Oracle Solaris Security
Oracle Solaris 11 Express

As the security foundation in Oracle, Oracle Solaris has continuously improved over the years to adapt to ever changing business needs, Oracle Solaris 11 Express offers a number of improvements and new features that can roughly be divided into four topic areas:

- Network Security – Securing system-to-system communications.
- Host-based Security – Securing access to hosts and their services.
- Data at Rest – Securing data stored on disk or other media.
- Trusted Extensions – Securing data with label-based mandatory access control.

Network Security

Oracle Solaris 11 Express adds the capability to create one or more fully virtualized and dedicated network stacks per Oracle Solaris Zone, using features called **Exclusive IP Stacks** and **Network Virtualization**. These features allow administrators to create fine-grained network security policies on a per zone basis. Examples are the configuration of zone-specific IP routing, DHCPv4 and IPv6 stateless address configuration, IP filter and NAT configurations, MAC, DHCP, and IP Anti-Spoofing functionality, and IP security (IPsec) and Internet Key Exchange (IKE) automating the provision of authenticated keying material for IPsec security associations.

With **Automatic Secure By Default**, network services are disabled by default or set to listen for local system communications only. Oracle Solaris follows the security principle of default secure configurations in a number of different ways. In Oracle Solaris 11 Express, this principle is applied to the default configuration of network services where all but one service, the ssh daemon, are either configured to listen for locally initiated connections only or are disabled. With the ssh daemon, authenticated administrators can remotely administer the system.

Oracle Solaris 11 Express includes a number of feature improvements to the **Kerberos** network authentication protocol implementation. This includes zero-configuration Kerberos client configuration through DNS and additional Active Directory and PAM cooperation to enhance interoperability with Windows clients. Users can now be initially authenticated using public key cryptography (PKINIT). The new kdcmgr(1M) utility provides interactive and non-interactive modes for configuring master and slave Key Distribution Center (KDCs). Additionally, authentication against an Active Directory server supports proper mapping of UNIX users and groups to Active Directory entities.

Host-Based Security

Oracle Solaris 11 Express introduces support for **Trusted Platform Modules** (TPM). Trusted Computing Group TSS 1.2 API headers and libraries are provided for third party applications. A new administration command, tpmadm(1M), manages the TPM and a pkcs11_tpm(5) plugin for the Oracle Solaris Cryptographic Framework enables the use of the TPM as a secure key store.

Extending some of the existing least privilege features of Oracle Solaris, Oracle Solaris 11 Express introduces two new features, called Root as a Role and In-Kernel pfexec.

With **Root as a Role**, the root account is now a role by default. Authorized users assume the root role rather than directly logging in to a root user account. This feature extends Oracle Solaris Role Based Access Control (RBAC) and enables authorized non-root users to complete tasks and scripts with superuser privileges.

Privileged actions can now be attributed to the user who invoked it. This enhancement is especially important in environments where several administrators share the root password, an approach that lacks accountability. Such attribution happens via Oracle Solaris Auditing, a service that no longer requires a reboot to enable.

The **In-Kernel pfexec**(1) implementation is used to execute administrative commands requiring a higher privilege level. A new process flag is used to specify that all subsequent program executions are subject to RBAC policy. The flag is set at the first invocation of any of the complete set of profile shells (pfsh, pfcsh, pfksh, pfksh93, pfbash, pftcsh, pfzsh, pfexec) and inherited by child processes. This feature eliminates the need to modify shell scripts to invoke pfexec or profile shells.

Another application of this feature is to limit the set of privileges given to programs with setuid to root. Processes that require the setuid mechanism traditionally ran with all privileges. Now they execute with only those privileges that are specified in their entry in the **Forced Privileges** rights profile, significantly reducing their potential to be an attack vector against the system.

Furthermore, it is now easier to restrict users' authorizations and the commands they can execute. A new rights profile called 'Stop' can be assigned to a user to prevent subsequent assignment of default settings. This configuration creates a **User Sandbox** in which users can only execute the commands with the authorizations that were assigned to their rights profiles.

Three new basic privileges(5) are added that enable the ability to restrict read access (file_read), write access (file_write), and outbound network access(net_access). These privileges provides additional sandboxing capabilities for services or processes.

The zone configuration and administration model in Oracle Solaris 11 Express is extended to include an option to specify which users and roles can act as administrators for each zone. This option is called **delegated zone administration**, set through the admin resource in zonecfg. Each administrator can be granted a set of authorizations for specific administrative functions. This delegation enables customers to restrict access to non-global zones from the global zone, rather than the original all-or-nothing approach. Individual authorizations for users and roles can now be specified on a per-zone basis.

Data at Rest

The data at rest enhancements focus on extending the use of cryptography and improving its performance. Both **ZFS** and **LOFI Block Devices** now allow **encryption**.

To greatly increase ZFS security, individual ZFS datasets can now opt in to be encrypted when they are created. ZFS volumes (ZVOLs) and filesystems can be encrypted, including ZVOLs that are used for swap and dump. Users can be delegated the ability to load and/or change their key encrypting keys (wrapping keys). Users can change their wrapping key at any time and can also request that from the current point of time onwards a new data encryption key be used for any new data.

Creating an encrypted filesystem can be as simple as issuing the command 'zfs create -o encryption=on tank/myproject'. In this simple example, the user is prompted for a passphrase from which the wrapping key is derived. Alternatively, a user might choose to store the wrapping key in a file. The file could be stored on removable media.

Equally, the lofiadm(1M) command and the lofi(7D) driver that allow a file to be presented as a block device, now provide the ability to encrypt all the blocks written to the backing file.

To help with the complex task of managing keys, the **Oracle Key Management System** can now be used for AES key storage by using the new 'pkcs11_kms' plugin for the Oracle Solaris Cryptographic Framework. This mechanism can be used by any PKCS#11-aware application.

For **Cryptographic Performance of the Database**, the SPARC T3 processor now supports the AES CFB mode. This mode is used by the tablespace encryption feature of the Oracle Database Advanced Security Option. It is closely related to the ability of the Oracle Solaris Cryptographic Framework to provide acceleration through on-board cryptographic mechanisms on both SPARC and Intel chips.

To meet more stringent government standards the **Oracle Solaris Cryptographic Framework** now supports **the NSA Suite B algorithms**. AES in CCM/GCM modes are used by IPsec and ZFS. IKE can now also use Elliptic Curve Cryptography (ECC) in addition to RSA and DSA for key exchange.

Trusted Extensions

Trusted Extensions was introduced in Oracle Solaris 10 as a special configuration of Oracle Solaris to enable a multilevel security environment. This security is enforced through mandatory access controls, that is, labels. In Oracle Solaris 11 Express, Trusted Extensions bases its desktop and windowing system on GNOME and Xorg X11. The **gnome-based multilevel login manager** (gdm), providing an accessible multilevel desktop for Trusted Extensions systems. The use of **XACE extension hooks** to implement the Trusted Extensions policy enables Trusted Extensions to more easily stay in sync with new releases of Xorg X11.

To enable greater flexibility and security Trusted Extensions now enables per-label and per-user credentials. This feature enables the administrator to require a unique password for each label. This password is in addition to the session login password, so enables the administrator to set a per-zone encryption key for each label of every user's home directory.

Trusted Extensions has been enhanced to explicitly set **Security Labels on ZFS datasets**. When Trusted Extensions labeling is configured, ZFS filesystems are now automatically labeled with the new 'mlslabel' feature. This feature ensures that ZFS filesystems for a specific security label cannot be mounted on a zone of a different label, and thus inadvertently upgrade or downgrade the data.

Finally, when labeled processes in a multilevel secure operating system, such as Oracle Solaris' Trusted Extensions, communicate across system boundaries, their network traffic needs to be labeled and protected. Traditionally, this requirement is met by using physically separate network infrastructures to ensure that data belonging to different labeled domains stays in separate physical infrastructures. The new feature of Labeled IPsec/IKE enables customers to reuse the same physical network infrastructure for labeled communications by transferring labeled data within separate labeled IPsec security associations, removing the need for redundant and expensive physical network infrastructures.