

Oracle Software Security Assurance

*An Oracle White Paper
January 2007*

Oracle Software Security Assurance

INTRODUCTION

Criticality of Security for Products and Processes

Security is of paramount concern to Information Technology organizations today. Protecting against computer criminals, limiting the “insider threat,” and ensuring compliance with privacy, data breach, and financial accountability laws are now top priorities for IT executives. Security features such as access control, user authentication, data encryption, and audit support have therefore become important software buying criteria. Survey after survey shows that security is the number one priority where new IT investment is planned¹.

Although the security features of software are important, the security assurance of software is just as important to overall system security. Security assurance depends on secure system design, development, and support processes that prevent the introduction of security flaws into systems as well as limit damage from them if they do occur. Security flaws are design or implementation errors in software that allow a user to gain unauthorized access to data or system resources, or damage the system on which that software is installed. Knowledgeable users with malicious intent (e.g. “hackers”) who are aware of security flaws in a system may exploit them to gain privileged access to that system, bypassing what would otherwise be effective security mechanisms within the system. In order for a software product to be secure, it must not only provide effective and robust security features, but also must avoid security flaws. Oracle’s product development and maintenance process includes a comprehensive set of security assurance mechanisms and processes that improve the strength of our security mechanisms and reduce the likelihood of security flaws in our products. Collectively these assurance mechanisms and processes are known as Oracle Software Security Assurance.

A Heritage of Security

As Oracle’s product suite has grown in the more than twenty-five years as a leading provider of enterprise information management software, its commitment to security has remained constant. Oracle’s first customers included security-aware government organizations. Oracle worked with the Central Intelligence

¹ Goldman Sachs, Independent Insight, US Technology Strategy IT Spending Survey, January 12, 2006

Agency (CIA) to design and implement their first relational database management system, which managed and protected highly classified information. Ever since, customers have relied on Oracle to protect their sensitive, mission-critical data. Unlike software that evolved from standalone desktop systems, where access to the software was assumed to be limited to the single user who had physical access to the computer at any one time, Oracle products were designed to support complex, multi-user deployments from the start. Protecting sensitive information against unauthorized user access in these environments has always been a key feature of Oracle's products.

Oracle Software Security Assurance Overview

A key element to Oracle Software Security Assurance is Oracle's lifecycle approach to securing its products corresponding to the various phases of the life of a product: from design and development throughout release. In the product definition phase, Oracle Software Security Assurance activities include product planning and developer training activities to improve knowledge of customer requirements and secure coding practices as well as awareness of security concerns. The product development phase is the one in which most of Oracle Software Security Assurance activities are focused. Oracle Software Security Assurance activities also extend to the ongoing maintenance of products after they have been released to customers. The following sections provide an overview of each of these process phases, and of the major process components in each.

More information about Oracle Software Security Assurance can be found online at <http://www.oracle.com/security/software-security-assurance.html>

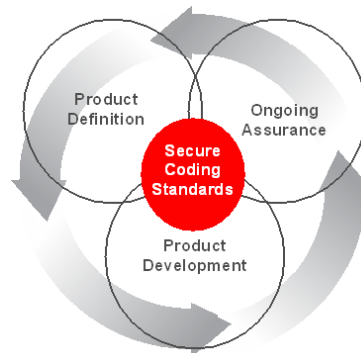


Figure 1: Oracle Software Security Assurance model

SECURITY ACTIVITIES IN THE PRODUCT DEFINITION PHASE

The Product Definition Phase lays the groundwork for building secure products. It includes those activities that focus on Oracle's product security requirements, but also those that ensure that Oracle maintains deep security expertise, infrastructure, and resources within its development organization. These ensure that Oracle developers are security aware, that security standards exist and are documented, that security tools and software libraries are available, and that

Oracle's security technology and processes are coordinated and customer-focused.

Importance Of Formal Secure Coding Standards

To ensure that Oracle products are developed with consistently high security assurance, and that developers avoid common insecure coding practices, Oracle employs formal secure coding standards. All Oracle developers must be familiar with these standards, and apply them when designing and building products. The coding standards have been developed over a number of years and incorporate best practices as well as lessons learned from continued vulnerability testing by Oracle's internal product assessment team. Oracle ensures that developers are familiar with its coding standards by requiring that they undergo secure coding training. Compliance with secure coding standards is enforced through a number of mechanisms, but principally through the secure release process described later in this document. The Secure Coding Standards are a key component of Oracle Software Security Assurance. Adherence to the Standards is assessed and validated throughout the useful life of all Oracle's products.

Secure Coding Training

Over the years, Oracle has internally developed training based on the Secure Coding Standards. Oracle delivers this training to its product development organization, including developers as well as product management, release management and quality assurance staff, on a continuous basis. Training is not limited to individual contributors; managers up to and including senior vice presidents are required to take the training classes. This ongoing education ensures that developers are familiar with all aspects of the secure coding standards, and understand the types of problems they must avoid and their potential consequences.

Common Security Functionality, Built by Experts

Oracle consolidates development of critical security functionality into core modules and services that are used by multiple development teams. This ensures that tested and proven security functionality is common across Oracle products. This also ensures that different development teams do not attempt to re-invent solutions or, more importantly, create new cryptographic libraries, user repositories, or authentication schemes that have not been extensively tested or reviewed. Since security functionality involves a number of complex, highly technical, and specialized disciplines, errors in design or implementation can have serious consequences.

Oracle maintains a core set of security functions and libraries that are designed and developed by experts. Many of these libraries are subjected to third party testing and independent certification. An example of this is Oracle's SSL libraries, which have been successfully evaluated against the US government's FIPS 140-2 cryptographic standard.

The secure development processes begin long before Oracle developers start building products. Oracle actively maintains a set of secure coding standards, as well as sets of libraries for security functions such as authentication and cryptography.

Technology Coordination

Oracle maintains a Security Steering Committee with representatives from its development teams across the company, as well as from its field organization. Members review and coordinate product security technology, helping to “cross-pollinate” security technology across divisions, and ensure all organizations are aware of and adopt common security architectures and technologies. This committee is overseen by Oracle’s Global Product Security organization. The Global Product Security group is a centralized security team with the mandate to supervise the various Oracle Software Security Assurance activities across Oracle. The Global Product Security organization is lead by Oracle’s Chief Security Officer.

Customer Focus and Feedback

Oracle additionally maintains a security Customer Advisory Council to solicit customer feedback and guidance on matters relating to the security of its products. While the focus is primarily on security feature and functional requirements, the council also looks at security processes, such as Oracle’s Critical Patch Update (CPU) and Security Alert processes. More than 20 organizations currently participate in the security CAC. These include representatives from diverse sectors including banking, manufacturing, pharmaceuticals, government, and education, and from the Americas, Europe, and Asia. Customers for every product family within Oracle are members of the security Customer Advisory Council. Having multiple product families represented provides synergy since security issues often span multiple product families. Customer feedback on the security of one product can oftentimes benefit other Oracle products.

SECURITY ACTIVITIES IN THE PRODUCT DEVELOPMENT PHASE

Oracle Software Security Assurance requires that security be incorporated into the multiple phases of the development process, including functional specification, design, implementation, and testing.

Design Review and Guidance

Oracle Software Security Assurance mandates that security be specified in all product design documents. Oracle’s standard design specification templates include sections for security, which must be completed before specifications are approved. Oracle Global Product Security maintains a core team of experts who provide review and guidance during product design and development phases. This team provides design assistance to development teams to ensure that they comply with Oracle’s Secure Coding Standards.

Secure Configuration Program

When customers transition software systems from development and testing to production environments, they typically subject them to a process known as “hardening.” The objective of hardening is to reduce the vulnerability of a

production system to attack. This generally involves securing the underlying networks and platforms, restricting user privileges, removing unneeded functionality, and closing off nonessential modes of access to the system, such as unused default user accounts or network ports.

Oracle's Secure Configuration Program is focused on ensuring that products provide an optimal security posture out of the box, with little or no effort required by customers to further "harden" these products. As part of this program, Oracle develops guidelines for secure product configuration, and works with its product development teams to implement these enhancements in new versions of its products. These guidelines are, in part, based on the standard security benchmarks developed by third party organizations, in particular the Center for Internet Security (CIS), of which Oracle is an active participant. Default configurations for improved security must be phased in over time in order to ease the impact on customers and partners who have built applications, or have established security policies and practices, based on earlier defaults. Oracle began to phase in new security default configurations with the release of its database version Oracle 10g.

While secure configuration defaults are phased in, Oracle has developed security best practices guides for its customers on prior product versions. These guides are available as part of Oracle's standard documentation set and provide guidelines to lock down product installations. In addition, Oracle has developed a number of tools to assist its customers in identifying specific areas in which their product implementations do not comply with best practice recommendations (for example, the continued use of default passwords for default accounts). When appropriate, such tools are made available with Critical Patch Update (CPU) releases and via Oracle's website, in particular the Security Technology Center on Oracle Technology Network web site at <http://www.oracle.com/technology/deploy/security/index.html>.

Oracle's system management tools also provide capabilities to monitor and report on the security aspects of a system configuration. System management tool capabilities are further detailed later in the Ongoing Assurance section of this paper.

Secure Development Tools

Oracle's secure development tools include both security-oriented regression testing as part of Oracle's overall Quality Assurance process, and testing via specialized security vulnerability analysis tools in the development phase of products.

Security Regression Testing

Oracle incorporates multiple security tests into its development processes. For each product Oracle offers there is an extensive suite of regression tests to exercise product functionality, including security features and functions. Security

tests are included in daily testing that Oracle performs during its product development process. Oracle runs the full set of regressions for product releases and patch sets, and partial regressions on CPU's. Oracle is further enhancing this testing process through the development of a suite of destructive regression tests for testing product ship homes. This means that Oracle is building a library of exploits that run against product ship homes that approximate customers' installed environments to validate that CPU's, once installed, ensure the underlying security vulnerability is patched. This testing is in addition to the unit testing that Oracle performs to ensure that a security patch addresses the base vulnerability.

Automated security vulnerability analysis tools

In addition to regression testing, Oracle uses automated tools to search for security vulnerabilities in its software. These are a combination of Oracle's own in-house tools specifically developed for this purpose as well as third party licensed tools. These tools enable Oracle to find and fix vulnerabilities prior to releasing products to its customers.

Product Assessments

Another important mechanism Oracle implements to find security vulnerabilities is its product assessment process, informally known as "ethical hacking." In product assessment, a team attempts to break ("hack") the security mechanisms in Oracle products, or find and exploit product defects that could allow a user to bypass security mechanisms. Oracle relies on both internal and external teams to do product assessments on Oracle products prior to their release.

Internal Product Assessment

Oracle has an internal product assessment team whose job it is to find vulnerabilities in Oracle products. The team also looks for vulnerabilities in production installations of Oracle products deployed within Oracle's IT infrastructure. Not only does this process improve product quality, it also betters Oracle's secure coding standards and security training program. Product assessments have identified new classes of vulnerabilities that have then been added to the secure coding standards and secure coding training. The product assessment team works closely with development teams whose products they have "hacked" to ensure that the teams understand how to avoid such vulnerabilities in their future development.

Oracle handles product vulnerability information with extreme sensitivity, to protect Oracle and its customers. Oracle therefore insists that its product assessment team members meet high ethical and reliability standards. All product assessment team members undergo extensive independent background checks and most have government security clearances.

External Product Assessment

In addition to maintaining an internal product assessment team, Oracle also contracts with outside security assessment firms. Oracle does this to augment its internal assessment resources, and to add another level of independent product security review and testing. Oracle selects outside assessment firms not only for their technical expertise, but also for reliability and discretion, so that Oracle is confident that they will not reveal vulnerabilities they find before Oracle has had an opportunity to correct those vulnerabilities. Revealing such information would put Oracle customers at risk.

Security Release Criteria

Oracle's development process provides for security exit criteria or "security checklists" for every component included in a shipping product. Security checklists give the product release management team another opportunity to re-validate that a product adheres to Oracle's secure coding standard requirements. The security checklists require developers to validate that their code follows certain security practices. Examples of checklist items include: the code does not contain over-privileged (default) permissions, no passwords are hard-coded, and only Oracle-approved encryption routines are implemented. The Global Product Security team reviews all security checklists before products are released. If security concerns are uncovered, the team investigates these concerns directly with the product development team. The product release process will be stopped and the product will not go production until security concerns are resolved. Security checklists have proven successful to find and fix security issues as well as instill the criticality of security in Oracle's development community.

Security checklists were developed in conjunction with the secure coding standards and security training curriculum. Checklists continue to evolve as Oracle's ever-growing knowledge of secure, as well as potentially insecure, coding practices evolves. Formal secure coding standards, and mandatory security training, ensure that the development process is initiated with security in mind. Checklists verify at the end of this process that these same standards have been adhered to.

In 1994, Oracle was the first vendor to complete ITSEC and TCSEC security evaluations.

With over twenty independent security evaluations for its products, Oracle is the undisputed leader in independent security evaluations.

Formal Security Evaluations

Oracle is recognized as an industry leader in the area of information assurance, as attested by numerous formal security evaluations against standards such as the International Common Criteria (CC) (ISO-15408), and the US Federal Information Processing Standard (FIPS-140). It is via independent, third-party security evaluations that users of commercial software offerings can have confidence in the security claims of a vendor. These security evaluations test for compliance with formally established criteria for security functionality and assurance. In addition to security functionality, evaluations also examine and validate a vendor's development processes. For example, evaluations at higher assurance levels, such as EAL4 at which Oracle evaluates most its products,

require that evaluators assess the security of a vendor's development environment. Successful evaluation at these levels requires that the vendor have an ongoing, documented record of secure development practices; Oracle provides such documentation when undertaking product evaluations. Oracle leads the industry in security software evaluations, with more than 20 successful evaluations for its products. For a complete list of Oracle security evaluations, please visit the Oracle Software Security Assurance web site at

<http://www.oracle.com/security/external-security-evaluations.html>

Security evaluations are a critical proof of the security worthiness of a software product. As an example, the United States government requires (NSTISSP #11) that software products used for national security applications are subjected to formal evaluation prior to their use. In addition to providing independent validation that a product adheres to internationally recognized, formally defined standards for security functionality and assurance, security evaluations also demonstrate ongoing commitment to security on the part of the vendor. Security evaluations are time consuming and expensive. Oracle's security evaluations represent an investment of more than \$19 million in independent security vetting, exclusive of the development work to build market-leading secure products.

SECURITY ASSURANCE IN THE ONGOING ASSURANCE PHASE

A number of Oracle Software Security Assurance activities are designed to ensure that Oracle products remain as secure as possible after they have been released to customers.

Security Vulnerability Handling

Oracle has extensive processes in place to identify, track, fix, and backport fixes for security vulnerabilities. Information on security vulnerabilities is managed and strictly limited on a "need to know" basis so that only those who are diagnosing or remedying a vulnerability can view security vulnerability details. This protects all of Oracle's customers. Oracle tracks and manages all significant security issues, regardless of whether they are found internally or externally, and handles issues in order of severity regardless of who uncovered the vulnerability. In fact, Oracle uncovers fully 75% of significant vulnerabilities in house. As Oracle continues to improve its development processes, including the incorporation of automated vulnerability assessment tools, this number continues an upward trend.

Security issues are fixed as follows: (1) in the main code line first, and then (2) in the next patch set. This ensures that the next product "train leaving the station" always contains fixes for critical security issues. This protects customers and lowers their security cost-of-ownership. Accordingly, customers on the most recent versions of Oracle products are on the most secure software versions available. Finally Oracle queues up security vulnerability fixes, in severity order, for backporting to older releases via its CPU program. This waterfall model for

In October 2006, Oracle was the first major software vendor to use the Common Vulnerability Scoring System (CVSS) to report the criticality of security flaws in its products. CVSS is a standardized method for assessing security vulnerabilities. For more information about CVSS, please visit FIRST's CVSS web site at: <http://www.first.org/cvss/>

security vulnerability handling fixes issues as quickly as possible, while maximizing quality and minimizing cost of applying needed security fixes.

Information about Oracle's Critical Patch Updates and Security Alerts can be found online at:

<http://www.oracle.com/technology/patch/updates/alerts.htm>

Vulnerability Remediation Through The Critical Patch Updates (CPUs)

Oracle releases information (and patches) for security issues through quarterly, bundled, integrated Critical Patch Updates. CPU's include fixes for the critical security issues, as well as for other issues needed to avoid patch conflict, or which are prerequisites for security fixes. The dates for release of CPU's are announced one year in advance and are selected based on most customers' financial calendars, so as to avoid "blackout dates" during which customers will generally not update or modify their financial or other critical systems. CPU's are cumulative for the Oracle Database, Oracle Application Server, Oracle Enterprise Manager Grid Control, Oracle Collaboration Suite, JD Edwards EnterpriseOne and OneWorld Tools, and PeopleSoft Enterprise Portal Applications. This means customers have the option to skip patches, but receive all prior updates issued through the next CPU. For example, if a customer elects to skip the January 2006 CPU and apply only the April 2006 CPU, he will still obtain the fixes released in both the April 2006 and January 2006 CPU's. CPU's for Oracle eBusiness Suite are currently not cumulative.

While Oracle has invested extensively in the Critical Patch Update process, it recognizes the need to constantly improve and ease this process for its customers. Oracle is particularly focused on improving CPU quality and patch automation so that customers will have faster time-to-patch and thereby lower their overall patching costs. Recent improvements now test for a rolling upgradeable capability so that customers using Real Applications Clusters (RAC) do not have to take their systems down in order to patch them.

Sharing Security Best Practices

Oracle maintains security best practices documents for all of its major product lines, including its Database, Application Server, Applications, and Collaboration Suite. Best practices documents provide guidelines and recommendations for configuring and deploying products to make them more secure in real-world customer environments. Best practices documents are living documents; they are updated as products evolve, as Oracle learns new information from customers on actual use case scenarios for new product features or technology, and when any new security problems associated with a specific product configuration or deployment are identified. The Resource Library page on the Oracle Software Security Assurance web site located on <http://www.oracle.com/security/resource-library.html> provides the relevant links to access Oracle's various security best practices documents.

Security Configuration Management and Validation Tools

Oracle's family of system management products, Oracle Enterprise Manager Grid Control, includes features that can assist customers in assessing and managing the security of their Oracle systems. In particular, they provide tools to monitor and report on configurations that do not adhere to security best practices. They allow customers to define policies about system security configuration for systems in their enterprise, and report on the extent to which systems comply with those policies. These policies can be built from a repository of over 200 product-specific configuration security issues. They can also be based on whether systems have installed specific security patches or the most recent CPU. Policy violations can be set to trigger notifications to system security administrators, so that they can quickly react to systems that are not in compliance with policy.

In addition to generating customizable security reports and flagging specific events, these products provide an overall security dashboard so that security administrators can view security-related configuration information in summary form, with historical trend information. These tools enable customers to readily and quickly gauge their security posture, and in particular determine whether their systems are locked down and patched appropriately.

Product Security Communications

The CPU documentation is the primary means by which Oracle communicates security vulnerability and patch information to its customers. Oracle uses this process to address security vulnerabilities that require it to issue a security patch. Oracle carefully manages the release of security patches, and of information associated with security vulnerabilities requiring patches, to protect as many customers as possible. By publicly sharing vulnerability information when patches are not yet available, Oracle potentially could put its customers at risk from those seeking to exploit such vulnerabilities.

Although Oracle's policy is to limit information about product security vulnerabilities that require Oracle patching until appropriate patches are ready, this policy does not apply when vulnerabilities do not require a patch. In particular, Oracle proactively notifies customers of security problems arising from product configuration or deployment issues when such problems place customers at risk. These notifications may also contain workarounds for those problems if they are proven to not result in additional problems, such as interfering with the functionality of customers' applications.

CONCLUSION

Oracle Software Security Assurance comprises all the processes, procedures, and technologies that have been implemented to ensure that Oracle's products are meeting our customers' security requirements, while providing for the most cost-effective ownership experience. An extensive and constantly evolving program, Oracle Software Security Assurance reflects the dynamic nature of IT security,

In order to provide the maximum level of protection for all its customers, Oracle will not provide additional information about the specifics of vulnerabilities beyond what is provided in the CPU or Security Alert notification, the pre-installation notes, the readme files, and FAQs.

This information is also available online on the Critical Patch Updates and Security Alerts page at <http://www.oracle.com/technology/deploy/security/alerts.htm>

and aims to ensure that all Oracle's products are as secure as the company can build them throughout all stages of the software lifecycle: initial design, in development, and following release to customers. Oracle's products have included security mechanisms as core product capabilities for decades. Oracle continues to refine its products to include new security technology and capabilities, make existing product security easier to use, eliminate product vulnerabilities, and ensure products install securely. Oracle Software Security Assurance has evolved over the company's history and will continue to evolve as the company identifies changing customers' requirements, new technology and processes to prevent security vulnerabilities in its products, improve the strength of its security mechanisms, and provide ongoing protection to its customers.

FOR MORE INFORMATION

The Oracle Software Security Assurance web site is located at <http://www.oracle.com/security/software-security-assurance.html>

Read Oracle Security documentation and view best practices guides at:

<http://www.oracle.com/technology/deploy/security/index.html>

See the CPU issuance calendar and learn more about Oracle CPU's at

<http://www.oracle.com/technology/deploy/security/alerts.htm>

Learn more about Oracle's security products and capabilities at

<http://www.oracle.com/security>



Oracle Software Security Assurance

January 2007

Author: John Heimann

Contributing Authors: Mary Ann Davidson, Wynn White, Eric Maurice

Oracle Corporation

World Headquarters

500 Oracle Parkway

Redwood Shores, CA 94065

U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Fax: +1.650.506.7200

oracle.com

Copyright © 2006, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle, JD Edwards, and PeopleSoft, are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners