Avocent

Secure Lifecycle and Threat Modeling

James Robinson Avocent Product Security Officer

April 28th, 2011
Agenda

- Who is Avocent?
- Daily Task and Focus
- Snapshot of our SDL components
- SDL Deliverables
- Threat Modeling
Who is Avocent?

• Division of Emerson Electric (www.emerson.com)
  – 130,000 global Employees
  – 22 Billion in sales a year
• Emerson Network Power Business Group
• Global Software Development
• Provide the following technologies
  – Baseboard Management Card (BMC) firmware for major computing hardware vendors
  – Remote console presence
  – Out of band management firmware
  – Data Center Management and Planning
Daily Tasks and Focus

• Security Officer:
  – New to Avocent and still being defined.
  – SDL and Security Assurance
  – Tools for Testing
  – Resource Manager
  – Vendor Management
  – PSIRT
Daily Tasks and Focus

• Security Architect:
  – Principles, Patterns, Standards
  – Architectural/Conceptual Architecture Threat Modeling
  – Product Management Interface
  – Encryption
  – Authentication and Authorization
  – Product Security Incident Response
  – Design Reviews
  – Threat Modeling
High-level Snapshot of SDL

Secure Development Lifecycle, Architecture, Design
- SDL for Waterfall
- SDL for Agile
- Security Principles, Patterns, Standards
- Reverse Eng. Customer Needs and Industry Std(s)

Detailed Requirements and Development
- Detailed Security Requirements
- Secure Development
- Static Code Analysis
- Fuzz Testing

Quality and Security Testing
- Binary Analysis
- Penetration Testing
- Vulnerability Scanning
- Vulnerability Rating and Defect Tracking

Sales, Secure Implementation Guides, and Support
- Default Secure Installer
- Secure Imp. Guidelines
- Security Specs for Sales

Intellectual Property Protection
- Data Classification
- SDL – Product Delivery
- IT Integration

Product Security Incident Response (PSIRT)

Risk Analysis and Threat Modeling
- Platform Frameworks
- Development Frameworks
- Security Model
- Trust, Authn, Authz, Encryption
SDL Deliverables

- SDL Deliverables

<table>
<thead>
<tr>
<th>Exploration/Kickoff</th>
<th>Development</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backlog</td>
<td>Backlog</td>
<td>Security Requirements</td>
</tr>
<tr>
<td>Architecture/Design</td>
<td>Architecture/Design</td>
<td>Security Objectives</td>
</tr>
<tr>
<td>Spikes</td>
<td>Spikes</td>
<td>Security Spikes and Stories</td>
</tr>
<tr>
<td>Vision / Scope</td>
<td>Vision / Scope</td>
<td>Architectural Threat Model</td>
</tr>
<tr>
<td>Stories / Scenarios</td>
<td>Stories / Scenarios</td>
<td>Security Specific Training</td>
</tr>
<tr>
<td>Project Planning</td>
<td>Project Planning</td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td>Training</td>
<td></td>
</tr>
</tbody>
</table>

| Sprint 1            | Team Setup           | Security Specific Training                  |
| Process Setup       | Process Setup        | Security Team Members/Interaction          |
| Infrastructure Setup| Infrastructure Setup | Security Spikes and Stories                |

| Sprint 1+N          | Backlog Prioritization| Detailed Security Objectives                |
| Incremental Delivery| Incremental Delivery  | Security Spikes and Stories                 |
| Deliver working     | Deliver working      | Architectural Threat Model                  |
| software            | software             | Security Code Reviews                       |
| Stories / Scenarios | Stories / Scenarios  | Security Deployments Inspections            |
| Retrospective       | Retrospective        | Security Unit Testing                       |

| Release Prep        | Final Acceptance Test| Security Validation                        |
| Release             | Release Complete     | Security Testing                            |
| Documentation       | Documentation        | Security Marketing Data                     |
| Finalized           | Finalized            |                                           |

| Release             | Publish              | Security Retrospective                      |
| Product Support     | Product Support      | Product Support/Advisories                  |
Security Principles

• Defense-in-Depth
• Least Privileges
• Maintain a Reluctance to Trust
• Default Secure
• Keep the “footprint” of the system small
• Promote Standards and Compliance

• (more in draft but wanted to spoon feed)
Goal: Determine functional and non-functional attacks and their threat actors with regards to our systems. Outcome of threat modeling helps us build mitigating controls we can architect, design, develop into our systems.
Threat Modeling Sprint Cycle.

**Threat Modeling Activities**

**Sprint Map**
- **Inputs:**
  - PRD
  - FDD
  - Feature Plan
  - Product Backlog
  - User Stories
  - SFS/SDD – where available

**Pre-Sprint Prep (6 days)**
- **Analysis** 3 days
  - Product Owners finalize and prioritize User Stories
  - Designers create Technical Stories

- **Design Workshop** 2-3 days
  - Design workshop is held (2 days)
  - Create HLADD for upcoming Sprint
  - Create DADD sections 1 & 2
  - HLADD signoff

**Sprint (20 days)**
- **Planning** 2 days
  - Poker planning
  - Tasking
  - Scope finalized
  - Review estimations

- **Execution** 17 days
  - Complete DADDs
  - Coding
  - Unit & feature testing
  - Reviews
    - Preliminary Design
    - Detailed Design
    - Code
  - Release to QA

- **Review** 1 day
  - Technical review
  - Product Mgmt. review
  - Retrospective

**Finish of This Sprint**

**Beginning of Next Sprint**

**QA**
- Build
- Release notes
- QA system integration testing

**Begin prep for next Sprint**
Factors for Success/Fail

- Organization
  - Engineer Mindset
  - Management Mindset
  - Understanding of security (functional/non-functional)

- SDLC
  - 2 methodologies merging

- PMO
  - PMO organization was defined however it did not have a strong presence.

- Technology
  - Changes and implementation in technology direction before knowing threats.

Key: Security is a hard sell. Security is not something we want to think about.
Questions/Contact Information

- James.Robinson@Emerson.com