Solaris Security
Recommendations from SANS Step by Step Guide, Titan, and YASSP

David J. Brumley
dbrumley@stanford.edu
http://www.theorygroup.com

October, 2000

Contents

1 Introduction

1.1 Overview

Computer security is a burgeoning field. Today firewalls, virtual private networks (VPNs), and gateways are all common security tools used by system and network administrators. These tools are applied in an attempt to fulfill two competing goals: a private, secure network vs. the ability to share information with the world.

This guide is a comparison between three tools that armor (sometimes called hardening) the core Solaris system. Each tool is tailored such that when properly applied, the resulting Solaris system is less vulnerable to hostile attacks. This guide is intended to outline the various mechanisms employed by each tool. The outline is used to extrapolate common security measures used to armor the Solaris operating system.

This guide is arranged into five major sections. The first section is an introduction to basic computer security. It outlines the vocabulary, terminology, and axioms used in armoring systems against attack.

The second section provides a brief introduction to each product. The introduction is not meant to be an exhaustive summary, but should give a general overview of each tool.

The third contains a detailed matrix comparing each product. The matrix is not exhaustive, but does represent the major functionality aspects of each tool.

The fourth section contains hardening recommendations that can be extrapolated from the matrix. These recommendations are meant to serve as a minimum standard for secure Solaris computing. The nature of the data being protected and particular site security policy may require more stringent measures.

The last section is a summary of how well each tool works in meeting those minimum recommendations.

1.2 What this guide is not

This guide is not a placebo for a competent system administrator with a well thought out security policy. It addresses only the minimum requirements for secure computing on a Solaris platform. Each service added to that platform will have additional security implications that should be evaluated.

1.3 Security Premises

In order to understand how YASSP, Titan, and SANS Step by Step guide compare, one must keep in mind the basic principles of computer security underlying each package. Cheswick and Bellovin in their landmark book "Firewalls and Internet Security,"[2] eloquently outline those principles. They are:

> **Axiom 1 (Murphy)** *All programs are buggy.*
>
> **Theorem 1 (Law of Large programs)** *Large programs are even buggier than their size would indicate.*
>
> **Theorem 2** *If you do not run a program, it does not matter whether or not it is buggy.*
>
> **Corollary 2.1** *If you do not run a program, it does not matter if it has security holes.*
>
> **Theorem 3** *Exposed machines should run as few programs as possible; the ones that are ran should be as small as possible* [2]

Though buggy programs are in general a problem, those that run with elevated privileges are the most often exploited. [1] There are two main genres of programs that have elevated privileges in the UNIX world:

- Set-uid/set-gid programs. Set-uid programs run as the owner for the file. Similarly, set-gid programs run with the group of the file. A common example of a setuid program is /usr/bin/passwd, which needs the setuid bit to update the root owned /etc/passwd file.
- Network Services. Network services typically run as superuser in order to access privileged network resources.

1.4 Defense in Depth

Castles often have multiple layers of defense. There may be a drawbridge, moat, or even cauldrons full of hot oil used to repel potential enemies. Just as with castles, defense in depth is important in computer security.

When protecting a host, security is applied in multiple layers. The layers are like an onion... to get to the center of the onion, you must successfully peel away each layer. For example, running network services should not only be scrutinized for common bugs, but also be filtered so only a limited number of hosts have access. Would-be intruders then must not only find a hole in the service, but also have access to a specific computer from which to launch their attack. Defense in depth is not redundancy, it is insurance.

[1] As an example of a program that does not run with elevated privileges that can be exploited, consider those programs that write to /tmp with a predictable file name. A nefarious person could create a symbolic link in /tmp with the predicted file name to, say, /etc/passwd. Then, when root ran the program, the symbolic link may be followed, overwriting /tmp

1.5 Default Solaris Installation

When initially installing a Solaris system, all security experts agree that only the minimum number of packages should be installed. Yet quite often an administrator will simply install the entire Solaris distribution, then walk away. What has an administrator just walked away from? Table 1 lists just a few facts. [2]

Table 1: Solaris Default Installation Facts

- 78 programs are setuid
- 30 programs are setgid
- 29 listening TCP ports
- 29 listening UDP ports
- 57 different recommended patches (as of Oct 6, 2000)

From our theorems regarding computer security, we know that the sheer number of privileged programs makes the default Solaris installation a ripe target for computer intruders.

2 Tool Overview

2.1 Solaris Security Step by Step

The guide "Solaris Security Step by Step"[8] is distributed by SANS[5] Institute. It serves as a survival guide for Solaris system administrators, leading them from initial system installation to putting a system into production.

The guide is a compilation of procedures "based entirely on the real-world experiences of the editor and an amazing team of reviewers".[8] It should be noted that the step by step guide was based upon many works, including Titan.

Solaris Security Step by Step is available from SANS on their website, http://www.sans.org. Version 1.0 of the booklet was used in this evaluation.

2.2 Titan

Titan was released in 1998 by

- Brad Powell, a Senior Security Architect for Sun Professional Services
- Dan Farmer, a security researcher for Earthlink

[2] Solaris 7 32-bit Full Distribution Installation

- Matthew Archibald, the Information and Networks Security Officer for Applied Materials Inc.

Titan is

> a collection of programs, each of which either fixes or tightens one or more potential security problems with a particular aspect in the setup or configuration of a Unix system. Conceived and created by Brad Powell, it was written in Bourne shell, and its simple modular design makes it trivial for anyone who can write a shell script or program to add to it .... [9]

Titan can be found on the web at http://www.fish.com/titan. Titan Version 3.7 was used in this evaluation.

2.3 YASSP

YASSP stands for "Yet Another Secure Solaris Package". The project started in 1997 by Jean Chouanard of the famous XEROX Palo Alto Research Center (PARC). YASSP uses native Solaris packages (called "pkgs") to modify default system settings.

The goals of YASSP are

1. To integrate as closely as possible with the Solaris SUN "pkg" standards.
2. To give the ability to cleanly install and uninstall all components
3. To provide as secure a system as possible by default. Administrators can then re-enable needed services and programs.

YASSP can be found on the web at http://yassp.parc.xerox.com. YASSP version 0 beta 11 was used in this evaluation. Please note that sections of YASSP were based upon Titan.

3 Evaluation Matrix

3.1 Overview

Table 2 lists the various levels of support each tool incorporates. [3]

Additional dependencies are enumerated in Table 3. Adding dependencies must be well thought out. Each added program may have additional security bugs. Moreover, each added program may have configuration, licensing, and administrative conditions and restrictions that need careful consideration.

However, programs added may yield additional functionality. Therefore, the additional program dependencies should be treated not as "features", but as components that can be used to fulfill a well thought out security policy.

[3] It is important to note that the *Step by Step* guide does not officially support Solaris 2.7. However, the guide has nothing that is version specific, so it was used for all testing in this guide.

Table 2: Support Overview

Description	*Step by Step*	*Titan*	*YASSP*
Supported Releases	2.5 - 2.6	4.1 - 8	2.6 - 8
Native Solaris Package			√
Add Dependencies	√		√
Undo available		√	√
Fully Documented	√	√	√

Table 3: Binary Dependencies

Dependency	*Step by Step*	*Titan*	*YASSP*
GNU Utilities[1]	Required	Not needed	Included
Offline Compiler	Required	Recommended	Not needed
SSH[10]	Recommended	Recommended	Included
Fix-Modes[3]	Recommended	Included	Included
TCP-Wrappers[11]	Recommended	Recommended	Included
Tripwire[4]	Not mentioned	Recommended	Included

Table 4 provides a simple metric for measuring system security. It simply counts the number of potential or actual privileged processes. The justification for this metric is a consequence of the basic theorems of computer security, i.e. that each additional privileged process generally decreases system security .

Note that the table lists the number of privileged programs from a full installation of Solaris 2.7. All tools surveyed recommend only installing the core distribution, which may significantly lower the total number of privileged programs. [4]

Table 4: Privileged Processes

Description	*Step by Step*	*Titan*	*YASSP*
TCP Ports open	ssh	telnet,ftp	ssh
UDP Ports open	syslog	syslog	syslog
# of setuid programs	53	53	78
# of setgid programs	55	55	30

3.2 Kernel Parameters

Solaris 2.6 and greater use /etc/system to modify kernel parameters. Note that YASSP sets several non-security related kernel parameters, which are not

[4]It is interesting to note that Titan actually increases the number of setgid applications. The increase is because Titan creates a "staff" administrative group from which to run programs. So while the number of setgid applications increases, the number of accounts that can run those applications decreases.

included here. [5]

Table 5 outlines kernel parameters set by each OS hardening method.

Table 5: Kernel Parameters

Description	*Step by Step*	*Titan*	*YASSP*
Stack protection	√	√	√
NFS port monitoring		√	√
Disable core dumps		√	√
Set max users processes			√

3.3 Network Services

Disabling unneeded or historically buggy network services is the number one recommended security practice. All too often systems are compromised via an unneeded or unnecessary service.

In addition to disabling unneeded network services, security conscious organizations should be working towards eliminating clear-text communications. Currently, the most popular program is secure shell (ssh). SSH is available both open source [7] and company supported [10].[6] SSH is a large (and hence potentially buggy) program, and does require a knowledgeable administrator to configure properly. It should be noted that these are some of the reasons Titan does not include SSH.

Table 6 compares network services enabled. Note the defense in depth in each package. For example, even though most tools disable telnet, they still add a warning banner just in case it is ever re-enabled.

[5] Examples of non-security related parameters are enabling priority paging and increasing psuedo-terminal count.

[6] There may be various export and patent issues regarding SSH in your locale.

Table 6: Network Services

Description	*Step by Step*	*Titan*	*YASSP*
Disables cleartext logins	√		√
Installs SSH	√		√
Installs TCP Wrappers	√		√
TCP Services Enabled	ssh	telnet/ftp	ssh
UDP Services Enabled	syslog	syslog	syslog
System accounts FTP disabled	√	√	√
FTP banner enabled		√	
Telnet banner enabled	√	√	√
Multicast disabled	√	√	√
DHCP disabled	√	√	√
Enables inetd logging		√	√
in.routed does not advertise routes		√	√
snmpd disabled	√	√	√
Sendmail vrfy/expn disabled		√	
Sendmail version displayed		√	√
Sendmail user .forwards disabled	√	√	
rhosts-style auth disabled	*surd*	√	√
Removes /etc/hosts.equiv		√	
Daemon umask set	√	√	√

3.4 Network Parameters

Network parameters are best described by SUN documentation. Introductions to setting network parameters are available at [12] and [6].

Please note that YASSP sets additional parameters that are performance, not security, related. Table 7 compares network parameters.

Table 7: Network Parameters

Description	*Step by Step*	*Titan*	*YASSP*
Disable router	√	√	√
IPV6 Supported			√
arp_cleanup_interval	60	60000	60000
ip_respond_to_address_mask_broadcast		0	
ip_forward_directed_broadcasts	0	0	0
ip_forward_src_routed	0	0	0
ip_forwarding	0	0	0
ip_icmp_err_interval			0
ip_ignore_redirect	1	1	1
ip_ire_flush_interval	60000	60000	120000
ip_ire_pathmtu_interval			600000
ip_respond_to_timestamp		0	0
ip_respond_to_timestamp_broadcast		0	0
ip_send_redirects	0	0	0
ip_strict_dst_multihoming	1	1	1
tcp_conn_req_max_q			512
tcp_conn_req_max_q0	10240	4096	10240
tcp_extra_priv_ports_add		2049	2049
tcp_ip_abort_cinterval		10000	60000
tcp_ip_abort_interval			600000
udp_extra_priv_ports_add		2049	2049
Strong TCP sequences numbers	√	√	√

3.5 System Logging

System logging under Solaris is less than adequate. Having accurate log information is important both for troubleshooting problems as well as monitoring for possible intrusion attempts. [7]

Table 8 compares logging information. Note only information logged to disk (e.g. not just to console) is counted.

[7] Local notices are used by tcp wrappers, for example. For more information, consult the syslog.conf man page

Table 8: System Logging

Program Type	*Step by Step*	*Titan*	*YASSP*
syslog auth	auth.info	auth.notice	auth.info
syslog *.emerg			
syslog mail.debug		√	√
syslog kern.debug		√	
syslog local levels			√
Enable failed login log	√	√	√

3.6 File Permissions and User Defaults

Solaris file permissions are generally regarded as adequate for a single-user system, but are not robust enough to support a multi-user environment. Casper Dik's[3] provides the de facto standard package fix-modes that armors file permissions.

Just as important as standard file permissions are the order in which they are searched. For example, the root user should never have the current directory in their search path. While editing /etc/profile can alter system-wide defaults, a robust secure installation will also change the default initialization files located in /etc/skel.

Table 9 compares hardening information.

Table 9: File Permissions and User Defaults

Program Type	*Step by Step*	*Titan*	*YASSP*
Uses fix-modes	√	√	√
Binaries owned by root		√	
Enables ASET		√	
Enables BSM		√	
Sets default umask		√	√
Sets secure default PATH		√	√

3.7 Miscellaneous Issues

Each tool contains miscellaneous other advice and scripts. Table 10 outlines the most common criteria.

4 Minimum Criteria

4.1 Network Service Recommendations

Every security professional agrees that critical network services should each be run on their own box when possible. The principle of "one box, one service" is meant to reduce the number of potential problems, both administrative and

Table 10: Miscellaneous

Description	*Step by Step*	*Titan*	*YASSP*
Disable CDE	√	√	√
Set EEPROM security	command	command	
Disable NFS	√	√	√
Disable autofs	√	√	√
Install Patches	√	√	√

security related. Table 11 lists the maximum recommended services, as well as configuration information for some well-known services.

The table is formatted such that a general type of service is listed, along with recommendations and a commentary. The recommendations are not the only solutions. For example, several protocols allow for encrypted network communication. SSH is only one choice. Many security experts would rather use the generally smaller One Time Password programs. Others rely upon scalable enterprise-wide security solutions such as kerberos.

The purpose of the commentary is to enumerate the criteria for selecting other utilities that may fulfill the same role.

Table 11: Service Recommendations

Description	*Recommendation*	*Commentary*
TCP Services Enabled	SSH	Run as few TCP services as possible. TCP services should encrypt authentication data.
UDP Services Enabled	syslog	Run as few UDP services as possible. UDP services should encrypt when possible.
Filter services	TCP Wrappers	Disable connections from unauthorized hosts. Firewall utilities have similar functionality.
OS Version revealed	disabled	Version information may be used by intruders.
TCP Banners	enabled	All services should display a banner detailing use and monitoring policy
Multicast	disabled	Multicast is not needed for most sites.
Daemon Umask	022	Network daemons should not create world or group readable files.
FTP system accounts	disabled	Administrative users should never use cleartext protocols such as ftp.
Sendmail vrfy/expn	disabled	Sendmail should not give out information about accounts.
Sendmail version displayed	disabled	Sendmail version information may be used to find exploits.
rhosts-style auth	disabled	Systems should not use the Berkeley "r" commands due to inherent weakness in the protocol.
DHCP	disabled	Prevent rogue DHCP servers from giving faulty information.
snmpd	disabled	SNMP may give out information to intruders.

4.2 Kernel Parameter Recommendations

Kernel parameters are defined in /etc/system, and are read at system boot. For that reason, any changes made to /etc/system normally require a reboot to take effect. Table 12 specifies the recommended kernel parameters for a secure system.

Table 12: Kernel Parameters Recommendations

Description	*Recommendation*	*Commentary*
Stack Protection	enabled	Stack protection thwarts some types of buffer overflows.
NFS port monitor	enabled	Enable NFS port monitoring.
Disable core dumps	enabled	Core dumps may give out confidential information. They should only be enabled on non-production machines.

4.3 Network Parameter Recommendations

Network parameters are used to change the way Solaris drivers respond. Table 13 are network parameters that should be set for security purposes.

Table 13: Network Parameter Recommendations

Description	*Recommendation*	*Commentary*
Act as router	disabled	Secure hosts should not route packets.
arp_cleanup_interval	60000	This is the time that ARP will hold on to unsolicited information in case IP needs it in milliseconds.
ip_ire_flush_interval	60000	Same as arp_cleanup_interval.
ip_forward_directed_broadcasts	0	Direct broadcast messages may be used in smurf-type attacks.
ip_forward_src_routed	0	Source routed packets are not needed by modern networks.
ip_forwarding	0	Workstation should not route packets. This is equivalent to touching /etc/notrouter
ip_ignore_redirect	1	Hosts with a single default router need not accept redirects.
ip_send_redirects	0	Only routers need to redirect errors.
ip_strict_dst_multihoming	1	Prevents packet spoofing on non-forwarding multihomed systems.
tcp_extra_priv_ports_add	2049	Increases the reserved TCP port range to 2049, most notable for NFS.
tcp_conn_req_max_q	10240	Protect against SYN flood by increasing queue size.
udp_extra_priv_ports_add	2049	Increases the reserved UDP port range to 2049, most notable for NFS.
Strong TCP Sequence numbers	2	RFC 1948 strong sequence numbers to prevent IP spoofing attacks.

4.4 File Permissions and User Default Recommendations

Secure file permissions primarily keep shell access users from gaining elevated privileges. They do not normally protect against remote attacks. Secure file permissions are important in case an intruder ever gains a non-privileged user password, as well as protect against security breaches from rogue authorized users.

Table 14 outlines the recommend default file and user settings.

Table 14: Permission Recommendations

Description	*Recommendation*	*Commentary*
fix-modes	enabled	fix-modes tightens file permissions and updates the pkginfo database.
User default umask	022	New user files should only be readable by owner.

4.5 System Logging Recommendations

YASSP generally logs everything, while Titan and Step by Step only add authentication information. The more information logged, generally the better. Table 15 outlines the minimum extra data to log in addition to the default Solaris /etc/syslog.conf. Note that when possible all log data should be duplicated to another host.

Table 15: System Logging Recommendations

Description	*Recommendation*	*Commentary*
Authentication	auth.info	Authentication information logged to disk
Failed login	/var/log/loginlog	Logs multiple failed login attempts.

4.6 Miscellaneous Recommendations

A specific site security policy will undoubtedly call to increase certain parameters. However, there are certain miscellaneous settings that all security experts agree on. Table 16 lists additional parameters needed for every secure Solaris system.

Table 16: Miscellaneous Recommendations

Description	*Recommendation*	*Commentary*
CDE	disabled	CDE and other X servers have a long history of security problems.
Set EEPROM security	command	Password is required to boot except off default media.
NFS	disabled	NFS has a long history of security problems.
AutoFS	disable	AutoFS is an extension of NFS, hence just as problematic.
Patches	Recommended Cluster	Recommended patches are the vendor supported way to remedy security issues.
Packet Filtering	Default Deny	All services should be filtered to ensure that only legitimate, authorized connections are accepted.

5 Tool Summary

5.1 Step by Step

Step by Step is a readable guide for Solaris security that not only documents recommended changes, but also warns of potential problems. Included in the guide are:

- Solaris installation instructions.
- Caveat boxes listing common problems that may be encountered.
- Backup and booting basics.
- Physical security.
- Securing network infrastructure.

Step by Step includes several examples and configuration scripts in the appendix. Step by Step clearly is a readable, comprehensive guide for securing a Solaris system.

5.2 Titan

Titan predates other hardening tools. It is clear that many other armoring utilities are indebted to Titan, as its features and recommendations are often duplicated.

Titan includes additional security enhancement scripts not mentioned specifically in this guide. Table 17 lists just a few of the additional security scripts included with Titan.

Table 17: Additional Titan Scripts

Name	*Description*
vold.sh	Specifically disables vold
lpsched.sh	Specifically disables lpsched
defpwparams.sh	Sets password aging information
cde.sh	Disables remote CDE XDMCP logins
dmi.sh	Specifically disables dmi
fix-cronpath.sh, cronset.sh	Hardens cron daemon
powerd.sh	Specifically disables powerd

All Titan modules have a "-v" option which will simply check what would be done to harden the operating system. Titan also provides several example configurations which can be used as starting points for hardening systems. Another nice feature of Titan is it can be run from the cron daemon to recheck at fixed intervals.

Titan's biggest strength is in its modularity. Each Titan module checks or fixes a particular security vulnerability. This, coupled with the fact each module is written in bourne shell, gives administrators the capability to readily understand each action Titan is performing.

Titan is the most comprehensive hardening tool. It has a long history, and is currently the most widely deployed Solaris hardening tool. Anyone with more than a casual interest in Solaris security should consider reading all Titan documentation. However, due to the deliberate design decision not to introduce additional dependencies Titan is not a one-stop solution to securing a host.

5.3 YASSP

YASSP attempts to provide a single solution to securing a host. It not only hardens a system against attack, but also provides programs to help administrators

YASSP's strength is it does everything at once. However, it is still quite new, and hence may need time to ensure that it is bug-free.

YASSP includes several features not outlined here, including:

- Network performance tuning
- Revision control tools
- Single configuration file /etc/yassp.conf

5.4 Comparison Results

Each hardening tool provides more than adequate security for a Solaris system on the internet. YASSP and Titan are the most readily usable, as Step by Step requires reading and manually executing commands.

YASSP is by far the easiest to install, but also is the newest. For that reason bugs should be expected. YASSP is recommended for administrators who want the quickest solution for hardening their systems.

Titan is the most thorough hardening tool. Titan is recommended for systems that not only need to be hardened, but need to be rechecked regularly.

References

[1] GNU Archive. http://www.gnu.org.

[2] William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security.* Addison-Wesley, 1994.

[3] Casper Dik. fix-modes. URL: http://www.science.uva.nl/pub/solaris/.

[4] Tripwire Inc.

[5] SANS Insitute. URL: http://www.sans.org.

[6] Alex Noordergraaf and Keith Watson. Solaris operating environment network security settings. http://www.sun.com/blueprints/1299/network.pdf.

[7] OpenSSH. URL: http://www.openssh.org.

[8] Hal Pomeranz. *Solaris Security Step by Step*. SANS Institute, v1.0 edition, 1999.

[9] Dan Farmer Brad Powell and Matthew Archibald. Titan documentation. Part of the Titan v3.7 documentation, 1998.

[10] SSH Communication Security. URL: http://www.ssh.fi.

[11] Wietse Venema. ftp://ftp.porcupine.org/pub/security/index.html.

[12] Jens S. Vockler. http://www.rvs.uni-hannover.de/people/voeckler/tune/EN/tune.html.