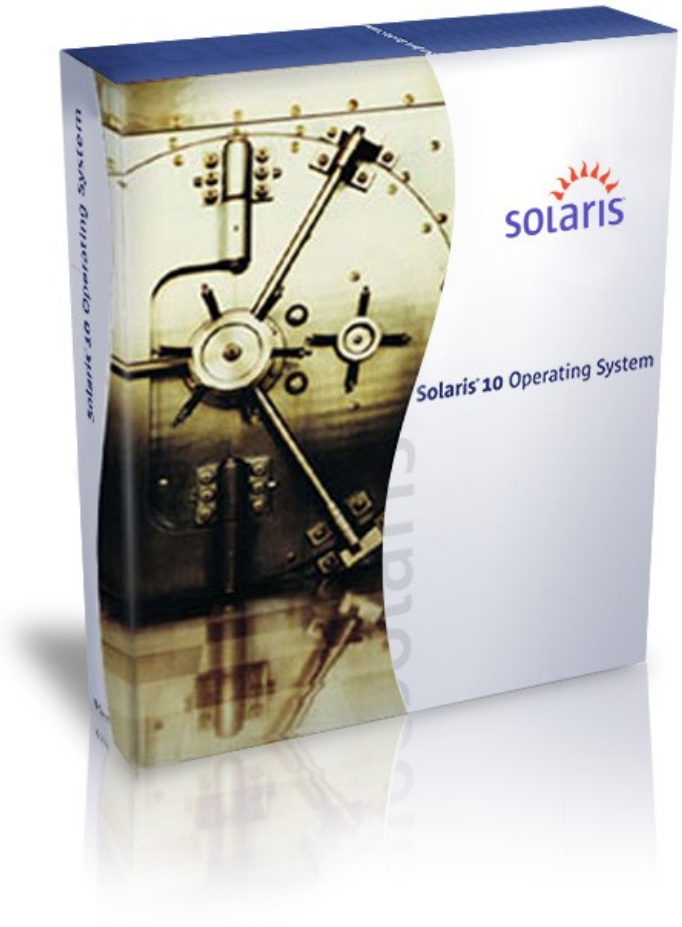
```
# svcprop -p httpd -p general apache2
general/enabled boolean false
general/action_authorization astring sunw.apache.oper
general/entity_stability astring Evolving
httpd/ssl boolean false
httpd/stability astring Evolving

# auths weboper
sunw.apache.oper

# profiles -l weboper

      Apache Operator:
          /usr/sbin/svcadm
          /usr/bin/svcs
```

User Rights Management Example

```
$ svcs -o state,ctid,fmri apache2
STATE          CTID   FMRI
online        91050   svc:/network/http:apache2

$ svcadm restart apache2

$ svcs -o state,ctid,fmri apache2
STATE          CTID   FMRI
online        91064   svc:/network/http:apache2

$ ls
ls: not found

$ echo *
local.cshrc local.login local.profile
```

Solaris Trusted Extensions

http://www.opensolaris.org/os/community/security/projects/tx/



Labeled Security for Solaris 10+

Multi-Level Desktop, Networking and Printing

Labeled Filesystems and Devices

Compatible with all Solaris hardware and applications

Common Criteria Target:

CAPP, RBACPP, LSPP @ EAL 4+

Available November 2006

Attack Detection Scenario

- Solaris Audit
- Basic Audit and Reporting Tool (BART)
- Cryptographically Signed ELF Objects
- Solaris Fingerprint Database
- Solaris Security Toolkit

Solaris Audit

- Kernel auditing of system calls and administrative actions.
  - Can record events happening in any zone (from the global zone).
- Example:

```
$ auditreduce -m AUE_su -r joe | praudit -s
  file,2005-04-12 07:25:06.000 -04:00,
  header,97,2,AUE_su,,10.8.31.9,2005-04-12
  07:28:30.220 -04:00
  subject,joe,joe,other,joe,other,1834,3097759606,121
  14 22 10.9.1.3
  text,bad auth. for user roleB
  return,failure,2
```

Example taken from the Sun BluePrint: Enforcing the Two-Person Rule Via Role-based Access Control in the Solaris 10 OS, http://www.sun.com/blueprints/0805/819-3164.pdf

Basic Auditing and Reporting Tool

File-level integrity validation tool:

- Evalutes: uid, gid, permissions/acls, contents, mtime, size, type, etc.

```
# cat ./rules
/etc
CHECK all

# find /etc | bart create -I > newManifest

# bart compare -r ./rules ./oldManifest ./newManifest
/etc/user_attr:
size control:28268  test:23520
acl  control:user::rw-,group::rw-,mask:r-x,other:r--
        test:user::rw-,group::rw-,mask:r-x,other:rw-
  contents  control:28dd3a3af2fcc103f422993de5b162f3
               test:28893a3af2fcc103f422993de5b162f3
```

[1] See: Sun BluePrint: Automating File Integrity Checks, http://www.sun.com/blueprints/0305/819-2259.pdf

Cryptographically Signed ELF Objects

- ELF Objects Cryptographically Signed
  - binaries, libraries, kernel modules, crypto modules, etc.

```
# file /usr/lib/ssh/sshd
/usr/lib/ssh/sshd:      ELF 32-bit MSB executable
SPARC Version 1, dynamically linked, stripped

# elfsign verify -e /usr/lib/ssh/sshd
elfsign: verification of /usr/lib/ssh/sshd passed.

# elfsign list -f signer -e /usr/bin/ls
CN=SunOS 5.10, OU=Solaris Signed Execution,
O=Sun Microsystems Inc
```

- Cryptographic modules must be signed by Sun.
  - Signature must be validated before module can be loaded.

Solaris Fingerprint Database

Searchable database of MD5 fingerprints for files included in Solaris, Trusted Solaris, and bundled software.

```
# digest -v -a md5 /usr/lib/ssh/sshd
md5 (/usr/lib/ssh/sshd) =
b94b091a2d33dd4d6481dffa784ba632

[Process fingerprint using the Solaris Fingerprint DB]

b94b091a2d33dd4d6481dffa784ba632 - (/usr/lib/ssh/sshd)
- 1 match(es)
     * canonical-path: /usr/lib/ssh/sshd
     * package: SUNWsshdu
     * version: 11.10.0,REV=2005.01.21.15.53
     * architecture: sparc
     * source: Solaris 10/SPARC
```

Solaris Security Toolkit

Configurable (and pluggable) security tool used to configure or assess the security posture of a Solaris system.

```
# jass-execute -a hardening.driver -V 2
[...]
disable-spc                 [FAIL]
   Service svc:/application/print/cleanup:default
   was enabled.
disable-spc                 [FAIL]
   Service svc:/application/print/cleanup:default
   was running.
disable-spc                 [FAIL] Script Total: 2 Errors

disable-ssh-root-login      [PASS]
   Service svc:/network/ssh:default was installed.
disable-ssh-root-login      [PASS]
   PermitRootLogin parameter is set to "no" in
   /etc/ssh/sshd_config.
disable-ssh-root-login      [PASS] Script Total: 0 Errors
```

Actions...

1. Evaluate, pilot and “beat up” Solaris 10 and Solaris Trusted Extensions today!
2. Share with us what you like, what you don't and how you would improve the product!
3. Join the OpenSolaris Community!

For More Information

- Sun Security Home
  - http://www.sun.com/security
- OpenSolaris Security Community
  - http://www.opensolaris.org/os/community/security
- Sun Security Coordination Center
  - http://blogs.sun.com/security & security-alert@sun.com
- Sun Security BluePrints
  - http://www.sun.com/blueprints
- Sun Security Bloggers
  - http://blogs.sun.com

Practical Solaris 10 Security

Glenn Brunette
Sun Microsystems, Inc.
glenn.brunette@sun.com
http://blogs.sun.com/gbrunett