Security Engineering
Case Studies and Lessons Learned

Arjuna Shunn and Jed Pickel
Joseph Scotto
Introduction

• Microsoft and BAE Systems Detica
• What is “Security Engineering”

Trends

• Emerging Regulatory Requirements
• Market Demand
• Standardization

Case Studies

• Microsoft
• Itron
• MidAmerican Energy

Next Steps

• Results
• Implementation Roadmap
• Supply chain
• Resources
What we do at BAE Systems Detica

We deliver solutions that protect governments and businesses from the rising and advancing risk of cyber crime. Our mission is the protection of your information and the application of intelligence to gain operational and competitive advantage.

<table>
<thead>
<tr>
<th>Cyber security</th>
<th>Communications Intelligence</th>
<th>Financial crime &amp; compliance</th>
</tr>
</thead>
</table>

- Information Intelligence division of BAE Systems, an FTSE30 company
- 2,500 dedicated staff in 26 countries*
- Delivering National Security grade solutions for Government, Telecommunications, Financial Services, Energy and Utilities sectors
- Protecting information, assets and people from the increasing risk of cyber crime

* Note: BAE Systems has 96,000 employees - clients in over 100 countries
Computing is going to be integral and indispensable part of almost everything we do."

- Bill Gates
Security Engineering

Applying relevant security controls across all phases of the engineering lifecycle with

- Policy, management support, and organization-wide accountability
- A risk based approach that
  - considers the current threat landscape
  - protects against exploitation, not just vulnerabilities
  - is applied across the application lifecycle
  - considers technical, business, and regulatory context
  - is documented, predictable, and systematic
- Continuous improvement
  - applying industry best practices
  - responding to changing risks
  - applying lessons learned and KPIs
Security Engineering Process Approach

• Forrester 2011 - Most organizations
  • Transfer risk from development to operations
  • See application security as tactical and compliance driven
  • Do not have an end-to-end strategic approach

• Aberdeen 2011 – Secure at the Source
  • Identified 8 steps that help increase ROI
  • Companies with a strategic approach get 4x ROI
Emerging Regulatory Requirements

Direct quote from a recent FTC announcement:
“Federal Trade Commission charges that the company failed to take reasonable steps to secure the software it developed”

The settlement required:

- “a comprehensive security program designed to address security risks during development”
- “independent security assessments every other year for the next 20 years.”
Recent Standardization Activity

NISTIR 7628 - Guidelines for Smart Grid Cyber Security v1.0
“Applications being developed for use in the Smart Grid should make use of a secure software development life cycle (SDLC).”

Cyber Security Executive Order - EO13686
“The Cybersecurity Framework shall be consistent with voluntary international standards”

ISO/IEC 27034-1 Application Security
“The purpose of ISO/IEC 27034 is to assist organizations in integrating security seamlessly throughout the life cycle of their applications.”
### Markets Demanding SD Practices

#### Organizations Adopting SD Practices
- MidAmerican Energy Holdings Company
- Itron
- Apache

#### Software Vendors Implementing SD Practices
- Adobe Secure Product Lifecycle (SPLC)
- Cisco Secure Development Lifecycle (CSDL)
- Accuvant
- BAE Systems
- SDL Process and training
- Security Compass
- SDL tools, training, and consulting

#### Delivering SDL Capability
Microsoft Security Development

Secure Windows Initiative
Prior to 2001
- We knew we had a problem
- Small team, ad hoc process

TwC Memo
2002-2003
- Training and Security Pushes
- Needed a consistent, scalable, prescriptive process

SDL Launched
2004
- Required for almost all products
- Integrated into all phases of product lifecycle

SDL Implementation
2005-2007
- Theory vs. Practice
- Automation

SDL and the Ecosystem
2008-2012
- Publication of SDL and free tools
- Adaptations SDL for Agile Simplified SDL

Standards-based Secure Development
Current
- Secure development is a core part of supply chain discussion
- International standard on secure development

Introduction
Trends
Case Studies
Next Steps
Itron

- Identified smart meter connectivity risks
- Found SDL as a good way to mitigate the risk
- Introduced SDL with on a critical project
- Added security engineering process to smart meter devices
- The process also helped address supply chain inquiries.

“The SDL isn’t just shorthand for telling customers that, yes, Itron has a comprehensive security plan, it serves as an invaluable tool for communicating with clients.”
Mid American Energy

- Experienced an attack, May 2008
  - SQL Injection
- Research approach to reduce future risk
- Identified Microsoft SDL model as an opportunity
- Selling a Culture Change eventually led to management support
- Secure Development Initiative
  - Found more than 14,000 risks that needed to be addressed.
  - In 273 days, reduced to fewer than 100 vulnerabilities.
- Results
  - Software moved from afterthought to top-of-mind.
  - Productivity gain +20%
  - Broke over-reliance on “security by obscurity.”
  - Continuous improvement

Name: MidAmerican Energy Company
Headquarters: Des Moines, Iowa
Operating Revenue: $3.5 billion
Total Assets: $10.3 billion
Customers:
  - 730,000 electric
  - 707,000 natural gas
Employees: 3,500

NOTE: Data from SEC filings
Security Engineering Results

Product

- Lower Patch Rates
- Lower exploitability
- Lower infection rates

Organizations

- Increased Productivity / ROI
- Continuous Improvement
- Communication and Procurement Efficiency
- Roadmap to conform with emerging standards

**Office vs. StarOffice 2003/7/10 Exploitable/Probably Exploitable**

http://dankaminsky.com/2011/03/11/fuzzmark/

<table>
<thead>
<tr>
<th>Year</th>
<th>Office Exploitable</th>
<th>OpenOffice Exploitable</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>126</td>
<td>73</td>
</tr>
<tr>
<td>2007</td>
<td>62</td>
<td>12</td>
</tr>
</tbody>
</table>
| 2010 | 20                 | 7                      

**Reduction in Infections by Major Autorun-Abusing Families**

as reported by the Microsoft Malicious Software Removal Tool
January and May 2011

- 62% decrease
- 68% decrease
- 92% decrease

<table>
<thead>
<tr>
<th>% of MSRT-Scanned Computers Reporting Infections</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2011 (after update)</td>
</tr>
<tr>
<td>Jan. 2011 (before update)</td>
</tr>
</tbody>
</table>

Win XP  | Win XP  | Win XP  | Win Vista | Win Vista | Win 7  |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>0.05%</td>
<td>0.05%</td>
<td>0.05%</td>
<td>0.05%</td>
<td>0.05%</td>
<td>0.05%</td>
</tr>
<tr>
<td>0.10%</td>
<td>0.10%</td>
<td>0.10%</td>
<td>0.10%</td>
<td>0.10%</td>
<td>0.10%</td>
</tr>
<tr>
<td>0.15%</td>
<td>0.15%</td>
<td>0.15%</td>
<td>0.15%</td>
<td>0.15%</td>
<td>0.15%</td>
</tr>
<tr>
<td>0.20%</td>
<td>0.20%</td>
<td>0.20%</td>
<td>0.20%</td>
<td>0.20%</td>
<td>0.20%</td>
</tr>
<tr>
<td>0.25%</td>
<td>0.25%</td>
<td>0.25%</td>
<td>0.25%</td>
<td>0.25%</td>
<td>0.25%</td>
</tr>
<tr>
<td>0.30%</td>
<td>0.30%</td>
<td>0.30%</td>
<td>0.30%</td>
<td>0.30%</td>
<td>0.30%</td>
</tr>
<tr>
<td>0.35%</td>
<td>0.35%</td>
<td>0.35%</td>
<td>0.35%</td>
<td>0.35%</td>
<td>0.35%</td>
</tr>
<tr>
<td>0.40%</td>
<td>0.40%</td>
<td>0.40%</td>
<td>0.40%</td>
<td>0.40%</td>
<td>0.40%</td>
</tr>
</tbody>
</table>

Introduction Trends Case Studies Next Steps
Implementation Roadmap

Simplified SDL provides an efficient path to adopt a security engineering process.

- Implement Verification and Response Simplified SDL Practices
- Systematic application of Simplified SDL process
- Standardize with Policy and Tools
- Validate with ISO/IEC 27034
Considering Security Engineering From Suppliers

• A effective approach is to inquire about suppliers secure development process
  - Do you have a secure development process?
    – Is the process documented, predictable, and systematic?
    – Does management support the process?
    – Is the process risk based and applied across the engineering lifecycle?
  - How does your process
    – consider technical, business, and regulatory context?
    – evolve to address new threats?

• Or more concisely, does your organization adopt ISO/IEC 27034?

• When formalizing requirements consider ISO/IEC 27036 - Information security for supplier relationships
  Example supplier requirement from ISO/IEC 27036-2 Annex A
  “Develop systems using a structured and approved system development methodology that ensures information security requirements are considered as part of the process, and consequently defined, documented and met.”
Security Engineering Summary

Why

- Market forces are creating demand for security engineering
- Leading to emerging standards, regulations, and requirements
- Aligning your engineering process will save time and money

What

- A risk based, continuously improving security management system applied across the engineering lifecycle

How

- Always specify the use of the SDL for new projects built in house
- Require contracted vendors to demonstrate use of an SDL process
- Use the available resources of Microsoft and the SDL partners
We work with clients across the complete cyber-risk lifecycle
BAE Systems Detica Resources

Implementation Guidance

General Resources
- https://www.baesystemsdetica.com/resources/
Microsoft SDL Resources

Implementation Guidance

- Simplified SDL

Case Studies

- Case studies – The SDL Chronicles

Standards

- ISO/IEC 27034-1 and ISO/IEC 27036 are available from www.iso.org
- The emergence of software security standards: ISO/IEC 27034-1:2011 and your organization