



There and Back Again – A Solaris Security Tale

Glenn Brunette

Distinguished Engineer
Sun Microsystems, Inc.



Agenda

- Solaris Security Goals
- Solaris and Trusted Solaris Security
- Government and Industry Collaboration
- Future of Solaris
- References

Solaris Security Goals

- **Defending**
 - > Provide strong assurance of system integrity.
 - > Defend system from unauthorized access.
- **Enabling**
 - > Secure authentication of all active subjects.
 - > Protect communications between endpoints.
- **Deploying**
 - > Emphasize an integratable stack architecture.
 - > Interoperate with other security architectures.
 - > Ease management and use of security features.
 - > Receive independent assessment of security.

Trusted Solaris - Past and Present

Trusted Solaris History

<u>Product</u>	<u>Year</u>	<u>Evaluation</u>
SunOS MLS 1.0	1990	TCSEC Conformance (1985 Orange Book)
SunOS CMW 1.0	1992	ITSEC Certified for E3 / F-B1
Trusted Solaris 1.2	1995	ITSEC Certified for E3 / F-B1
Trusted Solaris 2.5.1	1996	ITSEC Certified for E3 / F-B1
Trusted Solaris 8	2000	Common Criteria Evaluated: CAPP, RBACPP, LSPP at EAL4+

Mandatory Access Control, Labeled Desktop, Labeled Printing, Labeled Networking, Labeled Filesystems, Device Allocation, etc.

Solaris Security - Past and Present

Solaris Security: 1990 – 1994

Solaris 2.0* - Solaris 2.3

- Secure RPC (DES, Kerberos, Diffie-Hellman)
- NIS+
- Device Allocation
- Automated Security Enhancement Tool (ASET)
- Kernel-level Event Auditing
- Secure Programmable ROM (PROM)

** Includes functionality originally developed in older versions of the SunOS operating system.*

Solaris Security: 1995 – 1999

Solaris 2.4 – Solaris 7

- Access Control Lists (ACLs)
- Disable Executable Stacks
- Java Virtual Machine (JVM)
- Pluggable Authentication Mechanism
- Kerberos (V5)
- Generic Security Services (GSS) API (DH Mech.)

- Solaris 2.5.1, 2.6 Certified: ITSEC E3 / F-C2

Solaris Security: 2000 – 2001

Solaris 8

- Role-based Access Control (RBAC)
- Tightened OS File Permissions
- IP Security (IPsec) – AH and ESP
- GSS-API Kerberos Mech.
- Smartcard Framework

- Solaris 8 Certified: CC CAPP at EAL4

Solaris Security: 2002 – 2003

Solaris 9

- Granular OS Packaging
- Random Number Generator
- Bundled 128-bit Cryptography
- Flexible Password Encryption
- SunScreen Firewall
- Secure Shell
- Internet Key Exchange (IKE) (w/HW Crypto)
- TCP Wrappers
- Kerberos KDC

- Solaris 9 Certified: CC CAPP and RBACPP at EAL4+

Solaris Security: Today

Solaris 10

- Minimal OS Installation Option
- Enhanced Password Complexity Checks, History, Lockout
- Signed ELF Objects (Binaries, Libraries, Crypto, etc.)
- Zettabyte File System (ZFS)
- Process Rights Management (Privileges)
- Cryptographic Framework
- Solaris Containers (Zones, Resource Management, etc.)
- Basic Audit and Reporting Tool (BART)
- IP Filter

- Solaris 10 In Evaluation: CC CAPP and RBACPP at EAL4+

Solaris Security - Government and Industry Collaboration

Solaris Security: 1985 - Today

You!

Thank you to all of our customers who have shared with us your requirements, feature requests and bug reports so that we could continue to improve our product to better meet your needs!

Solaris Security: 1999 – Today

Sun Security BluePrints

- Publish Sun recommended practices and practical guidance for the use of Sun products and technologies.
- Over 80 security articles have been published to date:
 - > Solaris OS Security
 - > Solaris OS Network Settings for Security
- Recommendations built upon a Sun supported foundation leveraging experts from around the company.
- Extends product documentation by providing greater detail, use cases and integration information.

Solaris Security: 2000 – Today

Solaris Security Toolkit

- Sun's recommended and supported tool for hardening the Solaris OS (Solaris 2.5.1 – Solaris 10).
- Codification of the security recommendations published by the Sun BluePrints program.
- Flexible and extensible policy-based framework for rapidly and consistently securing Solaris platforms across an enterprise.
- Collection of Bourne shell scripts used to apply, undo or verify changes to the security configuration of Solaris OS systems.

Solaris Security Collaboration

- 2003
 - > Sun begins discussions with the NSA regarding content in the “60 Minute Network Security Guide”.
 - > NSA directs Sun to initiate contact with the Center for Internet Security (CIS) regarding their Benchmark program.
- 2004
 - > Sun, CIS, NSA, and DISA began to jointly work on the update to the CIS Solaris Benchmark for the Solaris 9 OS.
 - > Sun asks CIS, NSA, and NIST to participate in the NCSP “Common Security Configurations” working group.
 - > Sun participates in the NIST Security Checklists workshop.

National Cyber Security Partnership


A Few Highlights...

- > Vendors, user groups and government organizations should take a more proactive role in the development of and collaboration on product security recommendations.
- > Vendors should leverage heightened forms of collaboration with user communities and government organizations to improve the security capabilities of their products.
- > Vendors should provide stronger out-of-the-box security configurations and/or provide supported capabilities or tools that simplify and automate the process of securing their products.
- > Vendors should provide more substantive security recommendations, configuration checks, etc. in their product documentation.

Solaris Security Collaboration


- 2005
 - > Sun collaborates with CIS, NSA, and DISA on the publication of the CIS Solaris 10 Benchmark.
 - > Before the GA release of Solaris 10!
 - > Solaris 10 Benchmark becomes a NIST 800-70 Checklist.
- 2006
 - > Sun announces official support for the CIS Solaris 10 Benchmark.
 - > Sun, CIS, NSA, DISA begin work on updating the Solaris 10 Benchmark for Solaris 10 11/06.

Solaris Security Collaboration Future



Solaris™ Operating Environment Security
Updated for Solaris 9 Operating Environment

By Alex Noordergraaf and Keith Watson
Sun BluePrints™ OnLine—December 2002



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


Sun Microsystems, Inc.
4110 Network Circle
Sunnyvale, CA 95045 U.S.A.
950-560-5000
Part No. 800-542-10
Revision 1.1 (28 Oct 02)
Edition: December 2002

UNCLASSIFIED

1331 Technical Re
E331-007R-2

Guide to the Secure Configuration of Solaris 9



Operating Systems Division UNIX Team
of the
Systems and Network Attack Center (SNAC)



National Security Agency
9800 Savage Rd, Suite 6704
Ft. Meade, MD 20755-6704
SNAC.Guides@nsa.gov

UNCLASSIFIED

Dated: 16 July 2
Version



UNIX SECURITY CHECKLIST

Version 5, Release 1

15 July 2006

Developed by DISA for the DOD

UNCLASSIFIED

the CENTER for INTERNET SECURITY

Solaris Benchmark v2.0
(Solaris 10)

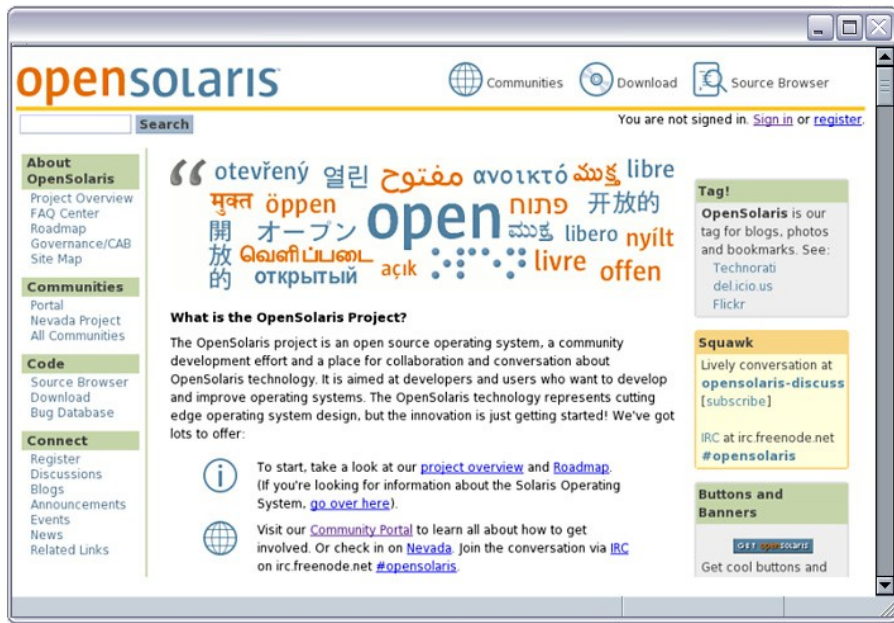
Copyright 2001-2005, The Center for Internet Security
<http://www.CISecurity.org/>

Ongoing Areas of Collaboration

- Common Configuration Enumeration (CCE)
 - > Supporting Mitre as a Working Group Member
- XCCDF / OVAL
 - > Supporting CIS (et al.) as a Benchmark Member
- NIST 800-70 FISMA Controls Mapping
 - > Supporting NIST via the CIS XCCDF/OVAL Efforts

Solaris Security - A Bright Future

opensolaris™



Innovation Happens Everywhere
www.opensolaris.org

Source: Sun 2/06 – For latest, see:

<http://www.opensolaris.org/os/community/marketing/metrics/latest/>

15,000 members

40 major community projects,
 BrandZ, DTrace, Solaris ZFS, Zones

31 User Groups Worldwide

250 Code Contributions

33,000 Downloads

5 Open Solaris Distros Available:
 Solaris, SchilliX, BeliniX, Nexenta, MartUX

Community Recognition:

2006 SIIA Codie Award
 2005 Open Source
 World Editor's Choice,
 Solaris Eng: InfoWorld
 Innovators Award, Bryan Cantrill:
 Top 35 Young Innovators – MIT



OpenSolaris Security Community

- Share your requirements and feedback, participate in shaping the future of the Solaris product:
 - > Discussions
 - > Security Projects
 - > Early Access Functionality
 - > Code Contributions
 - > Library
- Nearly all of the Solaris code base is available today:
 - > <http://www.opensolaris.org/>

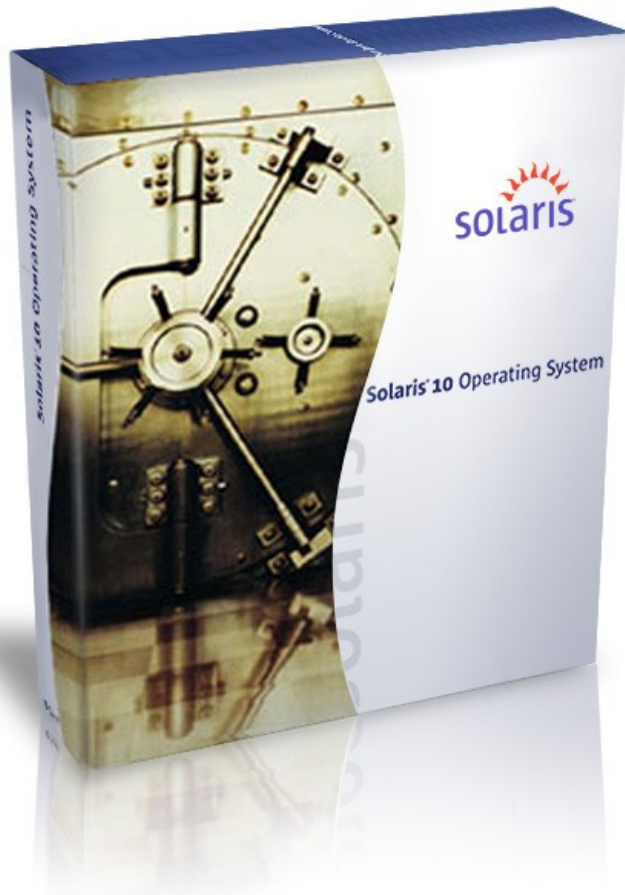
OpenSolaris Project:

Solaris Secure by Default

- Goal:
 - > Reduce network-based attack surface by eliminating or restricting available network services:
 - > During and immediately after initial installation
 - > Post-installation enabled by administration action
- Impact:
 - > Secure shell is the only permitted network service (by default)
 - > Other services can be added or enabled as necessary.
- Integrated:
 - > OpenSolaris (build 42), Solaris 10 11/06

OpenSolaris Project:

Solaris Trusted Extensions



Trusted Extensions

Labeled Security for Solaris 10+
Multi-Level Desktop, Networking
and Printing

Labeled Filesystems and Devices

Compatible with all Solaris
hardware and applications

Common Criteria Target:
CAPP, RBACPP, LSPP @ EAL 4+

Available November 2006

Solaris Security - There and Back Again

Participation Helps Improve Security



Innovation Happens Everywhere!

Actions...

1

Encourage greater collaboration on and sharing of recommended security practices!

2

Promote common formats for security guidance that help simplify configuration and deployment.

3

Share your requirements, experiences, etc. to help vendors improve their products!

For More Information

- Sun Security Home
 - > <http://www.sun.com/security>
- OpenSolaris Security Community
 - > <http://www.opensolaris.org/os/community/security>
- Sun Security BluePrints
 - > <http://www.sun.com/blueprints>
- Sun Security Blogs
 - > <http://blogs.sun.com>



There and Back Again – A Solaris Security Tale

Glenn Brunette

Sun Microsystems, Inc.

glenn.brunette@sun.com

<http://blogs.sun.com/gbrunett>

