Estimating Computer Security Sources of Effort: a Systematic Review

2018 Annual Research Review

Elaine Venson
Advisor: Dr. Barry Boehm
Smiths Medical confirms drug pump vulnerable to cyberhacking

Firm is latest device maker to acknowledges problems; no hacking reports yet received.

By Joe Carlson Star Tribune | SEPTEMBER 13, 2017 — 7:51PM

Massive ransomware cyber-attack hits nearly 100 countries around the world

ROBOT SECURITY VULNERABILITIES POSE SERIOUS THREAT TO HUMANS

BY ANTHONY CUTHBERTSON ON 3/1/17 AT 9:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Equifax breach could be most costly in corporate history

Equifax Inc said it expects costs related to its massive 2017 data breach to surge by $275 million this year, suggesting the incident at the credit reporting bureau could turn out to be the most costly hack in corporate history.

MAR 02 2018
Software Security

• **Definition**: engineering software that continues working under malicious attack [McGraw, 2004]

• Software is a **central and critical aspect** of the computer security problem [McGraw, 2013]

• Many issues faced in computer security today are **rooted in our approach** to developing software and systems [Heitzenrater, 2016]
## Software Security vs Application Security

<table>
<thead>
<tr>
<th>Software Security</th>
<th>Application Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive</td>
<td>Reactive</td>
</tr>
<tr>
<td>Build security in</td>
<td>Build security around</td>
</tr>
<tr>
<td>Preventive costs</td>
<td>Corrective costs</td>
</tr>
<tr>
<td>• Design for security</td>
<td>• Network centric approach</td>
</tr>
<tr>
<td>• Testing for security</td>
<td>• Protect software after development</td>
</tr>
<tr>
<td>• Software security education</td>
<td>• Finding and fixing security issues</td>
</tr>
</tbody>
</table>

What is the most effective way to protect software?
Software Security

• Security remains largely focused on post-development measures late in the SDLC [Heitzenrater, 2016]
• Building secure software is better than protecting bad software
• Cyber war is inevitable, unless we build security in [McGraw, 2013]
Estimating Software Security

• Challenges [Yang, 2015]:
  – Lack of validated methods or models for estimation of secure software systems
  – Large variation in existing security standards
  – Lack of historical data to validate methods

• SW Security solutions face financial and technical barriers, need of thorough approach to planning and execution [Heitzenrater, 2016]

• COCOMO III Security Cost Driver
USC-CSSE Modeling Methodology

Determine Model Needs
Step 1

Analyze existing literature
Step 2

Perform Behavioral analyses
Step 3

Define relative significance, data, ratings
Step 4

Perform expert judgment Delphi assessment, formulate a priori model
Step 5

Gather project data
Step 6

Determine Bayesian A-Posteriori model
Step 7

Gather more data; refine model
Step 8

Systematic Review on Security Costs

• Search and identify all relevant material related to Software Security Cost Estimation
• Follow objective, analytical and repeatable procedures
• A secondary study -> generate outcomes by aggregating material from primary studies
Context of a Systematic Review

Primary Studies

- case study
- laboratory experiment

Systematic Review

- provides input to
- influences
- creates

- objective summary of evidence about a technology, practice, etc.
- provides inputs to
- practice
- policies
- standards

Source: Kitchenham, B.A., Budgen, D., Brereton, P.: Evidence-Based Software Engineering and Systematic Reviews (adapted).
Systematic Review Process

Input 1  Input 2  Input 3  Input n

Search and Find

Include/Exclude

Synthesize

Map question to search strings

Review Conclusions

Knowledge Translation

Source: Kitchenham, B.A., Budgen, D., Brereton, P.: Evidence-Based Software Engineering and Systematic Reviews (adapted).
Research Questions

1. Which papers report experiences of measuring or estimating the cost of software security requirements in software development projects?
2. What are the major sources of effort in developing secure software?
3. What approaches have been used to estimate the costs of security in software development projects?
4. Which data sets have been used to analyze the cost of secure software?
Research Questions (cont)

5. Which and how cost drivers are affected by security requirements?

6. What issues have been observed when measuring or estimating costs for secure software development?

7. Which software security standards and formal assessments have been used to evaluate costs of secure costs?
Mechanism of the Search

Tittle:
- Research question 1
- Research question 2
- Research question 3

# Venues of Search

<table>
<thead>
<tr>
<th>Manual Search</th>
<th>Automated Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IEEE Transactions on Software Engineering (TSE)</td>
<td>• IEEE Digital Library</td>
</tr>
<tr>
<td>• ACM Transactions on Software Engineering Methodology (TOSEM)</td>
<td>• ACM Digital Library</td>
</tr>
<tr>
<td>• Empirical Software Engineering Journal</td>
<td>• SpringerLink</td>
</tr>
<tr>
<td>• Journal of Systems and Software</td>
<td>• Scopus</td>
</tr>
<tr>
<td>• Information and Software Technology</td>
<td>• Web of Science</td>
</tr>
<tr>
<td>• Proceedings of the International Conference on Software Engineering (ICSE)</td>
<td></td>
</tr>
<tr>
<td>• Empirical Software Engineering and Metrics Conference (ESEM)</td>
<td></td>
</tr>
<tr>
<td>• Workshop on Software Engineering for Secure Systems (SESS)</td>
<td></td>
</tr>
<tr>
<td>• Software and Systems Modeling</td>
<td></td>
</tr>
<tr>
<td>• Journal of Cyber Security and Information Systems</td>
<td></td>
</tr>
</tbody>
</table>
Completeness: Sensitivity & Precision

**Sensitivity**

\[
\text{Sensitivity} = \frac{\text{Number of relevant studies retrieved}}{\text{Total number of relevant studies}} \times 100\%
\]

**Precision**

\[
\text{Precision} = \frac{\text{Number of relevant studies retrieved}}{\text{Number of studies retrieved}} \times 100\%
\]

# Primary Study Selection

<table>
<thead>
<tr>
<th>Inclusion Criteria</th>
<th>Exclusion Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>research related to estimation/measuring the effort or cost of</td>
<td>reactive approach to software security issues</td>
</tr>
<tr>
<td>security in software development</td>
<td>research about software safety</td>
</tr>
<tr>
<td>research on software security and presents effort/cost results</td>
<td>not presented in English</td>
</tr>
<tr>
<td>published between 2000 up to and including 2017</td>
<td>not accessible in full-text</td>
</tr>
<tr>
<td></td>
<td>book or gray literature</td>
</tr>
<tr>
<td></td>
<td>tutorial, workshop or poster summary</td>
</tr>
<tr>
<td></td>
<td>study is duplicated</td>
</tr>
</tbody>
</table>
Next Steps in the Systematic Review

Select Studies • Inclusion/exclusion criteria

Assess Quality • Quality checklist • Rigor and relevance of primary studies

Extract Data • Extraction form • Evidence to support the RQ

Synthesize • Narrative synthesis • Thematic Analysis

Document

Validation Activities (check decisions)
References


