Costs of Secure Software Development
Models and Practice

Barry Boehm
Elaine Venson

September 22, 2020
Software Vulnerability

• Based on the US National Vulnerabilities DB (NVD) with more than 85K publicly reported vulnerabilities (2015)

93% of buffer errors involved only a single condition (typically, failure to check array bounds)

CyBoK

Software Security
Known categories of programming errors resulting in security bugs, & techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems.

Secure Software Lifecycle
The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default.

CyBok: Cyber Security Body of Knowledge

Source: https://www.cybok.org/
Secure Software Development (Touchpoints)

Outline

• Cost-effectiveness of secure software development
• Sources of cost in secure software development
  • Security practices
  • Security controls
• Security practices application survey
• Models for costing secure software development
• Open issues and opportunities
• Next steps
Outline

• Cost-effectiveness of secure software development
• Sources of cost in secure software development
  • Security practices
  • Security controls
• Security practices application survey
• Models for costing secure software development
• Open issues and opportunities
• Next steps
Software Security as a Trade-off

**Costs**
- Expertise
- Tools
- Training
- Improving processes
- Investment in early phases

**Benefits**
- Vulnerabilities prevention/detection
- Avoided risks

**Costs**
- Higher fixing costs
- Patching
- Down-time
- Recovery costs
- Reputation loss

**Benefits**
- Priority to features
- Time to market
Security Production Function

Outline

• Cost-effectiveness of secure software development
• Sources of cost in secure software development
  • Security practices
  • Security controls/features
• Security practices application survey
• Models for costing secure software development
• Open issues and opportunities
• Next steps
# Sources of Cost (from literature)

<table>
<thead>
<tr>
<th>Source</th>
<th>Papers</th>
<th>Source</th>
<th>Papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform Security Review</td>
<td>21</td>
<td>Perform Security Training</td>
<td>6</td>
</tr>
<tr>
<td>Apply Threat Modeling</td>
<td>18</td>
<td>Improve Development Process</td>
<td>5</td>
</tr>
<tr>
<td>Perform Security Testing</td>
<td>16</td>
<td>Perform Penetration Testing</td>
<td>5</td>
</tr>
<tr>
<td>Apply Security Requirements</td>
<td>11</td>
<td>Achieve Security Level</td>
<td>3</td>
</tr>
<tr>
<td>Apply Security Tooling</td>
<td>11</td>
<td>Document Technical Stack</td>
<td>3</td>
</tr>
<tr>
<td>Implement Countermeasures</td>
<td>9</td>
<td>Security Experts, Security Groups, Security Master</td>
<td>3</td>
</tr>
<tr>
<td>Fix Vulnerabilities</td>
<td>9</td>
<td>Track Vulnerabilities</td>
<td>3</td>
</tr>
<tr>
<td>Apply Secure Coding Standards</td>
<td>8</td>
<td>Functional Features</td>
<td>2</td>
</tr>
<tr>
<td>Apply Data Classifications Scheme</td>
<td>7</td>
<td>Hardening Procedures</td>
<td>2</td>
</tr>
<tr>
<td>Publish Operations Guide</td>
<td>7</td>
<td>Security by Design Paradigm</td>
<td>1</td>
</tr>
</tbody>
</table>

Developing secure software

Goals
- Build-in security to preserve assets (CIA)

Requirements
- Functional
- Non-functional

Development
- Features, controls, components
- Security practices (threat modeling, pen-testing, etc)

Measurement
- Lines of code, functions points, objective points
- Levels of application (scope and rigor)
Outline

• Cost-effectiveness of secure software development
• Sources of cost in secure software development
  • Security practices
  • Security controls
• Security practices application survey
• Models for costing secure software development
• Open issues and opportunities
• Next steps
Survey

• Participants of the Software Security group on LinkedIn
• 110 complete responses
• 29 countries
Poll – Security Practices

Which security practices does your organization apply during software development? (select all that apply)

- Secure Coding Standards
- Security Tooling
- Track Vulnerabilities
- Security Requirements
- Security Testing
- Development Process Improvement
- Document Technical Stack
- Security Review
- Threat Modeling
- Penetration Testing
- Security Training
- Data Classification Scheme
- Publish Operations Guide
Effort Dedicated to Security

By Development Type
Challenges in Estimating/Planning Security Practices

“Getting people to truly stop, and understand 100% why the best practices are needed, can be a challenge - when people get focused on delivery dates. Once you explain the ‘What could happen...’ - it tends to sink in.”

“Always people considered security as feature to add after business logic and programming are finished so it happens to delay the project a lot.”

“Convincing project manager to incorporate security related time and effort.”
Poll – Security effort estimation

How is effort for software security estimated in your organization? (select all that apply)

- Ad-hoc
- Expert opinion
- Analogy-based
- Model/parametric
- Other
- NA
Outline

• Cost-effectiveness of secure software development
• Sources of cost in secure software development
  • Security practices
  • Security controls
• Security practices application survey
• Models for costing secure software development
• Open issues and opportunities
• Next steps
## Approaches to Estimating Costs of SWSec

<table>
<thead>
<tr>
<th>Approach</th>
<th>Additional Cost</th>
<th>Productivity Range</th>
<th>Source</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>COCOMO II security extension [Reifer 2003]</td>
<td>0.94 (Low)</td>
<td></td>
<td>Expert estimation</td>
<td>Not validated</td>
</tr>
<tr>
<td></td>
<td>1.02 (Nominal)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.27 (High)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.43 (Very High)</td>
<td>1.86</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.75 (Extra High)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COSECMO [Colbert 2008]</td>
<td>0% (Nominal)</td>
<td></td>
<td>Expert estimation with two inputs provided by a Commercial Company</td>
<td>Not validated</td>
</tr>
<tr>
<td></td>
<td>20% to 80% (EAL 3 - High)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>50 to 200% (EAL 4 - Very High)</td>
<td>31.25</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>125% to 500% (EAL 5 - Extra High)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>313% to 1250% (EAL 6 - Super High)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>781% to 3125% (EAL 7 - Ultra High)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weapon systems cost model (COCOMO II based)</td>
<td>1.0 (Low or Nominal)</td>
<td></td>
<td>Expert estimation and 73 data points</td>
<td>Cross validation</td>
</tr>
<tr>
<td>[Lee 2014]</td>
<td>1.87 (High)</td>
<td>1.87</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure OS software cost model (COCOMO II based)</td>
<td>1 (Nominal)</td>
<td></td>
<td>Expert estimation</td>
<td>Case study</td>
</tr>
<tr>
<td>[Yang 2015]</td>
<td>1.25 to 1.5 (High)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.75 to 2.0 (Very High)</td>
<td>3.75</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.0 to 2.75 (Extra High)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.0 to 3.75 (Super High)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FPA security extension (GSC) [Abdullah 2010]</td>
<td>0 to 5% increase in the function points size of the project</td>
<td>1.05</td>
<td>Practices from survey with developers</td>
<td>Not validated</td>
</tr>
</tbody>
</table>

---

Center for Systems and Software Engineering
University of Southern California
Outline

• Cost-effectiveness of secure software development
• Sources of cost in secure software development
  • Security practices
  • Security controls
• Security practices application survey
• Models for costing secure software development
• Open issues and opportunities
• Next steps
Issues with CC/EAL

- Framework focused on product *certification*
- Used for security *benchmark* of IT products
- Certification is expensive and take time
- EALs are defined around the depth and rigor of design, tests and reviews of security features
- Not developed for secure software development in general
- Opportunity to develop a rating scale, based on security practices, that captures the current secure software development scenario
Opportunities for Validation

• No model has been properly validated with industry data
• COCOMO III initiative to collect data from industry
• Open source software repositories
• Involvement of the communities of security experts and estimation experts
Outline

• Cost-effectiveness of secure software development
• Sources of cost in secure software development
  • Security practices
  • Security controls
• Security practices application survey
• Models for costing secure software development
• Open issues and opportunities
• Next steps
Scale Development

1.1. Identification of domain and item generation
1.2. Content validity

3. Scale points description
4. Item reduction
5. Pre-testing scale
6. Sampling and data collection

7. Tests of reliability
Tests of validity

Modeling Methodology

1. Analyze Existing Literature
2. Perform Behavioral Analysis
3. Determine Form of the Model, Identify relative significance of parameters
4. Perform Expert-Judgement, Delphi Assessment
5. Gather Project Data
6. Determine Bayesian A Posteriori Update
7. Gather More Data, Refine Model
Proposed Model Form

\[ PM = A \cdot \text{Size}^E \cdot \text{SECU} \cdot \prod_{i=1}^{n} EM_i \]

**SECU**: Effort multiplier for secure software development level

\[ \text{Size} = \text{Functional Size} + \text{Security Features Size} \]

\[ \text{Size} = \text{Functional Size} \cdot \text{SSF} \]

**SSF**: Security Size Factor for security level
Data Collection

Security experts estimates for the security parameter

Estimation experts estimates for the security parameter

Wideband Delphi

Industry
Projects’ Data ➔ Manual Data Collection Form

OSS
Projects’ Data ➔ Automated Data Collection

Projects’ Data ➔ Survey
Evaluation

- Security rating scale
  - Reliability (repeatability)
  - Validity (ability to measure the latent variable)

- Effect of security on development effort
  - Significance of the coefficient for security (t-test)
  - Goodness of fit of the model to the data:
    - Adj-R² (variance explained by the predictors)
    - Standard Error (noise)
  - Model accuracy:
    - K-fold cross validation
    - MMRE (mean magnitude of relative error)
    - PRED(0.25) (% of predictions within 25% of the actuals)
Poll - Get involved!

1) Participate in an eDelphi study
   • Share your estimates and assumptions anonymously
   • Compare your estimates with other participants

2) Participate in data collection
   • Provide sanitized data
   • Receive a version of the model calibrated for your organization

Contact: Elaine Venson
venson@usc.edu

Contact: Brad Clark (COCOMO III Project Coordinator)
clarkbk@usc.edu
Thank you!

Barry Boehm
boehm@usc.edu

Elaine Venson
venson@usc.edu
References


