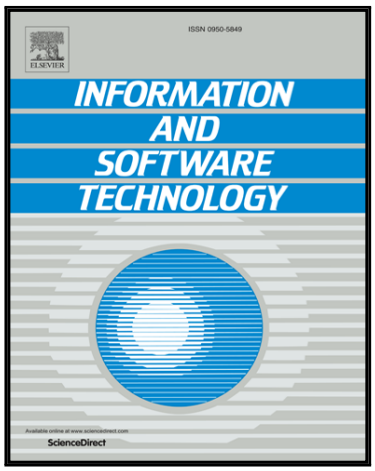

Mapping the Field of Software Life Cycle Security Metrics

Patrick Morrison, David Moye, Rahul Pandita, Laurie Williams

PII: S0950-5849(18)30096-X
DOI: 10.1016/j.infsof.2018.05.011
Reference: INFSOF 5998

To appear in: *Information and Software Technology*

Received date: 1 July 2017
Revised date: 29 May 2018
Accepted date: 29 May 2018

Please cite this article as: Patrick Morrison, David Moye, Rahul Pandita, Laurie Williams, Mapping the Field of Software Life Cycle Security Metrics, *Information and Software Technology* (2018), doi: 10.1016/j.infsof.2018.05.011

Mapping the Field of Software Life Cycle Security Metrics

Patrick Morrison[a,*], David Moye[a], Rahul Pandita[a,b], Laurie Williams[a]

[a]North Carolina State University,Raleigh, NC, USA
[b]Phase Change Software, LLC, Golden, CO, USA

Abstract

Context: Practitioners establish a piece of software's security objectives during the software development process. To support control and assessment, practitioners and researchers seek to measure security risks and mitigations during software development projects. Metrics provide one means for assessing whether software security objectives have been achieved. A catalog of security metrics for the software development life cycle could assist practitioners in choosing appropriate metrics, and researchers in identifying opportunities for refinement of security measurement.

Objective: *The goal of this research is to support practitioner and researcher use of security measurement in the software life cycle by cataloging security metrics presented in the literature, their validation, and the subjects they measure.*

Method: We conducted a systematic mapping study, beginning with 4,818 papers and narrowing down to 71 papers reporting on 324 unique security metrics. For each metric, we identified the subject being measured, how the metric has been validated, and how the metric is used. We categorized the metrics, and give examples of metrics for each category.

Results: In our data, 85% of security metrics have been proposed and evaluated solely by their authors, leaving room for replication and confirmation through field studies. Approximately 60% of the metrics have been empirically evaluated, by their authors or by others. The available metrics are weighted heavily toward the implementation and operations phases, with relatively few metrics for requirements, design, and testing phases of software development. Some artifacts and processes remain unmeasured. Measured by phase, Testing received the least attention, with 1.5% of the metrics.

Conclusions: At present, the primary application of security metrics to the software development life cycle in the literature is to study the relationship between properties of source code and reported vulnerabilities. The most-cited and most used metric, vulnerability count, has multiple definitions and operationalizations. We suggest that researchers must check vulnerability count definitions when making comparisons between papers. In addition to refining vulnerability measurement, we see research opportunities for greater attention to metrics for the requirement, design, and testing phases of development. We conjecture from our data that the field of software life cycle security metrics has yet to converge on an accepted set of metrics.

Keywords: Metrics, Measurement, Security.

1. Introduction

Software system builders, owners, operators, and users seek assurance that their interests, communications, and data are secure. McGraw [1] defines software security as "engineering software so that it continues to function correctly under malicious attack." Many aspects of the software development life cycle, including software requirements, design, implementation, and testing contribute to the security of the running software. Measuring whether security has been appropriately addressed at each stage of software development is likely to be a precondition to assuring the release of secure software. We seek to investigate whether some fundamental security questions that development teams

*Corresponding author
Email addresses: pmorrison@ncsu.edu (Patrick Morrison), cdmoye@ncsu.edu (David Moye), rpandita@phasechange.ai (Rahul Pandita), lawilli3@ncsu.edu (Laurie Williams)
URL: http://www.rahulpandita.me/ (Rahul Pandita), https://collaboration.csc.ncsu.edu/laurie/ (Laurie Williams)