Secure4Privilege (suGUARD)

A Technical White Paper

NOTICE

As Secure4Privilege is a software product which is subject to change, S4Software, Inc. reserves the right to make changes in the specifications and other information contained in this document, without prior notice. While S4Software, Inc. has made every effort to ensure the accuracy and completeness of this document, S4Software, Inc. cannot be held liable for any errors or omissions. No information contained in this document shall be deemed to be a warranty for any purpose whatsoever.

RESTRICTED RIGHTS LEGEND

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subprogram (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at subparagraph DFARS 252.227-7013.

S4Software, Inc.
6633 Convoy Ct.
San Diego, CA 92111

Phone: 858-560-8112
Fax: 858-560-8114
E-mail: sales@s4software.com

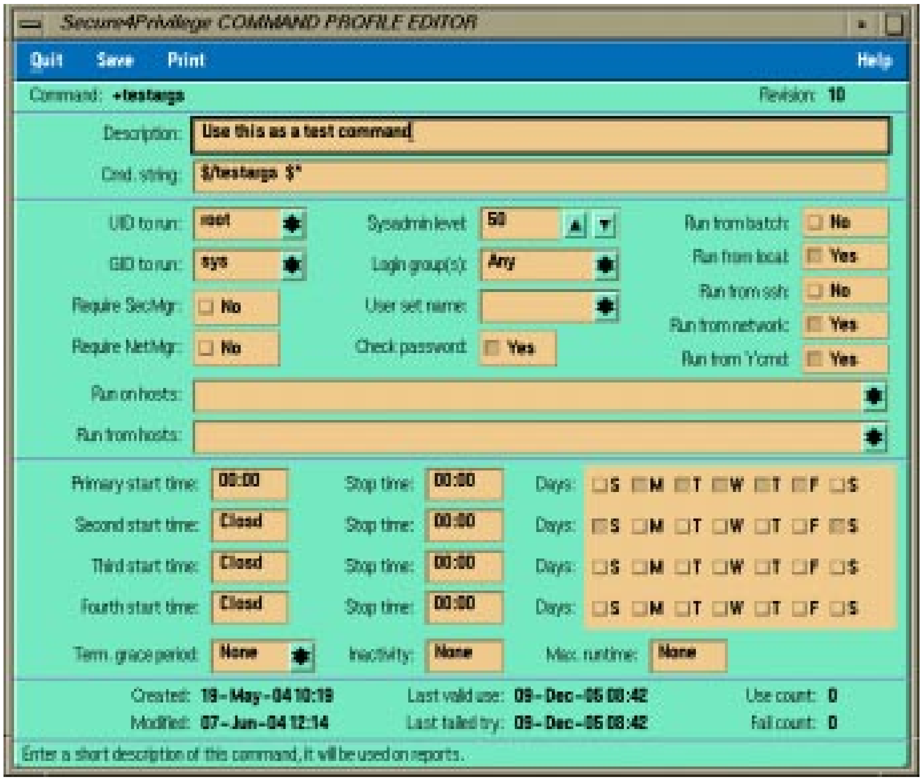
TABLE OF CONTENTS

The Issue

UNIX systems administration, particularly for large or widely distributed environments, is a complicated field which inevitably requires major trade-offs between functionality, security, and ease of administration. In order to make effective use of a UNIX system, management staff require access to many programs and scripts, some more critical or sensitive than others. Unfortunately, as UNIX was not designed with a concept of layered management levels, the only key needed to access most functions is knowledge of the `root` (or super-user) account password. Once a user knows this, they can effectively have access to the entire system. While the majority of individuals are completely trustworthy, there still exists a significant potential for problems, whether intentional or not. While products exist which attempt to solve this problem, including some in the public-domain, until now there have been none which fully integrate systems management and security in an easy-to-use and affordable package.

The Solution - Introduction to Secure4Privilege

Secure4Privilege is a software tool designed specifically to address security, system access, and layered management adding flexible and secure layered management capabilities to UNIX systems for control of local and distributed applications, programs and scripts. The Secure4Privilege command profile describes how to run a defined function, and gives information on how, when, where and by whom this command can be executed.



Command: +testargs Revision: 10

Description: Use this as a test command

Cmd. string: $/testargs $*

UID to run: root
GID to run: sys
Require SecMgr: □ No
Require NetMgr: □ No

Sysadmin level: 50
Login group(s): Any
User set name:
Check password: ☒ Yes

Run from batch: □ No
Run from local: ☒ Yes
Run from ssh: □ No
Run from network: ☒ Yes
Run from Y'cmd: ☒ Yes

Run on hosts:
Run from hosts:

Primary start time: 00:00 Stop time: 00:00 Days: □S ☒M ☒T ☒W ☒T ☒F □S
Second start time: Closd Stop time: 00:00 Days: ☒S □M □T □W □T □F ☒S
Third start time: Closd Stop time: 00:00 Days: □S □M □T □W □T □F □S
Fourth start time: Closd Stop time: 00:00 Days: □S □M □T □W □T □F □S

Term. grace period: None Inactivity: None Max. runtime: None

Created: 19-May-04 10:19 Last valid use: 09-Dec-05 08:42 Use count: 0
Modified: 07-Jun-04 12:14 Last failed try: 09-Dec-05 08:42 Fail count: 0

Enter a short description of this command, it will be used on reports.

Features

- Create and maintain command profiles with an easy-to-use menu and Motif-based GUI programs with context sensitive help.
- Use command line interface with script files to perform any menu program function which can be run without operator intervention.
- Establish required security level and other privileges to run a command.
- Define requirements for user authentication.
- Control access type (e.g. local, network, or SSH login/command execution, via ‘r’ commands and batch queues).
- Limit hosts on which and from which commands can be initiated.
- Restrict command execution based on time-of-day and day-of-week.
- Establish maximum runtime restrictions.
- Automatically terminate inactive commands.
- Set the UID and GID required to run the command.
- Detect unauthorized changes to executable files.
- Generate an extensive set of account and auditing reports.
- Log all command execution attempts, including what, who, where, and when.
- Optionally log each execution of a particular command; including the date, time, command name, executable program path, and arguments passed to the program or script.
- Run an optional alarm script when a command is invoked outside of its parameters.
- Build a distributed database of commands for ‘fail over’ resilience in a client-server environment.

Architecture

The Secure4Privilege software uses two databases, one to describe the commands (command profiles), and another to show the privileges for each user (user profiles). For systems where Secure4Access is also installed, Secure4Privilege will access Secure4Access user profiles rather than creating a separate user profile database.

If the Secure4Access Account Management and Access Control software package is also installed on your system, the Secure4Access menu programs can be used to create UNIX accounts and set the security level, login group, security manager and network manager privileges for each account.

If Secure4Access is not installed on the system, the Secure4Privilege menu programs can be used to create the needed account profiles once the UNIX accounts have been created using the system administration tool.

The Secure4Privilege software system consists of four components and two defined modules which are used to build, maintain, monitor and audit the use of a set of commands.

s4privmgr

The `s4privmgr` program builds, maintains and reports on command and account profiles.

s4privmgrX

The `s4prvmgrX` program is the graphic user interface (GUI) version of `s4privmgr`.

s4privrun

The `s4privrun` module is used to invoke commands and monitor their usage. If the command is installed into Secure4Privilege, it can be invoked directly by giving its name. For example, if the `user.backup` script is installed into Secure4Privilege, authorized users can invoke it by using its name. If it is not installed it can be run by: `s4privrun <command-name>`.

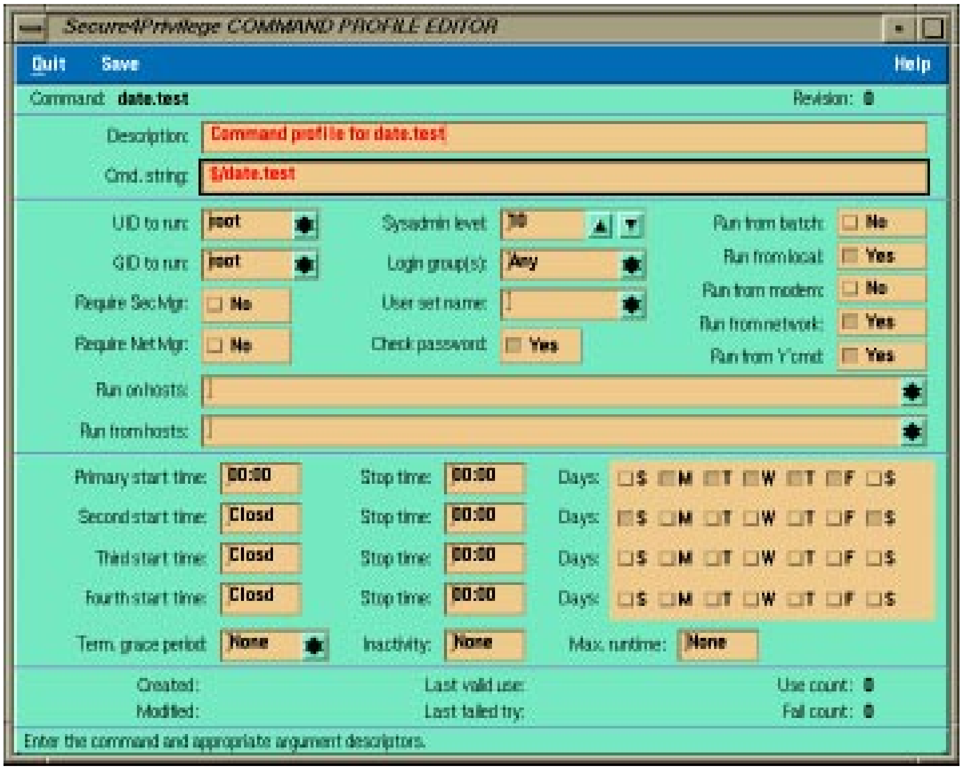
s4privdms

The s4privdms process is a network daemon which responds to remote host requests for comand profiles. When a command is issued on a host, s4privrun will first attempt to find the command profile on the local host. If the profile is not found, s4privrun queries each host listed in the configuration file as a command profile server. The Secure4Privilege network daemon (s4privdms) running on the remote host determines whether a copy of the profile exists, and whether it permits the command to be run on the requesting host. If both these conditions are satisfied, it sends a copy of the command profile which s4privrun uses to run the command. Otherwise, s4privdms returns a message indicating it does not have it and s4privrun will try the next host listed in the configuration file.

The s4privdms process uses {configurable} socket ports for transferring command profile data requests between servers. Administrators may also specify that requests be sent using remote procedure calls which will use the Secure4Privilege network daemon s4privnet.

The Secure4Privilege Command Profile

Secure4Privilege offers the option of a character-based or GUI menu program or the non-interactive command file mode. The Secure4Privilege menu program includes an easy-to-use program for creating and editing command profiles. Each of the fields is described below.



Command: date.test Revision: 0

Description: Command profile for date.test

Cmd. string: $/date.test

UID to run: root

GID to run: root

Require SecMgr: □ No

Require NetMgr: □ No

Sysadmin level: 30

Login group(s): Any

User set name:

Check password: ☒ Yes

Run from batch: □ No

Run from local: ☒ Yes

Run from modem: □ No

Run from network: ☒ Yes

Run from Y'cmd: ☒ Yes

Run on hosts:

Run from hosts:

Primary start time: 00:00 Stop time: 00:00 Days: □S ☒M ☒T ☒W ☒T ☒F □S

Second start time: Closd Stop time: 00:00 Days: ☒S □M □T □W □T □F ☒S

Third start time: Closd Stop time: 00:00 Days: □S □M □T □W □T □F □S

Fourth start time: Closd Stop time: 00:00 Days: □S □M □T □W □T □F □S

Term. grace period: None Inactivity: None Max. runtime: None

Created: Last valid use: Use count: 0

Modified: Last failed try: Fail count: 0

Enter the command and appropriate argument descriptors.

Specifics

Description

This field can be used to store any free-text information relating to the command. This field is not validated or used for validation.

Command string

This field defines the execution path and arguments for this command.

UID and GID to run

These fields contain the user ID (UID) and group ID (GID) under which the command must be run, or `-1` if the command is to be run under the login UID or GID. Typically it will be `0` (i.e. the root account). The `s4privrun` program will perform `setuid` and `setgid` calls to set the UID and GID before executing the command.

Required manager privileges

Defines the management privileges required to run this command. The *Network manager* privilege can only be set through Secure4Access.

Sysadmin level

This field sets the minimum user *Sysadmin level* required to run this command. This privilege can be set using the *Accounts* submenu or by using Secure4Access to set the *System administrator level*. This field accepts a numeric value from 0 to 99. A value of 0 allows the command to be run by any user, including those who do not have an account profile. The default value is 1.

Login group

This field specifies which Secure4Access login group (from 0 to 99) the user must belong to in order to execute this command. Setting it to `-1` (the default) allows any login group to run this command. The login group is set on a per user basis by using Secure4Access. The login group is assumed to be `0` if there is no profile for the user's account, or if your system is not running Secure4Access.

User set name

This field specifies the name of a set of users who are allowed to run this command. Only users who have a matching username/UID entry in the user set will be allowed to run the command.

The user set is a file named ’userset.xxx where `xxx` is the set name. This file is located in the `/usr/secure4/secure4.cpf` directory. Each line in this file will contain the username and UID of a user who belongs to this set.

Check password

If this field is set, the user will be required to enter their account password prior to the command being run.

Run from ...

These fields control how a command may be executed. They include: console, SSH, network, batch and via ‘r’ commands.

Run on hosts/Run from Hosts

These fields contain lists of host names and/or IP addresses for all hosts on which and from which this command can be run. If these fields are empty (the default), there are no restrictions.

Time windows

The time windows define the days and times during which a command can be run. Four sets of time and day windows are provided.

Term. grace period

Window grace time controls the action taken if a command is being run on the system when the current command access window expires, the maximum runtime is exceeded, or the command has been inactive for the specified time limit.

Inactivity

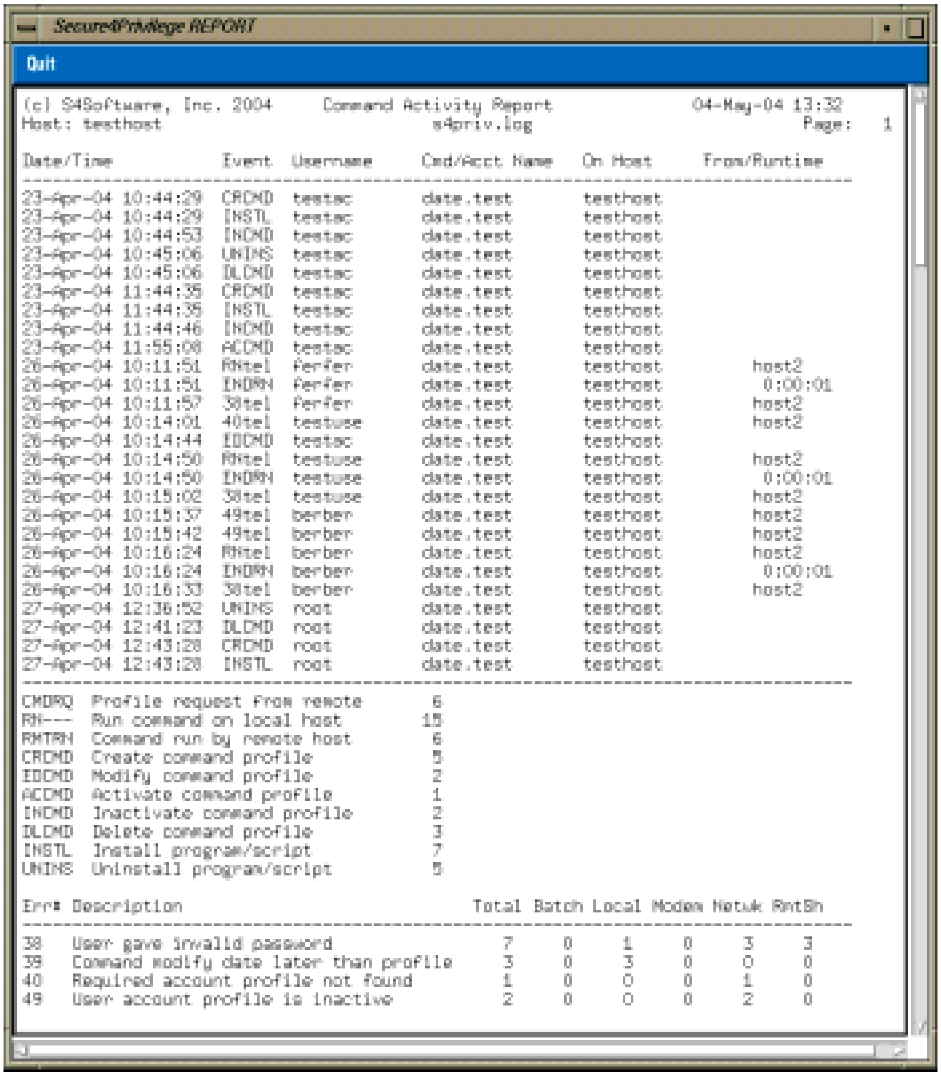
This value defines the time in minutes that a command may remain inactive before Secure4Privilege automatically terminates it. Inactivity is determined by looking at the total milliseconds of CPU time used by the command.

Maximum runtime

The maximum runtime field specifies the maximum allowed amount of clock time (in minutes) for each execution. The command execution may be automatically terminated if it is still running when the maximum execution time is exceeded depending upon the setting.

Report Options

The reports can be used to generate listings of command profiles, and reports of user activity and system auditing. Shown below is a sample of the *Command Activity Report*.



```
(c) S4Software, Inc. 2004     Command Activity Report             04-May-04 13:32
Host: testhost                           s4priv.log                          Page:   1

Date/Time           Event  Username     Cmd/Acct Name   On Host    From/Runtime
----------------------------------------------------------------------------------
23-Apr-04 10:44:29  CRCMD  testac       date.test       testhost
23-Apr-04 10:44:29  INSTL  testac       date.test       testhost
23-Apr-04 10:44:53  INCMD  testac       date.test       testhost
23-Apr-04 10:45:06  UNINS  testac       date.test       testhost
23-Apr-04 10:45:06  DLCMD  testac       date.test       testhost
23-Apr-04 11:44:35  CRCMD  testac       date.test       testhost
23-Apr-04 11:44:35  INSTL  testac       date.test       testhost
23-Apr-04 11:44:46  INCMD  testac       date.test       testhost
23-Apr-04 11:55:08  ACCMD  testac       date.test       testhost
26-Apr-04 10:11:51  RMtel  ferfer       date.test       testhost        host2
26-Apr-04 10:11:51  INDRN  ferfer       date.test       testhost         0:00:01
26-Apr-04 10:11:57  38tel  ferfer       date.test       testhost        host2
26-Apr-04 10:14:01  40tel  testuse      date.test       testhost        host2
26-Apr-04 10:14:44  EDCMD  testac       date.test       testhost
26-Apr-04 10:14:50  RMtel  testuse      date.test       testhost        host2
26-Apr-04 10:14:50  INDRN  testuse      date.test       testhost         0:00:01
26-Apr-04 10:15:02  38tel  testuse      date.test       testhost        host2
26-Apr-04 10:15:37  49tel  berber       date.test       testhost        host2
26-Apr-04 10:15:42  49tel  berber       date.test       testhost        host2
26-Apr-04 10:16:24  RMtel  berber       date.test       testhost        host2
26-Apr-04 10:16:24  INDRN  berber       date.test       testhost         0:00:01
26-Apr-04 10:16:33  38tel  berber       date.test       testhost        host2
27-Apr-04 12:36:52  UNINS  root         date.test       testhost
27-Apr-04 12:41:23  DLCMD  root         date.test       testhost
27-Apr-04 12:43:28  CRCMD  root         date.test       testhost
27-Apr-04 12:43:28  INSTL  root         date.test       testhost
----------------------------------------------------------------------------------
CMDRQ  Profile request from remote       6
RM---  Run command on local host        15
RMTRN  Command run by remote host        6
CRCMD  Create command profile            5
EDCMD  Modify command profile            2
ACCMD  Activate command profile          1
INCMD  Inactivate command profile        2
DLCMD  Delete command profile            3
INSTL  Install program/script            7
UNINS  Uninstall program/script          5

Err# Description                             Total Batch Local Modem Netwk RmtSh
----------------------------------------------------------------------------------
38   User gave invalid password                 7     0     1     0     3     3
39   Command modify date later than profile     3     0     3     0     0     0
40   Required account profile not found         1     0     0     0     1     0
49   User account profile is inactive           2     0     0     0     2     0
```

Command activity report

This option will generate a report summarizing all events relating to one or more commands.

Commands by runtime UID report

This option will generate a report listing all commands which have the *UID to run* field set to the specified UID.

Commands by security level report

This option will generate a report detailing the command profiles by security level.

Complete activity report

This option will generate a report detailing the date and time of all Secure4Privilege events and the user precipitating them. These events include running the menu program; running a command; creating, deleting, modifying, activating or inactivating a command profile; updating command file dates; and creating, deleting, modifying, activating or inactivating account profiles.

Complete commands report

This option will produce a report listing all the commands with profiles in Secure4Privilege.

Inactivated commands report

This option generates a report of all inactivated commands.

Installed commands report

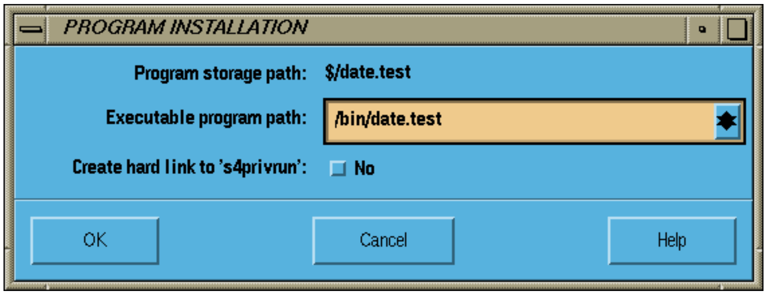
This option generates a report of all commands that are currently installed in Secure4Privilege.

User activity report

This option will generate a report detailing the date and time of particular events carried out from Secure4Privilege by a particular user or users. These events include running the menu program; running a command; creating, deleting, modifying, activating or inactivating a command profile; updating command file dates; and creating, deleting, modifying, activating or inactivating account profiles.

Utility Options

The Secure4Privilege Utility options provide a variety of functions for maintaining and monitoring the various profiles and command activity on the system. Shown below is a sample of the command program/script installation utility.



Program storage path: $/date.test

Executable program path: /bin/date.test

Create hard link to 's4privrun': □ No

Activate and inactivate account profiles

These options enable and disable account profiles. Inactivating an account profile prevents the user from running any command under Secure4Privilege control.

Activate and inactivate command profiles

This utility enables and disables commands. When a command is inactivated, it makes it unavailable for use.

Install a program/script

This option is used to install a command program or script so that entering the program name will automatically invoke `s4privrun` for profile validation prior to running the program/script.

List all commands

This option is used to generate a list of all command profiles that currently exist on the system. NOTE: This option is only available using the GUI menu program

Load a default command profile

This option allows the user to define an existing command profile for use as the template when creating other command profiles during this session. The default command profile name will always appear at the top right corner of the Secure4Privilege display screen.

Purge all inactivated commands

This option scans all commands with valid profiles and deletes any which are inactive. It is normally used in conjunction with option 2.

Reinstall all program/scripts

This option will allow the System Administrator to re-install all commands that were previously uninstalled using the ’Uninstall all programs/scripts’ option. (See below)

Reset command use counts

This option will allow the system manager to clear the *Use count* and *Fail count* for a specified group of commands. These use counts (maintained in the Secure4Privilege command profiles) are incremented for every successful use and failure respectively.

Run a command

This option allows you to execute a Secure4Privilege command from the menu system

Uninstall a program/script

This option is used to remove the link to `s4privrun` created by the *install* procedure, and to move the command program or script back to its original location.

Uninstall all program/scripts

This option allows the System Administrator to temporarily uninstall all commands from Secure4Privilege, to allow for events such as system upgrades. Often during system upgrades, system commands and executables are overwritten. This option allows the Admin to easily uninstall all commands currently installed in Secure4Privilege, perform the system upgrade, then reinstall all the commands again.

Update command file dates

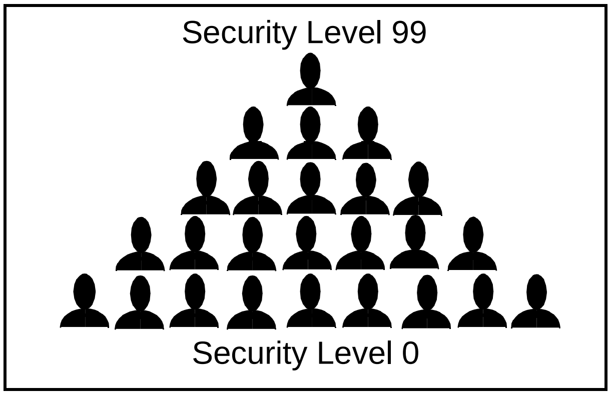
This option updates the profile ‘modified’ date to the current date. For purposes of security, the `s4privrun` program will not execute the program or script for any command if the ‘modified’ date for that program or command is later than the stored field in the profile. Should there be such a discrepancy, it would imply that someone has modified the program or script, therefore its integrity could not be guaranteed.

Granularity of Control

The Secure4Privilege system provides an effective and easily administered method of partitioning system management responsibilities by assigning each user an administrative privilege level between 0 and 99 which is matched against the required execution level for the command. Only those users who have an equal or higher level than required will be allowed to run the command. In addition, each command can require that the user have the security manager privilege, an option which is always required in order to run the command profile maintenance programs.

The user privilege database can be managed within Secure4Privilege, or can optionally use the account profile maintenance functions provided by the Secure4Access access control software. When used with Secure4Access, commands may also be restricted to specific login groups, or require the network management privilege in order to provide additional granularity of control.

In addition to providing system management control, Secure4Privilege can be used to create and maintain a complete application environment, including controlling which users are allowed to perform each function.



Frequently Asked Questions

How can my operator perform backups? I don’t want him to have the `root` password.

Secure4Privilege allows an operator to do backups and other operational functions without knowledge of the `root` password. This is accomplished by creating a command profile for the backup script similar to the one shown on page 1. If the user authentication and other checks succeed, Secure4Privilege will change the UID and GID to `0` as specified in the command profile, and run the backup script.

I need a log of every attempt to use certain programs. I don’t want to log every activity on my system.

Secure4Privilege logs all uses of a selected program (e.g. `su`). When a command is run under Secure4Privilege control, information about the command execution is written to the `s4priv.log` file. This information includes command name, run status, child PID, command termination, date, time, user’s UID, etc. In addition, by default, an additional log is kept for each command showing the arguments passed to it.

How can I give users access to an application using a restricted argument list? I don’t want them to be able to use some potentially dangerous switches.

Secure4Privilege can control switches passed to programs. The options include hard coding the arguments and/or ignoring those supplied by the user, passing all arguments to the program, specifying the order in which arguments passed to Secure4Privilege are passed to the program, etc. Special functions are also supplied which can be used to tell the program how many arguments were given to `s4privrun` by the user, and how many are being passed to the program.

There are certain applications which I need to protect from network access. Is that possible?

Secure4Privilege can protect applications from access via the network with command profile settings *Run from network*, and *Run from ‘r’ cmd*. If network and/or ‘r’ command access is permitted, it can be restricted to particular hosts by using the *Run from hosts* field.

My users supposedly don't have shell access, yet I worry that one of the applications in their menu may have a shell option. What can I do?

Secure4Privilege can control shell access (when you're not sure if those programs have 'backdoor' access). Shells, like any other program or script, can be brought under Secure4Privilege control and restricted to a security level above that given to normal users. It is very important when using this technique to insure that the shell used for booting the system is not rendered unavailable.

Availability

Secure4Privilege is currently available for most popular versions of Unix including the following:

OSF - Compaq Tru64	Digital UNIX 4+
Hewlett-Packard	HP/UX 10.0, 11.0+
IBM	AIX 4+
NCR (AT&T)	SVR4 for 3000 Series
SCO	UNIX Release 5
Silicon Graphics	IRIX 6.+
Sun	Solaris SPARC, Solaris Intel

To obtain a copy of Secure4Privilege to evaluate on your system visit us on our web page:

http://www.s4software.com

or send email to our sales department:

sales@s4software.com

Be sure to include your operating system type, required media (4mm, 8mm or QIC), and full name and address for delivery.

Or call us:

S4Software, Inc.   (858) 560 - 8112