Assessing information security maturity in an industrial company

Ekaterina Rudina
Critical Infrastructure Defense
KL ICS-CERT
Contents

1. Motivation
2. Security Maturity assessment as a base for security processes in IIoT
3. Security Maturity Model, its purpose and intended use
4. Security Maturity enhancement process
5. Identifying and targeting required Security Maturity level
6. Conclusions and further work
Security Facets
Which, when, where, and to which extent?

Security policy
Access control
Patch management

Internet of Things
Big data
Mobile threats
Financial phishing attacks

Threat modeling
Asset management
Incident response

Risk attitude
Vulnerability assessment
Difference between Security Level and Security Maturity Level

SECURITY LEVEL
is a degree for the implementation of security practices, mechanisms, and procedures

Consistency in the implementation
Assurance on the implementation
Confidence in assurance cases

SECURITY MATURITY LEVEL
is a degree of understanding of the current Security Level, its benefits, and cost of its support
Example. Approaches to Threat Modeling facet

++ valid across various IIoT domains.
-- sometimes they cannot be properly applied to the particular domain
-- in some other cases they do not cover the specific risks

**Horizontal models:**
general (such as STRIDE or CAPEC classification)
technology specific (OWASP Top 10)

**Vertical models:**
valid within one domain (LINDDUN, PASTA, template by NCC)

++ take into account the specific risks for the domains
-- may cover the narrow set of technologies
-- some “vertical” models address only certain objectives

Combining the methods and models is the best option
General objective:
Stakeholders collaboration in the process of getting the mature state

Different stakeholders consider the same aspects from the different viewpoints

Business level stakeholders define the security goals*

Technical level implements the mechanisms and procedures**

* Business level here means security aware stakeholders (not CEO but CISO)

** Technical level – not codewriters but architects, high-level developers, etc.
Creating the Security Maturity Target

Gap Analysis

Planning the roadmap

Security Maturity Assessment

Security Maturity Enhancement

Collaboration

Business level stakeholder
CISO level

Technical level stakeholders
Architects
High-level Developers
The Process

State 1 (initial)
- Perform evaluation
- Implement Plans
- Prioritize and Plan
- Analyze Identified Gaps

State 2
- Perform evaluation
- Implement Plans
- Prioritize and Plan
- Analyze Identified Gaps

State n
- Perform evaluation
- Implement Plans
- Prioritize and Plan
- Analyze Identified Gaps

Security Maturity Target

Measure, compare, describe, estimate the progress, visualize
Security Maturity Target

SM Target defines what the 100% Security Maturity for the system is.

- **Business level - Strategist**
  - Knows the concerns.
  - Determines the objectives for collaboration.

- **Business Level - Security Context Aware Practitioner**
  - Knows the Context.
  - Creates the new Target/
  - Reuses the Profile/...

- **Technical level stakeholders - Architects, High-level Developers**
  - Know the Technical Details.
  - Implement the Roadmap to get the Target.
Measuring scale for the Security Facet

Sophistication and specificity are measured independently.

Every box contains Business objectives/
Assessment guidance/
Enhancement guidance.

General  IIoT sector specific  System specific
The detailed scale

The rows describe the measure of the comprehensive, consistent, and highly assured implementation of security controls.

The columns relate to the customized, technically appropriate approach to the implementation of security controls.

<table>
<thead>
<tr>
<th>Sophistication/Specificity measured independently</th>
<th>General</th>
<th>IIoT Sector specific</th>
<th>System specific</th>
</tr>
</thead>
<tbody>
<tr>
<td>No information on of how the Security Facet is applied</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Security Facet is implemented somehow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Security Facet is implemented with taking into account the main use cases</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Security Facet employs the generally accepted methods, classifications, tools, software, etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Security Facet is implemented consistently, using the process-oriented approach</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security Facets and their maturity

- Threat Modeling
- Vulnerability & Patch management
- Compliance/conformance assessment
- Supply chain management

- Secure communications
- Incident handling
- Protection of endpoints
- Recovery and remediation
- ...
The Security Maturity Model

Specificity
Sophistication
Dimensions

Specificity
Sophistication
Domains
EXAMPLE. SM Target

- Security strategy and Governance
- Threat Modeling and Risk Assessment
- Supply Chain and External Dependencies Management
- Identity and Access Management
- Asset, Change and Configuration Management
- Vulnerability and Patch Management
- Situational Awareness
- Event and Incident Response, Continuity of Operations
- Information Sharing and Communication
EXAMPLE. SM State

- Security strategy and Governance
- Threat Modeling and Risk Assessment
- Supply Chain and External Dependencies Management
- Identity and Access Management
- Asset, Change and Configuration Management
- Vulnerability and Patch Management
- Situational Awareness
- Event and Incident Response, Continuity of Operations
- Information Sharing and Communication
EXAMPLE. How to get the Target?

- Security strategy and Governance
- Threat Modeling and Risk Assessment
- Supply Chain and External Dependencies Management
- Identity and Access Management
- Asset, Change and Configuration Management
- Vulnerability and Patch Management
- Situational Awareness
- Event and Incident Response, Continuity of Operations
- Information Sharing and Communication
The Roadmap

Asset, Change and Configuration Management

- **SMM allows choosing the direction and the strategy:**
  - use known security practices (increase maturity)
  - tailor the security processes to the system (increase specificity), or
  - step-by-step increase both parameters
Conclusions, current and further work

Two documents describing the SMM and its use
1. SMM description and intended use
2. SMM details and how to apply

The tool (currently Excel-based) to support the process of setting the SM Target
1. Questionnaire for the business level stakeholders
2. Visualization of SM Target and SM State

Work continues in the Security Applicability WG of Industrial Internet Consortium
A lot of IIC members are already interested in the results
Contributions, comments, reviews are welcomed!
LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com