ORACLE®

From EasySQL to CPUs:

Oracle's Journey Through Software Security Assurance

Duncan Harris
Senior Director, Security Assurance

12 July 2012

Agenda

- From EasySQL…
  - Oracle's first vulnerability
- Oracle Software Security Assurance
- …To CPUs
  - Oracle's quarterly security patch program
- Decentralised security model
- Assessing maturity of secure development practices

From Easy SQL… 1994

Oracle's first published vulnerability

- ALTER SESSION SET CURRENT_SCHEMA = 'schema-name'
  - Shortcut to avoid need for full name qualification, like *nix cd
- Undocumented command in Oracle7 (7.0)
- Vulnerability
  - Point to SYS (root) schema, in effect get SYS privileges for some commands, enough for full control of database
- EasySQL (EZ SQL), later EZSQL1
  - All versions, all platforms
  - No workaround
  - No mitigation – can't uninstall it, can't switch of its use, can't control with a privilege, can't audit it

1994 - 2004

Moving towards formal security advisories

- 1994
  - Response to EZSQL1 – issue tapes and CDs to all customers
- 1997
  - EZSQL2 – same expense, but patch also downloadable
- 2000
  - 1 vulnerability (777 permissions on database install file)
- 2001
  - 15 vulnerabilities, started numbering advisories
- 2002
  - 31, including EZSQL3
- 2004
  - Security Alert 68, single bundle of 28 vulnerability fixes including EZSQL4

Further back in time…

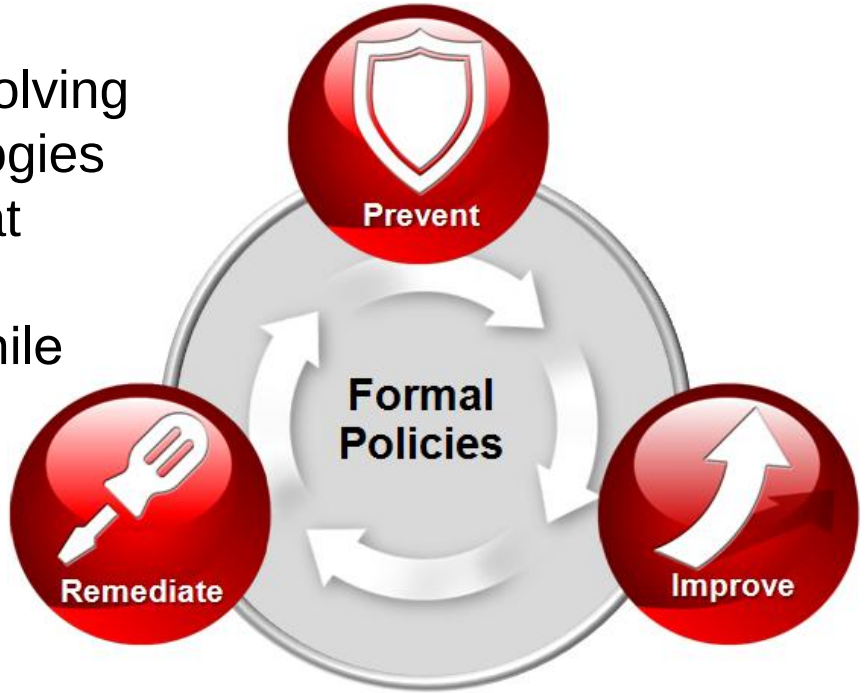
1994 was not the start!

- Oracle's history in security is much longer
  - CIA was first customer
  - Strong culture of state-of-the-art security functions, IP protection
- Security features/functions vs. Security vulnerabilities
- Independent review of culture (and product)
  - TCSEC ("Orange Book"), ITSEC, now replaced by Common Criteria (ISO 15408)
  - Focus on assurance that security functions are correctly implemented in a secure development environment
- Current concerns re. Supply Chain Integrity/Assurance

Oracle Software Security Assurance

Definition

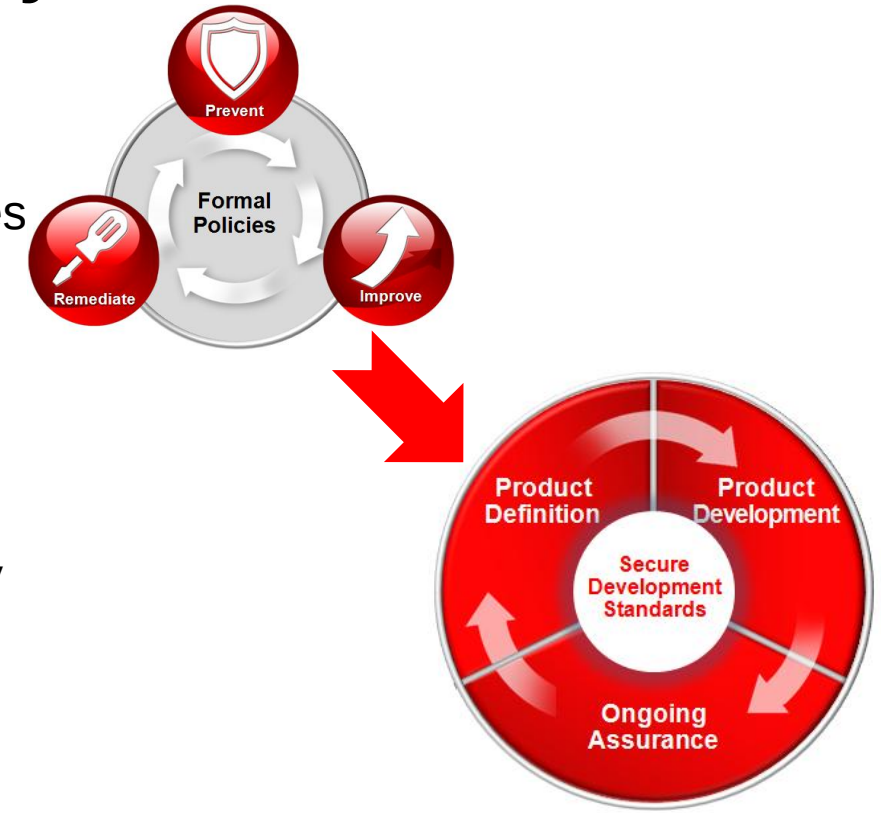
Oracle Software Security Assurance (OSSA) encompasses constantly-evolving processes, procedures, and technologies implemented by Oracle to ensure that Oracle's products are meeting our customers' security requirements, while providing for the most cost-effective ownership experience.



Oracle Software Security Assurance

Highlights

- Maintaining the security posture of all customers is one of our greatest priorities
  - Policies are greatly influenced by Security Customer Advisory Council
- Applies to all Oracle software products, including software components of hardware products (e.g. firmware), throughout their lifecycle, and constantly evolving to adapt to new technologies, threats, and product use cases



Oracle Software Security Assurance

- Major programs include:
  - Secure Development Standards
  - Security Design
  - Security Tools and Testing
  - Security Compliance
  - Internal Security Assessments
    - Ethical Hacking Team
  - External Security Assessments
    - Common Criteria, FIPS 140
  - Critical Patch Updates & Security Alerts
- OSSA affects the entire product lifecycle

Secure Development Standards

Directives for developers

- Secure Development Standards
  - Design level requirements, e.g.
    - Old, weak crypto is banned
    - No password parameters on command line
- Secure Coding Standards
  - Compliments C and Java coding standards
  - Revised frequently to address new attack methods
  - Uses Oracle “true stories” as examples
- Security Coding Practices Training
  - Mandatory for all staff in a development organisation, including product and release managers, QA, up to SVP

Secure Design

Processes for developers

- Development processes include security requirements through all phases:
  - Functional specs (architectural / high level)
  - Design specs (module / low level)
  - Test specs
- Core, vetted security modules facilitate stronger security
  - Crypto libraries (including database encryption)
  - Identity management (SSO, provisioning, etc.)
  - OWASP AntiSamy, ESAPI
  - “Build security once, use many” means developers are not “rolling their own” core security

Security Testing

Thorough testing regime

- Security testing - proactive
  - Regression tests for security modules exercises security features/functions
  - We run full regress for releases and patch sets
- Security testing - destructive
  - In-house tools (e.g., for SQL injection, buffer overflows, intelligent protocol fuzzers)
  - Regression tests for product vulnerabilities
  - 3rd party tools
    - Static source code analysis tools, e.g. Fortify, Parfait
    - Application vulnerability scanners, e.g. WebInspect

Security Compliance

Trust but verify…

- Product security acquisition checklists
  - Newly acquired products get health check, and often a rude awakening!
- Security release checklists
  - All product components validated against secure development and coding standards
  - Exceptions are tracked, resolved and deal-breakers stop releases
- Ethical Hacking Team
  - Focus is on new and critical technologies
  - Feedback loop of discoveries into Secure Coding Standards and training
  - Augmented by use of external security consulting firms

Security Evaluations

Independent 3rd Party Product Testing

- Third party product security evaluation against standards of ‘what you mean when you say you are secure’ (i.e., confirm that ‘it does what it says on the tin’)
- Evaluations check specific security functionality and the development processes used to build them
- Core evaluations standards
  - International Common Criteria (ISO/IEC 15408)
  - US/Canadian Federal Information Processing Standard 140-2
- 74 evaluation certificates to dates
  - Database has 21 evaluations, Solaris has 8, many other products

…To CPUs

2005 onwards

- Formal security vulnerability handling
  - Security patching is most public evidence of ongoing assurance
    - Vulnerabilities uncovered during ongoing assurance effort (internally discovered, ~87%)
    - Vulnerabilities resulting from new attack methods on customers or unusual use case scenario by our customers (~10%)
    - Vulnerabilities reported by external security researchers (~3%)
  - Critical Patch Updates (CPUs) are designed to protect all Oracle customers equally at lowest possible cost

Oracle Vulnerability Handling Practice

Critical Patch Updates and Security Alerts

- Predictable
  - Schedule announced one year ahead of time
  - Quarterly patches outside of typical blackout dates (end of fiscal year, end of quarter, etc.)
- Cumulative
  - Patch updates are cumulative for most Oracle products in order to easily allow customers to reach current release level even if previous patch applications were skipped
- Vulnerabilities fixed in severity order
  - CVSS v2, extended to give Partial+ impacts
- One-off Security Alerts for emergencies

Oracle Vulnerability Handling Practice

Lifecycle of a vulnerability

- Regardless of reporting source
  - Oracle SecAlert tracks and manages
- Details access controlled in bug database, even when fixed
- Fix order
  - In future major releases (main line)
  - In future patch sets (forward port)
  - In currently supported customer patch sets (back port)
  - On all currently supported OSs (platform port)
- Tested across entire stack
- Only announced when all customers can protect themselves

Oracle Vulnerability Publications

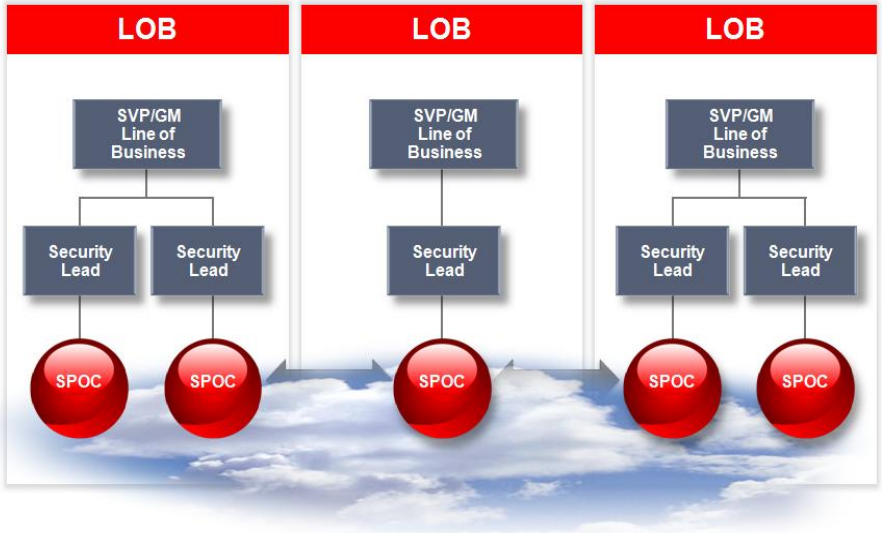
Don’t believe everything you read…

- The only authoritative source of information on Oracle vulnerabilities is Oracle’s own Critical Patch Update or Security Alert Advisories (and accompanying documentation)
- Virtually all third-party bulletins about vulnerabilities in Oracle products have significant errors:
  - Inaccurate information about conditions or impacts
  - Remedies/workarounds do not work and/or cause significant regressions
  - Alleged issues may not even be vulnerabilities
- Common Vulnerability Reporting Format (CVRF)

Delegated Security Model

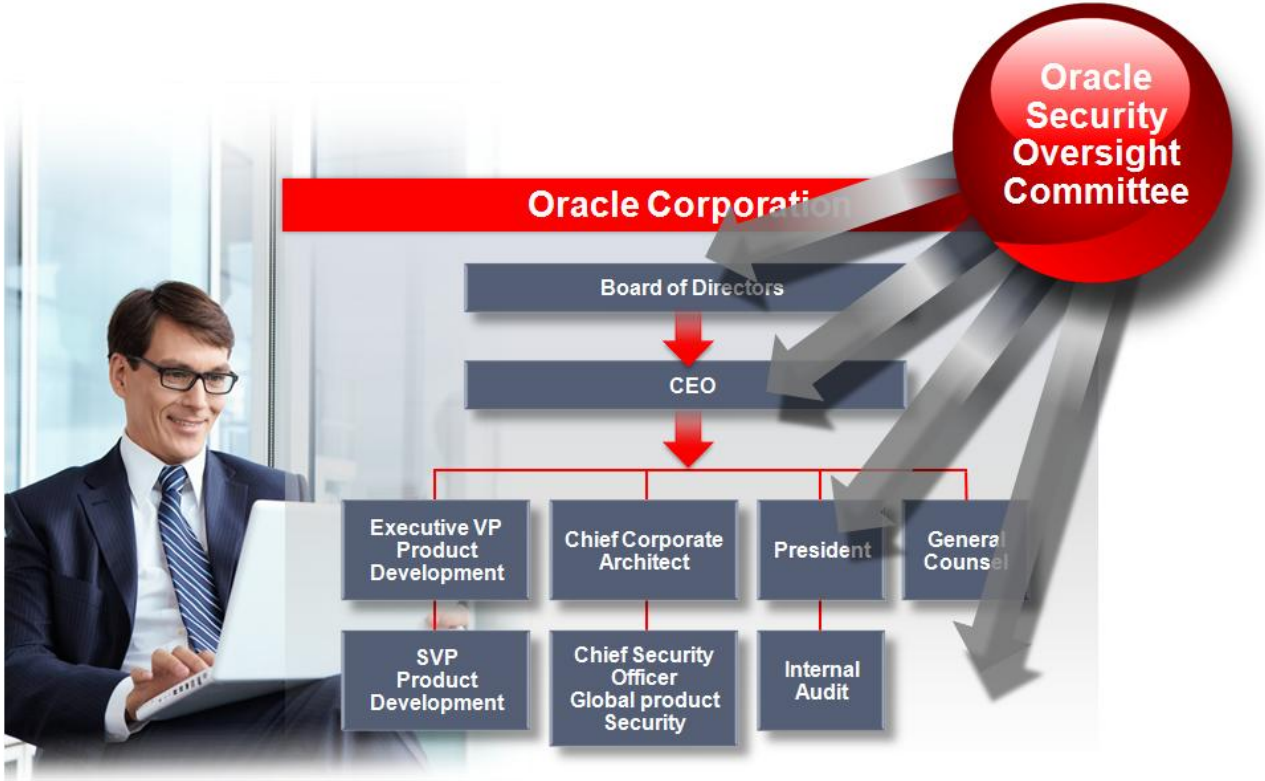
Decentralised security

- Global Product Security (GPS) leads a virtual community of Security Point of Contacts (SPOCs)
- Security Lead per product suite
  - Builds culture of security
  - Advocate for OSSA
  - Leads a virtual team of SPOCs



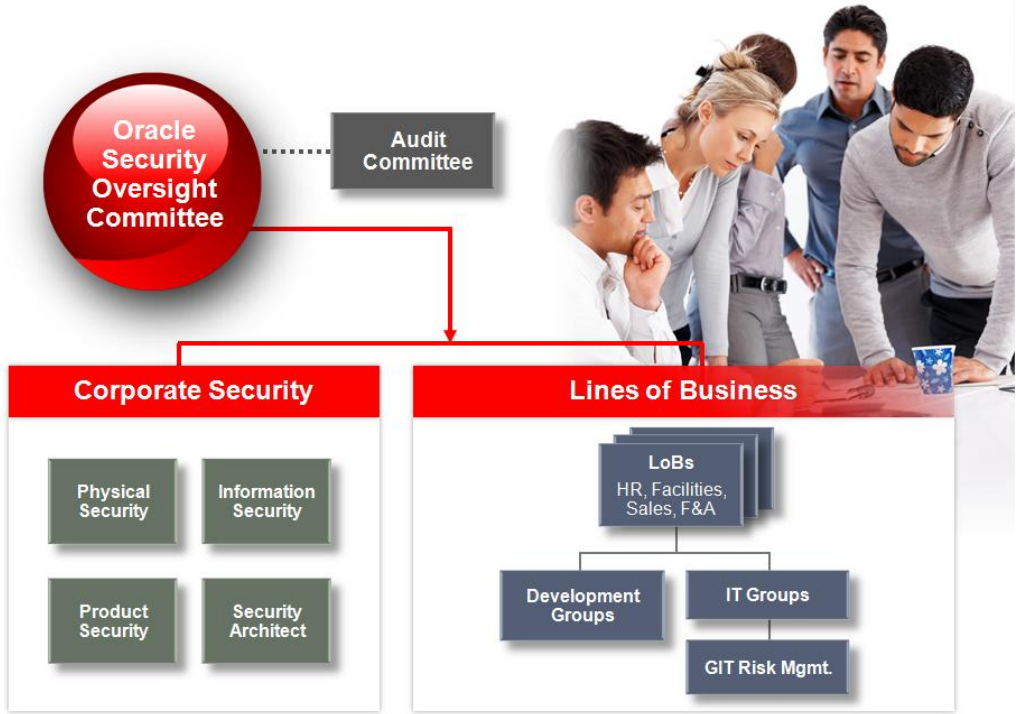
- SPOCs act as the tactical security resource for individual products
  - In-depth knowledge of product leads to building security in at the lowest level
  - Receive focused training in OSSA
  - Key role throughout the product lifecycle: participate in design reviews, document reviews, code reviews, bug triage, patching, etc.

Executive Security Oversight At Oracle



Accountability Model

- Security is a corporate governance issue.
- Senior executives ensure that every line of business adheres to Oracle's security practices
  - including Global Product Security's OSSA



Complete Developer Security Practices

Assurance is more than vulnerability avoidance

- Assessing your own security assurance practices
  - Maturity of secure development practices, BSIMM
  - Vulnerability handling, disclosure, and fixing policies
  - Independent security assessment (external security certifications)
  - Pen-testing or code scanning a product prior to use is of limited value, doesn't tell you if developer has culture of security
- Encourage end users to
  - Apply security patches in a timely manner
  - Keep current on releases, ongoing upgrade schedule
  - Make use of security documentation, lockdown guides

Assess Security Assurance Maturity

OWASP projects help

- External or third party testing after products are developed, while useful, is no substitute for good practices in development and for a well established culture of security within the development environment
- Use of and contribution to OWASP projects demonstrates both!

For More Information

- Oracle Software Security Assurance
  at http://www.oracle.com/us/support/assurance
  - Technical white papers and security guides
  - Online security seminars and webcasts
  - Defending against SQL Injection Attacks
    at http://st-curriculum.oracle.com/tutorial/SQLInjection/index.htm
  - Blog (http://blogs.oracle.com/security)
- Critical Patch Update & Security Alerts
  at http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Hardware and Software

ORACLE

Engineered to Work Together


ORACLE®