# Solaris™ 10 and Security

Advanced Features Enable Secure Systems with Peace of Mind

## Highlights

- Verifies the integrity of your system using Solaris™ Secure Execution and file verification features
- Reduces risk by granting only the privileges needed for user and process rights management
- Secures your systems by leveraging Secure Internet Protocol (IPSec), Internet Key Exchange (IKE), and Solaris IP Filter firewall to protect network traffic
- Simplifies administration by using open, standards-based Solaris Cryptographic Framework for file encryption

## Security is not bolted on, it is built in

Security is more than a mix of technologies. It is an ongoing discipline, a lifestyle for customers and technology providers. Sun understands this, and continues its 20-year commitment to building security in the Solaris™ Operating System (OS) with the release of Solaris 10, our most comprehensive, security-enabled OS yet.

## File integrity and secure execution

How do you know when and if your security has been compromised? More importantly, how do you prevent compromises from happening? Because most binaries in the Solaris 10 OS are digitally signed, administrators can track changes easily. All patches or enhancements are embedded with digital signatures, eliminating the false positives associated with most file integrity-checking software when upgrading or patching. In a future release, the Secure Execution feature of Solaris software will make it possible to lock down a system so that only valid, signed executables from a list of trusted authorities will be allowed to run. Rogue applications, Trojan horses, and viruses simply will not execute. Any binary can be signed — third-party commercial offering, open source, or your own code — without needing the source code.

The Solaris 10 OS also introduces a file integrity-checking application for data files and customer applications, the Basic Audit and Reporting Tool (BART). As part of the Solaris Fingerprint Database project, digital signatures are provided for all files shipped in the Solaris OS. These signatures allow you to check the integrity of Solaris files to ensure that no hacker has modified critical system files. Together, these tools provide powerful, flexible ways to monitor and protect against changes to your operating system platform.

## User and process rights management

In traditional UNIX® platform-based operating systems, applications and users often need administrative access to perform their jobs. However, most implementations offer just one level of higher privilege: root super-user. This means that any user or application given root access has the ability to make major changes to the operating system — and is typically the target of hacking attempts. Borrowing technology from our battle-proven Trusted Solaris™ OS, Solaris 10 offers unique user rights management (also known as role-based access control or RBAC) and process rights management (also known as privileges). These technologies reduce security risk by granting users and applications only the minimum capabilities needed to perform their duties. Unlike other solutions on the market, no application changes are required to take advantage of these security enhancements.

A Web server application is a good example of this; all UNIX platform-based Web server software traditionally requires root access to serve applications on port 80, a commonly used Web TCP/IP port. However, with process rights management, a Web server application on Solaris 10 can be granted just the privileges required to enable it to bind to low-numbered ports (port 80) without additional administrative access. If the Web server software is attacked, the hacker cannot escalate privileges, launch additional attacks, or gain further access to the system.

## Solaris IP Filter firewall and TCP Wrappers

For years, the Solaris OS has included firewall protection technology with every copy shipped, to protect individual systems from attack. Solaris 10 comes with Solaris IP Filter firewall software, which is based on the popular IP Filter project from the free and open source software community. This integrated firewall reduces the number of network services that are exposed to attack. In addition, TCP Wrappers are integrated in Solaris 10, limiting access to service-based, allowed domains.

## Cryptographic services and secure remote access

For high-performance, system-wide cryptographic routines, the new Solaris Cryptographic Framework adds a standards-based, common API. This provides a single point of administration and uniform access to hardware-accelerated, cryptographic functions for cryptographically-aware applications. The pluggable Framework can load balance across accelerators, increasing encrypted network traffic throughput. It is available to applications written to use Public Key Cryptography Standards (PKCS) #11, Sun Java™ Enterprise System, OpenSSL, or Java Cryptographic Services.

## Flexible enterprise authentication

The Solaris 10 OS delivers new, flexible, commonly requested authentication features. Sun Enterprise Authentication Mechanism software (Sun's implementation of the Kerberos protocol), Lightweight Directory Access Protocol (LDAP,) and interoperability enhancements enable enterprise-wide, secure, standards-based single sign-on (SSO) to your servers and applications. These enhancements reduce costs by centralizing system access administration across multiple operating systems while increasing security. New to the Solaris 10 OS are Kerberos-enabled remote applications such as rsh, rcp, telnet, Solaris Secure Shell, and others that were previously available only via download.

To enable easier integration with existing environments, existing native LDAP authentication software offers NIS and NIS+ to LDAP gateways. Local passwords have strong password encryption options, including MD5 and Blowfish, as well as account lockout, syntax checking, and dictionary checks. Kerberos-based protocols allow for enterprise SSO and are enhanced for better scalability. Pluggable Authentication Modules (PAMs) make it possible to add authentication services, and support smart card-based authentication, as well.

## Streamlined system security

New features in Solaris 10 make it easier than ever to minimize and harden a system. The Reduced Networking Metacluster install option creates a minimized Solaris image, ready for security administrators to add functionality to it. Administrators can also employ new Service Manager technology to create dynamic security profiles for a system that includes just the few network services needed by that system. The first of these profiles, Generic Limited Networking, can turn off nearly all unencrypted, remote communication to the system with one simple command.

Learn More

To learn how to safeguard your web servers, visit sun.com/solaris/teachme.

For additional information please see sun.com/solaris/features.

## Multilevel security

For those customers requiring absolute separation of data and processes based on data sensitivity, a multilevel operating system offers a strong deployment platform. Today, Sun offers a separate platform, Trusted Solaris 8 2/04, to address this need. It is binary compatible with Solaris 8, and a de facto standard in many government and financial institutions around the world.

With many of the features from Trusted Solaris integrated into Solaris 10, Sun is also developing a multilevel security policy for future Solaris 10 releases. Solaris Trusted Extensions will extend the security policy of Solaris 10 using containers, user, and process rights management, adding mandatory access control and sensitivity labels for increased privacy, protection, and separation.

## Conclusion

By focusing on security as an integral part of all of its products, Sun provides a solid foundation for preventing, not just fixing, security problems. The bottom line is secure operations for today's global marketplace.

**Sun Microsystems, Inc.** 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com