Enterprise Application Security Program

GE’s approach to solving the root cause and establishing a Center of Excellence

Darren Challey
GE Application Security Leader
Agenda

✓ Why is AppSec important?
✓ Why is it so hard?
✓ Changing the culture
✓ Critical success factors
✓ Structuring an enterprise program:
  • Guidance
  • Education
  • Tools
✓ Managing vendors
✓ Creating a center of excellence
Why is Application security important?
Press we like!

2005, 2006 Global Most Admired Companies (#1)
Fortune

Seven consecutive years:
World’s Most Respected Company
Financial Times

2004 – Named a member of the Dow Jones Sustainability Index
Press we can’t afford …

Significant reputational, regulatory & financial harm
AppSec is a large data loss source

Loss or disclosure of PII (Personally Identifiable Information) is required to be reported (thus good)

Source: Verizon’s 2009 Data Breach Investigations Report – Figure 13
Challenges, why is this so hard?
AppSec changes rapidly

OWASP Top10 2004:
A1 Unvalidated Input
A2 Broken Access Control
A3 Broken Auth. / Session Mgmt
A4 Cross Site Scripting
A5 Buffer Overflow
A6 Injection Flaws
A7 Improper Error Handling
A8 Insecure Storage
A9 Application Denial of Service
A10 Insecure Config. Management

OWASP Top10 2007:
A1 Cross Site Scripting (XSS)
A2 Injection Flaws (e.g., SQL injection)
A3 Malicious File Execution (i.e., PHP)
A4 Insecure Direct Object Reference
A5 Cross Site Request Forgery (XSRF)
A6 Info Leak / Improper Error Handling
A7 Broken Auth. / Session Mgmt
A8 Insecure Cryptographic Storage
A9 Insecure Communications
A10 Failure to Restrict URL Access

new!
Changing landscape

1. Increased skill and talent pool of technically proficient individuals willing to break the law
2. Growing volume of financially valuable data online (PII and corporate intellectual property)
3. Development of criminal markets (black markets) to facilitate conversion to money

*attackers now have effective skills, something to steal, and a place to sell it*

Completely one-sided: we must find all vulnerabilities while the bad guys only need to find one
Becoming an enabler (not a barrier)

Past
- InfoSec is the barrier

Future
- InfoSec is an enabler

Must inject application security earlier through Guidance, Education and Tools
Ineffective tollgates lead to ...

Must understand the development and deployment process and integrate rather than mandate
Applying security at the right time

Table 5-1. Relative Cost to Repair Defects When Found at Different Stages of Software Development (Example Only)
X is a normalized unit of cost and can be expressed terms of person-hours, dollars, etc.

<table>
<thead>
<tr>
<th>Requirements Gathering and Analysis/Architectural Design</th>
<th>Coding/Unit Test</th>
<th>Integration and Component/RAISE System Test</th>
<th>Early Customer Feedback/Beta Test Programs</th>
<th>Post-product Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>1X</td>
<td>5X</td>
<td>10X</td>
<td>15X</td>
<td>30X</td>
</tr>
</tbody>
</table>

Solving the problem for the enterprise

Culture Change
Some success factors

✓ Form a **mission** and **strategy**
✓ Develop **policy** (but not corporate “mandate”)
✓ Gain **executive buy-in** (cost / benefit / risk)
✓ Understand the **magnitude** of problem (metrics)
✓ Asset **inventory** and **vulnerability management**
✓ Develop **standards** (what should I do and when?)
✓ Establish a formal **program** (strong leadership)
✓ Focus on **education** and training materials
✓ Develop **in-house** expertise, services and “COE”
✓ Continuous improvement, **measurement**, KPI
✓ **Communicate**, **communicate**, **communicate** …
✓ **Drive a culture change** (shared need, WIIFM)
✓ **Communicate expectations** with vendors
✓ Implement **incentives** (and penalties)
✓ **Digitize** after the process is solid (tools)
The Application Security Program will achieve and maintain a strong application security posture across the company through the implementation of consistent and unified guidance, education, and tools.

**Guidance**
Provide clear direction to the company and vendors on the expectations for secure code development.

**Education**
Assist the businesses and vendors with educating their developers in secure coding practices.

**Tools**
Identify tools to ensure secure code, assist in the deployment of those tools.

**Metrics**
Underpinning the entire program is the use of metrics to track progress.
AppSec program strategy

- Monitor & improve
  - Inventory & tracking
  - Security tools
  - Metrics
  - Training
  - Policy
  - Standards

- Tools
- Guidance
- Education
AppSec Calendars helped increase visitors to key Guidance materials.


Downloads doubled in April when Quick Reference Card with “Quick links” appeared.
Education

**CBT1: Intro to AppSec at GE (60 min)**

**CBT2: GE Best Practices for Secure Coding (90 min)**

**CBT3: Attack Profiles & Countermeasures (120 min)**

**Developer Awareness Assessment:**
- 100’s of internally-developed questions
- Randomized questions, timed completion
- Vendors track their own results
- Allows tailoring of training / awareness programs
Tools

✓ COE AppSec assessment services
✓ Vendor framework & Metrics
✓ Compliance Handbook
✓ Common objects repository
✓ GE Enterprise Application Security
✓ Scanning & Monitoring tools

Automation is the way to go (but the tools are not quite there yet)
Managing vendor performance
GE secure SDL framework

Goal: prevent, detect or correct security defects earlier

**Requirements**
- Security Kick-off
- Use Security Requirements Checklist
- Identify regulatory and compliance considerations
- Ensure development team has access to [test tools]
- Ensure developers trained or certified on Secure Coding Skills

**Design**
- Follow GE Secure Architecture & Deployment Guidelines in design
- Cover all points in Architecture and Design Review checklist
- Develop Security Use cases
- Develop Security Abuse cases
- Perform risk assessment (recommended tool: Threat modeling)

**Development**
- Use GE Best Practices for Secure Coding
- Use Secure Common Objects (COR)
- Use Secure Code Review checklist during Peer Review
- Scan app. code using [test tools] and fix all High or Critical vulnerabilities
- Use GE AppSec COE services for early security review

**QA**
- Perform Risk based security test (use Security Test cases Template)
- Scan App. using [test tools] and fix all High or Critical vulnerabilities
- Use GE AppSec COE services for early security review

**Security Testing**
- Perform Internal Final Security Assessment (Refer Vulnerability Ratings & Categories)
- Fix all High or Critical vulnerabilities before delivering code to GE
- Obtain signoff from GDC AppSec Leader
- Use GE AppSec COE services for Assessments

**Deployment**
- Perform Infrastructure Security Review
- Use GE AppSec COE services for Assessments
Vendor AppSec Performance

GDC App Sec Trend

% Assessments With Zero Critical/High Vulnerabilities

Avg of Critical/High Vulnerabilities per Assessment

* GDCs without assessments during shown periods are not included

Jan 07 to May 09  Jun 09 to Aug 09

White Box + SCABBA Combined
N: 1019
Period: 01/19/07 - 08/31/09
So is any of this making a difference?
Is it making a difference?

Average of Critical/High Vulnerabilities Per Assessment

Vulnerabilities checked in assessments increasing
Forming a “center of excellence”
What is a COE?

A “Center of Excellence” combines the best available people, processes and tools to deliver low cost / high quality services and guidance under strong leadership with a clear mission.

<table>
<thead>
<tr>
<th>People</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expertise (internal and external)</td>
</tr>
<tr>
<td>Multi-disciplinary capability</td>
</tr>
<tr>
<td>Cross-business steering committee</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process Excellence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard engagement model</td>
</tr>
<tr>
<td>Cycle time reductions through Lean</td>
</tr>
<tr>
<td>Managed w/ metrics to drive behavior</td>
</tr>
<tr>
<td>Leverage Internal best practices</td>
</tr>
<tr>
<td>External benchmarking</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central deployment / management</td>
</tr>
<tr>
<td>Leverage enterprise agreements</td>
</tr>
<tr>
<td>Start with process, follow with tools</td>
</tr>
</tbody>
</table>
Softtek Facilities

Biometric Access:

Privacy Glass:
Formal training & defined roles

Comprehensive training program for all auditors to ensure skills are kept current and that auditors can provide more than one type of service.
COE team structure

- Tools
- Research
- Operations
- Stakeholder Management
- Queue Management

Application Security Auditors
Application Assessment Types

**Black / Gray Box**

**Benefits:**
- Quick, cost-effective and targeted
- No source code needed
- Identify configuration issues
- Many more findings vs. scanner

**Better at finding:**
- Access Control / Auth. issues
- Configuration Mgt. Issues
- Input Validation (faster)

**White Box**

**Benefits:**
- Comprehensive, seeks all vulnerabilities
- Does not require a “live instance”
- Detailed developer remediation help

**Better at finding:**
- Sensitive information
- Input validation problems
- Exception management issues
- Back doors, logic bombs
Application assessment process

GE Application Security Program – Darren Challey

©2009 General Electric Co. All Rights Reserved

GE Business Client (Requestor)

Submit Request

Approve?

Upload Source Code

Y

GE Business Security Leader (Approver)

Approve?

Y

Application Security Program (COE)

Prepare Statement of Work (SOW)

Perform Assessment

Prepare Report

Report Delivered

Verification Assessment (optional)
Vulnerability criticality ratings

1. **Impact**
   - **High** - important assets or functions compromised, total data corruption or all services completely lost
   - **Medium** - data corruption possible or primary services interrupted
   - **Low** - non-critical assets or minimal secondary services affected, minor data corruption

2. **Likelihood**
   - **Low** - vulnerability is very difficult to discover, very difficult to exploit or not directly exposed and attacker would gain very limited application access
   - **Medium** - vulnerability is relatively difficult to discover, relatively difficult to exploit and attacker would gain limited application access
   - **High** - vulnerability is publicly known, easy to discover, easy to exploit, and attacker would gain full application access
COE customer satisfaction survey

Overall Satisfaction with the service
- Excellent: 44%
- Very good: 4%
- Average: 4%
- Acceptable: 1%
- Unacceptable: 47%

Ease of Engagement
- Excellent: 49%
- Very good: 18%
- Average: 4%
- Acceptable: 2%
- Unacceptable: 8%

Responsiveness
- Excellent: 39%
- Very good: 1%
- Average: 52%
- Acceptable: 6%
- Unacceptable: 0%

COE Application Security Program

<table>
<thead>
<tr>
<th>Business</th>
<th>Cases</th>
<th>Responses</th>
<th>Resp. Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Solutions</td>
<td>11</td>
<td>1</td>
<td>9.1%</td>
</tr>
<tr>
<td>GE Commercial Finance</td>
<td>149</td>
<td>20</td>
<td>13.4%</td>
</tr>
<tr>
<td>GE Corporate</td>
<td>166</td>
<td>16</td>
<td>9.6%</td>
</tr>
<tr>
<td>GE Healthcare</td>
<td>60</td>
<td>17</td>
<td>28.3%</td>
</tr>
<tr>
<td>GE Industrial</td>
<td>59</td>
<td>21</td>
<td>35.6%</td>
</tr>
<tr>
<td>GE Infrastructure</td>
<td>404</td>
<td>60</td>
<td>14.9%</td>
</tr>
<tr>
<td>GE Money</td>
<td>110</td>
<td>19</td>
<td>17.3%</td>
</tr>
<tr>
<td>NBCU</td>
<td>38</td>
<td>1</td>
<td>2.6%</td>
</tr>
<tr>
<td>SABIC-IP</td>
<td>14</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>8</td>
<td>N/A</td>
</tr>
<tr>
<td>Total</td>
<td>1011</td>
<td>163</td>
<td>16.1%</td>
</tr>
</tbody>
</table>
Questions?
Tools

Communication plan

When:
- October 2008
- November 2008
- December 2008
- January 2009

Who:

Posters

Application Security Resource Kit

Guidelines

Education

Tools

Communicate ... Communicate ... Communicate

Newsletters

2009 Awareness calendar

GE Application Security Program

©2009 General Electric Co. All Rights Reserved
Darren Challey Biography

Currently GE Application Security Leader:
• Lead a cross-business “AppSec Working Group”
• Establish policies, procedures and best practices
• Provide company-wide guidance, services and tools
• Maintain company-wide AppSec metrics program
• Partner with GE vendors to “fix root cause”

Prior Roles and Businesses:
• IT Controller and IT SOx Leader (GE Corporate)
• Six Sigma Black Belt (GE Commercial Finance)
• Web Master & Program Manager (GE Commercial Finance)
• Electrical, Mechanical & Nuclear Engineer (GE Energy and GE KAPL)

Degrees and Certifications:
• Certified Information Systems Security Professional (CISSP)
• Certified Information Systems Auditor (CISA)
• Edison Engineering Development Program Graduate
• Master of Engineering, Computer Systems - Rensselaer Polytechnic Inst.
• Bachelor of Science, Mechanical Engineering – Union College
Secure SDLC and GE-EAS

Guidance

- Application Security Policy, Requirements, Regulatory and Compliance
- Developer On-boarding Portal
- Developer Skills Assessment
- CBT 1: Introduction to App Sec
- CBT 2: In-depth App Sec Training
- CBT 3: Threats & Countermeasures
- Secure Coding Best Practices
- Secure Deployment Guide
- Security Analyst Tools
- Static Code Analysis
- Dynamic Code Analysis
- Vulnerability Testing Tools & Monitoring
- 3rd Party Assessment; Security Reviews
- Vulnerability Tracking
- Secure SDLC and GE-EAS
- 3rd Party Assessment; Security Reviews
- Secure COR
- Secure Coding Best Practices
- CBT 3: Threats & Countermeasures
- CBT 2: In-depth App Sec Training
- CBT 1: Introduction to App Sec
- Developer Skills Assessment
- Developer On-boarding Portal

Education

- In process

Tools

- Threat Modeling Tool
- Common IDE with Tools
- Secure COR
- In process

©2009 General Electric Co. All Rights Reserved

GE Application Security Program – Darren Challey
SW Quality Assurance / Security Convergence

Positive Testing

Under-perform

Application’s Desired Functionality

Over-perform

Negative Testing

Functional Bugs

Technical Bugs

Performance Bugs

Security Bugs

(Doesn’t do what it should)

(Does more than it should)