Asset-Centric Security Risk Assessment of Software Components

Tobias Rauter, Institute for Technical Informatics

2016-01-19
Introduction

1. Introduction
2. Approach
3. Evaluation
4. Conclusion and Outlook
Context/Motivation

- Security in complex (software) systems
- Restrict access to critical resources
  - What are these resources?
- Separation of privilege
  - How?
- Security assessment and audits
  - Which parts?
Primary Security Goals of Your Organization

- Protect valuable objects (Assets)
  - value (=> impact)
  - exposure (=>probability)
- Risk

<table>
<thead>
<tr>
<th>Business Impact</th>
<th>Very Low</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Low</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>High</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Very High</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

Likelihood of Incident Scenario
Risk Management

- Basically: Identify -> Rate -> Treat
- On organizational level
  - Various (somewhat similar) approaches
  - Here: ISO 27005
Software Security

- ’Security by Design’
- Critical resources?
  - Organizational level assets mapped into SW architecture
- SW components use or protect these assets
  - ’Secondary assets’
  - Useful in organizational level assessment?
  - Asset risks depend on SW components?
- Critical Components?
This Work: Combination

- Feed-backed high to low level risk analysis
  - Use information of high level risk analysis in threat modeling
  - Feed-back adjustments on asset risks
- Classification based on criticality (of accessed assets)
- Separation of privilege with special components
- Evaluation with manufacturing system use-case
Approach

Topic

1. Introduction

2. Approach

3. Evaluation

4. Conclusion and Outlook
Overview

High-Level Risk Management according to ISO/IEC 27005

Context Establishment

Risk Assessment

Risk Identification

Risk Estimation

Risk Evaluation

Risk Treatment

Risk Acceptance

Software Risk Assessment

Asset Transformation

Component Classification

Trust Domain Reduction

Threat Modeling and Component Risk Assessment

Additional Threats to Assets

Assets
Asset Mapping

Server Room

Server 1
Risk Rating: 3

Server 2
Risk Rating: 5

DB System
Risk Rating: 10

Banking Application
Risk Rating: 10

Private Data
Risk Rating: 20

Money Transfer Function
Risk Rating: 20

Banking Application

User Interface

Component 1

Component 2

DB System

DB Interface

Private Data
Component Model

- Architectural model of software system
- Simple component model with (non-directed) data-flows
  - Software components
  - Assets
**Component Model**

- **Filter**
  - `inAssets : Set<Asset>`
  - `outAssets : Set<Asset>`

- **Privilege**
  - `Name`
  - `type : PrivilegeType`
  - `mode : PrivilegeAccessMode`

- **Component**
  - `Name`
  - `privileges : Set<Privileges>`
  - `directConnections : Set<Component>`

- **Asset**
  - `name`
  - `accessCriticality`
  - `typeName`
  - `accessPrivilege : Privilege`
  - `riskFactors : Map<Privilege, Weight>`
Component Classification

- Privilege rating
  - Value of accessed assets + 'risk factors'
- Represents impact-part of the risk
  - Probability may result from threat modeling process
- Access via privileges (foundation for future work)
Component Classification: Risk Factor

- Privileges may interfere
  - Access to sensitive data
  - Exposed to network
- ’Risk Factors’ are quantified per asset
- Map privilege => value
Component Classification: Privilege Rating

- Privilege Rating $PR$ of Component $C$
- 'Value' $Crit()$ of all accessed assets $A$
- Risk factors $RF$ of this assets for all other privileges $P$

$$PR(C) = \sum_{A=\text{Assets}(C)} \left( Crit(A) + \sum_{P=\text{Priv}(C)} RF(A, P) \right)$$
Approach

Classification: Component Composition

- Merge Privileges
- Calculate Privilege Rating
- Directed information flows
  - Future work
- Restricting components
  - Filter
Filter Components

- Special component
- Transform assets:

\[ A \Rightarrow \emptyset (block) \quad (1) \]
\[ A \Rightarrow A' (reduction) \quad (2) \]
\[ A, B \Rightarrow C (transformation) \quad (3) \]
Filter Components

- Authentication
  - 'All Data' $\Rightarrow$ 'Data of User X'
- Encryption
  - 'Data', 'Key' $\Rightarrow$ 'Encrypted Data'
Trust Domain

- Components that share privileges
- Minimize size (attack surface)
- Add filter components
  - Separation, Reduction
- Iterate until acceptable risk and size
Approach

Threat Modeling

- Prioritize
  - High risk components (domains)
  - Protection components (filter on borders)
- Unleashes new threats
  - Feed back to high-level risk management process
Evaluation

Topic

1. Introduction

2. Approach

3. Evaluation

4. Conclusion and Outlook
Use Case

- Manufacturing system
- Embedded control systems
- Manufatures receive test equipment
- Central database (of device vendor)
  - Send production data
  - Get images, certificates, etc.

Central server simplified for this paper
System Overview

- LAN: 5
- WAN: 10
- Webserver
- Application
- DB Access
- Backup Server
- Credentials: 100
- Man. Data: 20
- Common: 0
- Test Data Interface
- [Asset Name]: criticality
- Component Name

Tobias Rauter, ITI
2016-01-19
## Asset Mapping

<table>
<thead>
<tr>
<th>Name</th>
<th>Crit(A)</th>
<th>Risk Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentials</td>
<td>100</td>
<td>Network(WAN), 10</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>10</td>
<td>Network(WAN), 5</td>
</tr>
<tr>
<td>Common</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LAN</td>
<td>10</td>
<td>Network(WAN), 2</td>
</tr>
<tr>
<td>WAN</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>User-Specific Data</td>
<td>5</td>
<td>Network(WAN), 2</td>
</tr>
<tr>
<td>Test Data</td>
<td>5</td>
<td>Network(WAN), 2</td>
</tr>
</tbody>
</table>
Trust Domain Reduction

Evaluation

Tobias Rauter, ITI
2016-01-19
# Trust Domain Reduction

<table>
<thead>
<tr>
<th>Component Name</th>
<th>w/o Filter</th>
<th>with Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Domain</td>
<td>Criticality</td>
</tr>
<tr>
<td>Webserver</td>
<td>0</td>
<td>1120</td>
</tr>
<tr>
<td>Application</td>
<td>0</td>
<td>1120</td>
</tr>
<tr>
<td>DB Access</td>
<td>0</td>
<td>1120</td>
</tr>
<tr>
<td>Test Interface</td>
<td>0</td>
<td>1120</td>
</tr>
<tr>
<td>Backup Service</td>
<td>0</td>
<td>1120</td>
</tr>
<tr>
<td>Backup Server</td>
<td>0</td>
<td>1120</td>
</tr>
<tr>
<td>Authenticator</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>User-Specific</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Test-Filter</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Network-Filter</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Evaluation

- Domain 1
  - Full access
  - Critical

- Domain 2
  - Exposed through internet
  - User-specific data
  - Threat modeling should be done

- Domain 3
  - Relatively few privileges
  - Weakest security requirements
Component criticality is reduced drastically
Focus threat modeling efforts
New threats and assets are feeded back to high-level RM

- Supplementing threat trees for assets
- Ease decision for resource allocation and treatment strategies
Conclusion and Outlook

Topic

1. Introduction

2. Approach

3. Evaluation

4. Conclusion and Outlook
Conclusion

- Risk management in complex SW systems
- Systematic approach
- High-level assessment supports SW-assessment
- Systematic reduction of trust domains
- Prioritized threat modeling
- Feedback for high-level assessment
Future Work

- Directed information flows
- Fine grained privileges (read, write, etc.)
- Find good values for risk factors
- Automate trust domain reduction