

Solaris Security

Basudev Saha
Amarjot Walia

CERT-In

Department of Information Technology
Ministry of Communications & Information Technology
Electronics Niketan, 6 C.G.O. Complex
New Delhi- 110 003

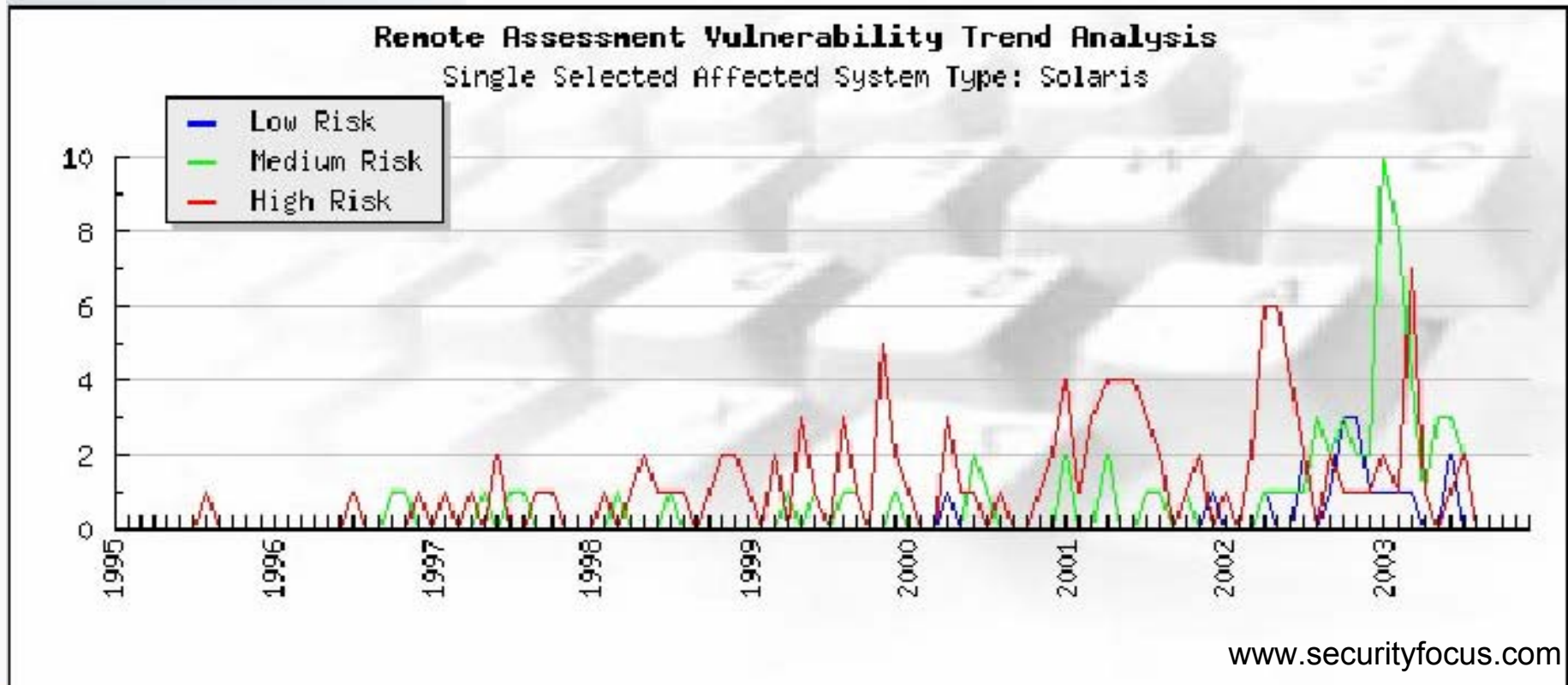
Solaris Vulnerability statistics

Total vulnerabilities since January 1, 1995: **1017**

Total high risk vulnerabilities: **488**

Total medium risk vulnerabilities: **338**

Total low risk vulnerabilities: **191**



Common issues

- Most Solaris security checklists recommend installing the minimum set of software needed to run the system.
 - Most sysadmins don't do this.
- General strategy
 - Remove all privilege and access and grant or enable only what is needed.
 - Enable as much system logging as possible!

Follow standards

- Use the SANS Securing Solaris checklist
- Use the Center for Internet Security Securing Solaris Benchmark
- Use the CERT Securing Solaris Server checklist.

Solaris Security

- Identify the role
- Install minimal/service minimization
- patch Updation
- Permissions
- User Management
- Kernel Tuning
- Logging
- Backup and Recovery
- Benchmark

Role Identification

- Identify services
 - Web server
 - Mail server
 - Database server
 - ftp server
 -
- Identify users
 - Public server
 - Internal server
 - Development server

Installation

- **Core** – base OS
- **End-user** – CDE/X Windows, UCB support, NIS/NIS+/LDAP
- **Developer** – man pages, include files(/usr/include), compiler libraries, make, ar, ld commands
- **Full OEM** – everything on the install CD

Patches

- Available from sunsolve.sun.com
- install tools
 - **Patchdiag** – available from sunsolve.sun.com
 - **GASP** – available from discovery.cc.vt.edu and Brian Reilly at Georgetown U
 - GUI front end to patchdiag
 - Patchdiag is required

Minimization

- Minimize inetd network services
- Minimize boot services
 - Find OS Package dependency
 - Startup and Boot Scripts to Check

Minimization (Contd.) inetd services

/etc/inetd.conf

```
#finger  stream  tcp      nowait  nobody  /usr/sbin/tcpd      in.fingerd
#systat  stream  tcp      nowait  root    /usr/bin/ps          ps -ef
#netstat  stream  tcp      nowait  root    /usr/bin/netstat     netstat -f inet
#
# Time service is used for clock synchronization.
#
time      stream  tcp      nowait  root    internal
time      dgram   udp      wait    root    internal
#
# Echo, discard, daytime, and chargen are used primarily for testing.
#
echo      stream  tcp      nowait  root    internal
echo      dgram   udp      wait    root    internal
discard   stream  tcp      nowait  root    internal
discard   dgram   udp      wait    root    internal
daytime   stream  tcp      nowait  root    internal
daytime   dgram   udp      wait    root    internal
```

Minimization (Contd.) (boot services)

- System services controlled by the `/etc/rcX.d` directories where
 - X=0 : shutdown
 - X=S : single user mode
 - X=1 : start
 - X=2 : multi-user, no network services
 - X=3 : multi-user (default)
 - X=4 : unused
 - X=5 : shutdown and power off
 - X=6 : shutdown and reboot

Minimization (Contd.)

- Start up scripts : *SxxService*
- Kill scripts : *KxxService*
- Main scripts live in */etc/init.d*
- Symlinks are in the */etc/rcX.d* directories

Minimization (Contd.)

```
# ls /etc/rc2.d
K03samba          S10lu             S72slpd           S89PRESERVE
K03sshd           S20syssetup      S73cachefs.daemon S89bdconfig
K05appserv        S21perf          S73nfs.client     S90wbem
K05volmgt         S30sysid.net     S74autofs         S91afbinit
K06nipagent       S33dca           S74syslog         S91gfbinit
K07dmi            S40llc2          S74xntpd          S91ifbinit
K07snmpdx         S42ncakmod       S75cron           S91jfbinit
K15img            S47pppd          S75flashprom     S91zuluinit
K16apache         S69inet          S75savecore      S93cacheos.finish
K21dhcp           S70sckm          S76nsd            S94ncalogd
K27boot.server   S70uucp          S77secd           S95sum.sync
K28kdc            S71ldap.client   S77sf880dr       S98efcode
K28kdc.master    S71rpc           S80lp             S99audit
K28nfs.server     S71sysid.sys     S80spc            S99dtlogin
README           S72autoinstall   S85power
S01MOUNTFSYS     S72directory     S88sendmail
S05RMTMPFILES    S72inetsvc       S88utmpd
#
```

Minimization (Contd.)

- Disable login: prompts on serial port (inittab)
- Turn on inetd tracing, disable inetd (?)
 - Modify inetdsvc
 - `Usr/sbin/inetd -s -t`
(logs connection related information)

User Management

- Block/delete unwanted system accounts
 - smtp, nuucp, listen
 - passmgmt -d <account name>
- No accounts with empty password file
- uid 0 account other than root
- Set account expiration parameters
 - etc/default/passwd
 - Maxweeks
 - Minweeks
 - Warnweeks

User Management

- user home directory permission (mode 750)
- Remove user `.netrc` files
- Default umask for users (077)
 - `/etc/profile`
 - `/etc/.login`
- JASS toolkit contains a `noshell` command that will generate a syslog entry when someone tries to login a disabled account.

User management

- Lock users: `passwd -l <userid>`
- Modify accounts: `passwd -e <userid>`
- System accounts in `/etc/passwd` have no shell assigned to them
- They also have NP in the password field of `/etc/shadow`
- UID/GID pairs must be unique across NFS. Recommend using the PID # as a UID

Permission

- File systems are mounted either 'ro' or 'nosuid'
- 'logging' option to root file system
- 'nosuid' option to /etc/rmmount.conf
- Verify passwd, shadow and group file permission
- World writable directories should have sticky bit set

Permission

- Find unauthorized world-writable files
- Find unauthorized suid-guid system executables
- Run *fix-modes*
 - Corrects insecure system file/directory perms:
 - Removes group/world write permissions
 - Makes most files owned by root
 - Uses `/var/sadm/install/contents` for list of programs to check
 - User files NOT installed with `pkgadd` will not be affected
 - Core files in Solaris 8 are fixed. Things like CDE aren't

Permission

System access, authentication and authorization

- Remove .rhosts support in /etc/pam.conf
- Create symlinks for dangerous files

System access authentication

- Remove .rhosts support in /etc/pam.conf
- Create symlinks for dangerous files
- Create etc/ftpd/ftpusers (default in sol 8)
- Create /etc/shells (default in sol 8)
- Prevent remote XDMCP access
 - /etc/dt/config/Xaccess
- Prevent X server from listening on 6000/tcp
 - etc/dt/config/Xaccess

System access authentication

- Set default locking screensaver timeout
- Restrict at/cron to authorized users
 - /etc/cron.allow , at.allow
- Remove empty crontab files and restrict file permissions
 - /var/spool/cron/crontabs
- Create warning banners
 - Eeprom oem-banner
 - /etc/motd
 - /etc/issue

System access authentication

- Limit number of failed login attempts
 - /etc/default/login (RETRIES=3)
- Set EEPROM security-mode and log failed access
 - eeprom security-#badlogins=0
 - Eeprom security-mode=command

Kernel Settings

- `/etc/system` contains kernel parameters
- Some kernel parameters can be adjusted to improve performance and security
- Disable core dumps
 - `set sys:coredumpsize = 0`
 - Prevents the creation of core files. Beware!
 - Use the `coreadm` command to define target directories and file name patterns for core files. Useful in creating a central core repository.
 - SUID/SGID will be prevented from creating core files if the above is set.

Kernel Settings (Contd.)

- Enable stack protection
 - set noexec_user_stack = 1
 - set noexec_user_stack_log = 1
- Helps defend against stack overflow attacks. Logs the attempt as well.
- All 64 bit Solaris use non-executable stacks by default

Network parameters

- **ndd** command display/sets kernel parms on the fly
 - `ndd /dev/arp \?`
 - `ndd /dev/icmp \?`
 - `ndd /dev/ip \?`
 - `ndd /dev/tcp \?`
 - \? = list all driver parms and status: RO, RW
 - Response of 0 means the option is disabled
- **ndd -set <driver> <option> <value>** to set a parameter
- **nddconfig**
 - <http://www.sun.com/blueprints/tools>.

IP Defense

- `/etc/notrouter` disables IP forwarding at boot time
 - `/etc/init.d/inetinit` determines the configuration at boot
- To dynamically disable IP forwarding:
 - `ndd -set /dev/ip ip_forwarding 0`
 - Solaris 8 allows you to set this per I/F

IP Defense- Directed Broadcast

- Directed broadcast is sent from a remote machine to all systems on another net
- Used by “smurf” attack. CNS router rules limit smurf to the same subnet
 - Forged ICMP echo request sent to broadcast w/ target source address

```
ndd -set /dev/ip \  
ip_forward_directed_broadcasts 0
```

- Default is 1

IP Defense-ICMP

- Usually safe to disable ICMP broadcasts
- All systems configured to respond to broadcast echo request will send an echo reply
- Disable:

```
ndd -set /dev/ip \  
ip_respond_to_echo_broadcast 0
```

 - This breaks PING. You won't be able to ping this system

IP Defense-ICMP

- Individual timestamp requests are ok. No reason for broadcast request.
- Disable:

```
ndd -set /dev/ip \  
ip_respond_to_timestamp_broadcast 0
```

```
ndd -set /dev/ip \  
ip_respond_to_timestamp 0 (unicast)
```

- Address mask used to get netmask. Printers, X-term use this. Solaris disables by default

```
ndd - set /dev/ip  
ip_respond_to_address_mask_broadcast 0
```

IP Defense-ICMP

Redirect errors used to tell a system to use a different router

Can be used in Man-in-the-Middle to install bogus routes

- Disable incoming:

```
ndd -set /dev/ip ip_ignore_redirect  
1
```

- Disable outgoing:

```
ndd -set /dev/ip ip_send_redirects  
0
```

IP Defense-TCP

- Syn Floods work on unestablished connections
- 2 queues
 - Q for established connections
 - Q for unestablished connections
 - Increase size on unestablished connect Q

```
ndd -set /dev/tcp \  
tcp_conn_req_max_q0 4096  
ndd -set /dev/tcp \  
tcp_ip_abort_cinterval 60000
```

IP Defense-TCP

- Connection Exhaustion Attack
- Works on established connections
- OS has max # connect limit. Attacker exceeds this limit
- Default Q is 128. Increase to 1024
 - `ndd -set \`
 - `/dev/tcp tcp_conn_req_max_q 1024`
 - This increases the amount of memory needed to process all TCP connections

IP Defense-TCP

- IP Spoofing uses TCP Hijacking based on ISN prediction
- RFC 1498 defines better way to generate ISN
- 3 types: 0 – predictable; 1 – improved with random increment; 2 – RFC 1498 method
- Solaris 8 uses 2, modify Solaris 7 by editing `/etc/default/inetinit` and add line:
 - `TCP_STRONG_ISS=2`

IP Defense-TCP

- Privileged Ports can only be acquired by root owned processes
- NFS uses 2049, 4045. Hacker can set up fake NFS server listening on these ports
- Extend port range:

```
ndd -set /dev/tcp \  
tcp_smallest_nonpriv_port 2050
```

- Add individual ports:

```
ndd -set /dev/tcp \  
tcp_extra_priv_ports_add 6112
```

Logging

/var/adm/sulog	Logs su attempts	Default
/var/adm/vold.log	Volume manager logs	Default
/var/adm/wtmpx, utmpx	login info - last ,who	Default
/var/adm/loginlog	Login logs	Touch this file
/var/cron/log	Logs all cron jobs success/failure	/etc/default/cron

Logging

- **Enable System Accounting**

Uses the `sar` command to gather system

- resource usage data:

- Cpu, memory, disk, file I/O, system calls
- `/etc/init.d/perf`
- Archives stored in `/var/adm/sa`

- `vmstat` command collects data in a real-time data

- **Enable Kernel-level auditing :**

- `/etc/security/bsmconv` (auditing)

- `/etc/security/audit_control` flags

- `ad` administrative Administrative actions: mount, exportfs, etc
- `lo` login_logout Login and logout events
- `fc` file_creation Creation of object
- `fd` file_deletion Deletion of object

Logging

- Create log rotation script
 - Use logadm (solaris 9 only)
 - Use cron

Ensure integrity (build checksum)

- Create checksum of
 - Critical system files
 - Configuration files
 - Important data files
- Regular check against checksum

tripwire

Backup and recovery

- Create backup policies
- Identify important files/data to backup
 - Important system files/binaries
 - Checksum database
 - Important logs
- Methods/commands
 - Tar
 - Dd
- Media
 - Tape
 - DLT
 - harddisk

Use TCP_wrappers, ssh

- TCP_wrappers
 - Controls access to various network services based on IP address.
 - Provides logging information via syslog
 - Etc/hosts.allow
 - Etc/hosts.deny
- SSH
 - Provides secure encrypted network logins and file transfer

Security Tools

- JASS
- TITAN

Testing & Verification

- CIS Solaris Benchmark
 - www.cisecurity.com

References

- TITAN
 - www.fish.com/titan
- JASS
 - www.sun.com/blueprints/tools
- Solaris Blueprints On-line
 - www.sun.com/blueprints/browsesubject.html

Questions ?

Thanks

basu@cert-in.org.in

amar@cert-in.org.in

<http://www.cert-in.org.in>