



Securing the Sun Fire™ 15K System Controller

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

Sun BluePrints™ OnLine - November 2001



<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.: 816-2727-10
Revision 1.0, 10/17/01//
Edition: November 2001

Copyright 2001 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, California 94303 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Sun BluePrints, Sun Fire, JumpStart, SunSolve Online, OpenBoot, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the US and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, Californie 94303 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Sun BluePrints, Sun Fire, JumpStart, SunSolve Online, OpenBoot, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Please
Recycle



Adobe PostScript

Securing the Sun Fire™ 15K System Controller

Securing the System Controller (SC) is the first priority in configuring a Sun Fire™ 15K system to be resistant to unauthorized access and able to function properly in hostile environments. The first step in securing a system is understanding what services and daemons are running on that system. This article describes the software, services, and daemons specific to the Sun Fire 15K SC. This SC-specific functionality is described at a high-level with references to the appropriate Sun documentation for more detailed information. The goal is to provide administrators with a baseline for what functionality is required for the SC to perform properly.

This article is the first of several articles providing recommendations on how to enhance the security of a Sun Fire 15K system. The next article will focus on Sun Fire 15K domain security and be titled:

- *Sun Fire 15K Domain Security*

All of these articles, and the entire library of Sun BluePrints™ OnLine security articles are available electronically from Sun BluePrints OnLine at:

<http://www.sun.com/security/blueprints>

The recommendations made in this article include specific references of how the Solaris™ Operating Environment (Solaris OE) image that runs on the SC should be configured for secured environments, and what additional software should be installed. In addition, this article describes the SC functions and what an SC really is.

Overview

The Sun Fire 15K SC is a multi-function system board within the Sun Fire frame. This system is dedicated to running the System Management Services (SMS) software. The SMS software is used to define what boards are associated with what domains, provide console access to each of the domains, control whether a domain is powered on or off, and to provide a variety of other functions critical to the operation and monitoring of the Sun Fire 15K system. There may be up to two SCs within a Sun Fire 15K frame. The security recommendations are the same for both SCs.

The focus of this article is on SC functionality not included in the Solaris 8 OE running on the SC. When discussing security functionality bundled with the Solaris OE, the reader is referred to the Sun BluePrints OnLine articles which address the security functions in more detail. Some SC-specific configurations are in addition to what is recommended by the other Sun BluePrints OnLine security articles and are explained in the following sections. The Sun BluePrints OnLine articles referenced in this article are in the Bibliography and include:

- *Building and Deploying OpenSSH in the Solaris Operating Environment*
- *Building Secure N-Tier Environments*
- *Solaris Operating Environment Minimization for Security: Updated for the Solaris 8 Operating Environment*
- *Solaris Operating Environment Security: Updated for the Solaris 8 Operating Environment*
- *The Solaris Security Toolkit - Quick Start: Updated for version 0.3*

The recommendations made in this article are based on Solaris 8 10/01 (Update 6) OE and version 1.1 of the System Management Services (SMS) software running on the Sun Fire 15K System Controller. These are the Solaris OE and SMS versions on which the Sun Fire 15K product is first being made available.

Functions of the SC

The Sun Fire 15K SC is responsible for managing the overall Sun Fire 15K frame. The following list is an overview of the many services the SC provides for the Sun Fire 15K system:

- Manages the overall system configuration.
- Acts as a boot initiator for its domains.

- Serves as the `syslog` host for its domains; note that an SC can still be a `syslog` client of a LAN-wide `syslog` host.
- Provides a synchronized hardware clock source.
- Sets up and configures dynamic domains.
- Monitors system environmental information, such as power supply, fan, and temperature status.
- Hosts Field Replacable Unit (FRU) logging data.
- Provides redundancy and automated SC failover in dual SC configurations.
- Provides a default name service for the domains based on NIS+, virtual hostids, and MAC addresses for the domains.
- Provides administrative roles for frame management.

Clearly, the SC provides many critical functions for the Sun Fire 15K system. The domains will not operate properly if a controlling SC is absent. Therefore, preserving the security of the SC is very important.

From a hardware perspective, the output of `uname` on an SC provides the following:

```
# uname -i
SUNW,UltraSPARC-III-cEngine
# uname -m
sun4u
```

This information is similar to the output of any other `sun4u` class server.

Redundant SCs

The Sun Fire 15K frame supports up to two SCs. The first SC (`sc0`) is referred to as the main SC, while the other SC (`sc1`) is referred to as the spare. The software running on the SC monitors the SCs to determine if an automatic failover should be performed. The two SCs should have the same configuration. This duplication of configuration should include the Solaris OE installation, security modifications, patch installations, and all other aspects of system configuration.

The failover functionality between the SCs is controlled by the daemons running on the main and spare SCs. These daemons communicate across a private network built into the Sun Fire 15K frame. Other than the communication of these daemons, there is no special trust relationship between the two SCs.

System Management Services (SMS) Software

Another significant aspect to the security of the SC is access to the various applications which an administrator uses to manage a Sun Fire 15K system. Some of the security issues associated with the software that controls these applications, called the System Management Services (SMS), are discussed in the *System Management Services (SMS) 1.1 Administrative Guide*. This article builds on the recommendations made in the *SMS Security* chapter of that guide.

Access to the SMS software is the core of the SC. Correspondingly, access to this software must be carefully controlled and only authorized accounts should have access. The SMS software provides a mechanism, over and above the Solaris OE access controls, to limit access to the SMS software. These features are described in the *Default SC SMS Software Configuration* section below.

Securing the Sun Fire SC

In order to effectively secure an SC, changes are required for both the Solaris OE software running on the SC and the configuration of the Sun Fire 15K platform. To simplify the Solaris OE installation and deployment of these recommendations, customized modules have been added to the Solaris™ Security Toolkit software to automate the implementation of these recommendations. These new modules are available in version 0.3.2 of the Solaris Security Toolkit software.

Solaris Security Toolkit Software

The primary function of the Solaris Security Toolkit software (*Toolkit*) is to automate and simplify building secured Solaris OE systems based on the recommendations contained in this and the other security-related Sun BluePrints OnLine articles. In the context of this article, a module has been developed specifically to harden Sun Fire 15K SCs.

The Toolkit focuses on Solaris OE security modifications to 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 which reduces the number of components that have to be patched and made secure. Reducing the number of components can potentially reduce entry points to an intruder. However, minimization is not addressed, recommended, or supported on Sun Fire 15K SCs at this time.

The Sun Fire 15K SC module of the Solaris Security Toolkit software version 0.3.2, called `sunfire_15k_sc-secure.driver`, exclusively performs hardening tasks. No minimization of the Solaris OE is performed.

Note – Configuration modifications for performance enhancements and software configuration are not addressed by the Toolkit.

The Toolkit was designed to be capable of hardening systems during installation; this is achieved by using the JumpStart™ technology as a mechanism for running the Toolkit scripts. Additionally, the Toolkit can also be run outside the JumpStart framework in a standalone mode. This standalone mode allows the Toolkit to be used on systems that require security modifications or updates but cannot be taken out of service to reinstall the OS from scratch.

The Sun Fire 15K SC module of the Toolkit can be used in either standalone or JumpStart mode to secure an SC. The module automates the hardening recommendations made in this article.

The latest version of the Solaris Security Toolkit is available from:

<http://www.sun.com/security/jass>

Supportability

The Sun Fire 15K SC configuration implemented by the Toolkit SC module (`sunfire_15k_sc-secure.driver`) is a Sun supported configuration. The Toolkit must be used to harden the SC. If the Toolkit is used, service calls made to Enterprise Services for support will be handled as any other service order.

Note – A hardened SC will only be supported by Sun Enterprise Services when the security modifications are performed through the use of the Solaris Security Toolkit software.

Please also note that the Toolkit itself is not a supported Sun product. Only the configuration created by the Toolkit is supported. Toolkit support is available through the Solaris Security Forum link on the following web page:

<http://www.sun.com/security/jass>

Assumptions and Limitations

The recommendations made in this article are based on several assumptions and limitations as to what may be done and still have a Sun supported configuration.

This article is based on Solaris 8 OE 10/01 or update 6 and SMS software version 1.1. All of the Solaris OE components discussed are included in this release. In some cases, there may be Solaris OE functionality discussed in this article which is not discussed in the Sun BluePrints OnLine article, *Solaris Operating Environment Security - updated for Solaris 8 Operating Environment*. These Solaris OE issues are discussed in the following sections, and may require an update of the *Solaris Operating Environment Security* article to be released.

Solaris OE hardening can be interpreted in a variety of ways. For the purposes of developing a hardened SC configuration, the following sections represent hardening of all possible Solaris OE configurations. That is, anything that can be hardened, is hardened. Configurations that are not hardened are not modified for a reason.

Solaris OE configurations hardened to the level described in this article may not be appropriate for all environments. Some installations may choose to perform fewer hardening operations than recommended in this article. The configuration will remain supported in these cases. However, additional hardening beyond what is recommended or discussed by this article will not be supported.

In addition, Solaris OE minimization or the removal of Solaris OE packages to minimize security exposures, is not a supported option on the Sun Fire 15K SC. Only the Solaris OE hardening tasks discussed in this article are supported configurations for the SC.

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

The Sun Fire 15K SC module of the Toolkit, `sunfire_15k_sc-secure.driver`, may be modified to disable certain hardening scripts.

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

Note – The Solaris Security Toolkit must be used to harden the SC in order for the final configuration to be supported.

Additional software which may be installed on the SC, such as Sun Remote Services or Sun™ Management Center (Sun MC) platform agent software, are not discussed in this article. The security implications implicit with the installation of these types of software should be carefully evaluated.

Default SC SMS Software Configuration

This section discusses the additional software which must be installed on a Sun Fire 15K SC. Specifically, this section covers the configuration of System Management Services (SMS) software.

SC Solaris OE SMS Packages

A Sun Fire 15K SC is based on Solaris 8 OE 10/01 (update 6) using the SUNWCall Solaris OE installation cluster.

The System Management Services (SMS) software, which is required on an SC, is critical for configuring the SC. It resides on the SC and oversees all SC operations. The entire SMS software bundle is comprised of the following fifteen packages:

application SUNWSMSdf	System Management Services Data Files
application SUNWSMSjh	System Management Services On-Line Javahelp
application SUNWSMSlp	System Management Services LPOST object files
application SUNWSMSmn	System Management Services On-Line Manual Pages
application SUNWSMSob	System Management Services OpenBoot PROM
application SUNWSMSod	System Controller Open Boot Prom
application SUNWSMSop	System Management Services Core Utilities
application SUNWSMSpd	System Controller Power On Self Test
application SUNWSMSpo	System Management Services POST Utilities
application SUNWSMSpp	System Management Services picld(1M) Plug-in Module
application SUNWSMSr	System Management Services, (Root)
application SUNWSMSsu	System Management Services User Environment
application SUNWufu	User Flash PROM Device Driver Header File
application SUNWufrx	User Flash PROM Device Driver (Root) (64-bit)
application SUNWscdvr	Sun Fire 15000 System Controller drivers

The preceding packages are specific to Sun Fire 15K SCs.

SC SMS Accounts and Security

The following are users added to the `/etc/passwd` file by SMS:

```
# grep sms /etc/passwd
sms-codd:x:10:2:SMS Capacity On Demand Daemon::
sms-dca:x:11:2:SMS Domain Configuration Agent::
sms-dsmd:x:12:2:SMS Domain Status Monitoring Daemon::
sms-dxs:x:13:2:SMS Domain Server::
sms-efe:x:14:2:SMS Event Front-End Daemon::
sms-esmd:x:15:2:SMS Environ. Status Monitoring Daemon::
sms-fomd:x:16:2:SMS Failover Management Daemon::
sms-frad:x:17:2:SMS FRU Access Daemon::
sms-osd:x:18:2:SMS OBP Service Daemon::
sms-pcd:x:19:2:SMS Platform Config. Database Daemon::
sms-tmd:x:20:2:SMS Task Management Daemon::
sms-svc:x:6:10:SMS Service User:/export/home/sms-svc:/bin/csh
```

Of the twelve preceding accounts, only one is actually used to administer the system. The `sms-svc` account is the default account for the administration of the Sun Fire 15K system. All of the other accounts provide privileges for the daemons they are associated with. These accounts should never be used to log into the system and can be secured in the same fashion as system accounts which are never used. These accounts are used for the daemons running the SC as described in the *SC SMS Daemons* section.

The following are the newly added SMS specific `/etc/shadow` contents:

```
# grep sms /etc/shadow
sms-codd:NP:::::::::
sms-dca:NP:::::::::
sms-dsmd:NP:::::::::
sms-dxs:NP:::::::::
sms-efe:NP:::::::::
sms-esmd:NP:::::::::
sms-fomd:NP:::::::::
sms-frad:NP:::::::::
sms-osd:NP:::::::::
sms-pcd:NP:::::::::
sms-tmd:NP:::::::::
sms-svc:lnrf2l0vf4G9s:11414:::::::::
```

All of the preceding accounts added, including the `sms-svc` account, are initially locked by having 'NP' as the encrypted password entry.

Note – The password for the `sms-svc` user should be set, on both SCs, immediately after installation of the SMS software or first power on of the Sun Fire 15K system.

The following are entries added to the `/etc/group` file by SMS:

```
# grep sms /etc/group
plataadm::15:sms-svc
platoper::16:sms-svc
platsvc :17:sms-svc
dmnaadm::18:sms-svc
dmnarcfg::19:sms-svc
dmnbadm::20:sms-svc
dmnbrcfg::21:sms-svc
dmncadm::22:sms-svc
dmncrcfg::23:sms-svc
dmndadm::24:sms-svc
dmndrcfg::25:sms-svc
dmneadm::26:sms-svc
dmnercfg::27:sms-svc
dmnfadm::28:sms-svc
dmnfrcfg::29:sms-svc
dmngadm::30:sms-svc
dmngrcfg::31:sms-svc
dmnhadm::32:sms-svc
dmnhrcfg::33:sms-svc
dmniadm::34:sms-svc
dmnircfg::35:sms-svc
dmnjadm::36:sms-svc
dmnjrcfg::37:sms-svc
dmnkadm::38:sms-svc
dmnkrcfg::39:sms-svc
dmnladm::40:sms-svc
dmnlrcfg::41:sms-svc
dmnmadm::42:sms-svc
dmnmrcfg::43:sms-svc
dmnnadm::44:sms-svc
dmnnrcfg::45:sms-svc
dmnoadm::46:sms-svc
dmnorcfg::47:sms-svc
dmnpadm::48:sms-svc
dmnprcfg::49:sms-svc
dmngadm::50:sms-svc
dmngrcfg::51:sms-svc
dmnradm::52:sms-svc
dmnrrcfg::53:sms-svc
```

At first glance the preceding entries seem to be a tremendous number of group additions, but they are simply the groundwork to allow delegation of administrative capabilities for the frame, and each of the 18 domains a Sun Fire 15K system is capable of supporting. This allows for separation of the administrative privileges and operator privileges for each domain and the entire frame. The *SMS Security* chapter in the *System Management Services (SMS) 1.1 Administrator Guide* referenced in the Bibliography has detailed descriptions of which commands require which group's privileges for execution.

SC SMS Daemons

The SMS-specific daemons can be broken up into three separate types. These three types are each listed below with sample `ps` output.

First, there are the platform or core SMS daemons which run on both the main and spare SC:

```
root      8108    1  0 17:53:04 ?      0:01 mld
root      8123    1  0 17:53:05 ?      31:35 hwad
root      8126    1  0 17:53:05 ?      0:00 mand
sms-frad  331     1  0 12:41:21 ?      0:00 frad
root      8132    1  0 17:53:06 ?      0:03 fomd
```

Secondly, there are the SMS daemons that only run on the main SC:

```
sms-pcd   393     1  0 12:41:43 ?      0:03 pcd
sms-tmd   402     1  0 12:41:43 ?      0:00 tmd
sms-dsmd  405     1  0 12:41:44 ?      0:00 dsmd
sms-esmd  414     1  0 12:41:45 ?      0:05 esmd
sms-osd   419     1  0 12:41:46 ?      0:00 osd
root      8218    1  0 17:53:33 ?      0:00 kmd
sms-efe   475     1  0 12:41:47 ?      0:00 efe
sms-codd  483     1  0 12:41:48 ?      0:00 codd
```

Lastly, there are the SMS daemons which communicate to the domains:

```
sms-dxs   4428    291  0 13:14:31 ?      0:00 dxs -d A
sms-dca   4429    291  0 13:14:31 ?      0:00 dca -d A
```

Note – The listing of services above is a sample of the services that may be encountered. Depending on how many domains are in use, more SMS daemons will be running for each of those domains.

These SMS daemons are started by `/etc/rc2.d/S99sms` based on its startup daemon (`ssd`) configuration file in `/etc/opt/SUNWSMS/SMS1.1/startup/ssd_start`.

Each of these SMS daemons is briefly described below:

- `dca` (Domain Configuration Administration) – supports remote Dynamic Reconfiguration (DR) by facilitating communication between applications and the `dcs` daemon running on the domain. A separate instantiation of the `dca` daemon is executed on the SC for each domain running Solaris OE.
- `dsmd` (Domain Status Monitoring Daemon) – monitors domain state, CPU reset conditions, and the Solaris OE heartbeat for up to 18 domains. This daemon notifies the `dxs` daemon and Sun Management Center software for all changes.
- `dxs` (Domain X Server) – provides a variety of software support for a running domain including DR, Hot-Pluggable PCI I/O Assembly (HPCI) support, domain driver requests and events, in addition to virtual console support. One `dxs` daemon is started on the SC for each running domain.

- `efe` (Event Front End) – receives notification of events from various SMS daemons and forwards them on to subscribed clients. With SMS 1.1, the only client that can subscribe is Sun Management Center 3.0 software.
- `esmd` (Environmental Status Monitoring Daemon) – provides monitoring of the environment conditions of the Sun Fire 15K system including system cabinet conditions and fan tray and power supply temperatures. One instance of the `esmd` is run on the main SC.
- `fomd` (Failover Management Daemon) – is the center of the SC failover mechanism through its ability to detect faults on remote and local SC, and take appropriate action. One instance of `fomd` will be run on the main SC. This daemon uses RPC services on the SC and is the reason why `rpcbind` is not disabled.
- `frad` (FRU Access Daemon) – is the field replaceable unit (FRU) access daemon for SMS. It is the mechanism by which access is provided to the SEEPROMs, within the Sun Fire 15K frame, to which the SC has access. The `frad` is run locally on the main and spare SCs.
- `hwad` (Hardware Access Daemon) – implements hardware access for SMS daemons which is used by the daemons to control, access, configure, and monitor hardware. The `hwad` is run on the main SC.
- `kmd` (Key Management Daemon) – is used to manage the secure socket communication between the SC and domains. One instance of `kmd` is run on the main SC.
- `mand` (Management Network Daemon) – supports the Management Network (MAN). The role played by the `mand` daemon is specified by `fomd`. Similar to `kmd`, one instance of `mand` is executed on the main SC.
- `mld` (Message Logging Daemon) – accepts the output of all SMS daemons and processes and logs those messages based on its configuration files. One instance of the `mld` is executed on the main SC.
- `osd` (OpenBoot PROM Support Daemon) – supports the OpeBoot™ PROM process running on a domain through the mailbox that resides on the domain. When the domain OpenBoot PROM writes requests to the mailbox, the `osd` daemon executes those requests. Only the main SC is responsible for booting domains; correspondingly, one instance of the `osd` is run on the main SC.
- `pcd` (Platform Configuration Database Daemon) – is responsible for managing and controlling access to platform and domain configuration information. As with `osd` the `pcd` is only executed on the main SC.
- `tmd` (Task Management Daemon) – implements task management services for the SMS software such as scheduling. Currently, this daemon is used by `setkeyswitch`, and other daemons, to schedule Hardware Power-On Self Test (HPOST) invocations. The main SC is responsible for these types of events, so one instance of `tmd` is run on the main SC.

Additional information on each of these daemons can be obtained in the SMS *Administration* and *Reference* guides listed in the Bibliography.

SC Network Interfaces

There are several network interfaces used on an SC to communicate with the platform, domains, and the other SC. These are defined in a similar fashion to regular network connections through `/etc/hostname.*` entries.

Note – For the purposes of this discussion the main SC is `sc0` while the spare SC is always `sc1`. If no hardware failures are present and the SCs are booted at the same time `sc0` will always become the main SC. As the network configuration is slightly different between `sc0` and `sc1`, they are referred to as main and spare respectively.

Main SC Network Interfaces

A typical main SC, or `sc0`, will have the following two files in `/etc` with contents similar to the following:

```
# more /etc/hostname.scman0
192.168.103.1 netmask + private up
# more /etc/hostname.scman1
192.168.103.33 netmask + private up
```

In addition, a typical `sc0` SC will have the corresponding entries in `/etc/netmasks`:

```
192.168.103.0 255.255.255.224
192.168.103.32 255.255.255.252
```

Note – Non-routed, or RFC 1918, IP addresses have been used in all SC examples. It is recommended that these types of IP addresses be used when deploying Sun Fire 15K SCs. The SMS software defines internal SC networks connections to be private, and not advertised.

The `/etc/hostname.scman0` entry sets up the I1 or Domain to SC Management Network (MAN). The IP address used in this example, 192.168.103.1, is a floating IP address controlled by the SMS software to always be available only on the main SC.

From a security perspective, the network between the domains and the SC, in addition to any network connection between the domains, is of concern. The I1 network addresses these concerns by only permitting SC-to-domain and domain-to-SC communication. This is implemented through a point-to-point physical network connection between the SC and each of the 18 domains supported by a Sun Fire 15K system. On the SC, these 18 separate networks are consolidated into one meta-interface to simplify administration and management. The MAN driver software performs this consolidation and also enforces domain separation and failovers to redundant communication paths.

Direct communication between domains, over the I1 network, is not permitted by the hardware implementation of the I1 network. This network is implemented through 18 separate point-to-point networks between the SCs and each domain. Each of these connections terminates at separate I/O boards on each domain and SC.

By implementing the network in this manner, each SC to domain network connection is physically isolated from the other connections. The only restriction is that the MAC addresses used by each domain are sequentially incremented from domain 1 to 18.

The `/etc/hostname.scman1` entry is used to configure the I2 or SC-to-SC Management Network (MAN). This network connection, on which both SC's have an IP address, is used for the heartbeat connections between the two SCs.

Both of these network connections are implemented through the Sun Fire 15K internal MAN. No external wiring is utilized.

Note – Do not use the MAN networks for any reason. These are Sun Fire 15K networks and not for general purpose use. Any use may interfere with the proper operation of the SMS monitoring agents.

Putting them all together, the network configuration appears as follows on the main SC which is `sc0` in this article:

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1 inet
127.0.0.1 netmask ff000000

hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2 inet
10.1.72.80 netmask fffff800 broadcast 10.1.79.255 ether 8:0:20:a8:db:2e

scman0: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500 index 3
inet 192.168.103.1 netmask fffffffe0 broadcast 192.168.103.31 ether 8:0:20:a8:db:2e

scman1: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500 index 4
inet 192.168.103.33 netmask fffffffc broadcast 192.168.103.35 ether 8:0:20:a8:db:2e
```

While the `scman0` and `scman1` networks are Internet Protocol (IP) based network segments they should not be used as a general purpose network segment. For example, even though an SC and a domain will be on `scman0`, network administrators should not use `scman0` for transferring files nor other administrative tasks. Refer to the `scman(7D)` and `dman(7D)` man pages for more details.

Note – Do not use the MAN networks for any reason. These are Sun Fire 15K networks and not for general purpose use. Any use may interfere with the proper operation of the SMS monitoring agents.

Spare SC Network Interfaces

The spare SC has the same physical network interfaces as the main SC but with a slightly different configuration as it is in spare mode. The status of the SC can be verified with the following command:

```
# showfailover -r
SPARE
```

The `scman0` network interface is plumbed by the Solaris OE through the `/etc/hostname.scman0` file on the spare SC in the same manner, and with the same information, as on the main SC. The difference between the main and spare SCs is that the interface will be inactive on the spare. The spare SCs `scman0` port on the I/O hubs is disabled and `mand` will not provide path information to `scman0` on the spare.

The `scman1` interface, which is used for SC to SC communications, will be plumbed and the spare SC has the following configuration information for this interface:

```
# more /etc/hostname.scman1
192.168.103.34 netmask + private up
```

In addition, the spare SC has the following corresponding `/etc/netmask` information:

```
192.168.103.32 255.255.255.252
```

Putting them all together, the network configuration appears as follows on the spare SC which is `sc1` in this example:

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000

hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.1.72.81 netmask ffffffff broadcast 10.1.72.255

scman0: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500 index 3
    inet 192.168.103.1 netmask fffffffe0 broadcast 192.168.103.31

scman1: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500 index 4
    inet 192.168.103.34 netmask fffffffc broadcast 192.168.103.35
```

Secured SC Solaris OE Configuration

Building a secure system requires that the entry points onto the system be limited and restricted, in addition to limiting how authorized users can gain additional privileges. Properly securing both SCs in a Sun Fire frame involves many steps.

First, the number of services offered by an SC to the network should be reduced to decrease the number of the access points offered to an intruder. The modifications to secure an SC's Solaris OE configuration result in reducing the number of TCP, UDP, and RPC services significantly.

This represents a considerable improvement in configuring Solaris OE on an SC to be dedicated to the task of being an SC and enhancing its security.

Secondly, additional security related software must be installed to provide secure access mechanisms for administrators and tools to validate the security of the Solaris OE running on the SCs.

Security Recommendations

The recommendations for securing the SC follow closely with the hardening described in the *Solaris Operating Environment Security - Updated for Solaris 8 Operating Environment* Sun BluePrints OnLine article.

There are several exceptions to these recommendations due to functionality that is required by the SC and due to supportability constraints.

1. The `in.rshd`, `in.rlogind`, and `in.rexecd` daemon entries listed in the `/etc/inetd.conf` are not disabled as the Failover Management Daemon (`fomd`) requires them.
2. In order for `fomd` to effectively use the daemons listed above a `.rhosts` file must be present on both of the SCs. This file contains the `scman1` network hostname of the other SC and will allow `fomd` to access the SC, as `root`, without requiring a password.
3. The Remote Procedure Call (RPC) system startup script is not disabled because RPC is used by `fomd`.
4. The Solaris Basic Security Module (BSM) is not enabled. The BSM subsystem is difficult to optimize for appropriate logging levels and its logs are difficult to interpret. This subsystem should only be enabled in those sites that have the expertise and resources to manage the generation and data reconciliation tasks required to use BSM effectively.
5. Solaris OE minimization is not currently supported for the SC.
6. The SC cannot be configured as a Network Time Protocol (NTP) client.

The creation of user accounts and their associated privileges are not discussed in this article. Adding a new user to a Sun Fire 15K requires that they be provided with privileges not only in the Solaris OE but also with SMS domain and platform privileges. The *SMS Security* chapter in the *System Management Services (SMS) 1.1 Administrator Guide* referenced in the Bibliography has detailed descriptions of how to define user access to the SMS software appropriately.

Implementation of Recommendations

This section describes the software installation procedures and the process of securing the SC with the Solaris Security Toolkit.

The security recommendations to secure the Sun Fire 15K SC involves the installation of four software packages. These packages are:

- Solaris Security Toolkit
- FixModes
- OpenSSH
- MD5

Note – Of the four packages described in this section, only the use of the Solaris Security Toolkit, FixModes, and MD5 are required. The use of OpenSSH, while being strongly recommended, is not required. A commercial version of SSH, available from <http://www.ssh.com> or <http://www.fsecure.com>, may be substituted for OpenSSH.

Software Installation

The first step in securing the SC is to install the required software. This section describes how each of the software packages should be installed.

Solaris Security Toolkit Installation

First, the Solaris Security Toolkit software must be downloaded and installed on the SC. The Toolkit will be used to automate the Solaris OE hardening tasks described later in this section.

The instructions included use filenames which are only correct for this release of the Toolkit. Use the following procedure to download and install the Toolkit:

1. **Download the source file** (`SUNWjass-0.3.2.pkg.Z`).

The source file is located at:

```
http://www.sun.com/security/jass
```

2. **Extract the source file into a directory on the server using the `uncompress` command as shown:**

```
# uncompress SUNWjass-0.3.2.pkg.Z
```

3. **Install the Toolkit onto the server using the `pkgadd` command as shown:**

```
# pkgadd -d SUNWjass-0.3.2.pkg SUNWjass
```

Executing this command creates the `SUNWjass` directory in `/opt`. This subdirectory will contain all the Toolkit directories and associated files. The script `make-pkg`, included in Toolkit releases since version 0.3 allows administrators to create custom packages using a different installation directory.

FixModes

This section describes how to download and install the FixModes software into the appropriate Solaris Security Toolkit directory so it can be used to tighten file permissions during the installation of the Toolkit. Selectively modifying system permissions makes it more difficult for malicious users to gain additional privileges on the system.

Note – A new version of FixModes supporting the Sun Fire 15K SC was created, tested, and released in parallel with the publication of this article. This new version of FixModes must be used to modify the permissions on the SC. The download instructions below must be followed to access this latest FixModes version. The use of any previous FixModes releases on the SC will adversely impact the performance of the SMS software running on the SC. The correct FixModes version must have `secure-modes.c` version 1.41 and `exempt-pkgs.h` version 1.1. Newer versions of either file are also acceptable. Earlier versions of FixModes must not be used to secure the SC.

Follow the following instructions to download FixModes:

1. Download the FixModes pre-compiled binaries from:

`http://www.Sun.COM/blueprints/tools/FixModes_license.html`

The FixModes software is distributed as a precompiled and compressed `tar` file format called `FixModes.tar.Z`.

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

Note – The compressed `tar` archive should not be uncompressed.

OpenSSH

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 some implementation of Secure Shell, whether commercially purchased or the freeware version.

The use of some Secure Shell variant is strongly recommended when implementing all the security modifications performed by the Solaris Security Toolkit software. The Toolkit will disable all non-encrypted user-interactive services and daemons on the system, in particular services such as `in.telnetd` and `in.ftpd` are all disabled. Access to the system can be gained with Secure Shell in a similar fashion to what was provided by RSH, TELNET, and FTP. It is strongly recommended that Secure Shell be installed and configured before executing a Toolkit run.

A Sun BluePrints OnLine article discussing how to compile and deploy OpenSSH titled: *Building and Deploying OpenSSH on the Solaris Operating Environment (July 2001)* is available at:

<http://www.sun.com/blueprints/0701/openSSH.pdf>

Information on where to obtain the commercial versions of SSH is provided in the *References* section.

Note – The Sun BluePrints OnLine article mentioned above provides recommendations on how to compile OpenSSH. However, OpenSSH should not be compiled on the SC itself nor should the compilers be installed on the SC. Instead a separate Solaris system, running the same Solaris OE version, architecture, and mode (i.e., 64 bit) should be used to compile OpenSSH. If a commercial version of SSH is used then this issue is avoided.

MD5

This section describes how to download and install the MD5 software used to validate MD5 digital fingerprints on the Sun Fire 15K SC. This ability to validate the integrity of Solaris OE binaries provides a robust mechanism to detect system binaries which may have been altered by unauthorized users of the system. By modifying system binaries, attackers can provide themselves with back-door access onto the system.

To Install the MD5 Program (Intel and SPARC™ Architecture):

1. Download the MD5 binaries from:

<http://sunsolve.Sun.COM/md5/md5.tar.Z>

The MD5 programs are distributed in compressed tar file format.

2. Save the file to a directory (for example /usr/local or /opt).
3. Unpack the archive with the following command:

```
# zcat md5.tar.Z | tar xvf -
```

The archive contents are extracted into a newly created directory called md5. The programs for Intel and SPARC architecture hardware platforms are placed in this directory.

4. The owner and group of the extracted files must also be modified to correspond to a system defined user and group ID. Due to the sensitivity of the operations being performed by the md5 programs, they should be owned by the root user and the root group. The following demonstrates performing this on the md5 programs:

```
# chown -R root:root /opt/md5
# ls -l
total 94
-rw----- 1 root    root      23892 Apr  5  2000 md5-sparc
-rw----- 1 root    root      23452 Apr  5  2000 md5-x86
```

5. The file permissions on the extracted files must be modified before they can be executed. The following command will permit only root to read, write, and execute the md5 programs:

```
# chmod -R 700 /opt/md5
# ls -l
total 94
-rwx----- 1 root    root      23892 Apr  5  2000 md5-sparc
-rwx----- 1 root    root      23452 Apr  5  2000 md5-x86
```

Once installed, the Solaris Fingerprint Database can be used to verify the integrity of the executables included in the package itself. More information on the Solaris Fingerprint Database can be found in the Sun BluePrints OnLine article titled *The Solaris™ Fingerprint Database - A Security Tool for Solaris Software and Files* and available from the following URL:

<http://www.sun.com/blueprints/0501/Fingerprint.pdf>

Two additional tools are described in the above Sun BluePrints OnLine article that simplify the process of validating system binaries against the database of MD5 checksums maintained by Sun at SunSolve OnlineSM Web site. These tools are called Solaris Fingerprint Database Companion and Solaris Fingerprint Database Sidekick.

It is strongly recommended to install these two tools in this section, in combination with the MD5 software, and use the tools frequently to validate the integrity of the Solaris OE binaries and files on the main and spare SC.

Securing the SC with the Solaris Security Toolkit Software

Now that all the software is installed, the Solaris OE image running on the Sun Fire 15K SC can be secured.

Note – Before implementing the security recommendations in this section, it should be understood that all non-encrypted access mechanisms to the SC will be disabled, such as TELNET, RSH, and FTP. The hardening steps will not disable console serial access over the SC serial port.

Solaris Security Toolkit Software Execution

The Solaris Security Toolkit provides specific drivers to automate the hardening of the Sun Fire 15K SC. This section steps through the process by which the Solaris Security Toolkit software is used to harden a Sun Fire 15K SC.

The Toolkit is executed in the following manner:

```
# cd /opt/SUNWjass
# ./jass-execute -d sunfire_15k_sc-secure.driver
./jass-execute: NOTICE: Executing driver,
sunfire_15k_sc-secure.driver

=====
sunfire_15k_sc-secure.driver: Driver started.
=====
[...]
```

By executing the `sunfire_15k_sc-secure.driver` script, all of the security modifications included in that script will be made on the system. The current release of this driver script, as implemented in this article, includes over one hundred security modifications on the SC.

Note – The `sunfire_15k_sc-secure.driver` will automatically execute the `FixModes` program to tighten filesystem permissions on the system.

In addition to displaying the output to the console, a log file is created in the `/var/opt/SUNWjass/run` directory. Each Solaris Security Toolkit run will create another run directory in `/var/opt/SUNWjass/run`. The names of these directories are based on the date and time the run was begun.

Note – The contents of the `/var/opt/SUNWjass/run` directories should not be modified under any circumstances. User modification of the files contained in those 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 used not only to track what modifications 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 had been performed, they would all be undone with the following command:

```
# pwd
/opt/SUNWjass
# ./jass-execute -u
Please select from one of these backups to restore to
1. September 25, 2001 at 06:28:12 (/var/opt/SUNWjass/run/20010925062812)
2. April 10, 2001 at 19:04:36 (/var/opt/SUNWjass/run/20010410190436)
3. Restore from all of them
Choice? 3
./jass-execute: NOTICE: Restoring to previous run
/var/opt/SUNWjass/run/20010925062812

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

Additional documentation on the Solaris Security Toolkit software is available in the `/opt/SUNWjass/Documentation` directory or online at the following URL:

<http://www.sun.com/security/jass>

Verification of SC Hardening

Once the SC has been hardened and all hardening processes are completed, the SC should be rebooted and its configuration verified by having it assume the main SC role. This must be done before hardening the spare SC.

Note – Do not harden the spare SC until the hardened configuration of the main SC has been verified to function properly in your environment.

Once the hardened SC has taken control of the frame, and SMS control of the platform has been verified, then the spare SC can be hardened. The spare SC (sc1) must not be hardened until the main SC (sc0) has been verified. After the main SC is verified, the entire software installation and hardening process described above should be performed on the spare SC.

Note – It is recommended that the failover be disabled before hardening any of the SCs. Once each SC is hardened it should be manually defined as the main SC and its functionality verified. Only after both SCs have been hardened and tested should failover be re-enabled.

Hardening Results

After the above hardening steps are completed the number of daemons and services running on the SC is significantly lower.

The SC on which these recommendations were tested, the number of TCP IPv4 services listed by `netstat` went from 31, prior to the Toolkit run, to six. Similarly, the number of UDP IPv4 services listed by `netstat` went from 57 to five. By reducing the number of services available, the exposure points of this system are reduced significantly:

```
# netstat -a

UDP: IPv4
  Local Address          Remote Address      State
-----
  *.sunrpc               *.                 Idle
  *.32771                *.                 Idle
  *.32773                *.                 Idle
  *.syslog               *.                 Idle
  *.32776                *.                 Idle
  *.*                   *.*               Unbound

TCP: IPv4
  Local Address          Remote Address      Swind Send-Q Rwind Recv-Q  State
-----
  *.sunrpc               *.*                0      0 24576    0 LISTEN
  *.32771                *.*                0      0 24576    0 LISTEN
  *.sun-dr               *.*                0      0 24576    0 LISTEN
  *.32772                *.*                0      0 24576    0 LISTEN
  *.32773                *.*                0      0 24576    0 LISTEN
  *.22                   *.*                0      0 24576    0 LISTEN
  *.*                   *.*                0      0 24576    0 IDLE
```

Conclusion

The Sun Fire System Controller controls the hardware components which comprise a Sun Fire 15K server. Because it is a central control point for the entire Sun Fire frame, it represents an excellent attack point for intruders. In order to improve reliability, availability, and serviceability (RAS), the SC must be secured against malicious misuse and attack.

The Sun Fire 15K SC runs the Solaris 8 OE and many of the recommendations made in other Sun BluePrints OnLine articles about hardening the Solaris OE apply to the Sun Fire SC. This article uses these recommendations, in addition to SC-specific suggestions, to improve the overall security posture of a Sun Fire 15K SC by dramatically reducing potential access points to the SC and installing secure access mechanisms. In addition, the implementation of these recommendations can be automatically installed by the Solaris Security Toolkit software.

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>
- 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/minimization-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_config_install-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 Brunette, Glenn, *The Solaris Security Toolkit - Release Notes: Updated for version 0.3*, Sun BluePrints OnLine, June 2001,
http://sun.com/blueprints/0601/jass_release_notes-v03.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/0401/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 of Sun Microsystems, he is developing, documenting, and publishing security Best Practices through the Sun BluePrints OnLine program. Published article topics include: SunFire 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).

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 SunPS. 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. Her last 4 years have been focused in secure software development and 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.