Systematically Developing Prevention, Detection, and Response Patterns for Security Requirements

ESPRE 2016

Maria Riaz, Sarah Elder, Laurie Williams
Realsearch
Sep 12th 2016
Agenda

• Motivation & Objectives

• Methodology

• Patterns Developed from NIST Security and Privacy Controls

• Evaluation: Security Requirement Analysis of a Network Product

• Conclusion
Motivation

Integrating Security Requirements with System Functionality

- 92% of the vulnerabilities are in the system implementation [NVD]
- Limited Security Expertise and Resources [RePa12]

[CWE-SANS Top 25 Vulnerabilities]

<table>
<thead>
<tr>
<th>CWE ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-09</td>
<td>Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')</td>
</tr>
<tr>
<td>CWE-78</td>
<td>Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')</td>
</tr>
<tr>
<td>CWE-494</td>
<td>Download of Code Without Integrity Check</td>
</tr>
<tr>
<td>CWE-829</td>
<td>Inclusion of Functionality from Untrusted Control Sphere</td>
</tr>
<tr>
<td>CWE-386</td>
<td>Missing Authentication for Critical Function</td>
</tr>
<tr>
<td>CWE-862</td>
<td>Missing Authorization</td>
</tr>
<tr>
<td>CWE-307</td>
<td>Improper Restriction of Excessive Authentication Attempts</td>
</tr>
<tr>
<td>CWE-250</td>
<td>Execution with Unnecessary Privileges</td>
</tr>
<tr>
<td>CWE-911</td>
<td>Missing Encryption of Sensitive Data</td>
</tr>
</tbody>
</table>

Missing Security-Related Functionality

https://www.sans.org/top25-software-errors/
## Security Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality (C)</td>
<td>The degree to which the &quot;data is disclosed only as intended“ [SECPAT]</td>
</tr>
<tr>
<td>Integrity (I)</td>
<td>“The degree to which a system or component prevents unauthorized access to, or modification of, computer programs or data.” [IEEE]</td>
</tr>
<tr>
<td>Availability (A)</td>
<td>&quot;The degree to which a system or component is operational and accessible when required for use.&quot; [IEEE]</td>
</tr>
<tr>
<td>Identification &amp; Authentication (IA)</td>
<td>The need to establish that &quot;a claimed identity is valid&quot; for a user, process or device. [NIST-SP800-33]</td>
</tr>
<tr>
<td>Accountability (AY)</td>
<td>Degree to which actions affecting software assets &quot;can be traced to the actor responsible for the action“ [SECPAT]</td>
</tr>
<tr>
<td>Privacy (PR)</td>
<td>The degree to which “an actor can understand and control how their information is used.” [RE14]</td>
</tr>
</tbody>
</table>
Related Work: Identifying Security Requirements

• **Identifying System Implementation Requirements**
  - Identifying and reusing explicitly stated security requirements [Schneider12]
  - Identifying implied security requirements using security goals and templates [Riaz14]

• **Reusable Security Requirements and Patterns**
  - Documenting security requirements templates and patterns [Daramalo12]
  - *Mapping study on reuse*: taxonomies of threats and vulnerabilities, assets; security requirements [Souag15]

• **Analysis of Security Knowledge Sources**
Research Objective

To support analysts in identifying and specifying security requirements by developing a systematic process for identifying security requirements patterns from existing knowledge sources.
Identifying Security Goals

Security Actions

- Prevent
- Detect
- Respond to

Security Properties

- Confidentiality (C)
- Integrity (I)
- Availability (A)
- Id & Authentication (ID)
- Accountability (AY)
- Privacy (PR)

a breach of

<Prevent> a breach of <Identification & Authentication> of the system users
Pattern Identification Methodology

Knowledge Source

Identify security goals

Group by related security goals

Provide context and traceability

Security requirements patterns
Requirements Patterns Suggestion:
Pattern Representation – Example Pattern

• **Name:** R-AY-1: Respond to failures in accountability.
  • **Problem:** <respond to> a breach of <Accountability> of user actions.

• **Context:** An attacker may compromise the mechanisms for accountability to covertly perform malicious activity in the system.
  o Scope: Security Functionality
  o ...

• **Solution:** The system shall:
  a) respond to audit processing failures by alerting <authorized user>.
  b) provision for alternate audit capability to record <designated actions> if the primary audit capability fails.

• **Source:** AU-5, AU-15.

• **See Also:** P-ALL-1: Enable continuous monitoring, D-ALL-1: Monitoring for security incidents, …
NIST Special Publication 800-53:

- Security and Privacy Controls for Federal Information Systems and Organizations
- Published by the National Institute of Standards and Technology (US)
- Guidelines for Federal Agencies, widely used
- 240 controls in 17 control families
- Examined 114 controls related to software implementation

https://pages.nist.gov
Requirements Patterns Suggestion [RePa2012]: Systematic Process for Developing Patterns

<table>
<thead>
<tr>
<th></th>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>44</td>
<td>14</td>
<td>10</td>
</tr>
<tr>
<td>Integrity</td>
<td>55</td>
<td>21</td>
<td>16</td>
</tr>
<tr>
<td>Availability</td>
<td>26</td>
<td>11</td>
<td>20</td>
</tr>
<tr>
<td>Identification &amp; Authentication</td>
<td>28</td>
<td>14</td>
<td>9</td>
</tr>
<tr>
<td>Accountability</td>
<td>13</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>Privacy</td>
<td>31</td>
<td>15</td>
<td>6</td>
</tr>
</tbody>
</table>

AU-5: Respond to Audit Processing Failures
The system shall respond to audit processing failures by alerting <authorized user>.

AU-15: Alternate Audit Capability
The system shall have provision for alternate audit capability to record <designated actions> if the primary audit capability fails.

R-AY-1: Respond to failures in accountability
Requirements Patterns Suggestion:
Pattern Representation – Example Pattern

• **Name:** R-AY-1: Respond to failures in accountability.
• **Problem:** <respond to> a breach of <Accountability> of user actions.

• **Context:** An attacker may compromise the mechanisms for accountability to covertly perform malicious activity in the system.
  - Scope: Security Functionality
  - ...

• **Solution:** The system shall:
  a) respond to audit processing failures by alerting <authorized user>.
  b) provision for alternate audit capability to record <designated actions> if the primary audit capability fails.

• **Source:** AU-5, AU-15.

• **See Also:** P-ALL-1: Enable continuous monitoring, D-ALL-1: Monitoring for security incidents.

35 security requirements patterns [20 prevention, 7 detection, 8 response]
Evaluation:
Case Study of a Networking Product

• Security Requirements Document for the Product
  o 108 security requirements

• Evaluation
  o Overlap between requirements in the product document and our patterns
  o Requirements in the product document that our patterns don’t cover
  o Additional patterns that are applicable but not in product document
Evaluation:  
Gap Analysis

- **Overlap (105 out of 108)**
- **Requirements missed by our process**
  - 2 non-technical (Training of developers and testers)
  - 1 related to installing a specific operating system (partially identified)
- **Additional security requirements patterns**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prevention</strong></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>P-ALL-2: Limit system exposure to persistent attackers.</td>
</tr>
<tr>
<td></td>
<td>Communication</td>
</tr>
<tr>
<td></td>
<td>P-C_PR-2: Prevent unauthorized remote sensing and activation.</td>
</tr>
<tr>
<td></td>
<td>Communication</td>
</tr>
<tr>
<td></td>
<td>P-I_A_ID-1: Security during name and address resolution.</td>
</tr>
<tr>
<td><strong>Detection</strong></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>D-I-2: Detect vulnerabilities in the system.</td>
</tr>
<tr>
<td><strong>Response</strong></td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>R-C_PR-1: Respond to unauthorized disclosure of information.</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>R-CIA-1: Respond to system failure conditions.</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>R-I-1: Respond to vulnerabilities in the system.</td>
</tr>
</tbody>
</table>
Evaluation:
Overlap between Product Document (PSB) and Patterns
Limitations and Future Work

Limitations

• Quality and comprehensiveness of patterns
• Instantiating requirements from the patterns

Future Work

• Further evaluation of process and patterns usability
Contributions:

• A systematic process for identifying security requirements patterns in existing knowledge sources
  ➢ Traceability between instantiated requirements and knowledge sources

• A catalogue of 35 security requirements patterns developed from NIST security and privacy controls
  ➢ [https://sites.google.com/site/secruritylocatordiscoverer/](https://sites.google.com/site/secruritylocatordiscoverer/)
References

References


[ICSE 2016] Industrial case study with Cisco – To Submit


Contact:

Maria Riaz – mriaz (at) ncsu.edu

Sarah Elder – seelder (at) ncsu.edu

Laurie Williams – williams (at) csc.ncsu.edu