CISQ Webinar

Costs of Secure Software Development
Models and Practice

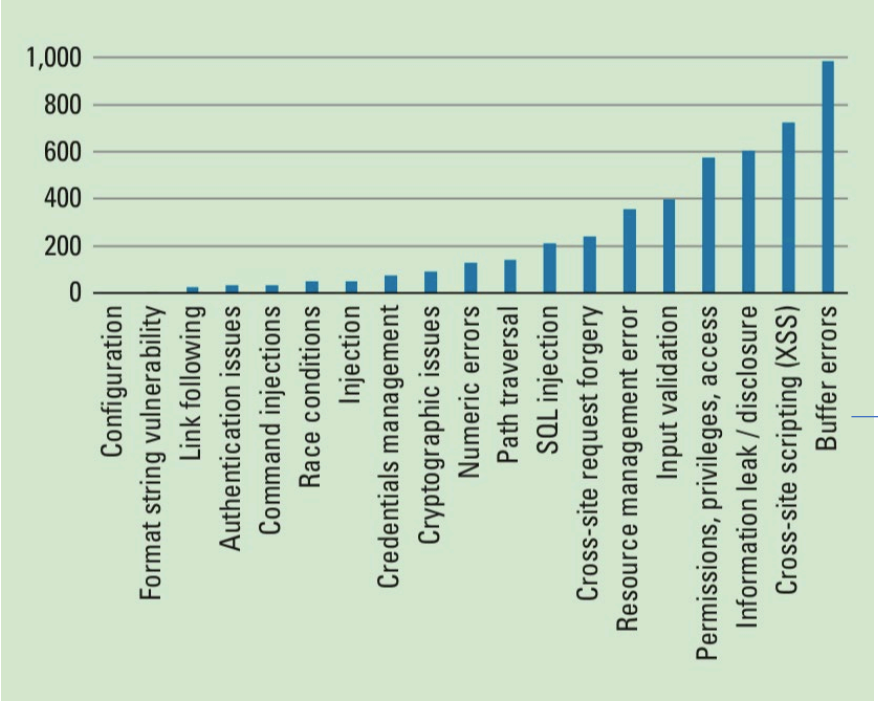
Barry Boehm

Elaine Venson

September 22, 2020

Software Vulnerability

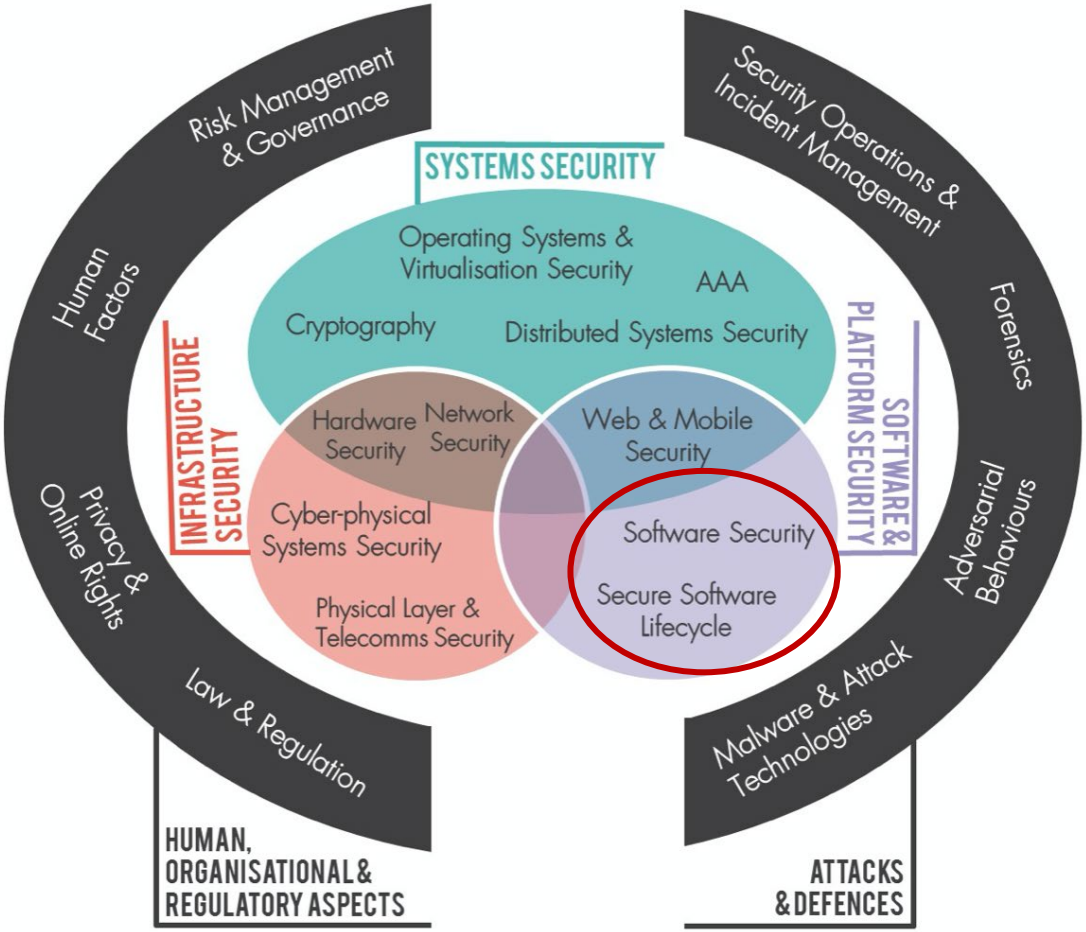
- Based on the US National Vulnerabilities DB (NVD) with more than 85K publicly reported vulnerabilities (2015)



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

R. Kuhn, M. Raunak, and R. Kacker, "It Doesn't Have to Be Like This: Cybersecurity Vulnerability Trends," *IT Professional*, vol. 19, no. 6, pp. 66–70, Nov. 2017.

CyBoK



CyBok: Cyber Security Body of Knowledge

Software Security

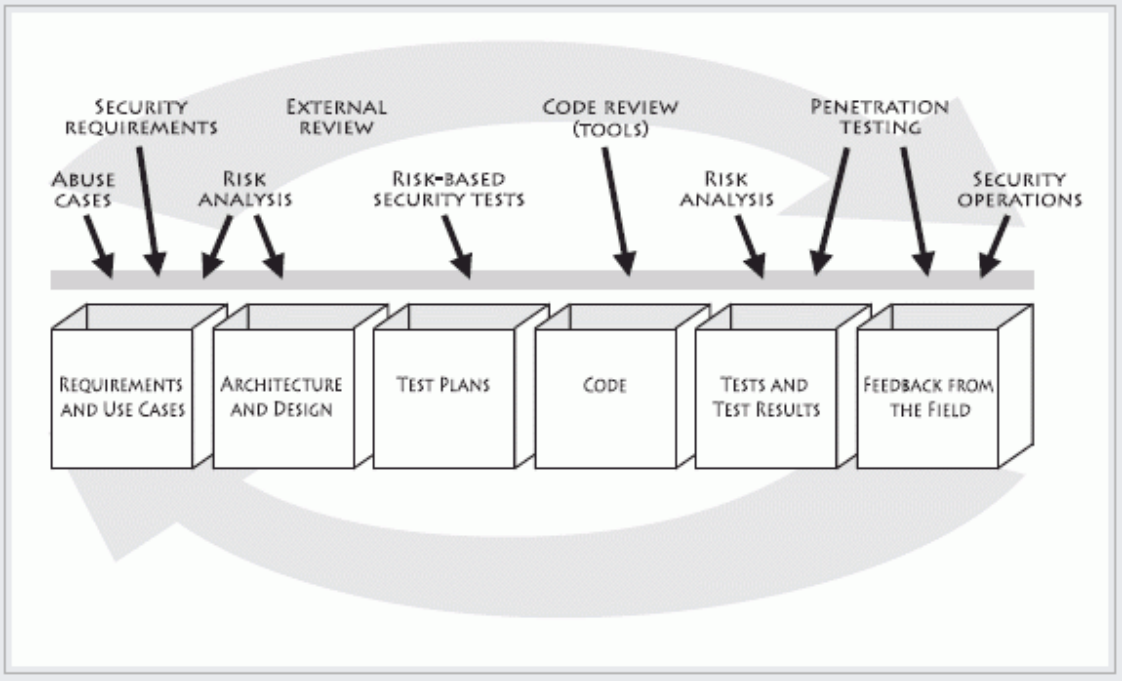
Known **categories of programming errors resulting in security bugs, & techniques for avoiding these errors**—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems.

Secure Software Lifecycle

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

Source: https://www.cybok.org/

Secure Software Development (Touchpoints)



McGraw, G., 2006. Software Security: Building Security In

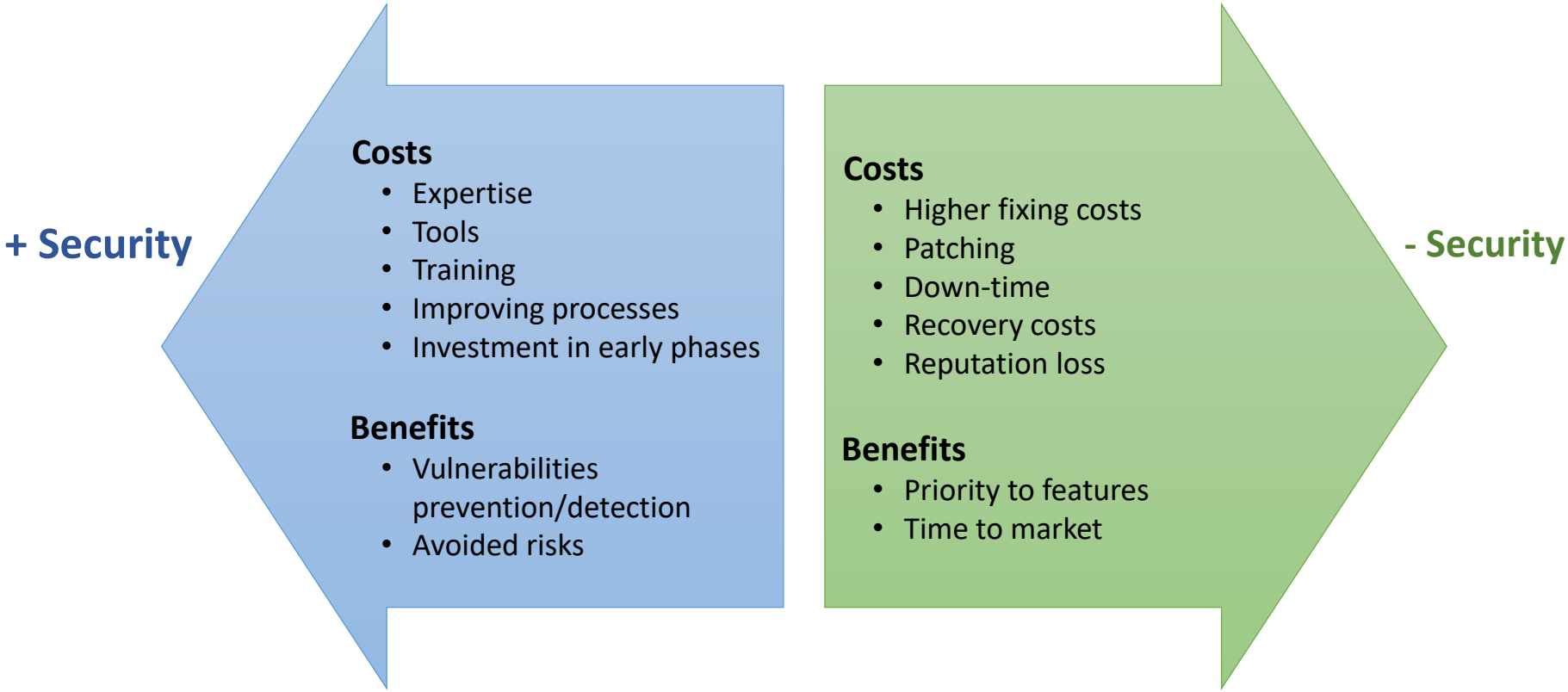
Outline

- 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

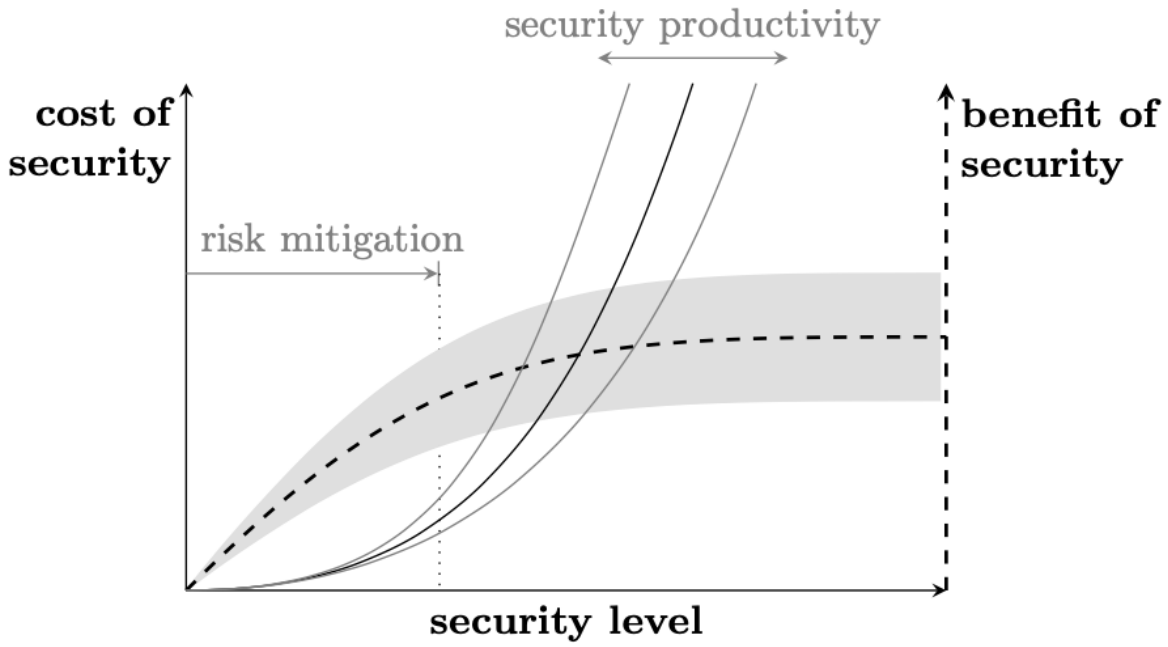
Outline

- 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



Security Production Function



Böhme, R., 2010. Security Metrics and Security Investment Models, in: Echizen, I., Kunihiro, N., Sasaki, R. (Eds.), Advances in Information and Computer Security.

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

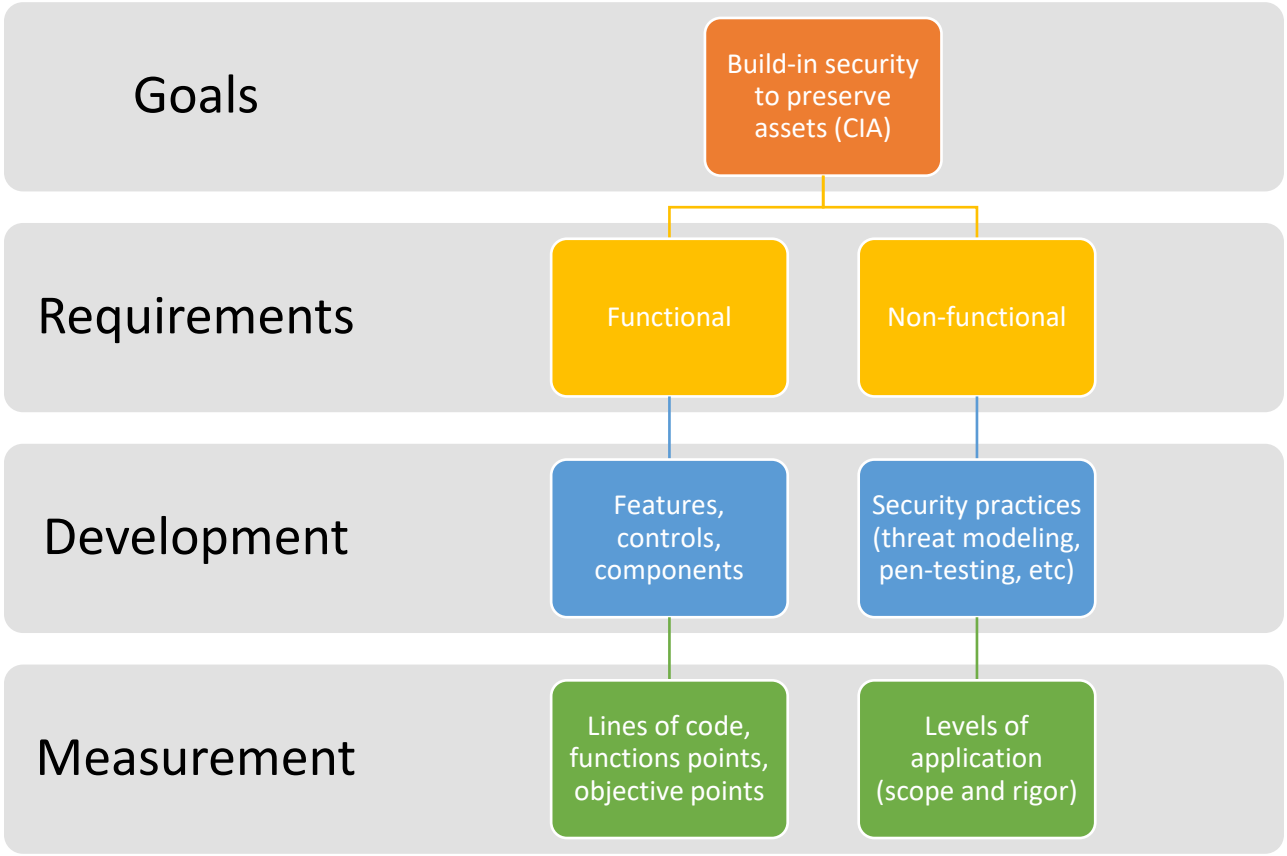
Sources of Cost (from literature)

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

SWSec Practices Other Sources

Venson, E., Guo, X., Yan, Z., Boehm, B., 2019. Costing Secure Software Development: A Systematic Mapping Study.

Developing secure software

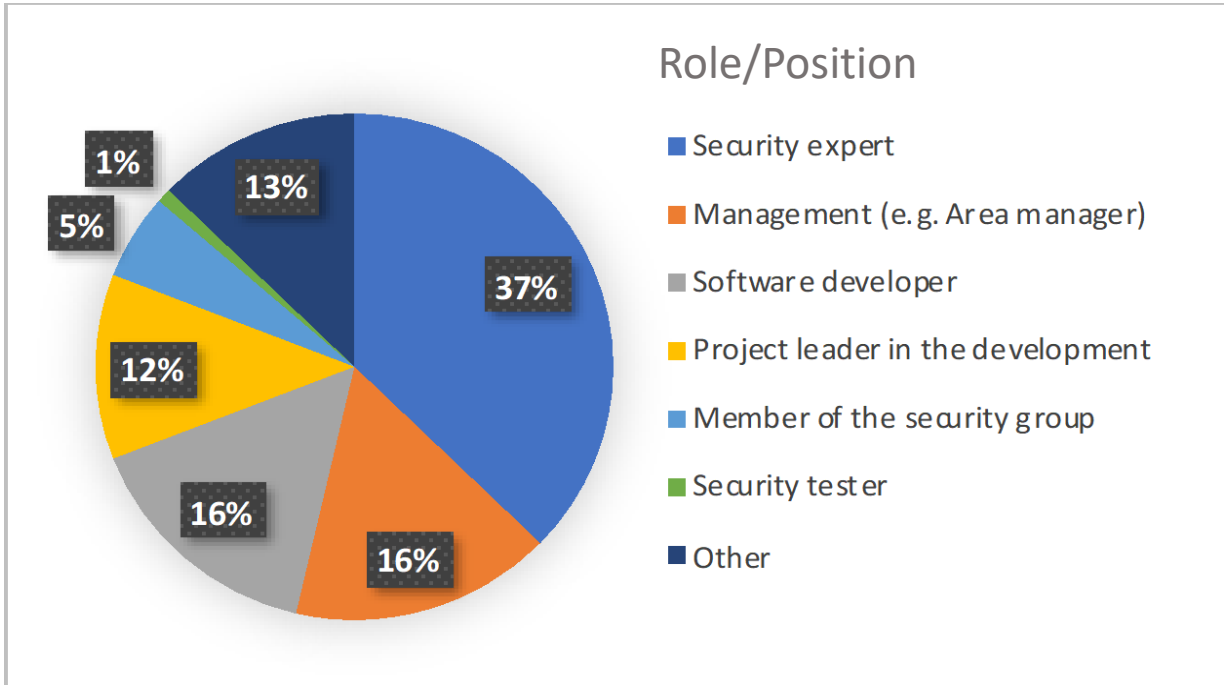


Outline

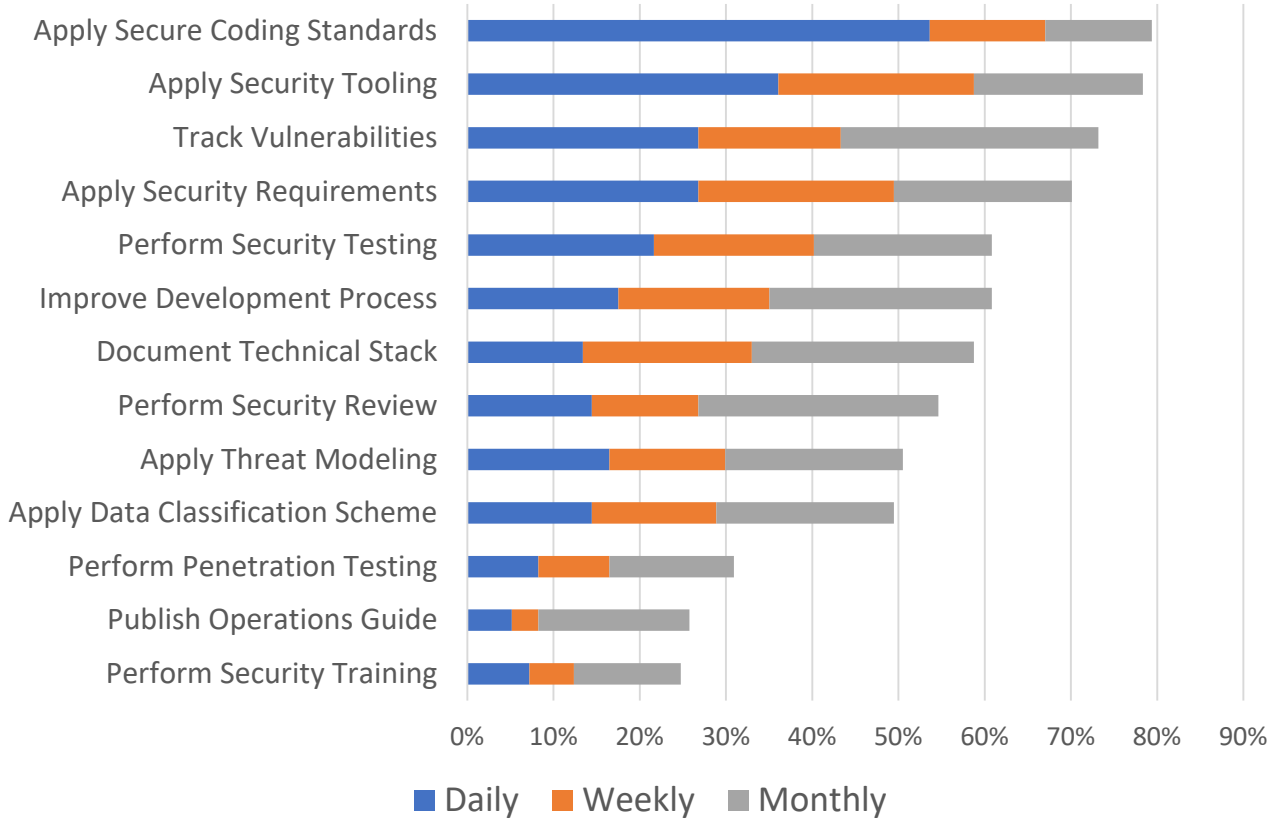
- Cost-effectiveness of secure software development
- Sources of cost in secure software development
  - Security practices
  - Security controls
- Security practices application survey
- Models for costing secure software development
- Open issues and opportunities
- Next steps

Survey

- Participants of the Software Security group on LinkedIn
- 110 complete responses
- 29 countries



Practices Usage



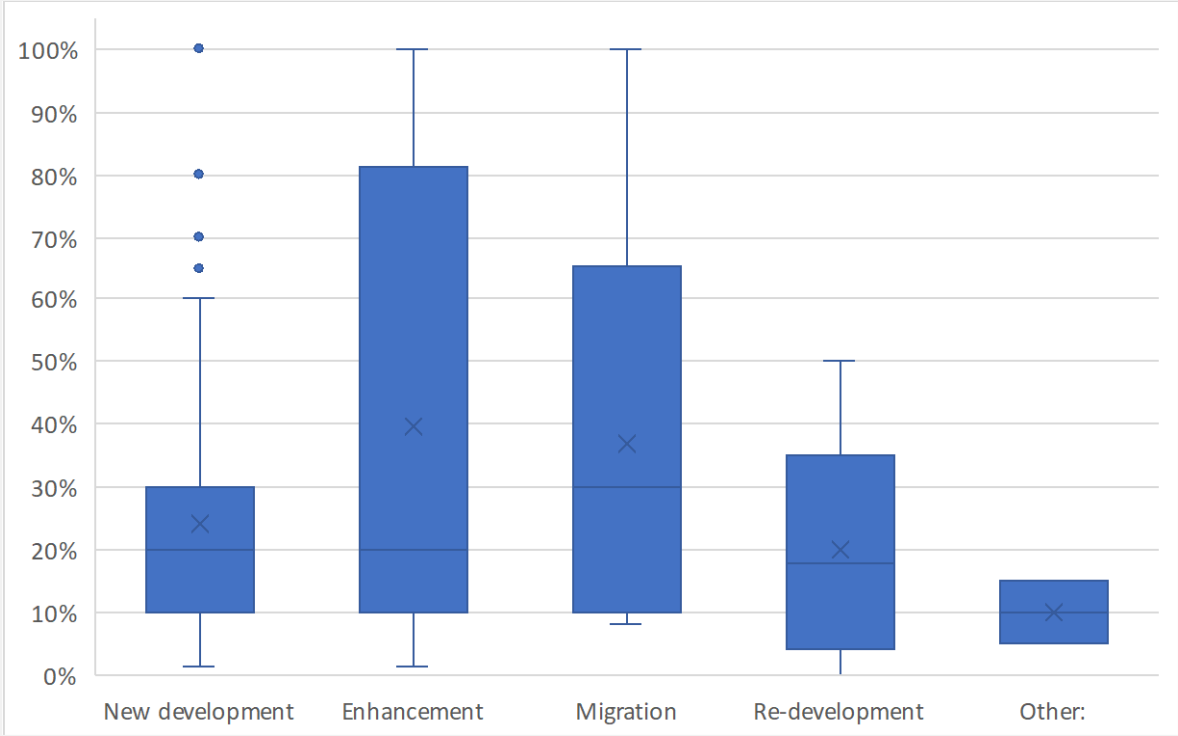
Poll – Security Practices

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."

"Convincing project manager to incorporate security related time and effort."

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

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

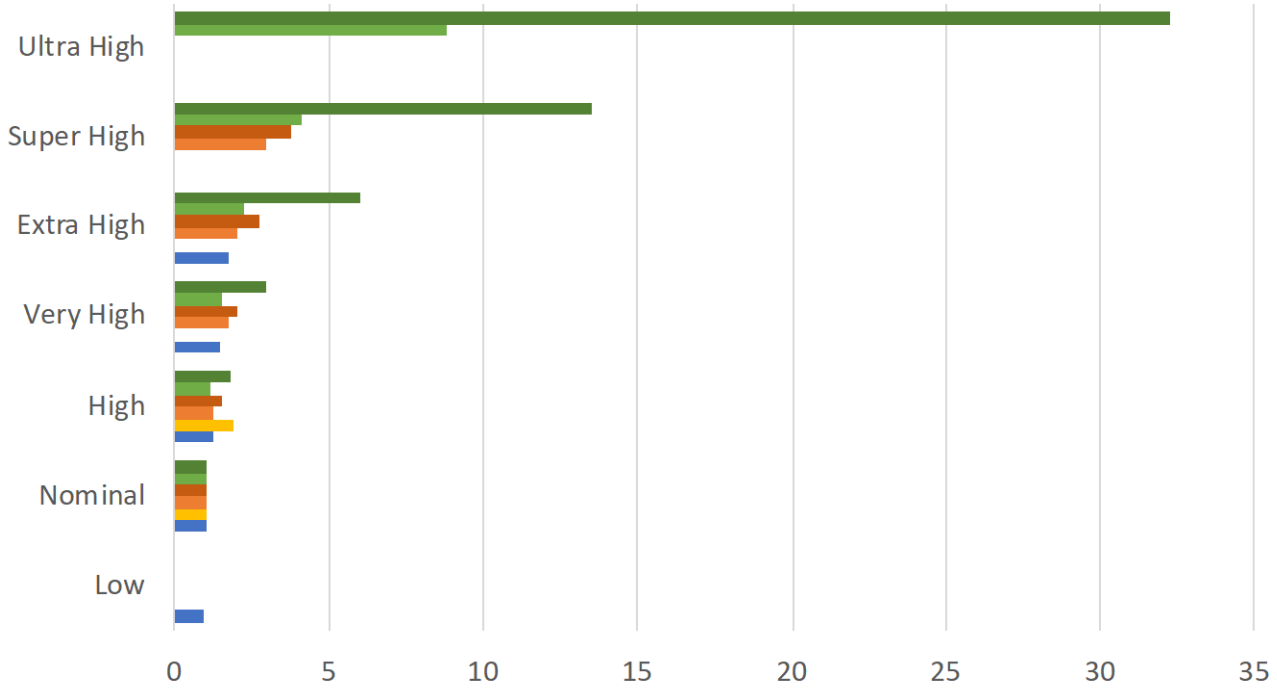
Outline

- 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

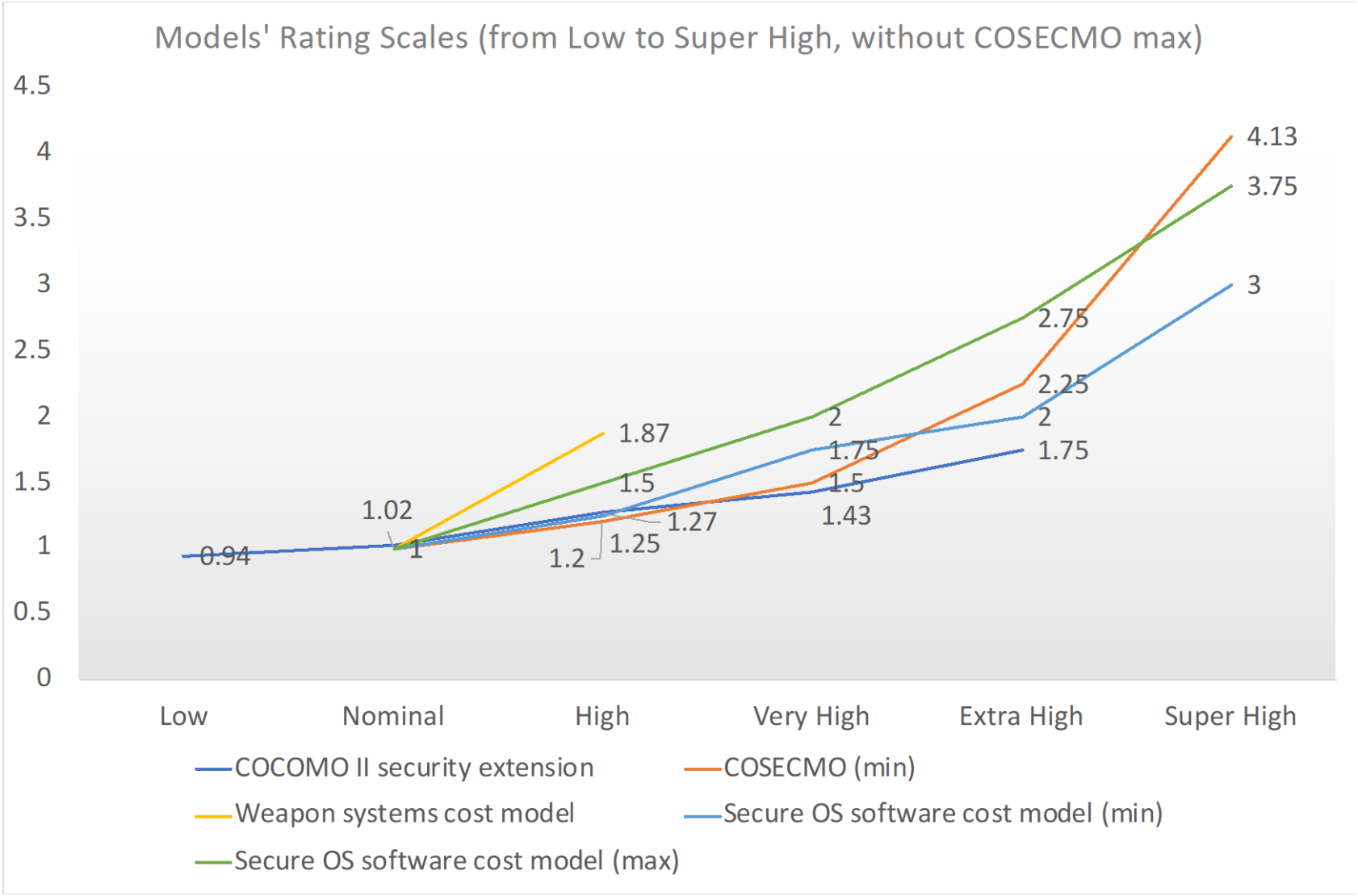
Approaches to Estimating Costs of SWSec

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

Models Compared



	Low	Nominal	High	Very High	Extra High	Super High	Ultra High
COSECMO (max)		1	1.8	3	6	13.5	32.25
COSECMO (min)		1	1.2	1.5	2.25	4.13	8.81
Secure OS software cost model (max)		1	1.5	2	2.75	3.75	
Secure OS software cost model (min)		1	1.25	1.75	2	3	
Weapon systems cost model		1	1.87				
COCOMO II security extension	0.94	1.02	1.27	1.43	1.75		


Models' Rating Scales (from Low to Super High, without COSECMO max)
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
0.94
1.02
1
1.87
1.5
1.27
1.2
1.25
2
1.75
1.5
1.43
2.75
2.25
2
1.75
4.13
3.75
3
Low
Nominal
High
Very High
Extra High
Super High
COCOMO II security extension
COSECMO (min)
Weapon systems cost model
Secure OS software cost model (min)
Secure OS software cost model (max)

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

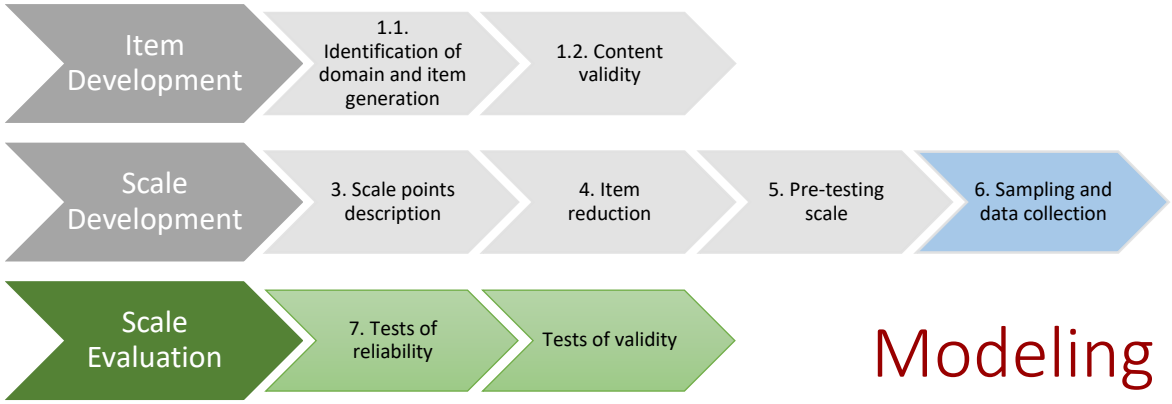
Opportunities for Validation

- 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

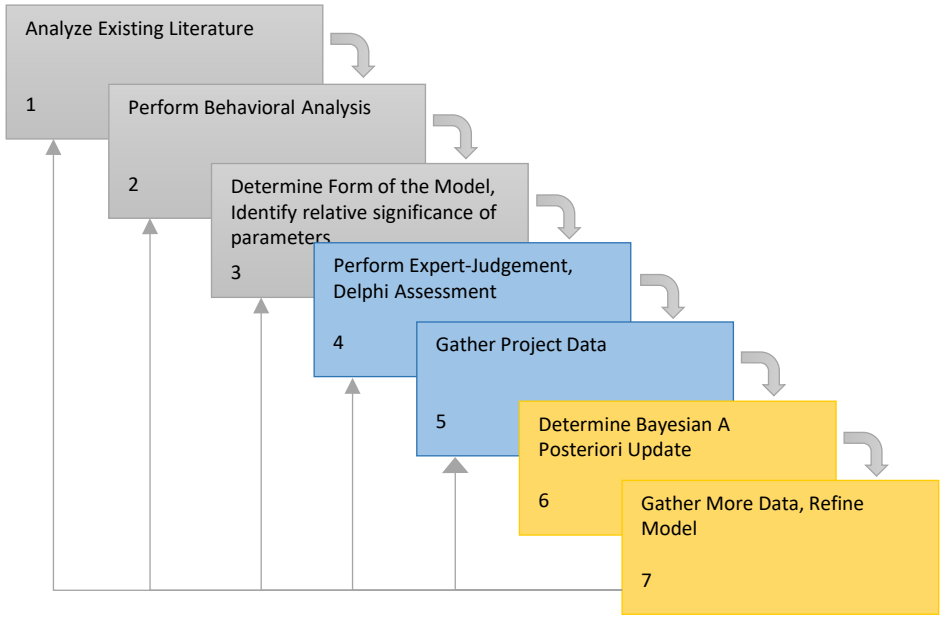
Outline

- 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



Modeling Methodology



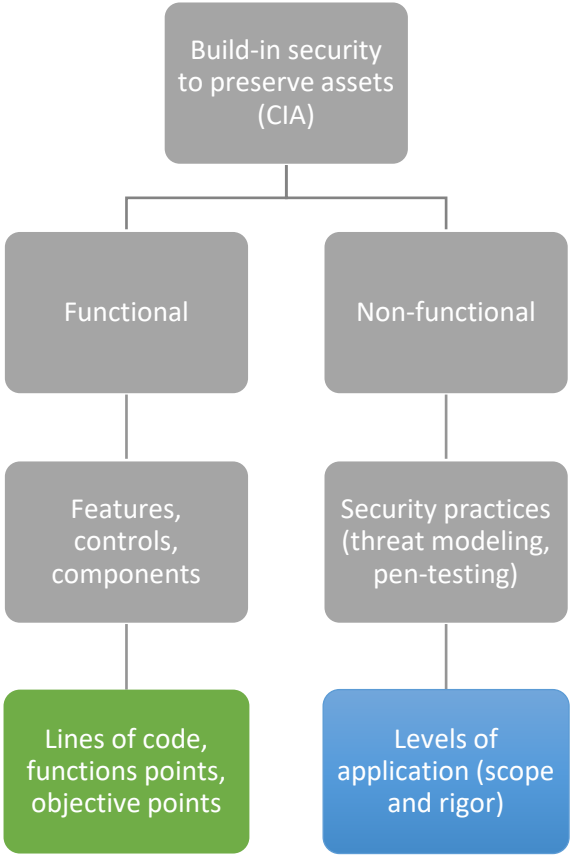
Proposed Model Form

$$PM = A \cdot Size^{E} \cdot SECU \cdot \prod_{i-1}^{n} EM_i$$

SECU: Effort multiplier for secure software development level

$$\begin{cases} Size = Functional\ Size + Security\ Features\ Size \\ \quad OR \\ Size = Functional\ Size \cdot SSF \end{cases}$$

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

Projects' Data → Manual Data Collection Form

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-R^2 (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

- N. A. S. Abdullah, R. Abdullah, M. H. Selamat, and A. Jaafar, "Extended function point analysis prototype with security costing estimation," in *2010 International Symposium on Information Technology*, Jun. 2010, vol. 3, pp. 1297–1301, doi: 10.1109/ITSIM.2010.5561460.
- R. Böhme, "Security Metrics and Security Investment Models," in *Advances in Information and Computer Security*, vol. 6434, I. Echizen, N. Kunihiro, and R. Sasaki, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 10–24.
- E. Colbert and D. B. Boehm, "Cost Estimation for Secure Software & Systems," in *ISPA/SCEA 2008 Joint International Conference*, The Netherlands, 2008, p. 9.
- R. Kuhn, M. Raunak, and R. Kacker, "It Doesn't Have to Be Like This: Cybersecurity Vulnerability Trends," IT Professional, vol. 19, no. 6, pp. 66–70, Nov. 2017.
- T. Lee, T. Gu, and J. Baik, "MND-SCEMP: an empirical study of a software cost estimation modeling process in the defense domain," *Empir Software Eng*, vol. 19, no. 1, pp. 213–240, Feb. 2014, doi: 10.1007/s10664-012-9220-1.
- G. McGraw, *Software Security: Building Security In*, 1 edition. Upper Saddle River, NJ: Addison-Wesley Professional, 2006.
- A. Rashid, H. Chivers, G. Danezis, E. Lupu, and A. Martin, "The Cyber Security Body of Knowledge." 2019, [Online]. Available: https://www.cybok.org/.
- D. J. Reifer, B. W. Boehm, and M. Gangadharan, "Estimating the Cost of Security for COTS Software," in *COTS-Based Software Systems*, Feb. 2003, pp. 178–186, doi: 10.1007/3-540-36465-X_17.
- E. Venson, R. Alfayez, G. Marília M. F., F. Rejane M. C., and B. Boehm, "The Impact of Software Security Practices on Development Effort: An Initial Survey," in 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), Sep. 2019, pp. 1–12, doi: 10.1109/ESEM.2019.8870153.
- E. Venson, X. Guo, Z. Yan, and B. Boehm, "Costing Secure Software Development: A Systematic Mapping Study," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, New York, NY, USA, 2019, p. 9:1–9:11, doi: 10.1145/3339252.3339263.
- Y. Yang, J. Du, and Q. Wang, "Shaping the Effort of Developing Secure Software," *Procedia Computer Science*, vol. 44, no. Supplement C, pp. 609–618, Jan. 2015, doi: 10.1016/j.procs.2015.03.041.