SOFTWARE SECURITY METRICS

Tao Xie and Laurie Williams

{xie, williams}@csc.ncsu.edu

Computer Science

NC STATE UNIVERSITY

"If you can not measure it, you can not improve it." **-- Lord Kelvin. Software security metrics are a critical component of science of security.**

A well-defined and fully validated suite of software security metrics are desirable to take into account

- **► software internal attributes**
- **► developers who develop the software**
- **► attackers who attack the software**
- **► users who use the software.**

"METRICS are desirable for every security touch points"

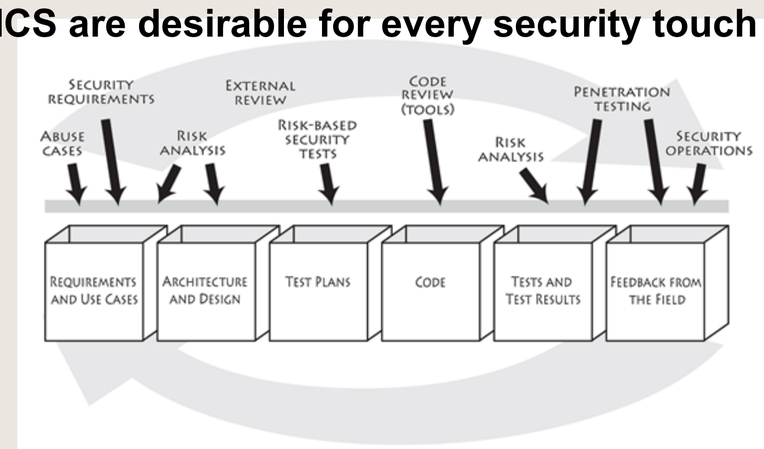

Image Source: "http://www.cigital.com/justice-league-blog/wp-content/uploads/2007/07/touchpoints.gif"

SCOPE

We aim to investigate existing and new security metrics to predict which code locations are likely to contain vulnerabilities. In particular, we outlined following broad categories to advance existing software engineering research in areas of software security metrics:

1) Security Metrics for Incorporating Global Attack Trends

2) Grounded Theory for the Identification of Security Metrics

3) Security Metrics for Incorporating Run-time Information from Deployed Systems

1) Security Metrics for Incorporating Global Attack Trends

National Vulnerability Database (NVD) is US Government maintained repository of standards-based vulnerability management data. In particular, NVD includes databases of

- security checklists
- misconfigurations
- impact metrics.
- security related software flaws
- product names

Target Security property: *Generic*

Target Software System: *Generic Configuration Related Software*

Approach:

1) Collect configuration information from NVD

2) Apply mining algorithms to infer vulnerability prediction metrics based on configurations

3) Refine inferred metrics using Natural Language Processing Techniques on vulnerability descriptions

4) Systematically validate the inferred metrics on EHR systems

2) Grounded Theory for the Identification of Security Metrics

With grounded theory, we examine data without a hypothesis. As the examination progresses, patterns generally begin to emerge in the data. We propose to use the stated methodology to discover new metrics with regards to software vulnerabilities.

Target Security property: *Non-Repudiation*

Target Software System: *Electronic Health Record (EHR) Systems*

Approach:

1) Gather set of log attributes (based on technical documentation and actual log implementation in open source EHR systems Tolven eCHR, OpenEMR, PatientOS, and WorldVista)

2) perform user studies to determine what attributes are crucial for ensuring non-repudiation within a software system as *"forensic-ability"* attributes

3) Propose a *"forensic-ability"* metric that captures the quantified observation and then Validate the performance of the *"forensic-ability"* metric

3) Security Metrics for Incorporating Run-time Information from Deployed Systems

The limited resources and steep delivery schedules of software systems leads to inefficient developer-site testing, often taking a toll on software quality and security. We examine the run-time information from deployed software; producing security-metrics to prioritize security related debugging an assisting in better design of future iterations

Target Security property: *Privacy, Information Leakage*

Target Software System: *Smartphone Software (Android Platform)*

Approach:

1) Create a static analysis framework to analyze Android application

2) In particular, create a mapping of how components interact at run-time

3) Use the mapping information to monitor and detect security vulnerabilities

4) Summarize and analyze the results to produce security-metrics

5) Evaluate the proposed security metrics

Real World Applications

1) **Security Metrics for Incorporating Global Attack Trends**

► *check for likely vulnerabilities in the software system under analysis using the vulnerability metric*

► *use the vulnerability metric as an input to software architects for choosing components while designing software*

2) Grounded Theory for the Identification of Security Metrics

► *use the forensic-ability metric to improve existing EHR systems to tackle the problem of repudiation*

3) Security Metrics for Incorporating Run-time Information from Deployed Systems

► *check for likely vulnerabilities existing Smartphone applications*

► *use the vulnerability metric to predict vulnerabilities across different versions of Smartphone platforms*

Progress

1) **Security Metrics for Incorporating Global Attack Trends**

► acquired configuration information from NVD

► created NLP infrastructure to analyze vulnerability description

► *TODO: Use data-mining algorithms to infer metrics*

2) Grounded Theory for the Identification of Security Metrics

► identified logging attributes related to non-repudiation in log files of existing EHR systems

► TODO: propose a security metric *"forensic-ability"* based on identified logging attributes

3) **Security Metrics for Incorporating Run-time Information from Deployed Systems**

► created static analysis infrastructure to create mapping of how components interact with each other.

► *TODO: Incorporate the mapping to perform run-time analysis*

► *TODO: summarize the results to propose a security metrics*

2012 Science of Security Community Meeting

Nov. 29-30, 2012

National Harbor, MD

Vote Here

Logo #1 Logo #2