SunScreen SKIP Open Issues and Late-breaking News, Release 1.1.1

Sun Microsystems, Inc.
901 N. San Antonio Road
Palo Alto, CA 94303-4900
U.S.A.

Part No: 805-6051–10
June 1998, Revision A

Copyright 1998 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, California 94303-4900 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, SunSoft, SunDocs, SunExpress, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. 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 1998 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, Californie 94303-4900 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 du système 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, SunSoft, SunDocs, SunExpress, 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.

Contents

CHAPTER 1

SunScreen SKIP Open Issues and Late-Breaking News

SunScreen SKIP Open Issues and Late-Breaking News contains information that was not available until immediately before the release of *SunScreen SKIP*. This document is the companion to the *SunScreen SKIP User's Guide, Release 1.1*. It incorporates information for *SunScreen SKIP*, Release 1.1.1.

A Word of Caution

Understand that a save core file contains your local secret or secrets. It would be difficult for someone to discern or discover, but it can be done! You should, therefore, protect a core file as carefully as any of your other local secrets. Remember, if you send your core file out-of-house for analysis, you are giving your local secret to the analyst.

Any system backups made while such a core file exists may contain the core file as well and so must be considered a possible means of discovering your local secret or secrets.

All regular system backups will also contain the files in which your local secrets or secrets are stored. These backups must be kept in a secure location.

Upgrading to *SunScreen SKIP*, Release 1.1.1, from *SunScreen SKIP*, Release 1.1

To upgrade to *SunScreen SKIP*, Release 1.1.1, from *SunScreen SKIP*, Release 1.1, follow the instructions in the *SunScreen SKIP User's Guide*, Chapter 1, "Installing *SunScreen SKIP*, "Upgrading from Earlier Versions of SKIP for Solaris."

To preserve the previous configurations (access control lists [ACL] files), certificates, and the key manager configuration file, do *not* remove the `/etc/opt/SUNWicg/skip` directory.

You may continue to use the old identities, whether UDH or CA, as long as you have not removed them.

Improved Security

SunScreen SKIP, Release 1.1.1, incorporates an improved random number generator that greatly increases security.

Error Messages

The following error messages were not included in the *SunScreen SKIP for Solaris User's Guide.*

N-counter out of range - either replayed packets or out of sync clocks

"Old" packets have been received by SKIP. This indicates either that, typically, the sending machine's clock is not in synchronization with your machine's clock or that, rarely, an intermediary is sending old packets in a replay attack.

Certificate g+p do not match dh_params

An entry in your access control list has a local identity and remote identity that do not have matching Diffie-Hellman parameters (*g* is the generator value, *p* is the prime value). This is typically caused when you try to talk to a system with moduli that do not match (*i.e.*, a 1024–bit system trying to talk to a 512–bit system using 1024–bit keys).

Local secret nsid=xx mkid=xx has expired. Deleting

Your local secret has expired. Generate a new local identity.

Unable to load skipsup.o – Exiting!

The SKIP support module could not be loaded. Typically, this means that one of the necessary libraries is not available on the machine that is attempting to run SKIP. Ensure that your system has the required software packages installed according to the instructions in the *SunScreen SKIP User's Guide*.

Modulus too big for U.S. export law

You have attempted to load a key that is not permitted under U.S. export law. Make sure that you have installed both the base SKIP package and any SKIP encryption upgrade packages that you have purchased under appropriate U.S. export license control.

```
skipd: passphrase required
issue skipd_restart to enable encryption
```

The key manager cannot start without a password to decrypt local secrets. Use the command `skip_restart` to start the key manager.

Limited Number of Local Keys

SunScreen SKIP is limited to a maximum of 100 local keys. All local keys in excess of the first 100 will silently fail.

Emergency Start Instructions

▼ System Hangs and You Cannot Access the Machine

1. If your system hangs when you are configuring SKIP and you do not have access to your machine, reboot your machine in the single-user mode and become root.
2. With a text editor, such as `vi`, edit the file `acl.<network_interface>` in the `/etc/opt/SUNWicg/skip/` directory so that line

```
skiphost -i <network_interface> -o on
```

   reads

```
skiphost -i <network_interface> -o off
```

to disable SKIP.

3. Reboot your machine normally to clean up the file system.
4. You, then, as root, may reconfigure your access control list as your security policy dictates.

▼ System Hangs, But You Still Can Become Root

1. If your system hangs when you are configuring SKIP and you still have access to your machine and can become root, enter

```
# skiphost -o off -i <network_interface>
```

   This will disable SKIP on the network interface

2. Then, as root, you may reconfigure your access control list as your security policy dictates.