Securing Sun Fire™ 15K Domains

By Alex Noordergraaf - Enterprise Engineering and
Dina Kurktchi - Enterprise Server Products

Sun BluePrints™ OnLine - January 2002

`http://www.sun.com/blueprints`

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300 fax 650 969-9131

Part No.: 816-3571-10
Revision 1.0, 01/08/02
Edition: January 2002

Please
Recycle

Adobe PostScript

Securing Sun Fire™ 15K Domains

The Sun Fire™ 15K server is the largest Sun server ever sold and will be used in a wide variety of projects and deployments from server-consolidation projects in financial institutions to extremely sensitive data-storage applications at government agencies. These deployments of Sun Fire 15K servers require that systems be secured against unauthorized access and misuse by malicious individuals.

Sun Fire 15K domains introduce a new variable to Solaris™ Operating Environment (Solaris OE) systems with platform-specific software components (for example, daemons) and services. These platform-specific software components impact the processes and procedures which must be used to secure the Solaris OE configuration running on the Sun Fire 15K domains. To properly secure a Sun Fire 15K domain, you must understand the impact of these new software components and have access to a well-documented and well-supported configuration to identify which modifications are appropriate and which are not.

This Sun BluePrints™ OnLine article documents all of the security modifications that can be performed on a Sun Fire 15K domain without affecting its behavior. The configuration described in this article, which includes all of the permitted security modifications, may not be appropriate for Sun Fire 15K domains with applications that require these disabled services. While configurations that do not use all of the security modifications in this article are acceptable, you should carefully evaluate services that are not disabled to ensure that they are absolutely required and that they are carefully protected against misuse.

This article focuses on Sun Fire 15K domain-specific software. While the configuration documented by this article performs generic Solaris OE hardening tasks, references to Sun BluePrints OnLine articles that provide more detailed information are provided, when necessary.

In addition, the article provides information about simplifying the installation and deployment of hardened Sun Fire 15K domains by automating security modifications with the Solaris Security Toolkit software. A Sun Fire 15K domain-specific driver for use with the toolkit is being released in parallel with this article, enabling you to implement all of the Solaris OE modifications possible on a Sun Fire 15K domain.

This Sun BluePrints article is the second in a series of Sun BluePrints articles that will provide specific recommendations for enhancing the security of a Sun Fire 15K server. The first article in this series, “Securing the Sun Fire™ 15K System Controller,” was published in November 2001. This article, as well as the Sun BluePrints OnLine articles it references, are available in electronic format from Sun BluePrints OnLine at `http://www.sun.com/security/blueprints`

Goal

The goal of this Sun BluePrints OnLine article is to provide a baseline security configuration for Sun Fire 15K domains by describing all of the possible security modifications. After reading about the Sun tested and Sun supported configuration presented in this article, you will understand how the configuration of a secured Sun Fire 15K domain differs from the secured configurations of other Sun servers.

A Solaris OE configuration hardened to the degree described in this article may not be appropriate for all environments. When installing and hardening a specific Solaris OE instance, you can perform fewer hardening operations than are recommended. For example, if your environment requires Network File System (NFS)-based services, you can leave them enabled. However, hardening beyond that which is presented in this article should not be performed and is neither recommended, nor supported.

Note – Standard security rules apply to hardening Sun Fire 15K domains: *That which is not specifically permitted is denied.*

Supportability

The Sun Fire 15K domain configuration implemented by the Solaris Security Toolkit domain driver is a Sun supported configuration. While it is not required that you use the toolkit to harden the domain, it is strongly recommended.

Note – Sun Support Services will support hardened domains whether security modifications are performed manually or through the use of the Solaris Security Toolkit software.

Please note that the toolkit is not a supported Sun product; only the end-configuration created by the toolkit is supported. Toolkit support is available through the Sun™ SupportForum discussion group at `http://www.sun.com/security/jass`

Assumptions and Limitations

The configuration described in this article has the following characteristics:

- Solaris 8 OE 10/01 software
- System Management Services (SMS) 1.1 software
- SUNWCall Solaris OE cluster
- Sun Quad FastEthernet™ card installed in each domain
- Solaris OE minimization not supported

The following sections describe each of these characteristics in greater detail.

Solaris 8 OE

This article is based on the Solaris 8 OE 10/01. All of the hardening results presented in this article were performed on this version of the Solaris OE. Using versions other than Solaris 8 OE 10/01 may produce results that are slightly different than those presented in this article.

SMS

The configuration described in this article was managed by a System Controller (SC) running SMS version 1.1. This was the configuration that was validated and verified. Using other SMS versions is not discussed in this article and is not supported.

Solaris OE Packages

The Solaris 8 OE installation discussed in this article is based on the `SUNWCall` cluster, which includes all Solaris OE software on the distribution CDs. In addition, required Sun Fire 15K packages must be installed. These packages will be enumerated.

Solaris Security Toolkit Software

The hardening of a Sun Fire 15K domain does not have to be performed through the use of the Solaris Security Toolkit software; however, because it provides an error free, standardized mechanism for performing the hardening process, and because it enables you to undo changes after they are made, it is highly recommended that you use the toolkit.

Network Cards

This Sun BluePrints OnLine article also assumes that at least one network card, such as a Sun Quad FastEthernet card, is installed in each domain being secured.

Minimization

Minimization is not supported on Sun Fire 15K domains at this time. Only the Solaris OE hardening tasks discussed in this article are supported for a Sun Fire 15K domain.

Domain Solaris OE Configuration

This section describes the additional packages, daemons, startup scripts, and other configuration modifications that are specific to a Sun Fire 15K domain. While not all of these daemons affect the security of the system directly, from a security perspective, you should always be aware of them and their impact on the system.

The following Sun Fire 15K domain-specific packages are installed as part of the SUNWCall cluster:

```
system  SUNWdrcrx   Dynamic Reconfiguration Modules for Sun Fire 15000 (64-bit)
system  SUNWsckmr   Init script & links for Sun Fire 15000 Key Management daemon
system  SUNWsckmu   Key Management daemon for Sun Fire 15000
system  SUNWsckmx   Key Management Modules for Sun Fire 15000 (64-Bit)
```

The Sun Fire 15K domain software does not change /etc/passwd, /etc/shadow, or /etc/group files. This is unlike the Sun Fire 15K SMS software on the System Controller (SC) which does modify these files.

The Sun Fire 15K domain-specific daemons are:

```
root   11   1 0 17:28:32 ? 0:00 /platform/SUNW,Sun-Fire-15000/lib/cvcd
root   121  1 0 17:28:46 ? 0:00 /usr/platform/SUNW,Sun-Fire-15000/lib/sckmd
```

While they are not Sun Fire 15K domain-specific, the following daemons are used for Dynamic Reconfiguration on Sun Fire 15K domains and should not be disabled:

```
root   324     1  0 07:47:24 ?        0:00 /usr/lib/efcode/sparcv9/efdaemon
root    58     1  0 05:32:57 ?        0:00 /usr/lib/sysevent/syseventd
root    60     1  0 05:32:57 ?        0:00 /usr/lib/sysevent/syseventconfd
root    65     1  0 05:32:59 ?        0:00 devfsadmd
root   371     1  0 05:33:12 ?        0:00 /usr/lib/saf/sac -t 300
root   631   295  0 16:30:34 ?        0:00 /usr/lib/dcs
```

Sun Fire 15K daemons are started by several different startup scripts including the /etc/init.d/cvc and /etc/init.d/sckm scripts.

The additional network used on a Sun Fire 15K domain to communicate with the Sun Fire 15K SC is defined similarly to regular network connections through an /etc/hostname.* entry. A typical Sun Fire 15K domain has a file that is similar to the following /etc file:

```
# more /etc/hostname.dman0
192.168.103.2 netmask 255.255.255.224 private up
```

The /etc/hostname.dman0 entry sets up the I1 or domain to the SC Management Network (MAN). This IP address, 192.168.103.2, is used for point-to-point communication between the domain and the SC. This network connection is implemented through the internal Sun Fire 15K MAN. No external wiring is utilized.

The network configuration appears as follows:

```
dman0: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4>
mtu 1500 index 2 inet 192.168.103.2 netmask ffffffe0 broadcast
192.168.103.31 ether 8:0:20:be:f8:f4
```

While the `dman0` network supports regular Internet Protocol (IP)-based network traffic, it should only be used by Sun Fire 15K management traffic. Any other use of this internal network may affect the reliability, availability, and serviceability (RAS) of the entire platform. Refer to the `scman` (7D) and `dman` (7D) man pages for more information.

Additionally, all Sun Fire 15K SC-to-domain communication over the MAN network is encrypted through the use of IPsec. The IPsec protocol suite is used to provide privacy and authentication services at the IP layer as defined by the Internet Engineering Task Force (IETF). For additional information about IPsec, refer to RFC 2411 at `http://www.ietf.org`.

Attempts to access Sun Fire 15K domain and SC daemons from non-MAN networks will generate `syslog` messages indicating that an access attempt was made. A log message appears as follows:

```
Sep 20 08:04:26 xc17p13-b5 ip: [ID 993989 kern.error]
ip_fanout_tcp_listen: Policy Failure for the incoming packet (not
secure); Source 192.168.181.252, Destination 010.001.073.042.
```

Note – Do not use MAN networks for anything other than Sun Fire 15K management traffic. These are Sun Fire 15K specific networks and they are not for general-purpose use.

Sun Fire 15K Domain Hardening

This section describes the Solaris Security Toolkit software and provides an overview of its two different modes of operation. In addition, this section summarizes the security modifications made to the domain.

Standalone Versus JumpStart™ Modes

Hardening a Sun Fire 15K domain can be done automatically during a JumpStart™ installation of the operating system (OS), or it can be performed following the installation of the OS. This article documents the methods for manually hardening a domain after the OS installation has been completed, as a discussion of the JumpStart environment is beyond the scope of this article. For information about setting up a JumpStart server and integrating the Solaris Security Toolkit software with a JumpStart server, refer to the following Sun BluePrints OnLine articles referenced in the Bibliography:

- "The Solaris™ Security Toolkit - Quick Start: Updated for version 0.3"
- "Building a JumpStart™ Infrastructure"

This article does not discuss the installation of the Solaris 8 OE 10/01 `SUNWCall` cluster or the initial configuration of the Sun Fire 15K domain software. Instead, this article focuses on the steps involved in securing a domain including installing security-related software, installing the latest patch clusters, and hardening the OS. This hardening is critical to the security of the domain, as the default configuration of Solaris OE may not provide the required level of security.

Solaris Security Toolkit Software

As previously mentioned, we strongly recommend that you use the Solaris Security Toolkit software to secure a domain. The toolkit implements the recommendations made in this article, as well as the security recommendations provided in the following articles:

- "Solaris™ Operating Environment Security: Updated for the Solaris 8 Operating Environment"
- "Solaris™ Operating Environment Network Settings for Security: Updated for Solaris 8"
- "The Solaris™ Security Toolkit - Installation, Configuration, and Usage Guide: Updated for version 0.3"

These articles are referenced in the Bibliography and are available from the Sun BluePrints OnLine Web site at `http://www.sun.com/security/blueprints`

Security Modifications

The security recommendations in this article include all Solaris OE modifications that do not impact required Sun Fire 15K domain functionality. This does not mean these modifications are appropriate for every domain. In fact, it is likely that some of the services disabled by the default `sunfire_15k_domain-secure.driver` script will affect some applications. Because applications and their service requirements vary, it is unusual for one configuration to work for all applications.

Note – Consider the role of a secured configuration in the context of the applications and services that the Sun Fire 15K domain will provide. The security configuration presented in this article is a high-watermark for system security, as every service that is not required by the Sun Fire 15K platform is disabled. This information should provide you with a clear idea of which services can and cannot be disabled without affecting the behavior of Sun Fire 15K domains. You can then include the application-specific requirements of your environment to identify which security modifications can and cannot be performed.

For information about Solaris OE services and for recommendations about mitigating their security implications, refer to the Sun BluePrints OnLine article “Solaris™ Operating Environment Security: Updated for the Solaris 8 Operating Environment” and the Sun BluePrints OnLine article “Solaris™ Operating Environment Network Settings for Security: Updated for Solaris 8.” The recommendations in these articles are implemented with the Solaris Security Toolkit software in standalone and JumpStart modes. In addition, the Sun BluePrints OnLine article “The Solaris™ Security Toolkit - Internals: Updated for version 0.3” describes the functions of each of the toolkit scripts.

The three scripts used by the toolkit to harden a Sun Fire 15K domain are:

- `sunfire_15k_domain-config.driver`
- `sunfire_15k_domain-hardening.driver`
- `sunfire_15k_domain-secure.driver`

These files should be copied and the copies used to make environment-specific modifications will simplify the migration to new versions of the toolkit as they become available.

To prevent the toolkit from disabling services, comment out the call to the appropriate finish script in the driver. For example, in the preceding NFS server example, it is necessary to comment out only the `disable-nfs-server.fin` and `disable-rpc.fin` scripts by appending a ‘#’ sign before them in the copy of the `sunfire_15k_domain-hardening.driver` script. For more information about editing and creating driver scripts, refer to the Sun BluePrints OnLine article titled “The Solaris™ Security Toolkit - Installation, Configuration, and Usage Guide: Updated for version 0.3.”

Each of the modifications performed by the toolkit falls into one of the following categories:

- Disable
- Enable
- Install
- Remove
- Set
- Update

In addition, the toolkit copies files from the toolkit distribution to increase the security of the system. These system configuration files change the default behavior of syslogd, system network parameters, and a variety of other system configurations.

The following sections briefly describe each of these categories and the script modifications they perform. For a complete listing of the scripts included in the sunfire_15k_domain driver, refer to Appendix A of this article.

Disable Scripts

These scripts disable services on the system. Disabled services include the NFS client and server, the automounter, the DHCP server, printing services, and the window manager. The goal of these scripts is to disable all of the services that are not required by the system.

A total of 31 disable scripts are included with the Sun Fire 15K domain-hardening driver. These scripts impose the following modifications to disable all, or part, of the following services and configuration files:

TABLE 1 Scripts Affected By Domain Hardening

apache	lpsched	printd
aspppd	mipagent	rpcbind
automountd	mountd	sendmail
core generation	nfsd	slp
dhcp	nscd	smcboot
dtlogin	pam.conf	snmpdx
IPv6	picld	snmpXdmid
keyservd	pmconfig	syslogd
ldap_cachemgr	lpsched	

Enable Scripts

These scripts enable the security features that are disabled by default on Solaris OE. These modifications include:

- Enabling optional logging for `syslogd` and `inetd`
- Requiring NFS clients to use a port below 1024
- Enabling process accounting
- Enabling improved sequence number generation per RFC 1948
- Enabling optional stack protection and logging

While some of these services are disabled by the toolkit, their optional security features remain enabled so that they are used securely if enabled in the future.

Install Scripts

These scripts create new files to enhance system security. In the Sun Fire 15K driver, the following Solaris OE files are created to enhance the security of the system:

- An empty `/etc/cron.d/at.allow` file to restrict access to `at` commands
- An updated `/etc/ftpusers` file with all system accounts restricts FTP access to the system
- An empty `/var/adm/loginlog` to log unsuccessful login attempts
- An updated `/etc/shells` file to limit which shells can be used by system users
- An empty `/var/adm/sulog` to log `su` attempts to root

In addition to creating the preceding files, some install scripts also add software to the system. Specifically, on Sun Fire 15K domains, the following software is installed:

- Recommended and Security patch clusters
- MD5 software
- OpenSSH software
- FixModes software

Remove Scripts

Only one remove script is distributed with the Sun Fire 15K driver; it used to remove unused Solaris OE system accounts. The accounts that are removed are no longer used by the Solaris OE and can safely be removed. The removed accounts include:

- smtp
- nuucp
- listen
- nobody4

Set Scripts

These scripts configure the security features of the Solaris OE that are not defined by default. Thirteen of these scripts are distributed with the Sun Fire 15K domain driver and can configure the following optional Solaris OE features not enabled by default:

- root password
- ftpd banner
- telnetd banner
- ftpd UMASK
- login RETRIES
- Power restrictions
- Use of SUID on removable media
- System suspend options
- TMPFS size
- User password requirements
- User UMASK

Update Scripts

These scripts update the configuration files that are shipped with the Solaris OE but that do not have all of their security settings properly set. Modifications are made to the following configuration files:

- `at.deny`
- `cron.allow`
- `cron.deny`
- `logchecker`
- `inetd.conf`

The modifications made to the `inetd.conf` file include disabling all of the entries the Solaris OE includes in the `/etc/inetd.conf` file. Disabling these entries turns off all interactive access mechanisms to the domain including TELNET, FTP, and all of the r* services. Serial access to the system is not affected.

Installing Security Software

The security recommendations to secure the Sun Fire 15K domain involve the installation of several security software packages. These packages include:

- Recommended and Security patch clusters
- FixModes software
- OpenSSH software
- MD5 software

Note – Of the packages described in this section, only the Solaris Security Toolkit software, the latest Recommend and Security patch clusters, the FixModes software, and the MD5 software are required. The use of OpenSSH, while strongly recommended, is not required. Commercial versions of SSH, available from a variety of vendors, may be substituted for OpenSSH.

The first step of securing a domain is to install the required software. This section describes how to install all required software packages.

Installing the Solaris Security Toolkit Software

First, download the Solaris Security Toolkit software and install it on the domain. The toolkit is used to automate the Solaris OE hardening tasks described later in this article.

The purpose of using the toolkit is to automate and simplify the building of secured Solaris OE systems based on the recommendations contained in this and other security-related Sun BluePrints articles referenced in this article. In the context of this article, a module has been developed to harden Sun Fire 15K domains.

Specifically, the toolkit focuses on Solaris OE security modifications that harden and minimize a system. Hardening is the modification of Solaris OE configurations to improve the security of the system. Minimization is the removal of unnecessary Solaris OE packages from the system to reduce the number of components that must be patched and secured. Reducing the number of components can potentially reduce entry points to an intruder.

Note – The toolkit does not address modifications for performance enhancement and software configuration.

The toolkit can harden systems during a Solaris OE installation by using the JumpStart technology as a mechanism for running toolkit scripts. Alternatively, the toolkit can be run outside of the JumpStart framework in standalone mode. This standalone mode enables you to use the toolkit on systems that require security modifications or updates but which cannot be taken out of service to reinstall the OS from scratch.

The Sun Fire 15K specific domain driver can be used in either standalone or JumpStart mode to secure a domain. It automates the hardening recommendations made in this Sun BluePrints article. This driver is included in version 0.3.4 of the Solaris Security Toolkit software.

When running the toolkit, either in standalone or JumpStart installation modes, copies of the files modified by the toolkit must not be deleted, which is the default behavior of the toolkit. The `JASS_SAVE_BACKUP` environment variable controls whether or not backup copies of files are kept.

Note – The following instructions use file names that are correct only for this release of the toolkit. It is recommended that you always use the most current version of the toolkit available from the URL provided in the first step of the following procedure.

Use the following procedure to download and install the toolkit:

1. **Download the source file (**`SUNWjass-0.3.4.pkg.Z`**).**

   The source file is located at `http://www.sun.com/security/jass`

2. **Use the** `uncompress` **command to extract the source file into a directory on the server as follows**:

```
# uncompress SUNWjass-0.3.4.pkg.Z
```

3. **Use the** `pkgadd` **command to install the Solaris Security Toolkit software on the server as follows:**

```
# pkgadd -d SUNWjass-0.3.4.pkg SUNWjass
```

Executing this command creates the `SUNWjass` directory in `/opt`, which contains all of the toolkit directories and associated files. The script `make-jass-pkg`, which is included in toolkit releases since 0.3, enables you to create custom packages using a different installation directory.

Installing the Recommended and Security Patch Clusters

The installation procedures in this section use the Solaris Security Toolkit software to install the most recent Recommended and Security Patch clusters which are available from the SunSolve^{SM} Online Web site. To install these patches with the toolkit, download them and store them, uncompressed, in the `/opt/SUNWjass/Patches` directory on the domain.

Sun regularly releases patches to provide Solaris OE fixes for performance, stability, functionality, and security reasons. It is critical to the security of the system that you install the most up-to-date patch clusters. This section describes how to use the Solaris Security Toolkit software to automatically install patches, thereby ensuring that the latest Recommended and Security patch clusters are installed on the domain.

1. **To download the latest cluster, go to the SunSolve Online Web site at** `http://sunsolve.sun.com` **and click the Patches link on the top of the left navigation bar.**

Note – Downloading the Solaris OE Recommended and Security patch clusters does not require a SunSolve^{SM} support contract.

---

2. **Next, select the appropriate Solaris OE version in the Recommended Solaris Patch Clusters box. This example uses Solaris 8 OE.**

3. **After selecting the appropriate Solaris OE version, select the best download option, either HTTP or FTP, with the associated radio button and click the Go button.**

4. **In the Save As window that appears in your browser, save the file locally in preparation for uploading it to the domain being hardened.**

5. **After downloading the cluster, move the file securely to the domain using either the** `scp` **SSH command or the** `sftp` **SSH command. If SSH is not yet installed, use the** `ftp` **command. The** `scp` **command used to copy the file to an domain called** `domain01` **should appear similar to the following:**

```
% scp 8_Recommended.zip domain01:/var/tmp
```

6. **Next, you must move the file to the** `/opt/SUNWjass/Patches` **directory and uncompress it. The following commands perform these tasks:**

```
# cd /opt/SUNWjass/Patches
# mv /var/tmp/8_Recommended.zip .
# unzip 8_Recommended.zip
Archive:  8_Recommended.zip
   creating: 8_Recommended/
  inflating: 8_Recommended/CLUSTER_README
  inflating: 8_Recommended/copyright
  inflating: 8_Recommended/install_cluster
[. . .]
```

Once unzipped in the `/opt/SUNWjass/Patches/8_Recommended` directory, the latest patch cluster is automatically installed by the Solaris Security Toolkit software.

Installing the FixModes Software

This section describes how to download and install the FixModes software into the appropriate toolkit directory so it can be used to tighten file permissions during the toolkit run. By selectively modifying system permissions, it will be more difficult for malicious users to gain additional privileges on the system.

Follow these instructions to download the FixModes software:

1. **Download the FixModes precompiled binaries from** `http://www.sun.com/blueprints/tools/FixModes_license.html`

   The FixModes software is distributed as a precompiled and compressed tar file.

2. **Save the downloaded file,** `FixModes.tar.Z`**, to the Solaris Security Toolkit** `Packages` **directory in** `/opt/SUNWjass/Packages`

Note – Do not uncompress the tar archive.

Installing the OpenSSH Software

In any secured environment, the use of encryption, in combination with strong authentication, is highly recommended. At a minimum, user interactive sessions should be encrypted. The tool most commonly used to implement this is an implementation of secure shell (SSH) software. You can use either the commercially purchased version of the software or the freeware version of the software.

The use of a SSH variant is strongly recommended when implementing all of the security modifications performed by the Solaris Security Toolkit software. The toolkit disables all nonencrypted user-interactive services and daemons on the system. In particular, services such as `in.rshd`, `in.telnetd`, and `in.ftpd` are disabled. Access to the system can be gained with SSH in a similar fashion to what is provided by RSH, TELNET, and FTP. It is strongly recommended that you install SSH during a toolkit run as described in this article.

For information about compiling and deploying OpenSSH, refer to the Sun BluePrints OnLine article “Building and Deploying OpenSSH on the Solaris™ Operating Environment (July 2001)” available at `http://www.sun.com/blueprints/0701/openSSH.pdf`

Information about obtaining commercial versions of SSH is provided in the Bibliography section of this article.

Installing the MD5 Software

This section describes how to download and install the MD5 software used to validate MD5 digital fingerprints on Sun Fire 15K domains. The ability to validate the integrity of Solaris OE binaries provides a robust mechanism for detecting system binaries that may have been altered by unauthorized users of the system. By modifying system binaries, attackers can gain back-door access to the system.

Once it is installed, you can use the Solaris Fingerprint Database to verify the integrity of the executables included in the package. For more information about the Solaris Fingerprint Database, refer to the Sun BluePrint OnLine article “The Solaris™ Fingerprint Database—A Security Tool for Solaris Operating Environment and Files” available at `http://www.sun.com/blueprints/0501/Fingerprint.pdf.` This article also provides information about additional tools that can be used to simplify the process of validating system binaries against the database of MD5 checksums maintained by Sun at SunSolve Online Web site.

It is strongly recommended that you use these tools, in combination with the MD5 software installed in this section, to frequently validate the integrity of the Solaris OE binaries and files on the domain. In addition, ensure that MD5 signatures generated on the server are protected until they are sent to the Solaris FingerPrint Database for validation. After they have been used, delete the MD5 signatures until they are regenerated for the next validation check.

To install the MD5 program (Intel and SPARC™ technologies), follow these steps:

1. **Download the MD5 binaries from** `http://www.sun.com/blueprints/tools/md5_license.html`

   The MD5 programs are distributed as a compressed tar file.

2. **Save the downloaded file,** `md5.tar.Z`**, to the Solaris Security Toolkit** `Packages` **directory in** `/opt/SUNWjass/Packages`

Note – Do not uncompress the tar archive.

After the MD5 software has been saved to the `/opt/SUNWjass/Packages` directory, it is installed during the execution of the Solaris Security Toolkit software.

Domain Solaris OE Modifications

Once all of the software is installed, you can secure the Solaris OE image running on the Sun Fire 15K domain.

Note – Before implementing the security recommendations in the following sections, note that all non-encrypted access mechanisms to the domain (for example, TELNET and RSH) will be disabled. The hardening steps will not disable console serial access from the Sun Fire 15K SC using the `console` command.

Executing the Solaris Security Toolkit Software

The Solaris Security Toolkit software provides specific drivers that automate the hardening of a Sun Fire 15K domain. This section explains the process of using the Solaris Security Toolkit software to harden a Sun Fire 15K domain.

Note – In this example, the toolkit is used in standalone mode for clarity and simplicity. All of the tasks performed in standalone mode can also be implemented in JumpStart mode. For additional information about integrating the toolkit with the JumpStart technology, refer to the Sun BluePrints OnLine article "The Solaris™ Security Toolkit - Installation, Configuration, and Usage Guide: Updated for version 0.3."

Execute the toolkit as follows:

```
# cd /opt/SUNWjass
# ./jass-execute -d sunfire_15k_domain-secure.driver
./jass-execute: NOTICE: Executing driver,
sunfire_15k_domain-secure.driver

============================================================
sunfire_15k_domain-secure.driver: Driver started.
============================================================
[...]
```

By executing the `sunfire_15k_domain-secure.driver` script, all of the security modifications included in the script are made on the system. The current release of this script includes over 100 security modifications to the domain.

Note – The `sunfire_15k_domain-secure.driver` script automatically installs the FixModes software and the MD5 software, if they are available. In addition, if the FixModes software is installed, the toolkit also executes it to tighten the file system permissions on the system.

In addition to displaying the output to the console, the toolkit creates a log file in the `/var/opt/SUNWjass/run` directory. Each execution of the Solaris Security Toolkit software creates an additional directory in `/var/opt/SUNWjass/run`. The names of these directories are based on the date and time the run began.

Caution – The contents of the `/var/opt/SUNWjass/run` directories should not be modified under any circumstances. User modification of the files contained in these directories may corrupt the contents and cause unexpected errors when using Solaris Security Toolkit software features such as `undo`.

The files stored in the /var/opt/SUNWjass/run directory are not only used to track the modifications that were performed on the system, but are also used for the jass-execute undo functionality. A run, or series of runs, can be undone with the jass-execute -u command. For example, on a system where seven separate toolkit runs were performed, they could all be undone with the following command:

```
# pwd
/opt/SUNWjass
# ./jass-execute -u
Please select from one of these backups to restore to
1.  December 10, 2001 at 19:45:15 (//var/opt/SUNWjass/run/20011210194515)
2.  December 10, 2001 at 19:25:22 (//var/opt/SUNWjass/run/20011210192522)
3.  December 10, 2001 at 19:07:32 (//var/opt/SUNWjass/run/20011210190732)
4.  December 10, 2001 at 19:04:36 (//var/opt/SUNWjass/run/20011210190436)
5.  December 10, 2001 at 18:30:35 (//var/opt/SUNWjass/run/20011210183035)
6.  December 10, 2001 at 18:29:48 (//var/opt/SUNWjass/run/20011210182948)
7.  December 10, 2001 at 18:27:44 (//var/opt/SUNWjass/run/20011210182744)
8.  Restore from all of them
Choice?  8
./jass-execute: NOTICE: Restoring to previous run
//var/opt/SUNWjass/run/20011210194515

===============================================================
undo.driver: Driver started.
===============================================================
[...]
```

For more information about the Solaris Security Toolkit software, refer to the /opt/SUNWjass/Documentation directory or access the documentation that is available online at http://www.sun.com/security/jass

Note – Software installations and actions performed by those software packages are not undone by the toolkit undo feature. This includes the installation of OpenSSH, FixModes, and MD5. In addition, the modifications performed by FixModes are not automatically undone by jass-execute -u.

Verifying Domain Hardening

Once the hardening process has been completed and a domain has been hardened, reboot the domain and verify its configuration by having it perform the tasks it should be capable of. At a minimum, this verification process should assure that each of the services to be provided by the hardened domain are running and functioning properly. Any additional software installed on the domain should also be verified and validated for correctness. Ideally, existing quality assurance or acceptance testing and scripts should be used to verify the operation of the hardened domain to assure that the hardening process has not adversely impacted any required features.

Secured Domain Solaris OE Configuration

The modifications to secure a Sun Fire 15K domain's Solaris OE configuration resulted in reducing the number of TCP and UDP services listening from 93 to 4. Similarly, the number of registered RCP services went from 149 to 0. This represents a significant improvement in the security of the Solaris OE on a domain to enhance its security. Once the domain has been hardened, appropriate versions of SSH have been installed, and the system has been rebooted, the only network services that should be available should be similar to those listed here:

```
# netstat -a
UDP: IPv4
    Local Address         Remote Address     State
-------------------- -------------------- -------
      *.*                                  Unbound

TCP: IPv4
Local Address Remote Address Swind Send-Q Rwind Recv-Q  State
-------------------- -------------------- ----- ------ ----- -
*.*                  *.*                0      0 24576      0 IDLE
*.cvc_hostd  *.*               0      0 24576      0 LISTEN
*.sun-dr        *.*               0      0 24576      0 LISTEN
*.32772          *.*               0      0 24576      0 LISTEN
*.22                *.*               0      0 24576      0 LISTEN

TCP: IPv6
Local Address Remote Address Swind Send-Q Rwind Recv-Q State If
-------------------------------- --------------------------
*.*         *.*                        0    0 24576   0 IDLE
*.cvc_hostd *.*                  0      0 24576   0 LISTEN
*.sun-dr    *.*                    0     0 24576   0 LISTEN
*.22        *.*                        0      0 24576   0 LISTEN

Active UNIX domain sockets
Address  Type         Vnode     Conn  Local Addr      Remote Addr
3000b987cb8 stream-ord 3000b989c98 00000000 /var/spool/prngd/pool
```

After hardening, the daemons left running are:

```
[xc4p02-b11/] uname -a
SunOS xc17p13-b5 5.8 Generic_108528-11 sun4u sparc SUNW,Sun-Fire-15000
[xc4p02-b11/] ps -ef
     UID   PID  PPID  C    STIME TTY      TIME CMD
root   0 0 0 19:26:36 ?   0:02 sched
root   1 0 0 19:26:36 ?   0:00 /etc/init -
root   2 0 0 19:26:36 ?   0:00 pageout
root   3 0 0 19:26:36 ?   0:00 fsflush
root 394 1 0 19:27:05 ?   0:00 /usr/lib/saf/sac -t 300
root 286 1 0 19:26:55 ?   0:00 /usr/lib/utmpd
root 246 1 0 19:26:53 ?   0:00 /usr/platform/SUNW,Sun-Fire-15000/lib/sckmd
root  11 1 0 19:26:38 ?   0:00 /platform/SUNW,Sun-Fire-15000/lib/cvcd
root  59 1 0 19:26:45 ?   0:00 /usr/lib/sysevent/syseventd
root  61 1 0 19:26:45 ?   0:00 /usr/lib/sysevent/syseventconfd
root  68 1 0 19:26:47 ?   0:00 devfsadmd
root 279 1 0 19:26:55 ?   0:00 /usr/sbin/nscd
root 254 1 0 19:26:53 ?   0:00 /usr/sbin/inetd -s -t
root 262 1 0 19:26:53 ?   0:00 /usr/sbin/syslogd -t
root 265 1 0 19:26:54 ?   0:00 /usr/sbin/cron
root 397 394 0 19:27:05 ? 0:00 /usr/lib/saf/ttymon
root 305 1 0 19:26:56 ?   0:00 /usr/lib/efcode/sparcv9/efdaemon
root 325 1 0 19:26:58 ?   0:00 /opt/OBSDssh/sbin/prngd --cmdfile /etc/
prngd.conf --seedfile /etc/prngd-seed /v
root 378 1 0 19:27:04 ?   0:00 /opt/OBSDssh/sbin/sshd
root 407 1 0 19:27:56 ?   0:00 /usr/lib/sendmail -q15m
root 631 1 0 19:28:34 ?   0:00 /usr/lib/dcs
```

An additional check to validate the services available on the domain was performed using nmap, as follows:

```
# ./nmap -p 1-65535 -sS -sU 10.0.0.200
```

This port scan, using the popular freeware network scanner nmap command, was performed from a system external to the Sun Fire 15K frame. For more information about the nmap command, visit http://www.insecure.org/nmap

The scan verified that only the following network services are available from outside the frame of the Sun Fire 15K domain.

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on xc4p02-b11.blueprints.Sun.COM (10.0.0.200):
Port       State       Service
22/tcp     open        ssh
442/tcp    filtered    cvc_hostd
665/tcp    filtered    sun-dr

Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
```

This scan generated the following `syslog` error messages:

```
Sep 20 08:04:26 xc17p13-b5 ip: [ID 993989 kern.error]
ip_fanout_tcp_listen: Policy Failure for the incoming packet (not
secure); Source 129.148.181.252, Destination 010.001.073.042.

Sep 20 08:04:27 xc17p13-b5 last message repeated 1 time

Sep 20 08:04:28 xc17p13-b5 sshd[357]: [ID 800047 auth.error]
error: setsockopt SO_KEEPALIVE: Invalid argument

Sep 20 08:04:29 xc17p13-b5 ip: [ID 993989 kern.error]
ip_fanout_tcp_listen: Policy Failure for the incoming packet (not
secure); Source 129.148.181.252, Destination 010.001.073.042.

Sep 20 08:04:30 xc17p13-b5 last message repeated 1 time
```

These error messages were produced by the `nmap` command as it attempted to access the Sun Fire 15K daemons `cvcd` and `sckmd.` Error messages were produced because the `nmap IP packets` did not conform to the IPsec security policies used to protect those ports. IPsec is used to encrypt all Sun Fire 15K traffic traversing the I1 or MAN internal network.

Conclusion

A SunFire 15K domain must be secured against unauthorized access to protect it and the information it contains. A secure system also improves RAS as the system will be more secure from malicious misuse and attack.

SunFire 15K domains run the Solaris 8 OE. Many of the recommendations made in other Sun BluePrints OnLine articles about hardening Solaris OE apply to SunFire 15K domains. This article uses these recommendations, in addition to domain-specific suggestions, to improve the overall security posture of a SunFire 15K domain by dramatically reducing potential access points to the domain and by installing secure access mechanisms. In addition, a mechanism is provided to automate the installation of these recommendations through the Solaris Security Toolkit software.

Appendix A

The following list contains all of the Solaris Security Toolkit scripts included, by default, in the `sunfire_15_domain-secure.driver` file. The scripts are executed in the order listed here:

TABLE 2 Solaris Security Toolkit Scripts

- `disable-dmi.fin`
- `set-root-password.fin`
- `set-term-type.fin`
- `disable-apache.fin`
- `disable-asppp.fin`
- `disable-autoinst.fin`
- `disable-automount.fin`
- `disable-core-generation.fin`
- `disable-dhcpd.fin`
- `install-recommended-patches.fin`
- `disable-dtlogin.fin`
- `disable-ipv6.fin`
- `disable-vold.fin`
- `disable-ldap-client.fin`
- `disable-lp.fin`
- `disable-mipagent.fin`
- `disable-nfs-client.fin`
- `disable-rhosts.fin`
- `disable-rpc.fin`
- `disable-sendmail.fin`
- `disable-slp.fin`
- `disable-snmp.fin`
- `disable-spc.fin`
- `disable-syslogd-listen.fin`
- `disable-system-accounts.fin`
- `disable-uucp.fin`
- `disable-keyserv-uid-nobody.fin`
- `disable-wbem.fin`
- `enable-ftp-syslog.fin`
- `enable-inetd-syslog.fin`
- `enable-priv-nfs-ports.fin`
- `enable-process-accounting.fin`
- `enable-rfc1948.fin`
- `enable-stack-protection.fin`
- `install-shells.fin`
- `install-sulog.fin`
- `remove-unneeded-accounts.fin`
- `set-banner-ftpd.fin`
- `set-banner-telnetd.fin`
- `set-ftpd-umask.fin`
- `set-login-retries.fin`
- `set-power-restrictions.fin`
- `set-rmmount-nosuid.fin`
- `set-sys-suspend-restrictions.fin`
- `set-system-umask.fin`
- `set-tmpfs-limit.fin`
- `set-user-password-reqs.fin`
- `set-user-umask.fin`
- `update-at-deny.fin`
- `update-cron-allow.fin`
- `update-cron-deny.fin`

TABLE 2 Solaris Security Toolkit Scripts *(Continued)*

`disable-nfs-server.fin`	`install-at-allow.fin`	`update-cron-log-size.fin`
`disable-nscd-caching.fin`	`install-ftpusers.fin`	`update-inetd-conf.fin`
`disable-preserve.fin`	`install-loginlog.fin`	`install-md5.fin`
`disable-picld.fin`	`install-newaliases.fin`	`install-fix-modes.fin`
`disable-power-mgmt.fin`	`install-sadmind-options.fin`	`install-strong-permissions.fin`
`disable-remote-root-login.fin`	`install-security-mode.fin`	

Bibliography

- *System Management Services (SMS) 1.1 Administrator Guide*, Sun Microsystems, Part No 816-0900-10, October 2001, Revision A, `http://docs.sun.com`
- *System Management Services (SMS) 1.1 Reference Guide*, Sun Microsystems, Part No 816-0901-10, October 2001, Revision A, `http://docs.sun.com`
- Deeths, David and Brunette, Glenn, “Using NTP to Control and Synchronize System Clocks - Part II: Basic NTP Administration and Architecture,” Sun BluePrints OnLine, August 2001, `http://sun.com/blueprints/0801/NTPpt2.pdf`
- Noordergraaf, Alex, “Building a JumpStart™ Infrastructure,” Sun BluePrints OnLine, April 2001, `http://sun.com/blueprints/0401/BuildInf.pdf`
- Noordergraaf, Alex, “Building Secure N-Tier Environments,” Sun BluePrints OnLine, October 2000, `http://sun.com/blueprints/1000/ntier-security.pdf`
- Noordergraaf, Alex, “Solaris™ Operating Environment Minimization for Security: Updated for the Solaris 8 Operating Environment,” Sun BluePrints OnLine, November 2000, `http://sun.com/blueprints/1100/minimize-updt1.pdf`
- Noordergraaf, Alex and Brunette, Glenn, “The Solaris™ Security Toolkit - Installation, Configuration, and Usage Guide: Updated for version 0.3,” Sun BluePrints OnLine, June 2001, `http://sun.com/blueprints/0601/jass_conf_install-v03.pdf`
- Noordergraaf, Alex and Brunette, Glenn, “The Solaris™ Security Toolkit - Internals: Updated for version 0.3,” Sun BluePrints OnLine, June 2001, `http://sun.com/blueprints/0601/jass_internals-v03.pdf`
- Noordergraaf, Alex and Brunette, Glenn, “The Solaris™ Security Toolkit - Quick Start: Updated for version 0.3,” Sun BluePrints OnLine, June 2001, `http://sun.com/blueprints/0601/jass_quick_start-v03.pdf`

- Noordergraaf, Alex and Kurktchi, Dina, “Securing the Sun Fire™ 15K System Controller,” Sun BluePrints OnLine, November 2001, `http://sun.com/blueprints/1101/sunfire15k.pdf`
- Noordergraaf, Alex and Watson, Keith, “Solaris™ Operating Environment Security: Updated for the Solaris 8 Operating Environment,” Sun BluePrints OnLine, April 2001, `http://sun.com/blueprints/0401/security-updt1.pdf`
- Reid, Jason M and Watson, Keith, “Building and Deploying OpenSSH in the Solaris™ Operating Environment,” Sun BluePrints OnLine, July 2001, `http://sun.com/blueprints/0701/openSSH.pdf`
- Watson, Keith and Noordergraaf, Alex, “Solaris™ Operating Environment Network Settings for Security: Updated for the Solaris 8 Operating Environment,” Sun BluePrints OnLine, December 2000, `http://sun.com/blueprints/1200/network-updt1.pdf`

Author’s Bio: Alex Noordergraaf

Alex Noordergraaf has over 10 years experience in the area of computer and network security. As a Senior Staff Engineer in the Enterprise Engineering group at Sun Microsystems, he is developing, documenting, and publishing security best practices through the Sun BluePrints OnLine program. Published article topics include: Sun Fire Midframe System Controller security, secure N-Tier environments, Solaris OE minimization, Solaris OE network settings, and Solaris OE security. In addition, he co-authored the recently published book JumpStart Technology- Effective Use in the Solaris Operating Environment. Alex is also one of the authors of the very popular freeware Solaris Security Toolkit (JASS) software.

Prior to his role in Enterprise Engineering, he was a Senior Security Architect with Sun Professional Services where he worked with many Fortune 500 companies on projects that included Security Assessments, Architecture Development, Architectural Reviews, and Policy/Procedure review and development. In addition to providing billable services to customers, he developed and delivered an Enterprise Security Assessment methodology and training curriculum to be used worldwide by the SunPS^{SM} *organization. His customers have included major telecommunication firms, financial institutions, ISPs, and ASPs.*

Author’s Bio: Dina Kurktchi

Dina Kurktchi is a Senior Software Engineer with 15 years of experience in many areas from device drivers to databases. For the past four years, Dina has focused on secure software development and the deployment of security system solutions such as vulnerability assessment tools, intrusion detection systems, and public key infrastructures. Currently, she works with the Enterprise Systems Group at Sun Microsystems.