The MITIGATE Methodology – An Overview

Prof. Christos Douligeris
University of Piraeus, Greece, cdoulig@unipi.gr

in cooperation with
Assoc. Prof. N. Polemi, Dr. S. Papastergiou,
PhD (C.) E.-M. Kalogeraki
ICT Systems

**Infrastructure**
(buildings, terminals, gates, data centers)

**Telecom**
(networks, routers, optical fibers, ..)

**IT equipment / Software**
(servers, navigation, RFID, cameras, ERPs, ..)

**e/m-Services**
(vessel, cargo, inland logistics, ..)

**Information/data**
(coastal, trade, ..)

**Users/ Procedures**
(internal, external, cargo, vessels)
Security is defined as the preservation of:

- **Confidentiality**: Making asset accessible only to those authorized to use it
- **Integrity**: Safeguarding accuracy, identity, completeness of asset and processing methods
- **Availability**: Ensuring that asset is available when required and it is not denied
Security & Safety

- **Security (cyber security):** Ensure the Confidentiality, Integrity and Availability of the ICT systems.

- **Safety (physical security):** Ensure the access control and availability of the physical assets

- ISO/IEC 27001:2005
  followed by draft ISO/IEC 27001:2013 (building a SM system)
- ISO/IEC 27005:2011 (security risk management)
- NIST SP 800-128, 2011
- ISO 31000:2009 Principles and Guidelines on Implementation
- ISO/IEC 31010:2009 RM- RA Techniques
- ISO/IEC 27002:2005 (best practice recommendations)
- AS/NZS 4360:2004 (Australian/New Zealand standard for RM)
Maritime Sector

Information and Communication Technology (ICT) infrastructure

Physical infrastructure

Masquerade

IT equipment

Malicious Code

e/m-Services

Software

Flood

Stevedores

Marines

Platforms

Fire

Thieves & Fraud

Eavesdropping

Terrorist attacks
CYSM - Collaborative Cyber/Physical Security Management System (cysm.eu)

**QUESTION A:** How can we estimate risks of ports’ cyber and physical assets??
CYSM Outputs (cysm.eu)

- CYSM risk assessment (RA) methodology of ports individual ICT assets
- CYSM collaborative tool offering RA services
MEASURES TO ENHANCE MARITIME SECURITY

Cyberphysical relationship in port security

CYSM project – "Collaborative Cyber/Physical Security Management System"

Submitted by the European Commission

SUMMARY

Executive summary: This document provides information on a project funded by the European Commission which aims to address potential gaps in security related to the cyberelements of port infrastructure

Strategic direction: 6.1

High-level action: 6.1.1

Planned output: 6.1.1.1

Action to be taken: Paragraph 9

Related document: MSC 94/21, paragraph 4.7
CYSM Consortium
## Identifying dependencies:

### Dependency graphs

<table>
<thead>
<tr>
<th>Dependent Type</th>
<th>Dep. Description</th>
<th>SImp</th>
<th>Imp Type</th>
<th>Scale/LH</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIₐ (Finance Sector)</td>
<td>Provides payment services</td>
<td>UA</td>
<td>Public Confidence</td>
<td>L</td>
<td>4</td>
</tr>
<tr>
<td>CI₉ (Energy Sector)</td>
<td>Depends for power</td>
<td>UA</td>
<td>Economic Impact</td>
<td>VL</td>
<td>3</td>
</tr>
<tr>
<td>CI₉ (Energy Sector)</td>
<td>Depends for power</td>
<td>UA</td>
<td>Public Confidence</td>
<td>H</td>
<td>5</td>
</tr>
<tr>
<td>CI₉ (Energy Sector)</td>
<td>Depends for power</td>
<td>UA</td>
<td>Economic Impact</td>
<td>VH</td>
<td>6</td>
</tr>
<tr>
<td>CI₉ (Energy Sector)</td>
<td>Depends for power</td>
<td>UA</td>
<td>Economic Impact</td>
<td>H</td>
<td>5</td>
</tr>
<tr>
<td>CI₉ (Government Sector)</td>
<td>Industrial action</td>
<td>UA</td>
<td>Economic Impact</td>
<td>M</td>
<td>6</td>
</tr>
</tbody>
</table>


Graph Representation: Vehicle Transport Service

(1) Access to Cyber systems
(2) Interaction with Cyber systems
(3) Access to Physical facilities
(4) Usage of physical facilities/goods
Risks of Port’s Supply Chain Services

QUESTION B: How can we estimate risks of a supply chain at the entity level???
ISO 28000 family of standards: designed to protect people, goods, infrastructure and equipment, including means of transport, against security incidents and to prevent their potentially devastating effects.

1. **ISO 20858:2007** on Ships and marine technology – to assist in the uniform implementation of ISPS;
2. **ISO 28000:2007** on Specification for security management systems for the SC;
3. **ISO 28001:2007** on Security management systems for SC – Best practices for implementing SC security);
4. **ISO 28003:2007** on Security management systems for the SC – Requirements for auditors of SC security management systems;
Research gaps in SC security

ISO 28001 is a guide for SC security management

- ...but not a specific methodology
- ...or tool to assist the risk assessor

Supply Chains are inherently (inter)dependent systems, however:

- ISO28001 (or any existing RA methodology) does not define ways to assess dependencies within SCs
- ... and eventually assess the cascading risks within a Supply Chain
**Obj. 1**: techniques for capturing multi-order dependencies of security incidents and risks

**Obj. 2**: algorithms for identifying and assessing the critical path of the inter-dependencies across the global supply chain

**Obj. 3**: A risk assessment (RA) methodology for identifying and analyzing the cascading effects of security incidents on port infrastructures, given their various dependencies
MEDUSA Integrated Risk Management Assessment Framework

Step 0: Scope of the SC Risk Assessment

Step 1: Analysis of the SCS

Step 2: Threat Scenario identification

Step 3: Threat Likelihood Analysis

Step 4: Consequence Analysis

Step 5: Risk Assessment

Step 6: Cascading Risk Assessment

Step 7: Risk mitigation

Methodology Flow

MEDUSA
MEDUSA Supply Chain Risk Management System

http://medusascrsra.cs.unipi.gr
QUESTIONS C: How can we estimate risks of a supply chain at the asset level???
ICT Maritime Supply Chain Service
Goal of MITIGATE is to realize a **radical shift** in risk management methodologies for the maritime sector towards a **dynamic evidence-driven** **Maritime Supply Chain Risk Assessment (g-MSRA)** approach that alleviates the limitations of state-of-the-art risk management frameworks.

The MITIGATE high-level architecture
MITIGATE evidence-driven Maritime Supply Chain Risk Assessment (g-MSRA)

**Boundary Setting**
- S0: Scope of the SCRA
- S1.1: Scope & Objectives of the SCS
- S1.2: SCS business partners and participants
- S1.3: SCS Modelling

**Threat Analysis**
- S2.1: SCS Threat Scenario and individual cyber threats’ Identification
- S2.2: SCS Threat Assessment

**Vulnerability Analysis**
- S3.1: Identification of confirmed vulnerabilities
- S3.2: Identification of zero-day vulnerabilities
- S3.3: Individual Vulnerability Assessment
- S3.4: Cumulative Vulnerability Assessment
- S3.5: Propagated Vulnerability Assessment

**Impact Analysis**
- S4.1: Individual Asset Impact Assessment
- S4.2: Cumulative Impact Assessment
- S4.3: Propagated Impact Assessment

**Risk Estimation**
- S5.1: Individual Asset Risk Assessment
- S5.2: Commutative Risk Assessment
- S5.3: Propagated Risk Assessment

**Mitigate Strategy**
- S6: Risk Mitigation
Seven step methodology

- Based on the risk management process in the standards ISO 28001 and ISO 31000
- Covers the main activities from context definition to risk identification and analysis up to mitigation actions

Main objectives of the methodology are to:

- Identify and measure all relevant cyber threats
- Predict potential attacks/threats paths and patterns
- Estimate the existence of zero-day exploitable vulnerabilities
- Evaluate the individual, cumulative and propagated vulnerabilities
- Assess the potential impacts
- Derive and prioritize the corresponding risks
- Formulate a proper mitigation strategy
Steps of the Methodology

Step 0: Scope of the Supply Chain Risk Assessment
Step 1: Analysis of the Supply Chain Service
Step 2: Supply Chain Service Cyber Threat Analysis
Step 3: Vulnerability Analysis
Step 4: Impact Analysis
Step 5: Risk Assessment
Step 6: Risk Mitigation
Step 0: Scope of the SC Risk Assessment

- **Scope:**
  - Selection of the Supply Chain Service (SCS)
  - Definition of the *boundaries* for the assessment (overall scope, main goals, expected outcome)

- **Outcome:**
  - Specification of the boundaries for the SC risk assessment

- **Example:**

<table>
<thead>
<tr>
<th>Supply Chain Risk Assessment (SCRA): Vehicles Transport Service Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope of the SC RA</strong></td>
</tr>
<tr>
<td><strong>Goal of the SC RA</strong></td>
</tr>
<tr>
<td><strong>Expected output</strong></td>
</tr>
</tbody>
</table>
Step 1: Analysis of the SCS

- **Step 0:** Scope of the Supply Chain Risk Assessment
- **Step 1:** Analysis of the Supply Chain Service
  - **Step 1.1:** Scope & Objectives of the SCS
  - **Step 1.2:** SCS Business Partners
  - **Step 1.3:** SCS Modeling
- **Step 2:** Supply Chain Service Cyber Threat Analysis
- **Step 3:** Vulnerability Analysis
- **Step 4:** Impact Analysis
- **Step 5:** Risk Assessment
- **Step 6:** Risk Mitigation
Step 1:
Analysis of the SCS

• **Scope:**
  - Description of the SCS
  - Identification of the **business partners**, $b_p_n$, participating in the SCS
  - Identification and modeling of the **main processes** involved in the SCS

• **Outcome:**
  - Textual description of the SCS
  - List of **business partners and participants** involved in the SCS risk assessment
  - List of **Supply Chain Service’s Business Processes** (SCSBPs)
  - Set of **SCS cyber assets** as well as their **interconnections and interdependencies** (hosting, exchange data/information, storing, controlling, processing, accessing, installing, trusted)
Supply Chain Service

Purchase & shipment of the Vehicles Transport Service

Description:
The Vehicles Transport Chain Service is a massively complex system with numerous players, including shippers, transport operators aiming at the shipment and receipt of various types of vehicles and equipment such as trucks, vans, truck trailers, threshing machines etc. This Service is a relatively long and complicated process that involves domestic and international transportation, warehouse management, order and inventory control, materials handling, import/export facilitation, and information technology.

Goal of the SCS
Deliver the Vehicles to the Source Port and complete all the required preparations for shipping.

Expected output
Delivery of vehicles to source port

<table>
<thead>
<tr>
<th>Node ID (x_i)</th>
<th>Asset Code</th>
<th>Name</th>
<th>Category</th>
<th>Product Name</th>
<th>Version</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>bp_0</td>
<td>A_1</td>
<td>Port Community System</td>
<td>Web Application</td>
<td>Custom Application</td>
<td>Oracle Supply Chain Products Suite 12.0.6</td>
<td>Custom Application</td>
</tr>
<tr>
<td></td>
<td>A_2</td>
<td>PCS Application Server</td>
<td>Web Server</td>
<td>Apache HTTP Server</td>
<td>Apache HTTP Server 2.0.37</td>
<td>Apache</td>
</tr>
<tr>
<td></td>
<td>A_3</td>
<td>PCS Operating System</td>
<td>Operating system</td>
<td>Microsoft Windows Server 2012</td>
<td>Windows 2012 (Version 1, Release 4)</td>
<td>Microsoft</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Node ID (x_i)</th>
<th>Asset Source</th>
<th>Asset Destination</th>
<th>Dependency Type</th>
<th>Dependency Access Vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>bp_0</td>
<td>A_1</td>
<td>A_3</td>
<td>1. hosting</td>
<td>Local (L)</td>
</tr>
<tr>
<td></td>
<td>A_2</td>
<td>A_3</td>
<td>7. installing</td>
<td>Local (L)</td>
</tr>
</tbody>
</table>

A_1 hosted_by A_2
A_2 installed_on A_3
Step 2: SCS Cyber Threat Analysis

Step 0: Scope of the Supply Chain Risk Assessment
Step 1: Analysis of the Supply Chain Service
Step 2: Supply Chain Service Cyber Threat Analysis
Step 3: Vulnerability Analysis
Step 4: Impact Analysis
Step 5: Risk Assessment
Step 6: Risk Mitigation

Step 2.1: Individual Cyber Threat Identification
Step 2.2: SCS Threat Assessment
Step 2.1: Ind. Cyber Threat Identification

- **Scope:**
  - Identification of all individual cyber threats against the cyber assets within the SCS
  - Information can come from
    - **business partners** (based on their expertise),
    - existing **repositories** of cyber threats,
    - from **crowdsourcing** (a community of online users/security experts/stakeholders) or
    - from **social media** (discussion groups or forums)

- **Outcome:**
  - List of individual cyber threats applicable to the SCS cyber assets
  - Set of correspondences of individual cyber threats to the cyber assets within the SCS

- **Example:**

<table>
<thead>
<tr>
<th>Code</th>
<th>Cyber Threats Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_{1,A0,1}$</td>
<td>Information tampering</td>
</tr>
<tr>
<td>$T_{2,A0,1}$</td>
<td>Information loss</td>
</tr>
<tr>
<td>$T_{3,A0,1}$</td>
<td>Communication interruption or loss</td>
</tr>
</tbody>
</table>
## WASC Threat Classification 2.0 and CAPEC

<table>
<thead>
<tr>
<th>Category</th>
<th>CWE Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Issues</td>
<td>CWE-287</td>
<td>When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct.</td>
</tr>
<tr>
<td>Buffer Errors</td>
<td>CWE-119</td>
<td>The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer.</td>
</tr>
<tr>
<td>Code</td>
<td>CWE-17</td>
<td>Weaknesses in this category are typically introduced during code development, including specification, design, and implementation.</td>
</tr>
<tr>
<td>Code Injection</td>
<td>CWE-94</td>
<td>The software constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.</td>
</tr>
<tr>
<td>Command Injection</td>
<td>CWE-77</td>
<td>The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component.</td>
</tr>
<tr>
<td>Configuration</td>
<td>CWE-16</td>
<td>Weaknesses in this category are typically introduced during the configuration of the software.</td>
</tr>
<tr>
<td>Credentials Management</td>
<td>CWE-255</td>
<td>Weaknesses in this category are related to the management of credentials.</td>
</tr>
<tr>
<td>Cross-Site Request Forgery (CSRF)</td>
<td>CWE-352</td>
<td>The web application does not, or cannot, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.</td>
</tr>
<tr>
<td>Cross-Site Scripting (XSS)</td>
<td>CWE-79</td>
<td>The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.</td>
</tr>
<tr>
<td>Cryptographic Issues</td>
<td>CWE-310</td>
<td>Weaknesses in this category are related to the use of cryptography.</td>
</tr>
<tr>
<td>Data Handling</td>
<td>CWE-19</td>
<td>Weaknesses in this category are typically found in functionality that processes data.</td>
</tr>
<tr>
<td>Format String Vulnerability</td>
<td>CWE-134</td>
<td>The software uses externally-controlled format strings in printf-style functions, which can lead to buffer overflows or data representation problems.</td>
</tr>
<tr>
<td>Improper Access Control</td>
<td>CWE-284</td>
<td>The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.</td>
</tr>
<tr>
<td>Indicator of Poor Code Quality</td>
<td>CWE-398</td>
<td>The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.</td>
</tr>
</tbody>
</table>
**Step 2.2: SCS Threat Assessment**

- **Scope:**
  - Assessment of the probability of occurrence for each cyber threat scenario on each cyber asset
  - Calculation based on
    - **expected frequency of appearance** (history of previous incidents)
    - information retrieved from **existing repositories and social media** and
    - business partner’s **expert knowledge**
- **Outcome:**
  - List of threat levels of each threat scenario to each cyber asset

<table>
<thead>
<tr>
<th>Threat scale</th>
<th>Description of threat level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat class</td>
<td>Value Range (%)</td>
</tr>
<tr>
<td>Very High (5)</td>
<td>(80-100)</td>
</tr>
<tr>
<td>High (4)</td>
<td>(60-80)</td>
</tr>
<tr>
<td>Medium (3)</td>
<td>(40-60)</td>
</tr>
<tr>
<td>Low (2)</td>
<td>(20-40)</td>
</tr>
<tr>
<td>Very low (1)</td>
<td>[1 – 20]</td>
</tr>
</tbody>
</table>
Step 0: Scope of the Supply Chain Risk Assessment

Step 1: Analysis of the Supply Chain Service

Step 2: Supply Chain Service Cyber Threat Analysis

Step 3: Vulnerability Analysis
  - Step 3.1: Identification of Confirmed Vulnerabilities
  - Step 3.2: Identification of Zero-Day Vulnerabilities
  - Step 3.3: Individual Vulnerability Assessment
  - Step 3.4: Cumulative Vulnerability Assessment
  - Step 3.5: Propagated Vulnerability Assessment

Step 4: Impact Analysis

Step 5: Risk Assessment

Step 6: Risk Mitigation
**Scope:**

- Identification of vulnerabilities existing in the cyber assets of the SCS
- Confirmed vulnerabilities (not been treated by the business partners) corresponding to each asset will be found as follows:
  - from the online databases (e.g. NVD, CVEdetails)
  - from open source and commercial vulnerability scanners (e.g. OpenVas)
  - from the list of the applied security controls identified in the Enhanced Business Partner Declaration (see Step 1.3)

**Outcome:**

- Set of all confirmed vulnerabilities for the cyber assets
- List of specific attributes (defined by the NVD or CVEdetails) for identified confirmed vulnerabilities

---

**Example:**

---

**Microsoft » Windows Server 2012 : Vulnerability Statistics**

<table>
<thead>
<tr>
<th>Year</th>
<th># of Vulnerabilities</th>
<th>DoS</th>
<th>Code Execution</th>
<th>Overflow</th>
<th>Memory Corruption</th>
<th>Sql Injection</th>
<th>XSS</th>
<th>Directory Traversal</th>
<th>Http Response Splitting</th>
<th>Bypass something</th>
<th>Gain Information</th>
<th>Gain Privileges</th>
<th>CSRF</th>
<th>File Inclusion</th>
<th>% of exploits</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>2013</td>
<td>51</td>
<td>12</td>
<td>17</td>
<td>17</td>
<td>3</td>
<td></td>
<td>2</td>
<td>2</td>
<td>21</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>2014</td>
<td>38</td>
<td>9</td>
<td>11</td>
<td>5</td>
<td>3</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>6</td>
<td>5</td>
<td>12</td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>2015</td>
<td>155</td>
<td>16</td>
<td>46</td>
<td>11</td>
<td>9</td>
<td></td>
<td>1</td>
<td></td>
<td>31</td>
<td>26</td>
<td>5</td>
<td>12</td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>2016</td>
<td>156</td>
<td>9</td>
<td>42</td>
<td>19</td>
<td>7</td>
<td></td>
<td>1</td>
<td></td>
<td>16</td>
<td>28</td>
<td>76</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>2017</td>
<td>141</td>
<td>20</td>
<td>24</td>
<td>6</td>
<td>2</td>
<td></td>
<td>1</td>
<td></td>
<td>3</td>
<td>32</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>546</td>
<td>65</td>
<td>142</td>
<td>62</td>
<td>24</td>
<td></td>
<td>1</td>
<td></td>
<td>59</td>
<td>129</td>
<td>186</td>
<td></td>
<td></td>
<td></td>
<td>9</td>
</tr>
</tbody>
</table>

% Of All: 11.9 26.0 11.4 4.4 0.0 0.2 0.4 0.0 10.8 23.6 34.1 0.0 0.0

Warning: Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)
• **Example:**

**Vulnerability Details:** [CVE-2016-0037](#)

The forms-based authentication implementation in Active Directory Federation Services (ADFS) 3.0 in Microsoft Windows Server 2012 R2 allows remote attackers to cause a denial of service (daemon outage) via crafted data, aka "Microsoft Active Directory Federation Services Denial of Service Vulnerability."

**Publication Date:** 2016-02-10 **Last Update Date:** 2017-03-23

---

- **Scope:**
  - Investigation of the probability for existing zero-day vulnerabilities
  - Undisclosed vulnerabilities are not present in online repositories
  - Zero-day vulnerabilities are modelled in the same way as confirmed vulnerabilities (using the same attributes)

- **Outcome:**
  - Zero-day vulnerabilities related to all cyber assets

---

- **Scope:**
  - Estimation of the severity of all identified vulnerabilities
  - Calculation of the (qualitative) probability of successfully exploiting each vulnerability
    - Using the CVSS metrics (retrieved from the online databases)
    - Taking into account the applied controls described in the Enhanced Security Declaration (e.g., for policy related/social/organizational vulnerabilities)

- **Outcome:**
  - The Individual Vulnerability Levels (IVL) of all (confirmed and zero-day) vulnerabilities to all cyber assets

---

- **CVSS Scores & Vulnerability Types**
  - CVSS Score: **5.0**
  - Confidentiality Impact: None (There is no impact to the confidentiality of the system.)
  - Integrity Impact: None (There is no impact to the integrity of the system)
  - Availability Impact: Partial (There is reduced performance or interruptions in resource availability.)
  - Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
  - Authentication: Not required (Authentication is not required to exploit the vulnerability.)
  - Gained Access: None
  - Vulnerability Type(s): Denial Of Service
  - CWE ID: **20**

---

- **Products Affected By CVE-2016-0037**

<table>
<thead>
<tr>
<th>#</th>
<th>Product Type</th>
<th>Vendor</th>
<th>Product</th>
<th>Version</th>
<th>Update</th>
<th>Edition</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OS</td>
<td>Microsoft</td>
<td>Windows Server 2012</td>
<td>R2</td>
<td>-</td>
<td>~~~datacenter~~~~</td>
<td>Version Details Vulnerabilities</td>
</tr>
<tr>
<td>2</td>
<td>OS</td>
<td>Microsoft</td>
<td>Windows Server 2012</td>
<td>R2</td>
<td>-</td>
<td>~~~standard~~~~</td>
<td>Version Details Vulnerabilities</td>
</tr>
<tr>
<td>3</td>
<td>OS</td>
<td>Microsoft</td>
<td>Windows Server 2012</td>
<td>R2</td>
<td>-</td>
<td>~~~essentials~~~~</td>
<td>Version Details Vulnerabilities</td>
</tr>
</tbody>
</table>

---

- **Number Of Affected Versions By Product**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
<th>Vulnerable Versions</th>
</tr>
</thead>
</table>

---

**CWE - 20 : Improper Input Validation**

<table>
<thead>
<tr>
<th>CWE Definition</th>
<th><a href="http://cwe.mitre.org/data/definitions/20.html">http://cwe.mitre.org/data/definitions/20.html</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of vulnerabilities</td>
<td>4542</td>
</tr>
<tr>
<td>Description</td>
<td>The product does not validate or incorrectly validates input that can affect the control flow or data flow of a program. When software fails to validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.</td>
</tr>
<tr>
<td>Background Details</td>
<td></td>
</tr>
<tr>
<td>Other Notes</td>
<td></td>
</tr>
</tbody>
</table>
### Example:

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Asset</th>
<th>CVE Number</th>
<th>CVSS Exploitability</th>
<th>Individual Vulnerability Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_1$</td>
<td>$A_1$</td>
<td>N/A</td>
<td>N L S</td>
<td>VH</td>
</tr>
<tr>
<td>$V_2$</td>
<td>$A_1$</td>
<td>N/A</td>
<td>A M S</td>
<td>M</td>
</tr>
<tr>
<td>$V_3$</td>
<td>$A_1$</td>
<td>N/A</td>
<td>N M N</td>
<td>VH</td>
</tr>
<tr>
<td>$V_4$</td>
<td>$A_2$</td>
<td>CVE-2013-6111</td>
<td>N M N</td>
<td>VH</td>
</tr>
<tr>
<td>$V_5$</td>
<td>$A_2$</td>
<td>CVE-2014-4721</td>
<td>N H N</td>
<td>H</td>
</tr>
<tr>
<td>$V_6$</td>
<td>$A_3$</td>
<td>CVE-2016-0099</td>
<td>L L N</td>
<td>M</td>
</tr>
<tr>
<td>$V_7$</td>
<td>$A_3$</td>
<td>CVE-2016-0037</td>
<td>N L N</td>
<td>VH</td>
</tr>
<tr>
<td>$V_8$</td>
<td>$A_3$</td>
<td>CVE-2016-0016</td>
<td>L M N</td>
<td>L</td>
</tr>
</tbody>
</table>

### CVSS Exploitability

- **AV**: Access Vector
- **AC**: Attack Complexity
- **Auth**: Authentication

- **Local**: High, Medium, Low
- **Adjacent**: High, Medium, Low
- **Network**: High, Medium, Low

#### Access Vector

- **Multiple**: VL, VL, L
- **Single**: VL, L, L
- **None**: L, L, M

#### Attack Complexity

- **Multiple**: L, M, M
- **Single**: M, M, M
- **None**: M, M, H

#### Authentication

- **Multiple**: M, M, M
- **Single**: H, H, VH
- **None**: H, VH, VH
Step 3.4: Cumulative Vulnerabilities

- Example:

  ![Diagram of cyber assets with vulnerabilities]

  - **Scope:**
    - Individual vulnerability level does not take the “way to reach the cyber asset” into account (i.e., the preconditions)
    - Vulnerability of a cyber assets can be accessed by exploiting vulnerabilities on other cyber assets in the supply chain
    - Exploitation probability can be different to the individual vulnerability
      - Individual vulnerability level is calculated “high”, but the cyber asset may reside at a location that is very difficult for an attacker to access
      - Individual vulnerability level is calculated “low”, but an attacker might easily access the asset using a connected cyber asset with a “high” vulnerability
    - Path to reach the cyber assets needs to be taken into account

  - **Outcome:**
    - The Cumulative Vulnerability Levels (CVL) including all sub-chains with vulnerabilities, entry and target points
Propagation and Path Construction Rules

- Rules to discover which vulnerabilities on the SCS can be used as stepping stones (traversed) by the attacker to reach other vulnerabilities

\[ \forall \text{vuln, asset1, asset2, attacker} \quad \text{Attacked(vuln, asset1, attacker)} \land \\
(\text{ExecuteCode(vuln)} \lor \text{Overflow(vuln)} \lor \text{XSS(vuln)} \lor \text{BypassSomething(vuln)} \lor \\
\text{GainPrivilege(vuln)} \lor \text{MemoryCorruption(vuln)}) \land \\
\text{Connected(asset1, asset2)} \Rightarrow \text{Traversable(vuln, asset1, asset2, attacker)} \]

A connection between two assets is traversable if the starting vulnerability has been successfully attacked and its vulnerability type allows the attacker to use it as a stepping stone to access the end asset.

- Rules to discover which vulnerabilities on the SCS can be used as stepping stones (traversed) by the attacker to reach other vulnerabilities

\[ \forall \text{vuln1, asset1, vuln2, asset2, attacker} \quad \text{Attacked(vuln1, asset1, attacker)} \land \\
(\text{ExecuteCode(vuln1)} \lor \text{Overflow(vuln1)} \lor \text{XSS(vuln1)} \lor \\
\text{BypassSomething(vuln1)} \lor \text{GainPrivilege(vuln1)} \lor \text{MemoryCorruption(vuln1)}) \land \\
\text{Traversable(vuln1, asset1, vuln2, asset2, attacker)} \]

A connection between two vulnerabilities affecting assets (or the same asset) is traversable if the starting vulnerability has been successfully attacked and its vulnerability type allows the attacker to use it as a stepping stone to access the end vulnerability.
### Example:

<table>
<thead>
<tr>
<th>Entry Point</th>
<th>Chain</th>
<th>Categories</th>
<th>Probability</th>
<th>ICVL</th>
</tr>
</thead>
<tbody>
<tr>
<td>V₁</td>
<td>V₁ → V₄ → V₆</td>
<td>VH → VH → H</td>
<td>0.93 × 0.93 × 0.75 = 0.65</td>
<td>H</td>
</tr>
<tr>
<td>V₁</td>
<td>V₁ → V₅ → V₆</td>
<td>VH → H → H</td>
<td>0.93 × 0.75 × 0.75 = 0.52</td>
<td>M</td>
</tr>
<tr>
<td>V₃</td>
<td>V₃ → V₄ → V₆</td>
<td>VH → VH → H</td>
<td>0.93 × 0.93 × 0.75 = 0.65</td>
<td>H</td>
</tr>
<tr>
<td>V₃</td>
<td>V₃ → V₅ → V₆</td>
<td>VH → H → H</td>
<td>0.93 × 0.75 × 0.75 = 0.52</td>
<td>M</td>
</tr>
<tr>
<td>V₄</td>
<td>V₄ → V₆</td>
<td>H → H</td>
<td>0.75 × 0.75 = 0.56</td>
<td>M</td>
</tr>
<tr>
<td>V₅</td>
<td>V₅ → V₆</td>
<td>H → H</td>
<td>0.75 × 0.75 = 0.56</td>
<td>M</td>
</tr>
</tbody>
</table>

### MITIGATE Probability Scale

<table>
<thead>
<tr>
<th>Qualitative Values</th>
<th>Range</th>
<th>Representative</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>0.85 – 1.00</td>
<td>0.93</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>0.65 – 0.84</td>
<td>0.75</td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>0.35 – 0.64</td>
<td>0.50</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>0.15 – 0.34</td>
<td>0.25</td>
<td></td>
</tr>
<tr>
<td>Very Low</td>
<td>0.00 – 0.14</td>
<td>0.07</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IVL</th>
<th>Very Low</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Low</td>
<td>VL</td>
<td>VL</td>
<td>L</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>Low</td>
<td>VL</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Moderate</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>High</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>VH</td>
</tr>
<tr>
<td>Very High</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>VH</td>
<td>VH</td>
</tr>
</tbody>
</table>
Scope:

- Individual vulnerability level does not take into account, "how deep an attacker can reach into the network".
- Access to a cyber asset might allow an attacker to move further into the network, accessing other assets in the supply chain.
- Exploitation probability can be different to the individual vulnerability.

Outcome:

- Individual vulnerability level is calculated "high", but after an exploitation the attacker is not likely to move further into the network.
- Individual vulnerability level is calculated low", but an exploitation is highly likely to cause attacks on other cyber assets.

### Step 3.5: Propagated Vulnerabilities

<table>
<thead>
<tr>
<th>Entry Point</th>
<th>Chain</th>
<th>Categories</th>
<th>Probability</th>
<th>ICVL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_1$</td>
<td>$V_1 \rightarrow V_4 \rightarrow V_6$</td>
<td>VH $\rightarrow$ VH $\rightarrow$ H</td>
<td>$0.93 \times 0.93 \times 0.75 = 0.65$</td>
<td>H</td>
</tr>
<tr>
<td>$V_1$</td>
<td>$V_1 \rightarrow V_4 \rightarrow V_7$</td>
<td>VH $\rightarrow$ VH $\rightarrow$ VH</td>
<td>$0.93 \times 0.93 \times 0.93 = 0.80$</td>
<td>H</td>
</tr>
<tr>
<td>$V_1$</td>
<td>$V_1 \rightarrow V_4 \rightarrow V_8$</td>
<td>VH $\rightarrow$ VH $\rightarrow$ M</td>
<td>$0.93 \times 0.93 \times 0.50 = 0.43$</td>
<td>M</td>
</tr>
<tr>
<td>$V_1$</td>
<td>$V_1 \rightarrow V_5 \rightarrow V_6$</td>
<td>VH $\rightarrow$ H $\rightarrow$ H</td>
<td>$0.93 \times 0.75 \times 0.75 = 0.52$</td>
<td>M</td>
</tr>
<tr>
<td>$V_1$</td>
<td>$V_1 \rightarrow V_5 \rightarrow V_7$</td>
<td>VH $\rightarrow$ H $\rightarrow$ VH</td>
<td>$0.93 \times 0.75 \times 0.93 = 0.65$</td>
<td>H</td>
</tr>
<tr>
<td>$V_1$</td>
<td>$V_1 \rightarrow V_5 \rightarrow V_8$</td>
<td>VH $\rightarrow$ H $\rightarrow$ M</td>
<td>$0.93 \times 0.75 \times 0.50 = 0.35$</td>
<td>M</td>
</tr>
</tbody>
</table>

#### PVL

![Graph showing propagated vulnerabilities](attachment:image.png)
Step 4:
Impact Analysis

Step 0: Scope of the Supply Chain Risk Assessment
Step 1: Analysis of the Supply Chain Service
Step 2: Supply Chain Service Cyber Threat Analysis
Step 3: Vulnerability Analysis
Step 4: Impact Analysis
Step 5: Risk Assessment
Step 6: Risk Mitigation

Step 4.1: Individual Impact Assessment
Step 4.2: Cumulative Impact Assessment
Step 4.3: Propagated Impact Assessment
Step 4.1: Individual Impacts

- **Scope:**
  - Estimation of the **impact of all identified vulnerabilities**
  - Calculation of the (qualitative) damage in case a vulnerability is successfully exploited
    - Using the CVSS metrics (retrieved from the online databases)
    - Taking into account the applied controls described in the Enhanced Security Declaration (e.g., for policy related/social/organizational vulnerabilities)

- **Outcome:**
  - **Individual Impact Levels** (IIL) of each vulnerability in all cyber assets

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Asset</th>
<th>CVE Number</th>
<th>CVSS Impact</th>
<th>Individual Impact Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_1$</td>
<td>$A_1$</td>
<td>N/A</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>$V_2$</td>
<td>$A_1$</td>
<td>N/A</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>$V_3$</td>
<td>$A_1$</td>
<td>N/A</td>
<td>C</td>
<td>P</td>
</tr>
<tr>
<td>$V_4$</td>
<td>$A_2$</td>
<td>CVE-2013-6111</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>$V_5$</td>
<td>$A_2$</td>
<td>CVE-2014-4721</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>$V_6$</td>
<td>$A_3$</td>
<td>CVE-2016-0099</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>$V_7$</td>
<td>$A_3$</td>
<td>CVE-2016-0037</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>$V_8$</td>
<td>$A_3$</td>
<td>CVE-2016-0016</td>
<td>C</td>
<td>C</td>
</tr>
</tbody>
</table>
**Step 4.2: Cumulative Impacts**

**Example:**

<table>
<thead>
<tr>
<th>Entry Point</th>
<th>Chain</th>
<th>Categories</th>
<th>ICVL</th>
<th>Impact</th>
<th>ICIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_1$</td>
<td>$V_1 \rightarrow V_4 \rightarrow V_6$</td>
<td>$\text{VH} \rightarrow \text{VH} \rightarrow \text{H}$</td>
<td>$\text{H}$</td>
<td>$\text{VH}$</td>
<td>$\text{VH}$</td>
</tr>
<tr>
<td>$V_1$</td>
<td>$V_1 \rightarrow V_5 \rightarrow V_6$</td>
<td>$\text{VH} \rightarrow \text{H} \rightarrow \text{H}$</td>
<td>$\text{M}$</td>
<td>$\text{VH}$</td>
<td>$\text{H}$</td>
</tr>
<tr>
<td>$V_3$</td>
<td>$V_3 \rightarrow V_4 \rightarrow V_6$</td>
<td>$\text{VH} \rightarrow \text{VH} \rightarrow \text{H}$</td>
<td>$\text{H}$</td>
<td>$\text{VH}$</td>
<td>$\text{VH}$</td>
</tr>
<tr>
<td>$V_3$</td>
<td>$V_3 \rightarrow V_5 \rightarrow V_6$</td>
<td>$\text{VH} \rightarrow \text{H} \rightarrow \text{H}$</td>
<td>$\text{M}$</td>
<td>$\text{VH}$</td>
<td>$\text{H}$</td>
</tr>
<tr>
<td>$V_1$</td>
<td>$V_4 \rightarrow V_6$</td>
<td>$\text{H} \rightarrow \text{H}$</td>
<td>$\text{M}$</td>
<td>$\text{VH}$</td>
<td>$\text{H}$</td>
</tr>
<tr>
<td>$V_2$</td>
<td>$V_5 \rightarrow V_6$</td>
<td>$\text{H} \rightarrow \text{H}$</td>
<td>$\text{M}$</td>
<td>$\text{VH}$</td>
<td>$\text{H}$</td>
</tr>
</tbody>
</table>

**ICVL**

- ICVL: Impact Category Value Level

**Impact**

- Impact: The severity of the impact after exploiting a specific asset/vulnerability combination.

**ICIL**

- ICIL: Impact Cumulative Impact Level

**CIL**

- CIL: Cumulative Impact Level

**Diagram:**

A diagram illustrating the relationship between entry points, chains, and categories is shown, along with a chart depicting the cumulative impact levels (CIL) for different vulnerability levels (VL, L, M, H, VH).
Step 4.3: Propagated Impacts

- **Scope:**
  - Definition of the **impact** after exploiting a specific asset/vulnerability combination and **further moves on into the network**
  - Relates to the damage an attack can cause at **any asset/vulnerability combination on his way through the network**
  - All damage on all paths of length $l$ through the network is taken into account

- **Outcome:**
  - **Propagated Impact Level** (PIL) of each vulnerability in all SCS cyber assets
<table>
<thead>
<tr>
<th>Entry Point</th>
<th>Chain</th>
<th>Categories</th>
<th>ICVL</th>
<th>Impact</th>
<th>IPIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>V₁</td>
<td>V₁ → V₄ → V₆</td>
<td>VH → VH → H</td>
<td>H</td>
<td>VH</td>
<td>H</td>
</tr>
<tr>
<td>V₁</td>
<td>V₁ → V₄ → V₇</td>
<td>VH → VH → VH</td>
<td>H</td>
<td>VL</td>
<td>L</td>
</tr>
<tr>
<td>V₁</td>
<td>V₁ → V₄ → V₈</td>
<td>VH → VH → M</td>
<td>M</td>
<td>VH</td>
<td>H</td>
</tr>
<tr>
<td>V₁</td>
<td>V₁ → V₅ → V₆</td>
<td>VH → H → H</td>
<td>M</td>
<td>VH</td>
<td>H</td>
</tr>
<tr>
<td>V₁</td>
<td>V₁ → V₅ → V₇</td>
<td>VH → H → VH</td>
<td>H</td>
<td>VL</td>
<td>L</td>
</tr>
<tr>
<td>V₁</td>
<td>V₁ → V₃ → V₈</td>
<td>VH → H → M</td>
<td>M</td>
<td>VH</td>
<td>H</td>
</tr>
<tr>
<td>V₁</td>
<td>V₁ → V₄</td>
<td>VH → VH</td>
<td>VH</td>
<td>VH</td>
<td>VH</td>
</tr>
<tr>
<td>V₁</td>
<td>V₁ → V₅</td>
<td>VH → H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>V₁</td>
<td>V₁</td>
<td>VH</td>
<td>VH</td>
<td>VH</td>
<td>VH</td>
</tr>
</tbody>
</table>
Step 5: Risk Assessment

Step 0: Scope of the Supply Chain Risk Assessment
Step 1: Analysis of the Supply Chain Service
Step 2: Supply Chain Service Cyber Threat Analysis
Step 3: Vulnerability Analysis
Step 4: Impact Analysis
Step 5: Risk Assessment
Step 6: Risk Mitigation

Step 5.1: Individual Risk Assessment
Step 5.2: Cumulative Risk Assessment
Step 5.3: Propagated Risk Assessment
Step 5.1: Individual Risks

- **Scope:**
  - Individual risk consisting of all the collected values for each asset in the SCS
  - Individual Vulnerability Level (IVL)
  - Individual Impact Level (IIL)
  - Threat Level
  - All three **qualitative values are combined**
  - Result is again a qualitative value

- **Outcome:**
  - **Individual Risk Levels (IRL)** for a specific threat on specific asset

---

Step 5.2: Cumulative Risks

- **Scope:**
  - The Cumulative Risk refers to the risk of a specific threat occurring due to a vulnerability in a **specific target point**
  - Possible ways to reach and exploit that vulnerability are considered

- **Outcome:**
  - **Cumulative Risk Level (CRL)** for a specific threat on specific asset

---

Step 5.3: Propagated Risks

- **Scope:**
  - The Propagated Risk refers to the risk of a specific threat occurring due to a vulnerability in a **specific entry point**
  - Possible ways to reach and exploit other vulnerabilities are considered

- **Outcome:**
  - **Propagated Risk Level (PRL)** for a specific threat on specific asset
Step 0: Scope of the Supply Chain Risk Assessment
Step 1: Analysis of the Supply Chain Service
Step 2: Supply Chain Service Cyber Threat Analysis
Step 3: Vulnerability Analysis
Step 4: Impact Analysis
Step 5: Risk Assessment
Step 6: Risk Mitigation
• **Scope:**
  - Current risk levels might be **above** a required threshold
  - **Additional security controls** need to be chosen by the business partners and by the SCS (as a whole) to meet that thresholds
  - Selection of an **optimal set of security controls** using game theory
    - Based on potential attack strategies
    - Based on available security measures
    - Based on potential damage done by the attacker

• **Outcome:**
  - Optimal security strategy (set of security measures) to be applied by all business partners
  - Maximum risk level (damage) that can be caused by an attacker

• **Action space of attacker**
  - Each **path in the asset graph** describes a possible attack strategy
  - Characterized through the **exploited vulnerability** of the target asset

• The defender has a **list of possible actions** to perform
  - Integration of new security systems
  - Periodical update/upgrades of software
  - Periodical security awareness trainings
• Action space of defender
  ▪ **Countermeasures that reduce vulnerabilities** of the target node (e.g. patch the system)
  ▪ Countermeasures that reduce vulnerabilities earlier on an attack path

• Payoff is **damage on target asset** (goal of attacker)
• Determine this damage for each possible attack path
  ▪ Count number of paths yielding a specific loss
  ▪ Summarize the result in a histogram (do not aggregate)
• Main goal for the defender is to **reduce vulnerabilities** in the attack graph that could be exploited
  ▪ Reduce the number of attack paths (and attack strategies)
  ▪ Lower the probability for a specific attack strategy to be successful

• Mathematical approach towards **minimization of the risk** as a decision support for security experts

Example:
Benefits of the Methodology

- Provision of up-to-date threat and vulnerability information
  - Integration of information from vulnerability databases
  - Application of open data sources and social media
  - Dynamic adaption to currently changing threat level

- Addressing the highly-interconnected port infrastructures’ area
  - Identification of interdependencies of cyber security assets
  - Assessment of cascading effects on these assets

- Compliant with standards, EU and international regulations
  - ISO 31000, ISO 28001, ISO 27005, ISPS, etc.
  - Applicable to various transport-related sectors (not port-specific)
- Static Ports’ RM methodology and tool (ISO27001, 27005, ISPS, CIIP)
- Dynamic evidence-driven Maritime SC RM environment (simulation, crowd-sourcing, open data) (ISO27001, 27005, ISPS, CIIP, ISO28000)
- Static SC RM’ methodology and tool (ISPS, CIIP, ISO28000)
- Situational Awareness platform

Protection of CIs

Thank You