The Case for Information Assurance

Mary Ann Davidson
Chief Security Officer
Oracle
“A few lines of code can wreak more havoc than a bomb.”

- Tom Ridge
(Former) Secretary of the U.S. Department of Homeland Security
Agenda

• State of Information Security
• Problem Encapsulation
• Is There a Market Failure in IT Security?
• Hopeful Signs in Information Assurance
• Why Secure Coding Matters
• Oracle Software Security Assurance Program
• Some Wild Eyed Ideas…
• Q and A
State of Information Security
“The Long Knives Are Out”

- The cost of poor security in the US alone is between $22.2B and $59.5 billion per year (NIST)
  - Cost per patch applied: $900 per server, $700 per client (Economist)
- Tipping point: the poor security of commercial software is a board level issue
  - Business Roundtable blames defective, easily exploitable software for increase in cyber incidents
- ...and a US national security issue
  - Multiple US government-led initiatives on information software assurance,
- Many CSOs think the IT industry should be regulated
What If Civil Engineers Built Bridges Like Developers Write Code?

• “Structural integrity is a legacy problem. It’s not really interesting. Or elegant.”
• “We can add some rebar later, so what if the concrete has set?”
• “The bridge has crumbled? Sorry, I can’t reproduce that problem here.”
• “But it wasn’t designed to have so many trucks on it.”

IT means “infrastructure technology”: it has to be designed and built to be as reliable and secure as physical infrastructure.
Is Poor IT Security Is a Market Failure?

• Customers
  – Have insufficient information to *caveat emptor*
  – Think “cost to secure” is the *license* cost
  – Have no idea if there is a security ROI
  – Are well trained by vendors to patch, patch, patch

• Vendors
  – Still driven by time to market, since “it works”
  – Often lack tools / will to do a better job in security
  – Can’t tell customers how to secure their products and what it costs to do so
Is Poor IT Security Is a Market Failure? (2)

• Venture Capitalists
  – Make more money on band-aids than vaccines
  – Often don’t want to solve the real problem

• Universities
  – Don’t have standard CS curricula that include secure programming practice
  – Are reluctant to change their curriculum (with some notable exceptions…)
  – Graduate good coders, not software engineers
What Isn’t a Market Failure…

• Hackers/ “security research” firms
  – Collude well
  – “Find a need and fill it”
  – (Sometimes) create businesses from bad behavior
  – Have excellent automated tools to increase hacking efficiency and time to exploit
  – (Sometimes) are “for hire” by bad guys
Should the IT Industry Be Regulated?

• Governments typically **regulate** industries where there is a compelling public safety requirement and/or a market failure

• IT reliability and safety is a **public safety issue** because IT is the backbone of critical infrastructure

• “Social costs” of bad code are generally not reflected in pricing – a **market failure**
  – Vendors have no liability
  – To-date very little “market correction” (e.g., through insurance)

• **Conclusion:** Market correction needed
  – Preferably through procurement power…
  – But possibly through regulation if market fails to correct
Hopeful Signs in Information Assurance

• More Information on Assurance
  – Books! Seminars! Collect the Set!
• More industry collusion, in a good way
  – US Department of Homeland Security sponsoring forums on software assurance, with lots of participants
    – Common Body of Knowledge, Procurement Guide, etc.
    – Secure Software Forum
• Increased customer awareness
• More automated tools to help (static analysis, web vulnerability, etc.)
Why Secure Coding Matters to Oracle Customers

- Oracle builds mission-critical software that protects customers’ most sensitive information
- All our products rest on a foundation of secure development practice
- Most of secure coding practice is just good coding practice
- Ripple effect of patching multiple critical systems
- Oracle’s security brand directly depends on secure development processes
Secure Product Definition

- Oracle Secure Coding Standards
  - Compliments C and Java coding standards
  - Revised frequently for new hacks
  - Uses Oracle “true stories” as examples

- Oracle Secure Coding Standards Training
  - Web-based, interactive class
  - Mandatory for development, up to SVP, including PMs, QA, release management...
  - Status: has been rolled out across ST, Apps just beginning
Secure Product Definition (2)

- **Product Security Steering Committee**
  - Security representatives from all development groups
  - Focus on common problems and common solutions

- **Customer Advisory Council**
  - More than 20 organizations, from banking, manufacturing, pharma, government, education, and all major geographic areas
  - Customers from every product family in Oracle are security CAC members
Secure Product Development

• Development processes include security requirements through all phases:
  – Functional specs
  – Design specs
  – Test specs
• Additional design reviews for security
• Core, vetted security modules facilitate stronger security
  – Crypto libraries (including database encryption)
  – Identity management (SSO, provisioning, etc.)
  – “Build security once, use many” means developers are not “rolling their own” core security
Secure Product Development (2)

• 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., checks for SQL injection, buffer overflows)
  – Licensed static analysis tool from Fortify; is being deployed across Server Technologies
  – Web application vulnerability tool (SPI Dynamics) licensed for App Server
  – Oracle can also turn our 250K regression suite into destructive security tests
Secure Product Development (3)

• Security release checklists
  – All components on bill-of-materials validate against secure coding standards
  – Exceptions are tracked, resolved and deal-breakers stop releases

• Secure configuration
  – Global Product Security initiative focused on “default secure” product delivery across the stack
  – Benchmark under development for 11g, based on Center for internet Security guidelines
Ongoing Assurance

• Security Evaluations
  – *Third party* product validation against standards of ‘what you mean when you say you are secure’
  – Evals vet specific security functionality and the development processes used to build them
  – Core evaluations standards
    – International Common Criteria (ISO 15408)
    – US Federal Information Processing Standard-140
  – Database has most evals (19), but we evaluate other products, as well (App Server – 2, Oracle Internet Directory –1)
  – Evals are *required* by some customers for some implementations (NSTISSP #11)
Ongoing Assurance (2)

• **Product Assessments**
  - Core group of ethical hackers in Global Product Security
  - Focus is on new/critical modules
  - Knowledge transfer (coding standards…)
  - Augmented by use of external hacking firms (e.g., Pentest, ltd.)

• **Security best practices guides**
  - Multiple, typically part of the doc set and/or on OTN or Metalink
Ongoing Assurance (3)

• Critical Patch Updates
  – Quarterly, scheduled security patch bundles
  – Dates picked around most customers’ financial calendars so that they can apply patches in an “open IT window”
  – Cumulative for most products on applicable patch sets
  – We fix security issues in main code line first, then queue for backport
  – We backport issues in severity order (highest to lowest)
  – Result: maximum security, lowest cost-to-patch (as compared with one-off security fixes)

• Trends
  – More fixes per CPU
  – More testing
Ongoing Assurance (4)

- Security Configuration Management and Validation Tools (Oracle Enterprise Manager Grid Control)
  - Validate / customize secure configurations
  - Build from over 200 product specific security configuration issues
  - OEM also can determine whether critical security patches are missing
  - Provides security reports and security dashboard
  - Policy violations can trigger email or pager to admin
Some Wild-eyed Ideas (1)

• What if CS degree programs had the same level of required content, and stringent accreditation as CE programs?

• What if software developers had to be licensed, like licensed professional engineers (PEs)?
  – Changing lightbulbs, adding a dimmer switch and designing the power grid need different levels of electrical engineering expertise
  – Increased accountability for IT professionals is the ultimate process improvement

• What if product development processes were certified, and customers required this as proof of “best development practice?”
Some Wild-eyed Ideas (2)

• What if we had better, more automated tools to find security faults in software, that were widely available – from large vendors to small startups?
  – … and if customers required that code be scanned for avoidable, preventable security faults?
• What if products were required to be secure on installation, and continuously monitored for best practice?’
• What if the IT industry colluded on secure development practice?
• What if the IT industry doesn’t improve?
  – “At Dawn We Slept”
"A nation, as a society, forms a moral person, and every member of it is personally responsible for his society."

-Thomas Jefferson
(in letter to George Hammond, 1792)