# MITRE ICS/SCADA Cyber Repository

Jackson Wynn, MITRE Corporation

International Atomic Energy Agency (IAEA)
Research Coordination Meeting (RCM)

Erlangen, Germany
20-24 March 2017

Approved for Public Release; Distribution Unlimited: 17-0876.

# Abstract

- **MITRE CRP deliverables for FY17 include an open source catalog of CAPEC-like attack patterns specific to ICS/SCADA systems**
  - Providing an extensible taxonomy for organizing ICS/SCADA attack patterns that promotes alternative search strategies

- **MITRE now hosts an open source catalog called TARA in its corporate DMZ**
  - This presentation discusses the catalog capability, its data model, and a MITRE-developed cyber risk assessment methodology that the catalog tool supports

# Agenda

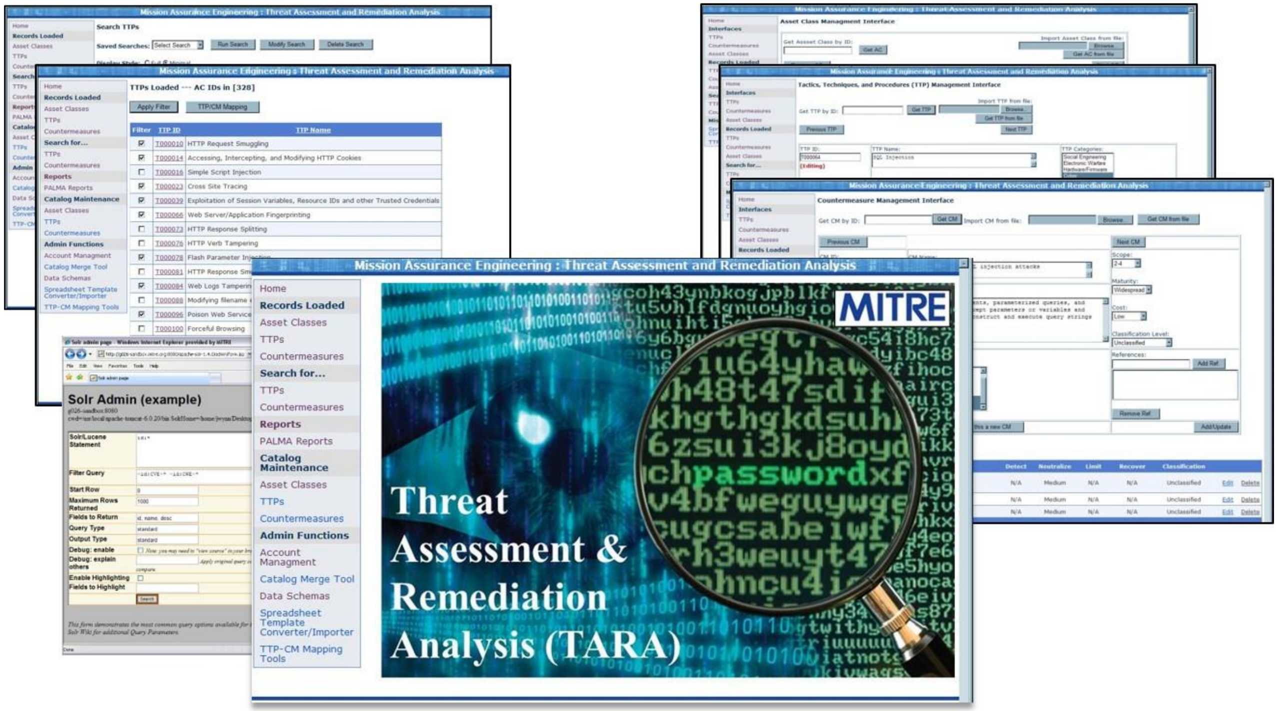
- **TARA Catalog Tool**
- **Data Model Details**
  - Vector Groups / Taxonomies
  - Attack Vectors
  - Countermeasures
  - Countermeasure Mappings
- **Catalog Tool Demo**
- **Catalog Data Sources**
- **Threat Assessment & Remediation Analysis (TARA)**
  - Methodology Description

# Threat Assessment and Remediation Analysis (TARA) Catalog Tool

- **Web-based capability used to compile and search for information about cyber attacks and countermeasures**
  - Developed to support cyber risk assessments that apply MITRE-developed TARA methodology

Catalog Search Tools

Catalog Update Tools



Mission Assurance Engineering : Threat Assessment and Remediation Analysis

Search TTPs

Saved Searches: Select Search

TTPs Loaded --- AC IDs in [328]

| Filter | TTP ID | TTP Name |
|---|---|---|
| ☑ | T000010 | HTTP Request Smuggling |
| ☑ | T000014 | Accessing, Intercepting, and Modifying HTTP Cookies |
| □ | T000016 | Simple Script Injection |
| ☑ | T000023 | Cross Site Tracing |
| ☑ | T000039 | Exploitation of Session Variables, Resource IDs and other Trusted Credentials |
| ☑ | T000066 | Web Server/Application Fingerprinting |
| □ | T000073 | HTTP Response Splitting |
| □ | T000076 | HTTP Verb Tampering |
| ☑ | T000078 | Flash Parameter Injection |
| □ | T000081 | HTTP Response Sm |
| ☑ | T000084 | Web Logs Tamperin |
| □ | T000088 | Modifying filename |
| ☑ | T000096 | Poison Web Service |
| □ | T000100 | Forceful Browsing |

Solr Admin (example)

Asset Class Managment Interface

Tactics, Techniques, and Procedures (TTP) Management Interface

Countermeasure Management Interface

Approved for Public Release

# Uses of the TARA Catalog Tool

- **Casual browsing**
- **Compilation of attack vector and countermeasure information**
- **Taxonomy development**
- **Threat model development**

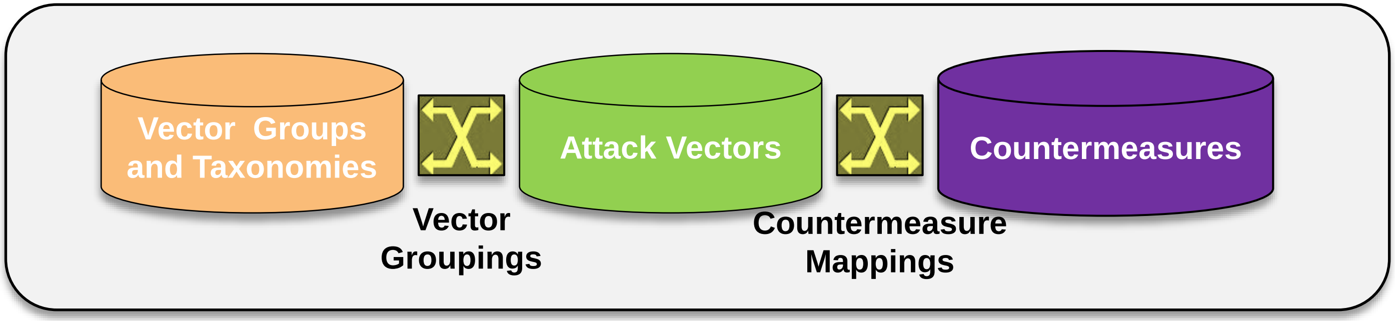
# TARA Catalog usage for the CRP

- **The TARA catalog will support MITRE/University of Massachusetts Lowell (UML) IAEA research**
  - Compilation of ICS/SCADA attack vectors and countermeasures
  - Development of ICS/SCADA cyber threat taxonomies
  - Development of cyber threat models of hypothetical nuclear facilities

- **Read-only access to the catalog can be provided to IAEA Collaborative Research Program (CRP) participants**
  - Emails will be sent to CRP participants with details on accounts and access
  - A catalog user guide is currently in development

# TARA
# Data Model

# Objectives of the TARA Catalog



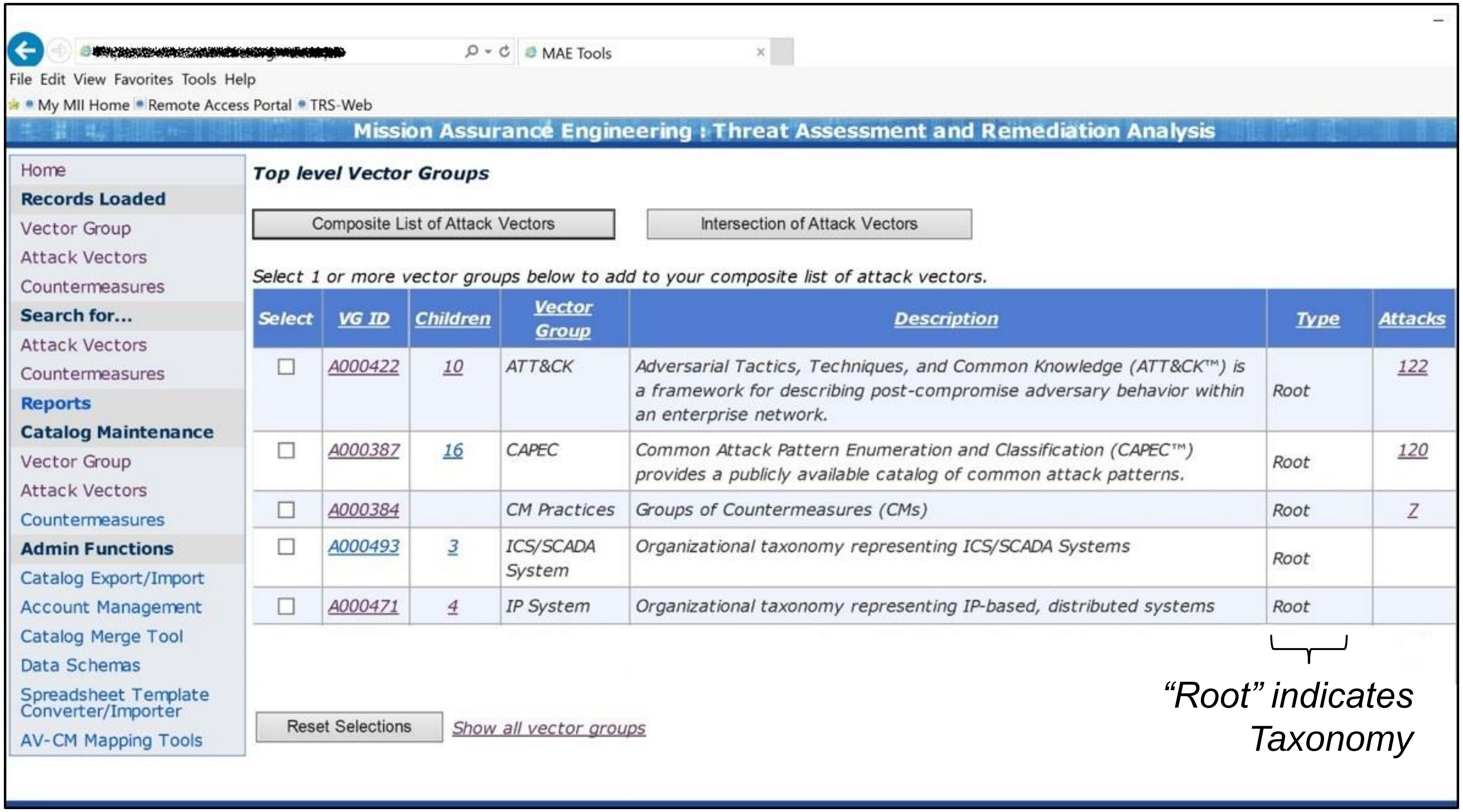
- **Provides a repository of Attack Vector (AV) and Countermeasure  (CM) data used in TARA assessments**
- **Serves as a collection point for data derived from variety of sources**
- **Supports mappings and groupings that can be used to connect and traverse catalog data**

Understanding the data model makes it easier to use the TARA catalog tool

# Vector Groups and Taxonomies

**Vector Group** – Named collection of attack vectors

**Taxonomy** – Hierarchically structured collection of vector groups



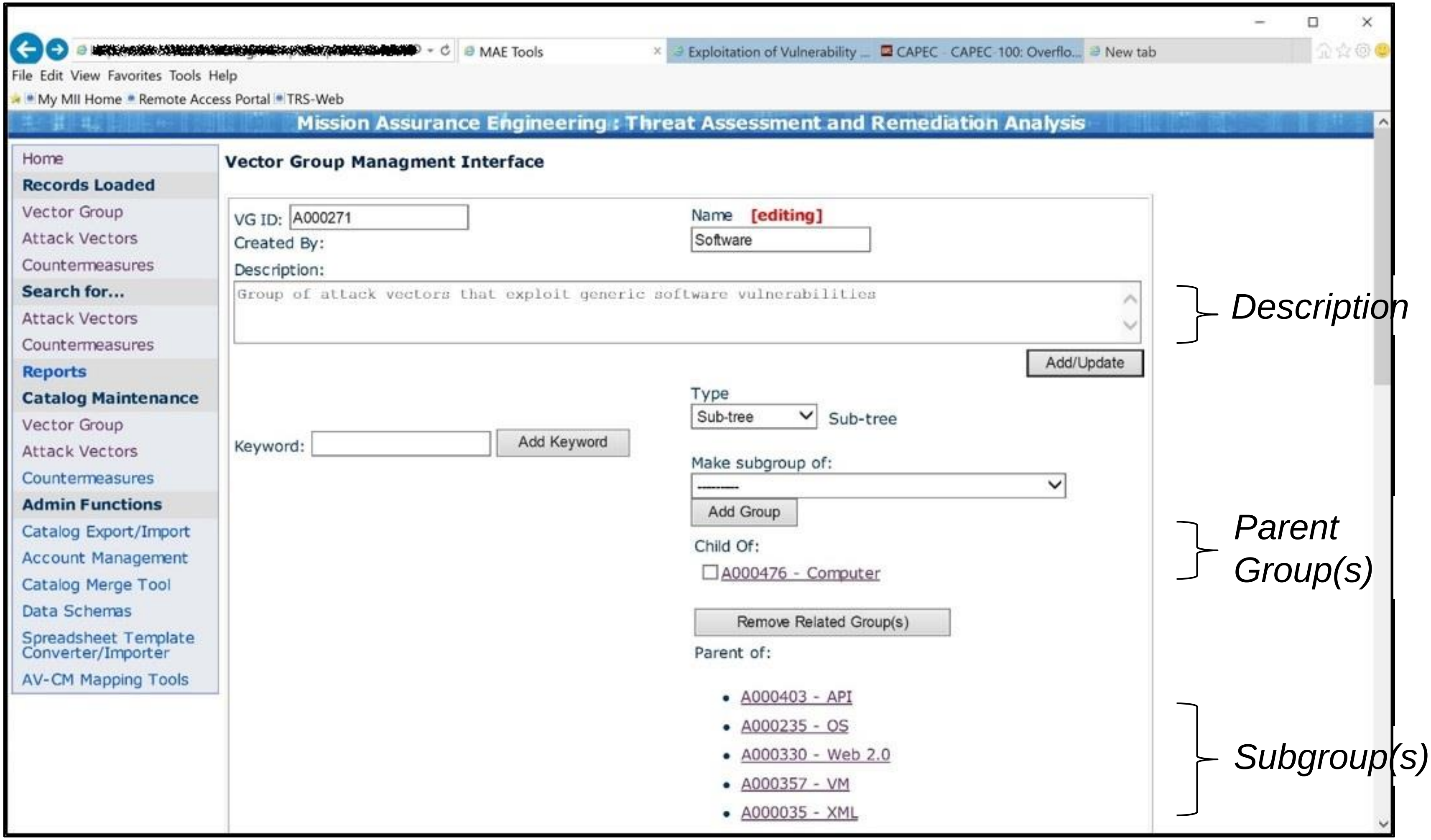
***Top level Vector Groups***

*Select 1 or more vector groups below to add to your composite list of attack vectors.*

| Select | VG ID | Children | Vector Group | Description | Type | Attacks |
|---|---|---|---|---|---|---|
| ☐ | A000422 | 10 | ATT&CK | Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a framework for describing post-compromise adversary behavior within an enterprise network. | Root | 122 |
| ☐ | A000387 | 16 | CAPEC | Common Attack Pattern Enumeration and Classification (CAPEC™) provides a publicly available catalog of common attack patterns. | Root | 120 |
| ☐ | A000384 | | CM Practices | Groups of Countermeasures (CMs) | Root | 7 |
| ☐ | A000493 | 3 | ICS/SCADA System | Organizational taxonomy representing ICS/SCADA Systems | Root | |
| ☐ | A000471 | 4 | IP System | Organizational taxonomy representing IP-based, distributed systems | Root | |

*“Root” indicates Taxonomy*

# Vector Group Example: Software (Top)



[redacted]
MAE Tools
Exploitation of Vulnerability ...
CAPEC - CAPEC-100: Overflo...
New tab
File Edit View Favorites Tools Help
My MII Home
Remote Access Portal
TRS-Web

Mission Assurance Engineering : Threat Assessment and Remediation Analysis

**Vector Group Managment Interface**

VG ID: A000271

Name **[editing]** Software

Created By:

Description:

Group of attack vectors that exploit generic software vulnerabilities

Type Sub-tree Sub-tree

Keyword:

Make subgroup of: ---------

Child Of:

□ A000476 - Computer

Parent of:

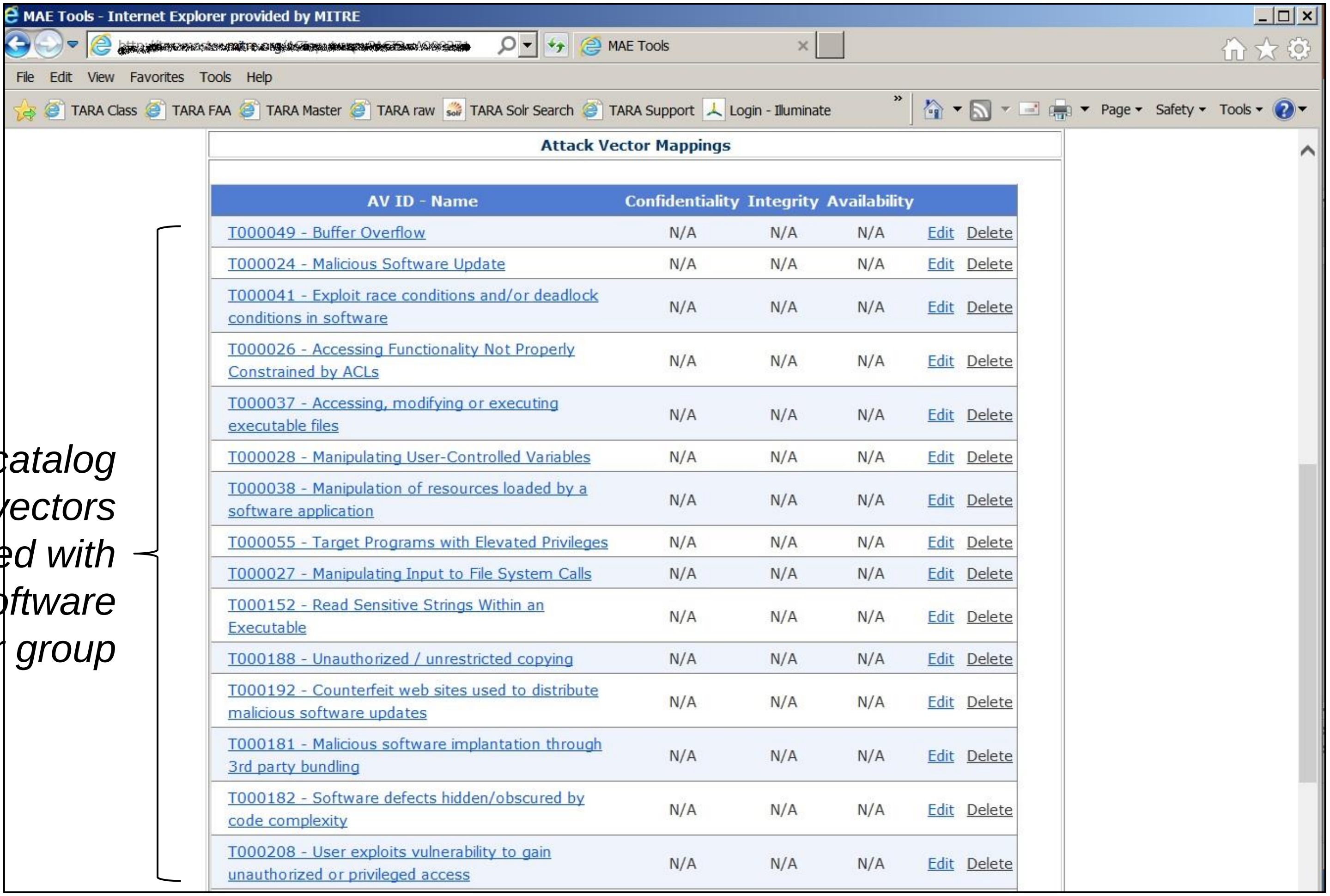
- A000403 - API
- A000235 - OS
- A000330 - Web 2.0
- A000357 - VM
- A000035 - XML

*Description*

*Parent Group(s)*

*Subgroup(s)*

# Vector Group Example: Software (Bottom)



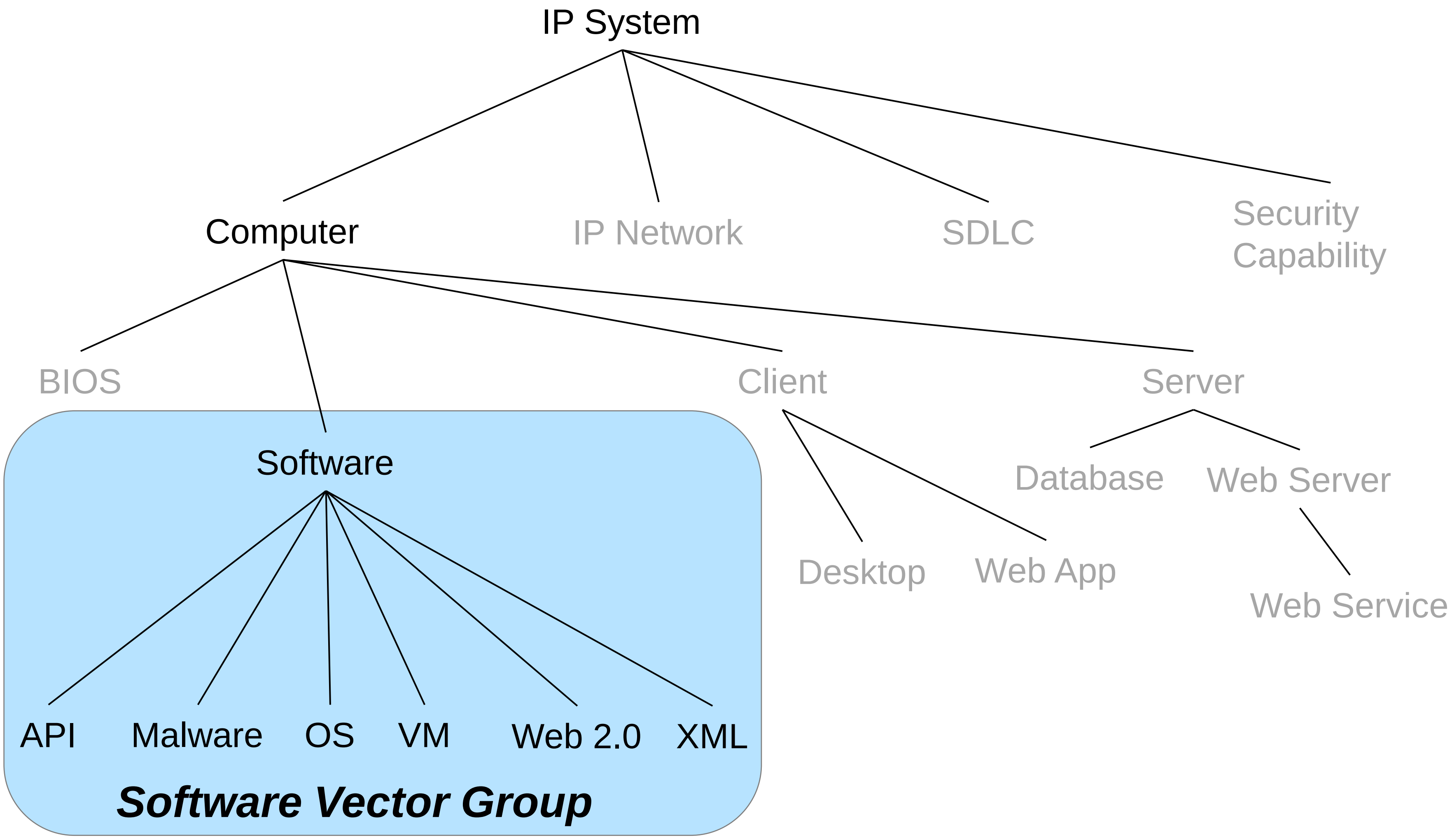
Attack Vector Mappings

| AV ID - Name | Confidentiality | Integrity | Availability | | |
|---|---|---|---|---|---|
| T000049 - Buffer Overflow | N/A | N/A | N/A | Edit | Delete |
| T000024 - Malicious Software Update | N/A | N/A | N/A | Edit | Delete |
| T000041 - Exploit race conditions and/or deadlock conditions in software | N/A | N/A | N/A | Edit | Delete |
| T000026 - Accessing Functionality Not Properly Constrained by ACLs | N/A | N/A | N/A | Edit | Delete |
| T000037 - Accessing, modifying or executing executable files | N/A | N/A | N/A | Edit | Delete |
| T000028 - Manipulating User-Controlled Variables | N/A | N/A | N/A | Edit | Delete |
| T000038 - Manipulation of resources loaded by a software application | N/A | N/A | N/A | Edit | Delete |
| T000055 - Target Programs with Elevated Privileges | N/A | N/A | N/A | Edit | Delete |
| T000027 - Manipulating Input to File System Calls | N/A | N/A | N/A | Edit | Delete |
| T000152 - Read Sensitive Strings Within an Executable | N/A | N/A | N/A | Edit | Delete |
| T000188 - Unauthorized / unrestricted copying | N/A | N/A | N/A | Edit | Delete |
| T000192 - Counterfeit web sites used to distribute malicious software updates | N/A | N/A | N/A | Edit | Delete |
| T000181 - Malicious software implantation through 3rd party bundling | N/A | N/A | N/A | Edit | Delete |
| T000182 - Software defects hidden/obscured by code complexity | N/A | N/A | N/A | Edit | Delete |
| T000208 - User exploits vulnerability to gain unauthorized or privileged access | N/A | N/A | N/A | Edit | Delete |

*Links to catalog attack vectors associated with the Software vector group*

*Attack vectors listed are in no particular order*

# Taxonomy Example: *IP System*



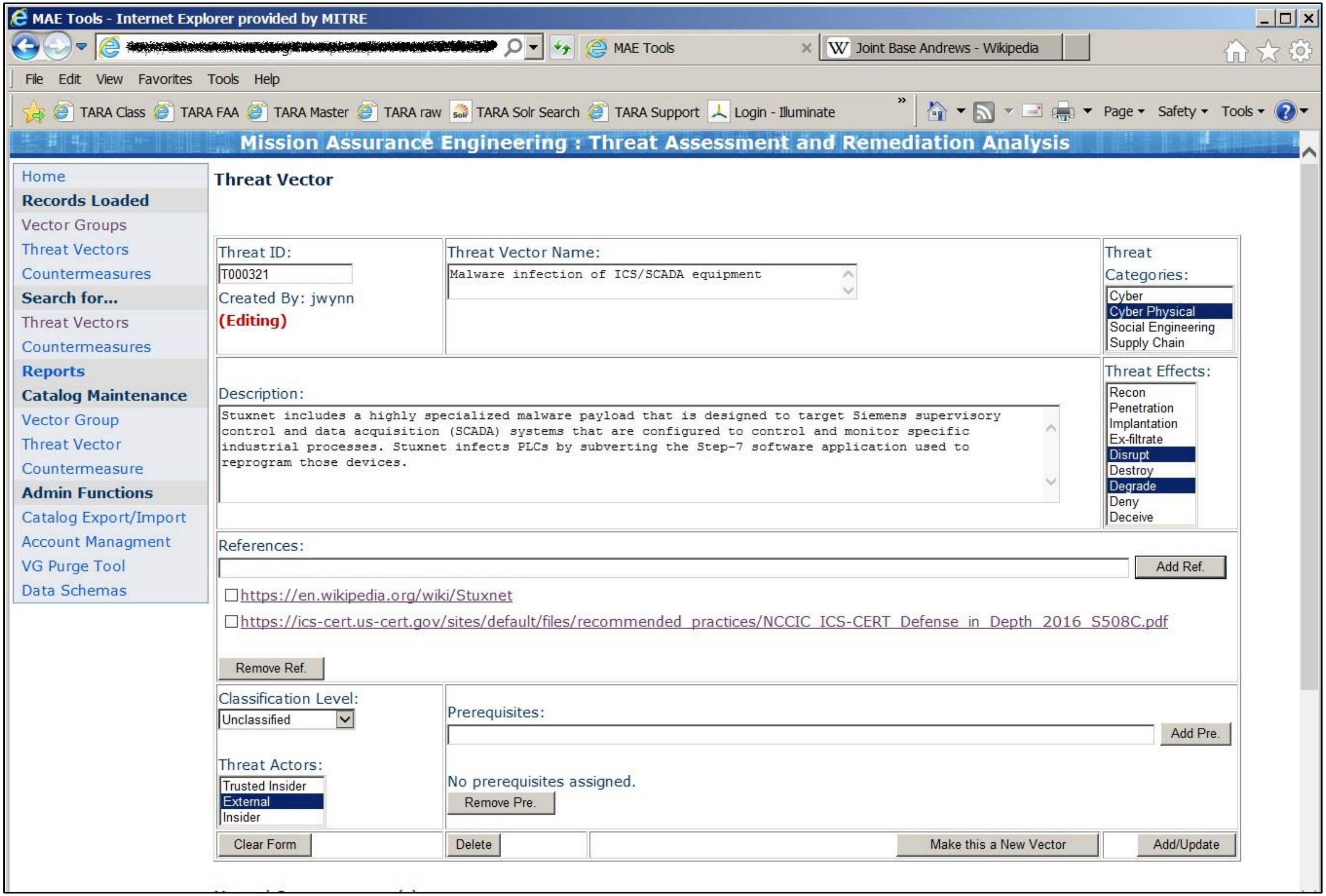
# Attack Vectors (AVs)

**A sequence of steps performed by an adversary in the course of conducting a cyber attack**

- **Sources of Attack Vector data**
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)
  - Common Weakness Enumeration (CWE)
  - Common Vulnerabilities and Exposures (CVE)
  - ICS-CERT Advisories

**All attack vector data derived from public domain sources**

# Attack Vector Example: Stuxnet (Top)



**Threat Vector**

Threat ID: T000321

Created By: jwynn

**(Editing)**

Threat Vector Name: Malware infection of ICS/SCADA equipment

Threat Categories:
Cyber
[✓ Cyber Physical]
Social Engineering
Supply Chain

Description:

```
Stuxnet includes a highly specialized malware payload that is designed to target Siemens supervisory
control and data acquisition (SCADA) systems that are configured to control and monitor specific
industrial processes. Stuxnet infects PLCs by subverting the Step-7 software application used to
reprogram those devices.
```

Threat Effects:
Recon
Penetration
Implantation
Ex-filtrate
[✓ Disrupt]
Destroy
[✓ Degrade]
Deny
Deceive

References:

☐ https://en.wikipedia.org/wiki/Stuxnet

☐ https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Classification Level: Unclassified

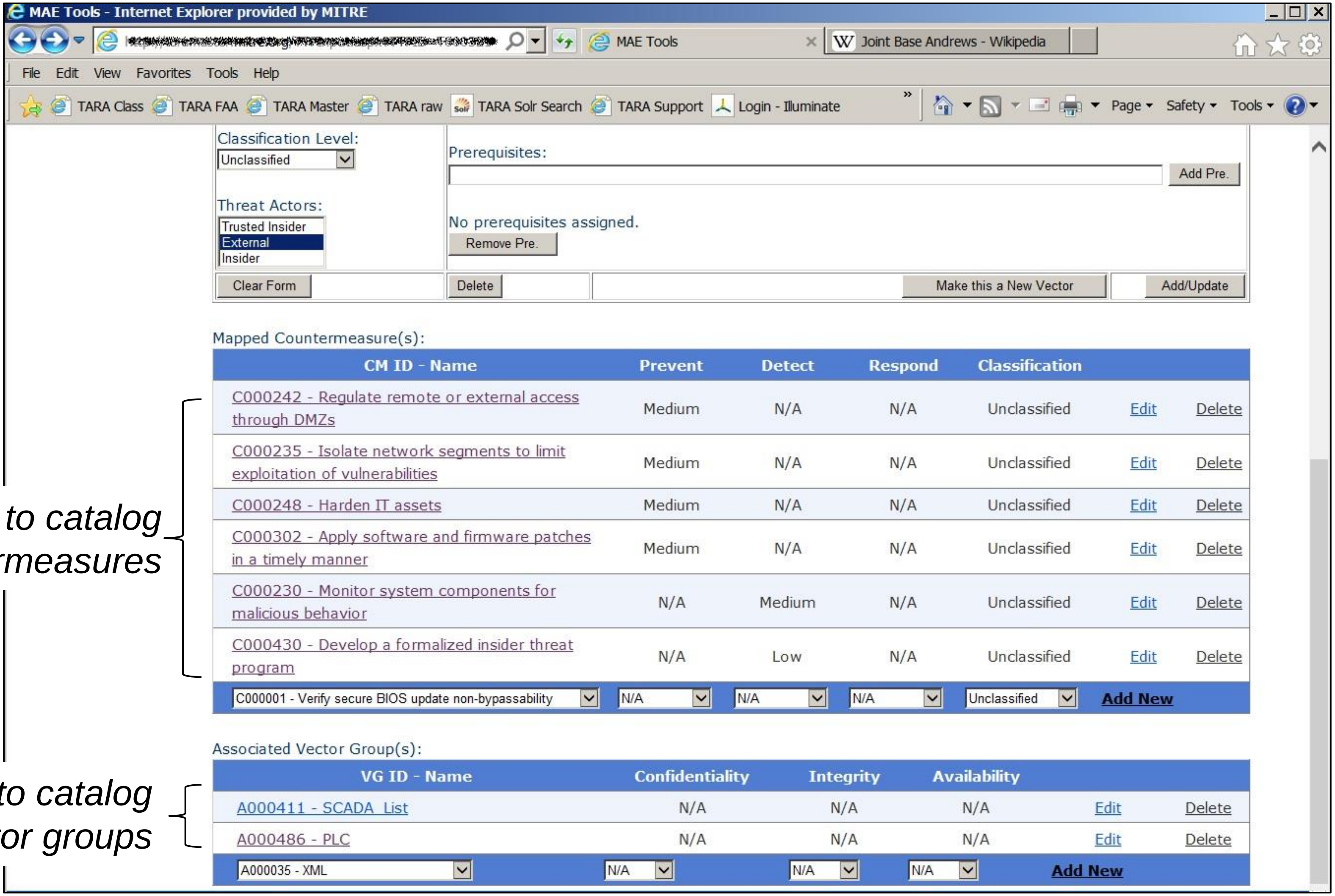
Threat Actors:
Trusted Insider
[✓ External]
Insider

Prerequisites:

No prerequisites assigned.

Approved for Public Release

# Attack Vector Example: Stuxnet (Bottom)



Classification Level: Unclassified

Threat Actors: Trusted Insider, External (selected), Insider

Prerequisites:

Add Pre.

No prerequisites assigned.

Remove Pre.

Clear Form | Delete | Make this a New Vector | Add/Update

Mapped Countermeasure(s):

| CM ID - Name | Prevent | Detect | Respond | Classification | | |
|---|---|---|---|---|---|---|
| C000242 - Regulate remote or external access through DMZs | Medium | N/A | N/A | Unclassified | Edit | Delete |
| C000235 - Isolate network segments to limit exploitation of vulnerabilities | Medium | N/A | N/A | Unclassified | Edit | Delete |
| C000248 - Harden IT assets | Medium | N/A | N/A | Unclassified | Edit | Delete |
| C000302 - Apply software and firmware patches in a timely manner | Medium | N/A | N/A | Unclassified | Edit | Delete |
| C000230 - Monitor system components for malicious behavior | N/A | Medium | N/A | Unclassified | Edit | Delete |
| C000430 - Develop a formalized insider threat program | N/A | Low | N/A | Unclassified | Edit | Delete |
| C000001 - Verify secure BIOS update non-bypassability | N/A | N/A | N/A | Unclassified | Add New | |

Associated Vector Group(s):

| VG ID - Name | Confidentiality | Integrity | Availability | | |
|---|---|---|---|---|---|
| A000411 - SCADA List | N/A | N/A | N/A | Edit | Delete |
| A000486 - PLC | N/A | N/A | N/A | Edit | Delete |
| A000035 - XML | N/A | N/A | N/A | Add New | |

*Links to catalog countermeasures*

*Links to catalog vector groups*

Approved for Public Release

# Countermeasures (CMs)

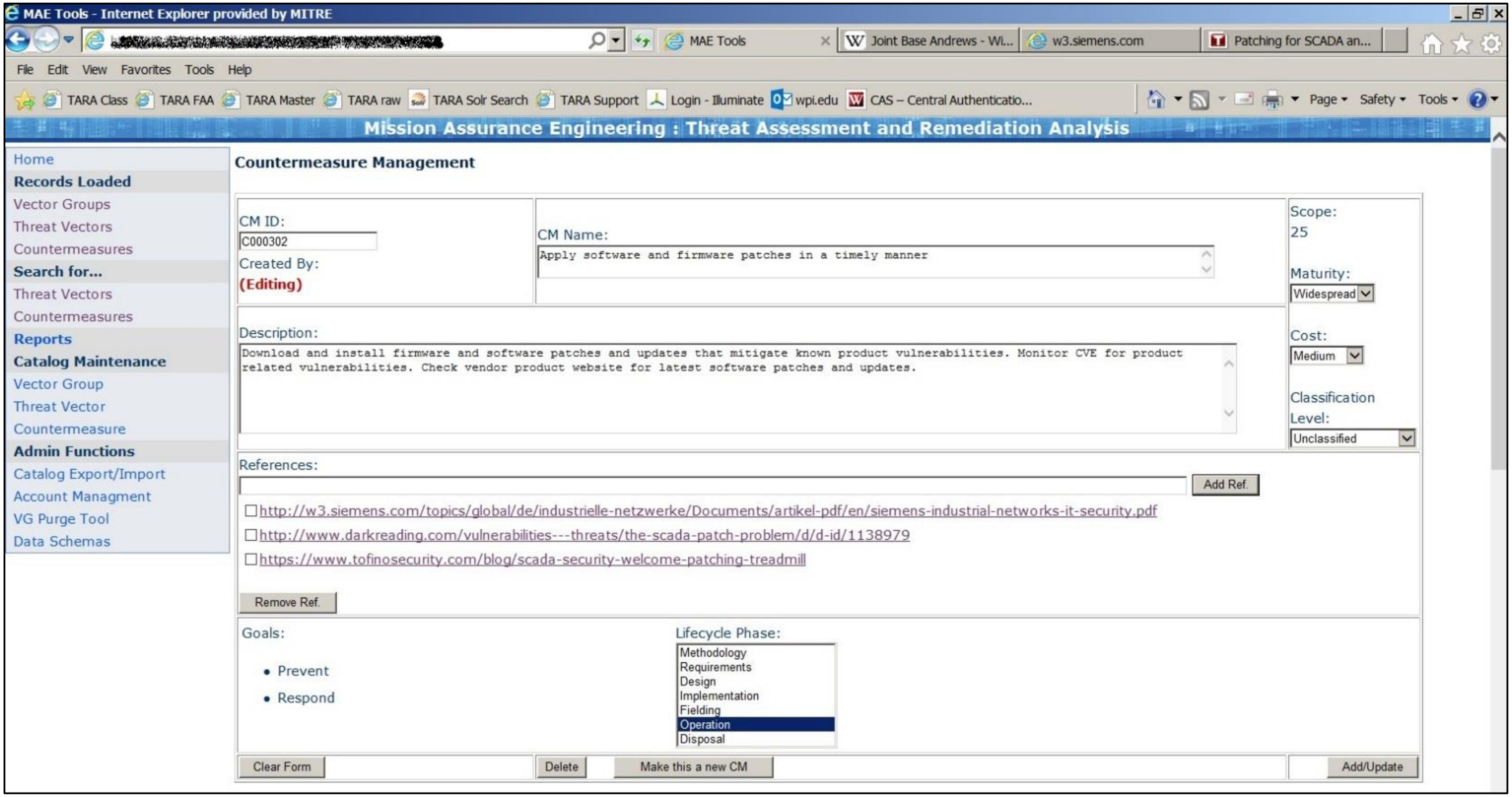
***"Actions, devices, procedures, or techniques that meet or oppose (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken."***

Source: CNSS 4009

- **Sources of Countermeasure data**
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)
  - Common Weakness Enumeration (CWE)
  - Common Vulnerabilities and Exposures (CVE)
  - ICS-CERT Advisories
  - DoD and NIST publications
  - Industry recognized security best practices

**All countermeasure data derived from public domain sources**

# Countermeasure Example: Patch Management (Top)



Countermeasure Management

CM ID: C000302

Created By: **(Editing)**

CM Name: Apply software and firmware patches in a timely manner

Scope: 25

Maturity: Widespread

Cost: Medium

Classification Level: Unclassified

Description: Download and install firmware and software patches and updates that mitigate known product vulnerabilities. Monitor CVE for product related vulnerabilities. Check vendor product website for latest software patches and updates.

References:

- □ http://w3.siemens.com/topics/global/de/industrielle-netzwerke/Documents/artikel-pdf/en/siemens-industrial-networks-it-security.pdf
- □ http://www.darkreading.com/vulnerabilities---threats/the-scada-patch-problem/d/d-id/1138979
- □ https://www.tofinosecurity.com/blog/scada-security-welcome-patching-treadmill

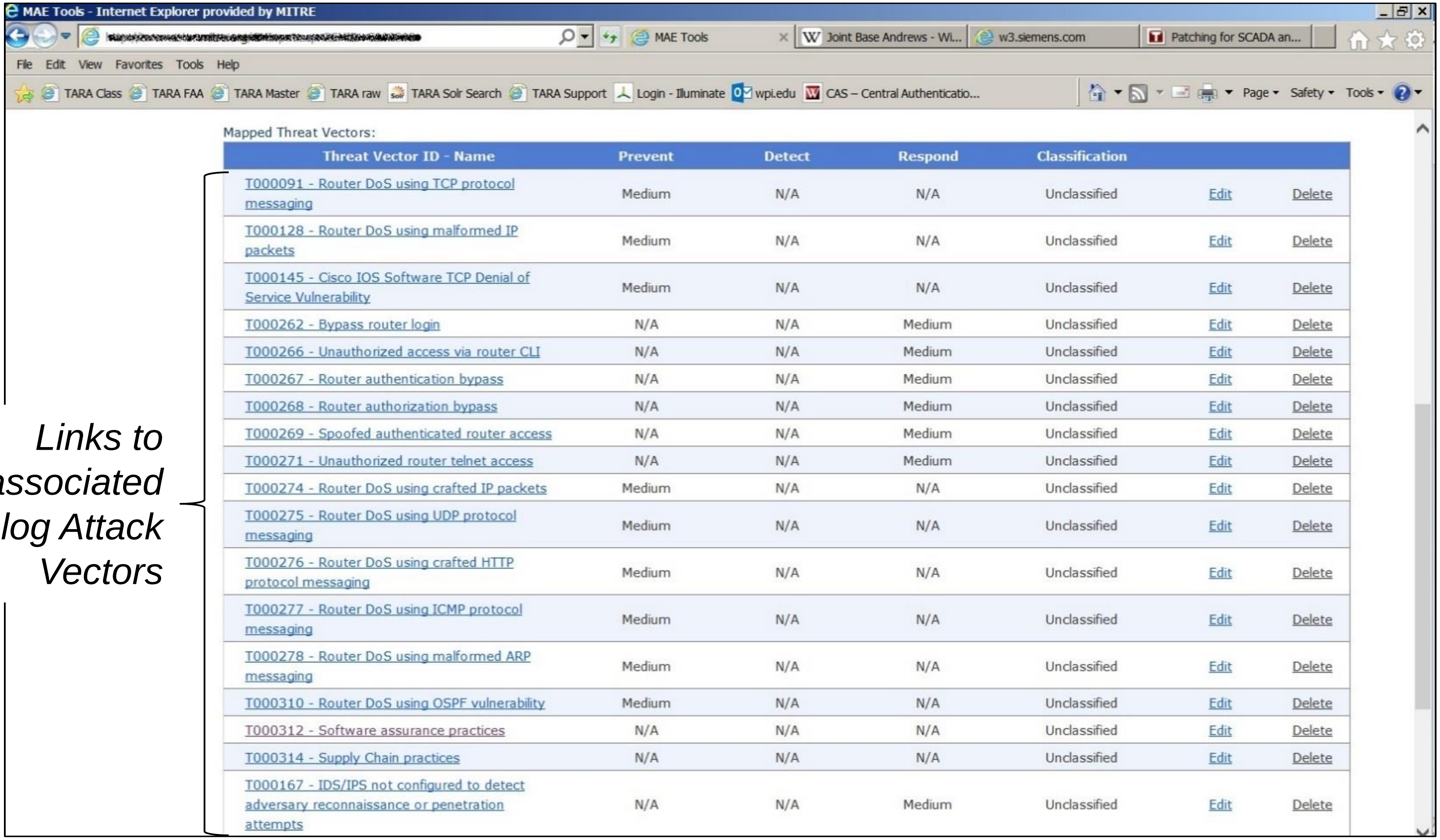
Goals:

- Prevent
- Respond

Lifecycle Phase:

Methodology
Requirements
Design
Implementation
Fielding
Operation
Disposal

# Countermeasure Example: Patch Management (Bottom)

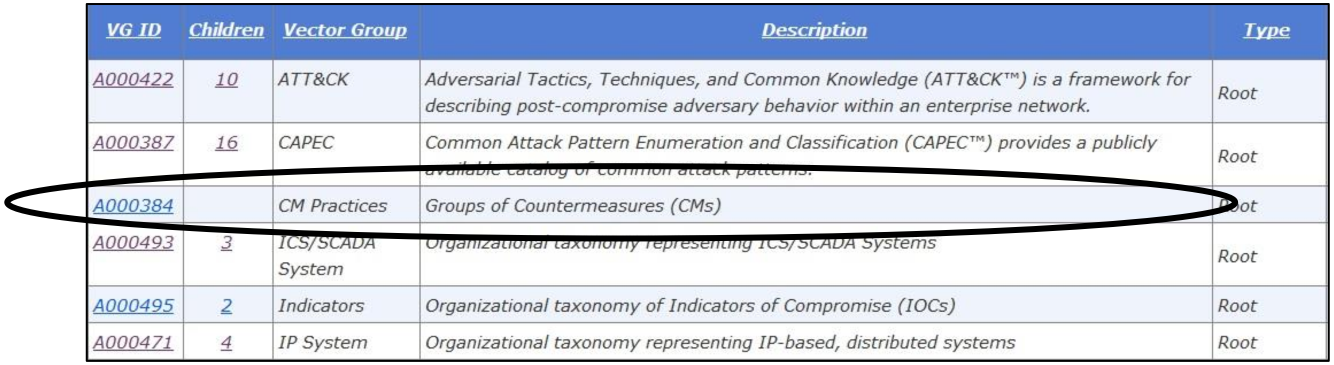


Mapped Threat Vectors:

| Threat Vector ID - Name | Prevent | Detect | Respond | Classification | | |
|---|---|---|---|---|---|---|
| T000091 - Router DoS using TCP protocol messaging | Medium | N/A | N/A | Unclassified | Edit | Delete |
| T000128 - Router DoS using malformed IP packets | Medium | N/A | N/A | Unclassified | Edit | Delete |
| T000145 - Cisco IOS Software TCP Denial of Service Vulnerability | Medium | N/A | N/A | Unclassified | Edit | Delete |
| T000262 - Bypass router login | N/A | N/A | Medium | Unclassified | Edit | Delete |
| T000266 - Unauthorized access via router CLI | N/A | N/A | Medium | Unclassified | Edit | Delete |
| T000267 - Router authentication bypass | N/A | N/A | Medium | Unclassified | Edit | Delete |
| T000268 - Router authorization bypass | N/A | N/A | Medium | Unclassified | Edit | Delete |
| T000269 - Spoofed authenticated router access | N/A | N/A | Medium | Unclassified | Edit | Delete |
| T000271 - Unauthorized router telnet access | N/A | N/A | Medium | Unclassified | Edit | Delete |
| T000274 - Router DoS using crafted IP packets | Medium | N/A | N/A | Unclassified | Edit | Delete |
| T000275 - Router DoS using UDP protocol messaging | Medium | N/A | N/A | Unclassified | Edit | Delete |
| T000276 - Router DoS using crafted HTTP protocol messaging | Medium | N/A | N/A | Unclassified | Edit | Delete |
| T000277 - Router DoS using ICMP protocol messaging | Medium | N/A | N/A | Unclassified | Edit | Delete |
| T000278 - Router DoS using malformed ARP messaging | Medium | N/A | N/A | Unclassified | Edit | Delete |
| T000310 - Router DoS using OSPF vulnerability | Medium | N/A | N/A | Unclassified | Edit | Delete |
| T000312 - Software assurance practices | N/A | N/A | N/A | Unclassified | Edit | Delete |
| T000314 - Supply Chain practices | N/A | N/A | N/A | Unclassified | Edit | Delete |
| T000167 - IDS/IPS not configured to detect adversary reconnaissance or penetration attempts | N/A | N/A | Medium | Unclassified | Edit | Delete |

*Links to associated catalog Attack Vectors*

# Countermeasure Categories



| VG ID | Children | Vector Group | Description | Type |
|---|---|---|---|---|
| A000422 | 10 | ATT&CK | Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a framework for describing post-compromise adversary behavior within an enterprise network. | Root |
| A000387 | 16 | CAPEC | Common Attack Pattern Enumeration and Classification (CAPEC™) provides a publicly available catalog of common attack patterns. | Root |
| A000384 | | CM Practices | Groups of Countermeasures (CMs) | Root |
| A000493 | 3 | ICS/SCADA System | Organizational taxonomy representing ICS/SCADA Systems | Root |
| A000495 | 2 | Indicators | Organizational taxonomy of Indicators of Compromise (IOCs) | Root |
| A000471 | 4 | IP System | Organizational taxonomy representing IP-based, distributed systems | Root |

The countermeasure taxonomy provides a list of countermeasure categories

Each category contains 20-40 related countermeasures

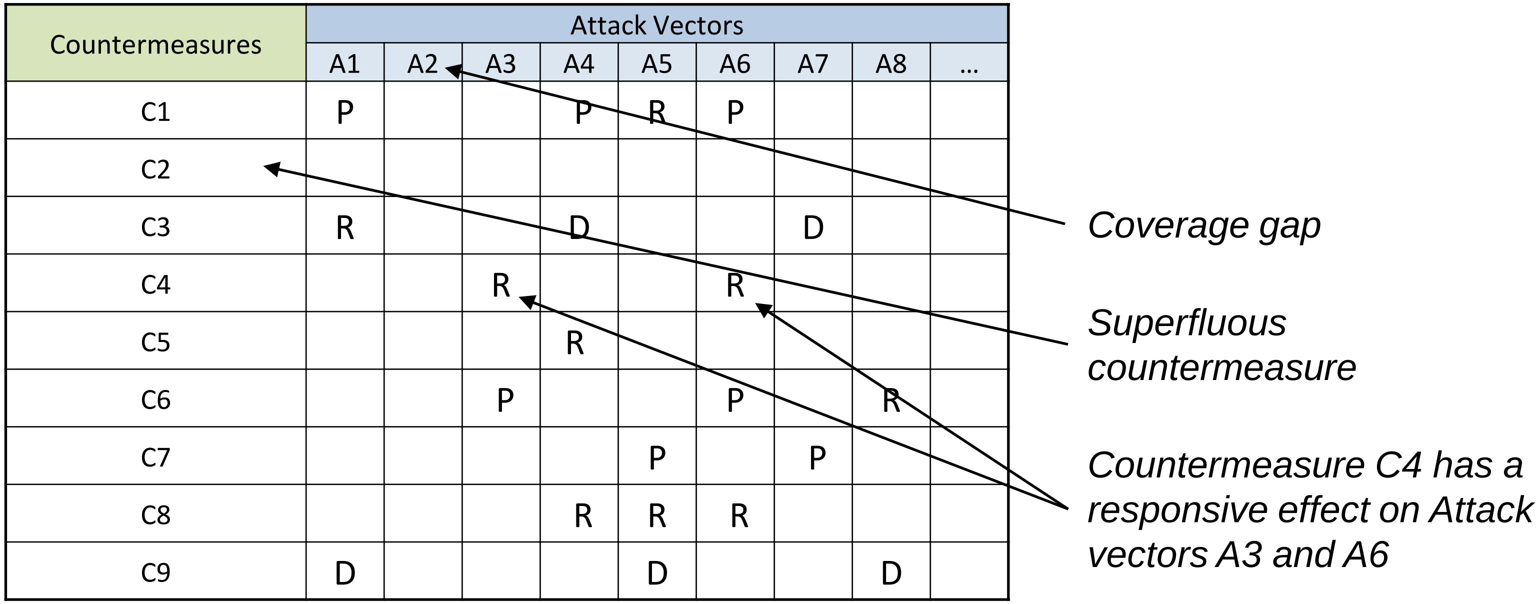
# Countermeasure Mappings

- **Represents the effect a countermeasure has on an attack vector**
  - **Range of countermeasure effects**
    - **Detect (denoted by a ‘D’)**
      - The countermeasure makes it possible to determine if the attack has occurred, is occurring, or potentially could occur
        - Examples: Intrusion Detection Systems (IDS), continuous monitoring, etc.
    - **Prevent (denoted by a ‘P’)**
      - The countermeasure partially or completely eliminates conditions that make the attack possible
        - Examples: network segmentation, cyber threat awareness training, etc.
    - **Respond (denoted by a ‘R’)**
      - The countermeasure reduces the likelihood that the attack will occur or that its impact will be significant
        - Examples: System restoration from backup, maintaining a cyber playbook, forensic analysis of compromised systems, etc.

# Mitigation Mappings Table

**A mitigation mapping table conveys the effects that a range of countermeasures has over a range of attack vectors**

- Attack vectors represented as columns in the mapping table
- Countermeasures represented as rows in the mapping table
- Matrix cells can be used to identify what effect {**P**revent, **R**espond, **D**etect} a countermeasure has on an attack vector



| Countermeasures | Attack Vectors | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | … |
| C1 | P | | | P | R | P | | | |
| C2 | | | | | | | | | |
| C3 | R | | | D | | | D | | |
| C4 | | | R | | | R | | | |
| C5 | | | | R | | | | | |
| C6 | | | P | | | P | | R | |
| C7 | | | | | P | | P | | |
| C8 | | | | R | R | R | | | |
| C9 | D | | | | D | | | D | |

*Coverage gap*

*Superfluous countermeasure*

*Countermeasure C4 has a responsive effect on Attack vectors A3 and A6*

**Mitigation Mappings Table**

# Effect Confidence

- **Assesses the certainty that a given effect will be realized**
  - **High (denoted by 'H')**
    - Engineering verification confirms the effect, i.e., demonstration, inspection, testing, or analysis
  - **Moderate (denoted by 'M')**
    - Mapping based on Subject Matter Expert (SME) judgment
  - **Low (denoted by 'L')**
    - Plausible effect that has not yet been confirmed or substantiated

# Example Mitigation Mappings Table

| Countermeasure (CM) | | Effect (by Attack Vector ID) | | | | | |
|---|---|---|---|---|---|---|---|
| CM ID | Name | T000014 | T000049 | T000050 | T000052 | T000071 | T000170 |
| C000103 | Match buffer size to data input size | | PH | PH | | | |
| C000293 | Disable file and printer sharing | | | RM | RL | | PL |
| C000134 | Select programming languages that minimize potential software defects | | PM | PM | PM | | |
| C000238 | Enforce software quality standards and guidelines that improve software quality | | PM | PM | PM | | |
| C000117 | Apply principle of least privilege | | | | | RM | RM |
| C000135 | Avoid use of dangerous memory functions and operations | | RM | | RM | | |
| C000039 | Convert input data into the data format in which it is used | | | | PM | | |
| C000059 | Enable use of the HTTP Referrer header field | RM | | | | | |
| C000093 | Merge data streams prior to validation | | | | PM | | |
| C000096 | Use vetted runtime libraries | | PH | | | PH | |
| C000123 | Design software to fail securely | | PM | | RM | | |
| C000136 | Utilize processor-based protection capabilities | | PL | | | | PM |
| C000045 | Utilize high quality session IDs | RM | | | | | |
| C000047 | Encrypt session cookies | PH | | | | | |
| C000051 | Use digital signatures/checksums to authenticate source of changes | PH | | | | | |
| C000089 | Validate the range of numeric input | | | PM | | | |
| C000095 | Convert input to canonical form before validating | | | | PM | | |
| C000101 | Verify buffer sizes | | PH | | | | |
| C000102 | Verify message size data | | | | | DH; PH | |
| C000137 | Use unsigned variables to represent whole numbers | | | PM | | | |
| C000094 | Validate data exchanges across language boundaries | | | | RM | | |
| C000132 | Use sandboxing to isolate running software | | | | | | PM |
| C000146 | Apply transport-level mechanisms such as TLS and or VPNs to protect sensitive content | PH | | | | | |

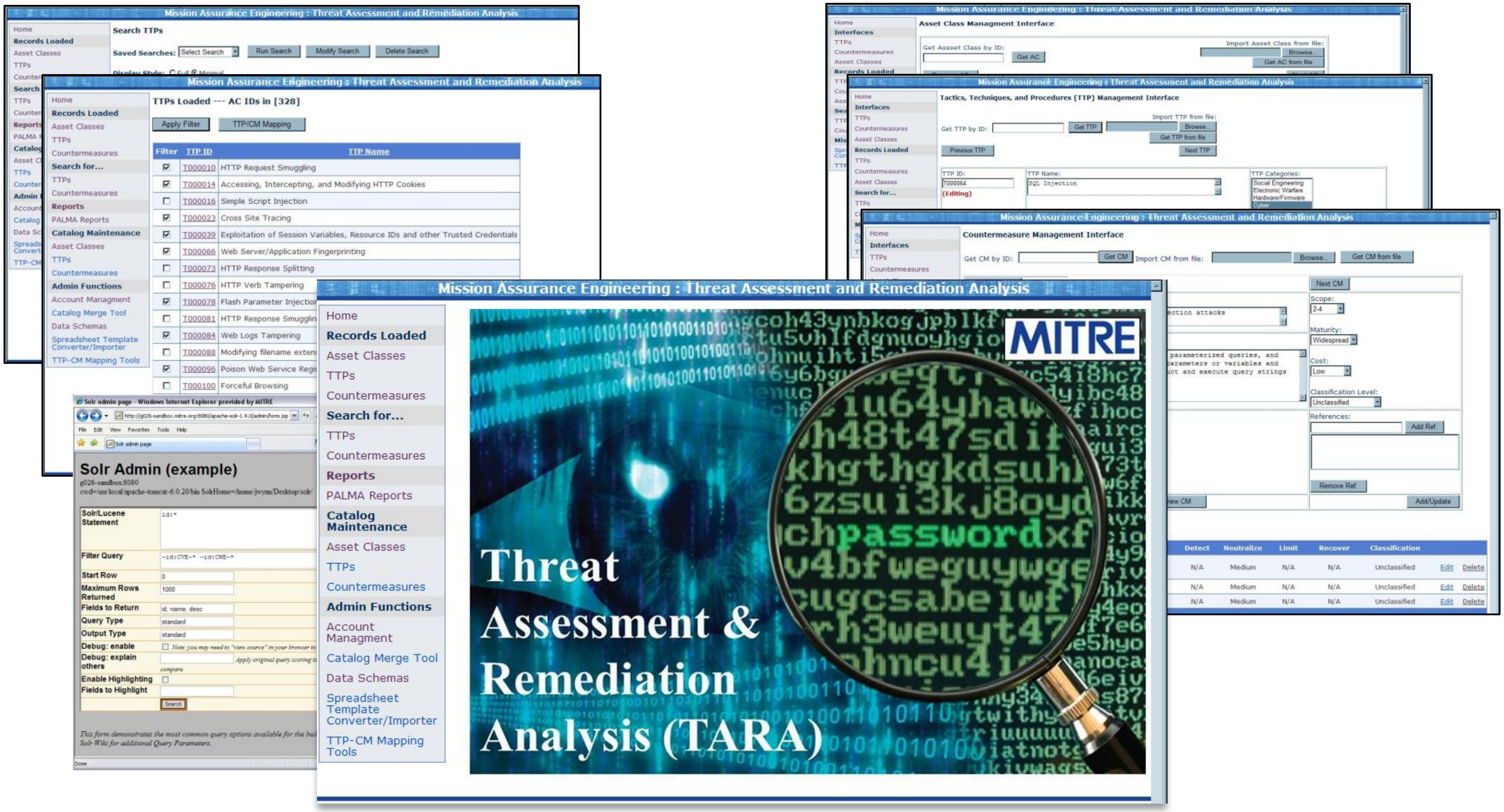
***Mapping Table***

***Effects (P, R, D) x Confidence (H, M, L):***
***{PH, PM, PL, RH, RM, RL, DH, DM, DL}***

# Tools Demo

## Catalog Search Tools

## Catalog Update Tools



Mission Assurance Engineering : Threat Assessment and Remediation Analysis

Search TTPs

Saved Searches: Select Search

TTPs Loaded --- AC IDs in [328]

Apply Filter | TTP/CM Mapping

| Filter | TTP ID | TTP Name |
|---|---|---|
| ☑ | T000010 | HTTP Request Smuggling |
| ☑ | T000014 | Accessing, Intercepting, and Modifying HTTP Cookies |
| □ | T000016 | Simple Script Injection |
| ☑ | T000023 | Cross Site Tracing |
| ☑ | T000039 | Exploitation of Session Variables, Resource IDs and other Trusted Credentials |
| ☑ | T000066 | Web Server/Application Fingerprinting |
| □ | T000073 | HTTP Response Splitting |
| □ | T000076 | HTTP Verb Tampering |
| ☑ | T000078 | Flash Parameter Injectior |
| □ | T000081 | HTTP Response Smugglin |
| ☑ | T000084 | Web Logs Tampering |
| □ | T000088 | Modifying filename extens |
| ☑ | T000096 | Poison Web Service Regis |
| □ | T000100 | Forceful Browsing |

Solr admin page - Windows Internet Explorer provided by MITRE

http://g026-sandbox.mitre.org:8080/apache-solr-1.4.0/admin/form.jsp

Solr Admin (example)

g026-sandbox:8080

cwd=/usr/local/apache-tomcat-6.0.20/bin SolrHome=/home/jwynn/Desktop/solr/

| | |
|---|---|
| Solr/Lucene Statement | id:* |
| Filter Query | -id:CVE-* -id:CWE-* |
| Start Row | 0 |
| Maximum Rows Returned | 1000 |
| Fields to Return | id, name, desc |
| Query Type | standard |
| Output Type | standard |
| Debug: enable | □ Note: you may need to "view source" in your browser to |
| Debug: explain others | Apply original query scoring to<br>compare |
| Enable Highlighting | □ |
| Fields to Highlight | |

Search

*This form demonstrates the most common query options available for the buil Solr Wiki for additional Query Parameters.*

Asset Class Managment Interface

Get Asset Class by ID: Get AC

Import Asset Class from file: Browse... Get AC from file

Tactics, Techniques, and Procedures (TTP) Management Interface

Get TTP by ID: Get TTP

Import TTP from file: Browse... Get TTP from file

Previous TTP | Next TTP

TTP ID: T000064 (Editing)

TTP Name: SQL Injection

TTP Categories: Social Engineering, Electronic Warfare, Hardware/Firmware, Cyber

Countermeasure Management Interface

Get CM by ID: Get CM

Import CM from file: Browse... Get CM from file

Next CM

ection attacks

parameterized queries, and parameters or variables and uct and execute query strings

Scope: 2-4

Maturity: Widespread

Cost: Low

Classification Level: Unclassified

References: Add Ref

Remove Ref

ew CM | Add/Update

| Detect | Neutralize | Limit | Recover | Classification | | |
|---|---|---|---|---|---|---|
| N/A | Medium | N/A | N/A | Unclassified | Edit | Delete |
| N/A | Medium | N/A | N/A | Unclassified | Edit | Delete |
| N/A | Medium | N/A | N/A | Unclassified | Edit | Delete |

Approved for Public Release

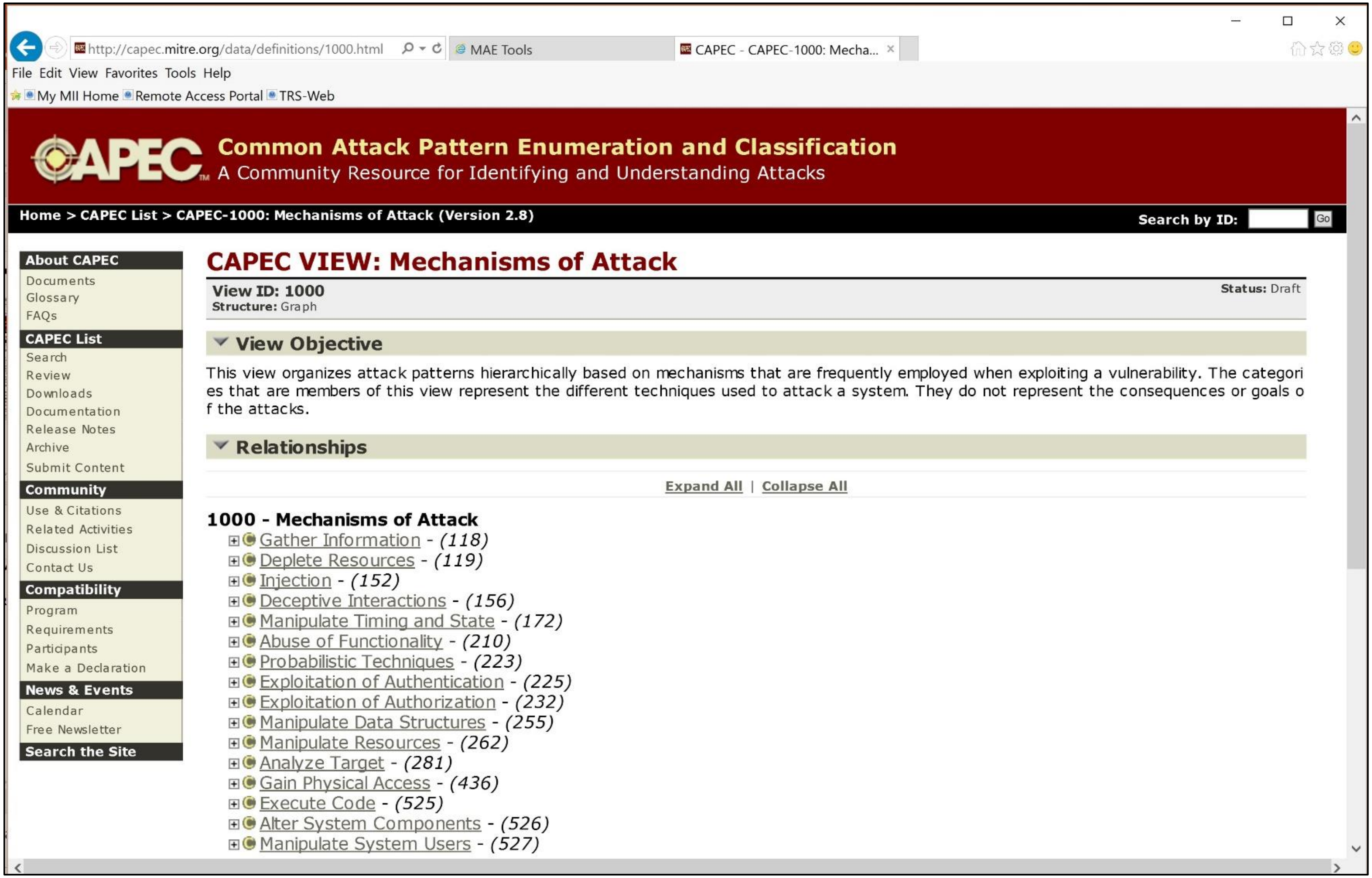
# Sources of Catalog Data

# Common Attack Pattern Enumeration and Classification (CAPEC)

- **MITRE open source repository of cyber attack patterns**
  - Includes postulated attacks and real world security incidents
  - DHS-hosted, Community-contributed, MITRE-moderated
  - Updated quarterly

- **CAPEC includes over 450 attack patterns**
  - Attack patterns contributed by the security research community at large, subject to MITRE review for quality and completeness
  - Patterns conform to XML schema and include fields that characterize the sophistication and resources required
    - CAPEC patterns provide analysis of underlying design weaknesses, which is key to follow-on mitigation engineering activities

# CAPEC Taxonomy: Mechanisms of Attack



## CAPEC VIEW: Mechanisms of Attack

**View ID: 1000**
**Structure:** Graph
**Status:** Draft

### View Objective

This view organizes attack patterns hierarchically based on mechanisms that are frequently employed when exploiting a vulnerability. The categories that are members of this view represent the different techniques used to attack a system. They do not represent the consequences or goals of the attacks.

### Relationships

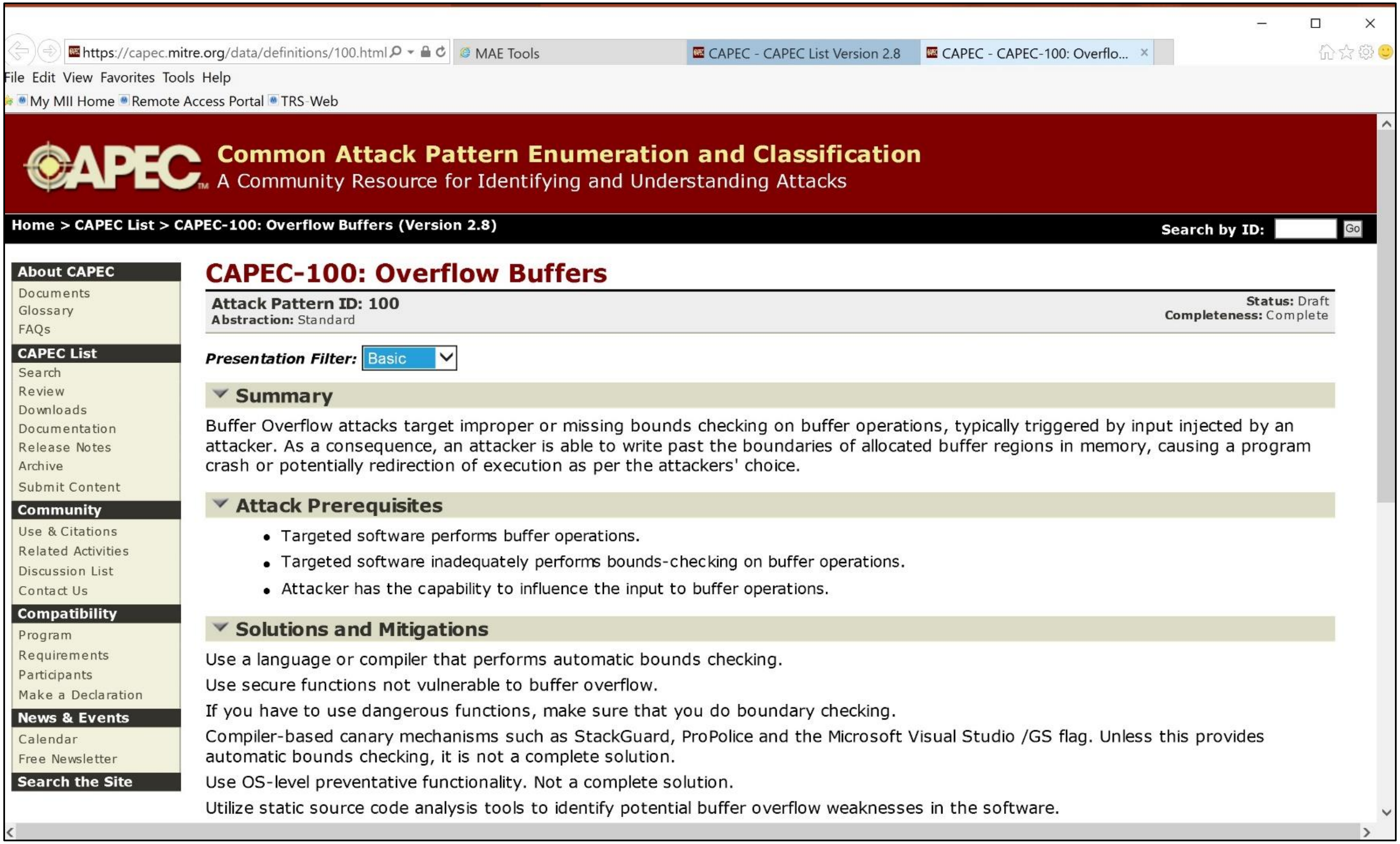
Expand All | Collapse All

**1000 - Mechanisms of Attack**

- Gather Information - *(118)*
- Deplete Resources - *(119)*
- Injection - *(152)*
- Deceptive Interactions - *(156)*
- Manipulate Timing and State - *(172)*
- Abuse of Functionality - *(210)*
- Probabilistic Techniques - *(223)*
- Exploitation of Authentication - *(225)*
- Exploitation of Authorization - *(232)*
- Manipulate Data Structures - *(255)*
- Manipulate Resources - *(262)*
- Analyze Target - *(281)*
- Gain Physical Access - *(436)*
- Execute Code - *(525)*
- Alter System Components - *(526)*
- Manipulate System Users - *(527)*

http://capec.mitre.org/

# Example CAPEC Attack Pattern



## CAPEC-100: Overflow Buffers

**Attack Pattern ID:** 100
**Abstraction:** Standard

**Status:** Draft
**Completeness:** Complete

***Presentation Filter:*** Basic

### Summary

Buffer Overflow attacks target improper or missing bounds checking on buffer operations, typically triggered by input injected by an attacker. As a consequence, an attacker is able to write past the boundaries of allocated buffer regions in memory, causing a program crash or potentially redirection of execution as per the attackers' choice.

### Attack Prerequisites

- Targeted software performs buffer operations.
- Targeted software inadequately performs bounds-checking on buffer operations.
- Attacker has the capability to influence the input to buffer operations.

### Solutions and Mitigations

Use a language or compiler that performs automatic bounds checking.

Use secure functions not vulnerable to buffer overflow.

If you have to use dangerous functions, make sure that you do boundary checking.

Compiler-based canary mechanisms such as StackGuard, ProPolice and the Microsoft Visual Studio /GS flag. Unless this provides automatic bounds checking, it is not a complete solution.

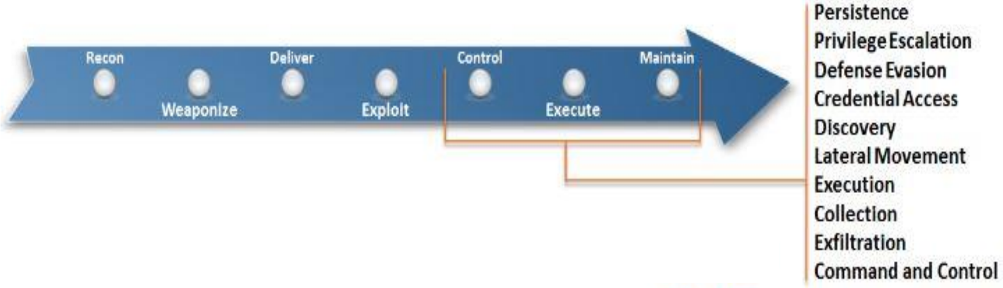
Use OS-level preventative functionality. Not a complete solution.

Utilize static source code analysis tools to identify potential buffer overflow weaknesses in the software.

https://capec.mitre.org/data/definitions/100.html

# Adversary Tactics, Techniques, and Common Knowledge (ATT&CK)

- **Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a model and framework for describing the actions an adversary may take while operating within an enterprise network**
  - Can be used to characterize post-Exploit adversary behavior
    - Focuses on Control, Execute, and Maintain steps within the cyber attack lifecycle[1]



Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control

  - Can be used to help prioritize network defense against advanced persistent threat (APT) threat actors operating within the network
  - TTPs provide technical descriptions, indicators, targeted platforms, sensor data, detection analytics, and potential mitigations

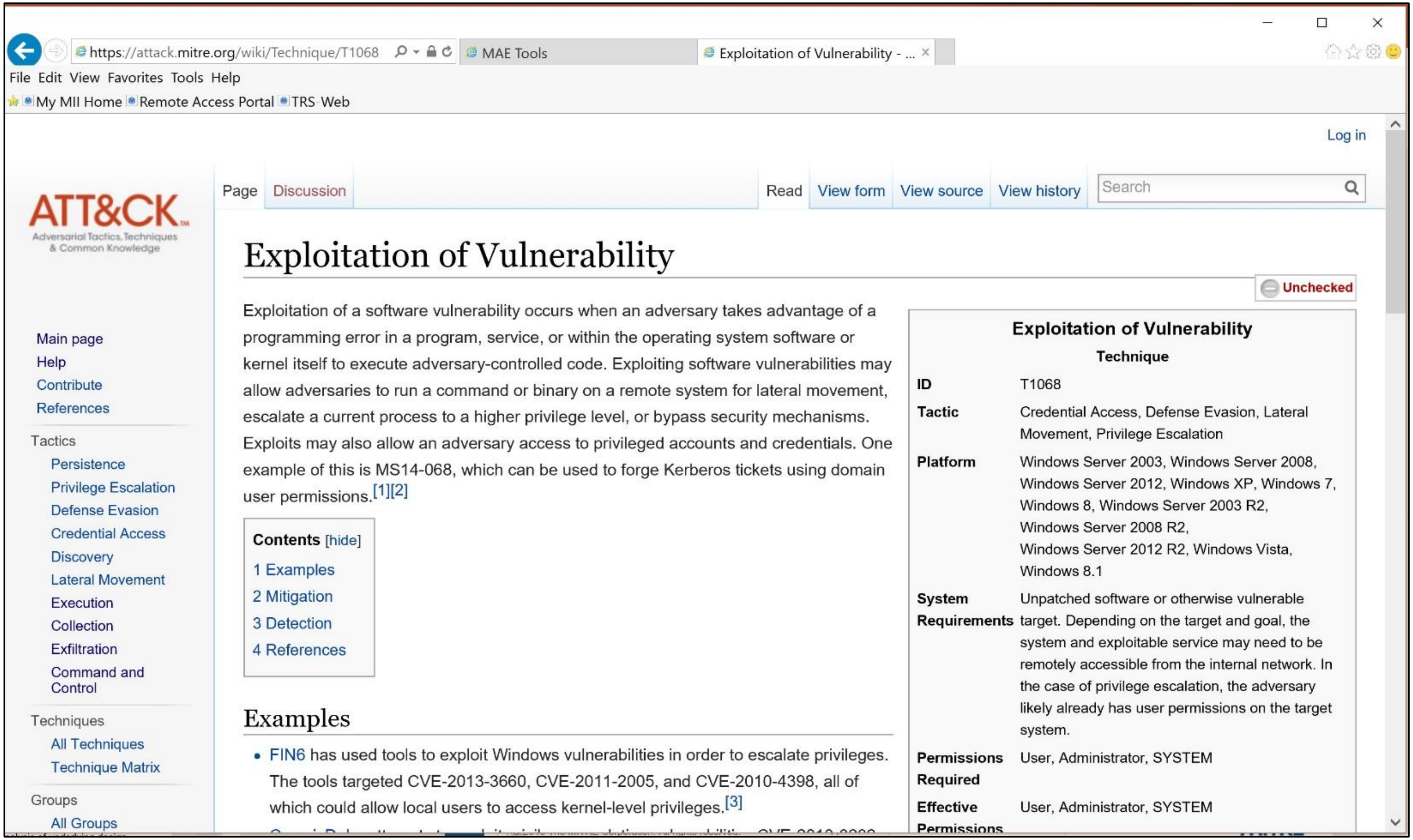
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

# ATT&CK Taxonomy: Post Exploit Adversary TTPs

| Persistence | Privilege Escalation | Defense Evasion | Credential Access | Host Enumeration | Lateral Movement | Execution | C2 | Exfiltration |
|---|---|---|---|---|---|---|---|---|
| Legitimate Credentials | Legitimate Credentials | Legitimate Credentials | Credential Dumping | Account enumeration | Application deployment software | Command Line | Commonly used port | Automated or scripted exfiltration |
| Accessibility Features | Accessibility Features | Binary Padding | Credentials in Files | File system enumeration | Exploitation of Vulnerability | File Access | Comm through removable media | Data compressed |
| AddMonitor | AddMonitor | DLL Side-Loading | Network Sniffing | Group permission enumeration | Logon scripts | PowerShell | Custom application layer protocol | Data encrypted |
| DLL Search Order Hijack | DLL Search Order Hijack | Disabling Security Tools | User Interaction | Local network connection enumeration | Pass the hash | Process Hollowing | Custom encryption cipher | Data size limits |
| Edit Default File Handlers | Edit Default File Handlers | File System Logical Offsets | Credential manipulation | Local networking enumeration | Pass the ticket | Registry | Data obfuscation | Data staged |
| New Service | New Service | Process Hollowing | | Operating system enumeration | Peer connections | Rundll32 | Fallback channels | Exfil over C2 channel |
| Path Interception | Path Interception | Rootkit | | Owner/User enumeration | Remote Desktop Protocol | Scheduled Task | Multiband comm | Exfil over alternate channel to C2 network |
| Scheduled Task | Scheduled Task | Bypass UAC | | Process enumeration | Windows management instrumentation | Service Manipulation | Multilayer encryption | Exfil over other network medium |
| Service File Permission Weakness | Service File Permission Weakness | DLL Injection | | Security software enumeration | Windows remote management | Third Party Software | Peer connections | Exfil over physical medium |
| Shortcut Modification | Shortcut Modification | Indicator blocking on host | | Service enumeration | Remote Services | Windows management instrumentation | Standard app layer protocol | From local system |
| Web shell | Web shell | Indicator removal from tools | | Window enumeration | Replication through removable media | Windows remote management | Standard non-app layer protocol | From network resource |
| BIOS | Bypass UAC | Indicator removal from host | | | Shared webroot | | Standard encryption cipher | From removable media |
| Hypervisor Rootkit | DLL Injection | Masquerading | | | Taint shared content | | Uncommonly used port | Scheduled transfer |
| Logon Scripts | Exploitation of Vulnerability | NTFS Extended Attributes | | | Windows admin shares | | | |
| Master Boot Record | | Obfuscated Payload | | | | | | |
| Mod. Exist’g Service | | Rundll32 | | | | | | |
| Registry Run Keys | | Scripting | | | | | | |
| Serv. Reg. Perm. Weakness | | Software Packing | | | | | | |
| Windows Mgmt Instr. Event Subsc. | | Timestomp | | | | | | |
| Winlogon Helper DLL | | | | | | | | |

http://attack.mitre.org

# An Example ATT&CK Technique



https://attack.mitre.org/wiki/Technique/T1068
MAE Tools
Exploitation of Vulnerability - ...
File Edit View Favorites Tools Help
My MII Home
Remote Access Portal
TRS Web
Log in
Page
Discussion
Read
View form
View source
View history
Search
ATT&CK
Adversarial Tactics, Techniques & Common Knowledge

Main page
Help
Contribute
References

Tactics
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

Techniques
- All Techniques
- Technique Matrix

Groups
- All Groups

## Exploitation of Vulnerability

Unchecked

Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Exploiting software vulnerabilities may allow adversaries to run a command or binary on a remote system for lateral movement, escalate a current process to a higher privilege level, or bypass security mechanisms. Exploits may also allow an adversary access to privileged accounts and credentials. One example of this is MS14-068, which can be used to forge Kerberos tickets using domain user permissions.[1][2]

**Exploitation of Vulnerability**

**Technique**

| | |
|---|---|
| **ID** | T1068 |
| **Tactic** | Credential Access, Defense Evasion, Lateral Movement, Privilege Escalation |
| **Platform** | Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1 |
| **System Requirements** | Unpatched software or otherwise vulnerable target. Depending on the target and goal, the system and exploitable service may need to be remotely accessible from the internal network. In the case of privilege escalation, the adversary likely already has user permissions on the target system. |
| **Permissions Required** | User, Administrator, SYSTEM |
| **Effective Permissions** | User, Administrator, SYSTEM |

**Contents** [hide]
1 Examples
2 Mitigation
3 Detection
4 References

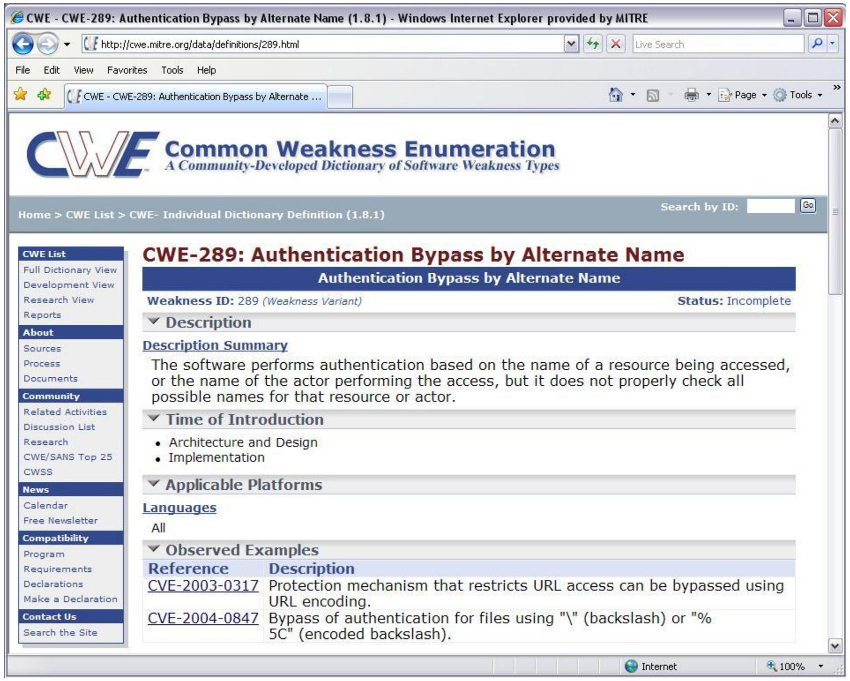
## Examples

- FIN6 has used tools to exploit Windows vulnerabilities in order to escalate privileges. The tools targeted CVE-2013-3660, CVE-2011-2005, and CVE-2010-4398, all of which could allow local users to access kernel-level privileges.[3]

https://attack.mitre.org/wiki/Technique/T1068

# Common Weakness Enumeration (CWE)

- **MITRE open source repository of software weaknesses**
  - Over 800 weaknesses currently identified
  - Updated quarterly


CWE - CWE-289: Authentication Bypass by Alternate Name (1.8.1) - Windows Internet Explorer provided by MITRE
http://cwe.mitre.org/data/definitions/289.html
Live Search
File
Edit
View
Favorites
Tools
Help
CWE - CWE-289: Authentication Bypass by Alternate ...
Page
Tools
Internet
100%

Common Weakness Enumeration
*A Community-Developed Dictionary of Software Weakness Types*

Home > CWE List > CWE- Individual Dictionary Definition (1.8.1)

Search by ID: Go

**CWE List**
Full Dictionary View
Development View
Research View
Reports
**About**
Sources
Process
Documents
**Community**
Related Activities
Discussion List
Research
CWE/SANS Top 25
CWSS
**News**
Calendar
Free Newsletter
**Compatibility**
Program
Requirements
Declarations
Make a Declaration
**Contact Us**
Search the Site

**CWE-289: Authentication Bypass by Alternate Name**

**Authentication Bypass by Alternate Name**

**Weakness ID:** 289 *(Weakness Variant)* **Status:** Incomplete

**Description**

Description Summary

The software performs authentication based on the name of a resource being accessed, or the name of the actor performing the access, but it does not properly check all possible names for that resource or actor.

**Time of Introduction**

- Architecture and Design
- Implementation

**Applicable Platforms**

Languages

All

**Observed Examples**

| Reference | Description |
|---|---|
| CVE-2003-0317 | Protection mechanism that restricts URL access can be bypassed using URL encoding. |
| CVE-2004-0847 | Bypass of authentication for files using "\" (backslash) or "%5C" (encoded backslash). |

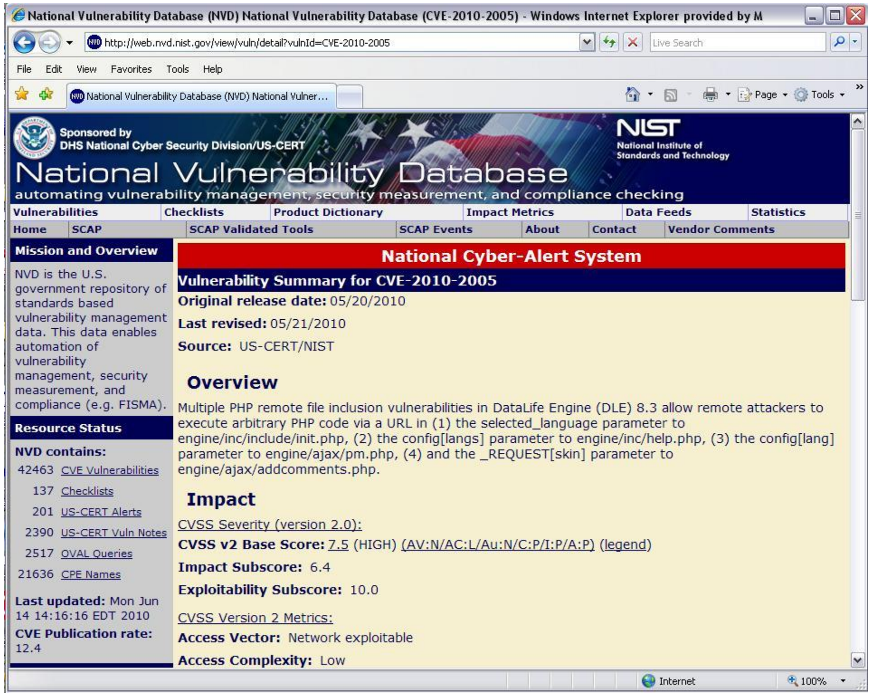
http://cwe.mitre.org/

## Derivation of Attack Vectors

- Cross-reference CWE and CAPEC to identify a range of attack patterns for a given set of software weaknesses
  - Example: Top 25 SANS/CWE weaknesses

# Common Vulnerabilities and Exposures (CVE)

- **Open source repository of software vulnerabilities**
  - Over 79000 CVEs reported across commercial software products
  - Weekly release cycle
- **Derivation of Attack Vectors**
  - Cross reference CVE with CAPEC to identify patterns that can exploit a given software vulnerability
  - Can be used to correlate vulnerabilities with specific technologies
    - Example: SNMP related attack vectors added to TARA catalog based on CVE vulnerabilities reported for SNMP agents


National Vulnerability Database (NVD) National Vulnerability Database (CVE-2010-2005) - Windows Internet Explorer provided by M
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2005
Live Search
File
Edit
View
Favorites
Tools
Help
National Vulnerability Database (NVD) National Vulner...
Page
Tools
Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
Product Dictionary
Impact Metrics
Data Feeds
Statistics
Home
SCAP
SCAP Validated Tools
SCAP Events
About
Contact
Vendor Comments
Internet
100%

**Mission and Overview**

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

**Resource Status**

**NVD contains:**

| | |
|---|---|
| 42463 | CVE Vulnerabilities |
| 137 | Checklists |
| 201 | US-CERT Alerts |
| 2390 | US-CERT Vuln Notes |
| 2517 | OVAL Queries |
| 21636 | CPE Names |

**Last updated:** Mon Jun 14 14:16:16 EDT 2010

**CVE Publication rate:** 12.4

**National Cyber-Alert System**

**Vulnerability Summary for CVE-2010-2005**

**Original release date:** 05/20/2010

**Last revised:** 05/21/2010

**Source:** US-CERT/NIST

**Overview**

Multiple PHP remote file inclusion vulnerabilities in DataLife Engine (DLE) 8.3 allow remote attackers to execute arbitrary PHP code via a URL in (1) the selected_language parameter to engine/inc/include/init.php, (2) the config[langs] parameter to engine/inc/help.php, (3) the config[lang] parameter to engine/ajax/pm.php, (4) and the _REQUEST[skin] parameter to engine/ajax/addcomments.php.

**Impact**

CVSS Severity (version 2.0):

**CVSS v2 Base Score:** 7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) (legend)

**Impact Subscore:** 6.4

**Exploitability Subscore:** 10.0

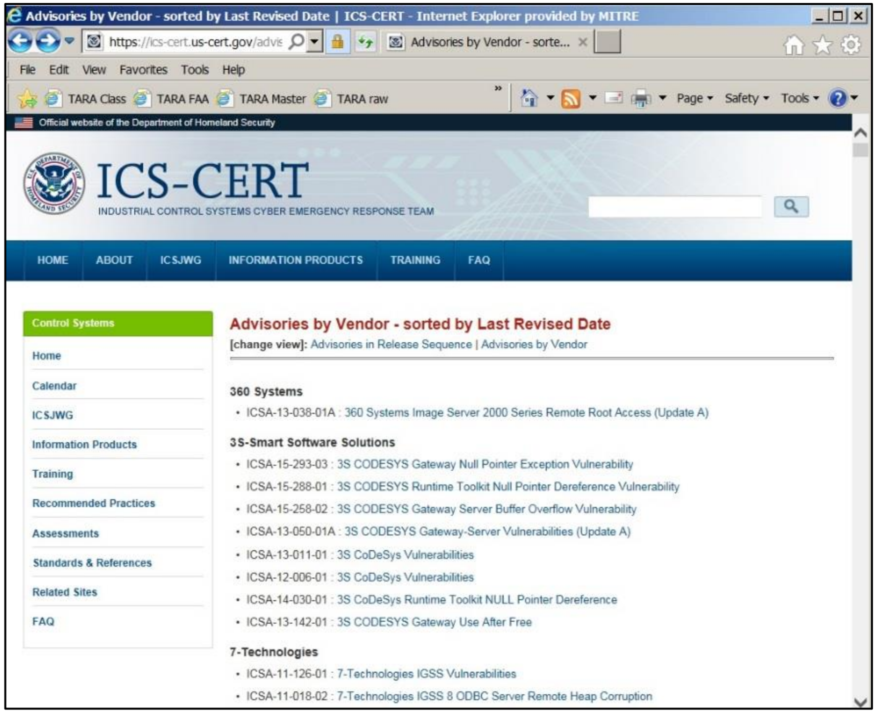
CVSS Version 2 Metrics:

**Access Vector:** Network exploitable

**Access Complexity:** Low

http://cve.mitre.org/

# ICS-CERT Advisories


Advisories by Vendor - sorted by Last Revised Date | ICS-CERT - Internet Explorer provided by MITRE
https://ics-cert.us-cert.gov/advis
Advisories by Vendor - sorte...
File Edit View Favorites Tools Help
TARA Class
TARA FAA
TARA Master
TARA raw
Page
Safety
Tools
Official website of the Department of Homeland Security
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
HOME
ABOUT
ICSJWG
INFORMATION PRODUCTS
TRAINING
FAQ
Control Systems
Home
Calendar
ICSJWG
Information Products
Training
Recommended Practices
Assessments
Standards & References
Related Sites
FAQ

**Advisories by Vendor - sorted by Last Revised Date**

[change view]: Advisories in Release Sequence | Advisories by Vendor

**360 Systems**

- ICSA-13-038-01A : 360 Systems Image Server 2000 Series Remote Root Access (Update A)

**3S-Smart Software Solutions**

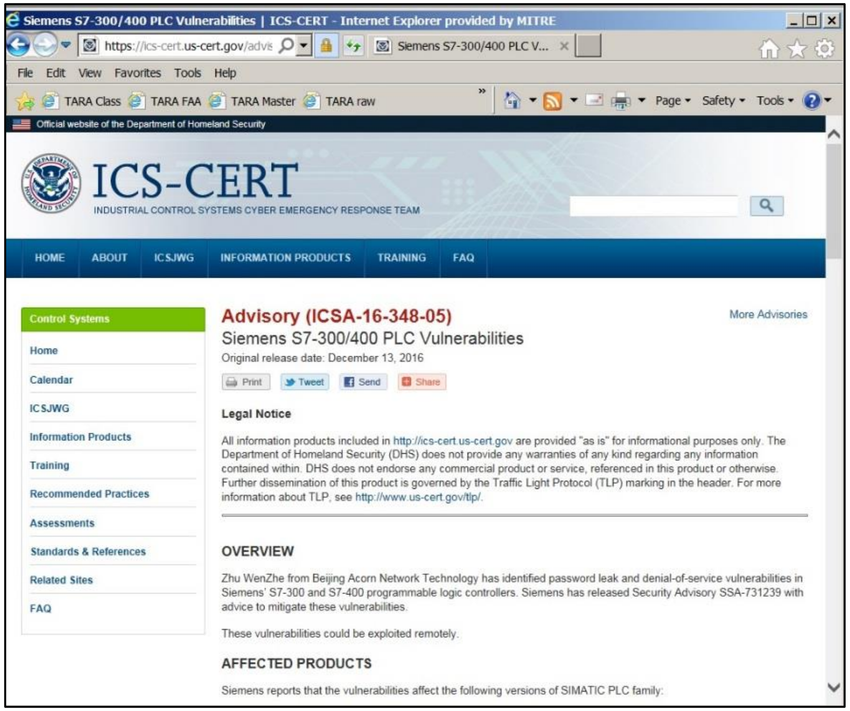
- ICSA-15-293-03 : 3S CODESYS Gateway Null Pointer Exception Vulnerability
- ICSA-15-288-01 : 3S CODESYS Runtime Toolkit Null Pointer Dereference Vulnerability
- ICSA-15-258-02 : 3S CODESYS Gateway Server Buffer Overflow Vulnerability
- ICSA-13-050-01A : 3S CODESYS Gateway-Server Vulnerabilities (Update A)
- ICSA-13-011-01 : 3S CoDeSys Vulnerabilities
- ICSA-12-006-01 : 3S CoDeSys Vulnerabilities
- ICSA-14-030-01 : 3S CoDeSys Runtime Toolkit NULL Pointer Dereference
- ICSA-13-142-01 : 3S CODESYS Gateway Use After Free

**7-Technologies**

- ICSA-11-126-01 : 7-Technologies IGSS Vulnerabilities
- ICSA-11-018-02 : 7-Technologies IGSS 8 ODBC Server Remote Heap Corruption

Each advisory identifies the affected product(s), impact, vulnerability, and mitigation.

Advisories provide information about current security issues, vulnerabilities, and exploits, organized by vendor.


Siemens S7-300/400 PLC Vulnerabilities | ICS-CERT - Internet Explorer provided by MITRE
https://ics-cert.us-cert.gov/advis
Siemens S7-300/400 PLC V...
File Edit View Favorites Tools Help
TARA Class
TARA FAA
TARA Master
TARA raw
Page
Safety
Tools
Official website of the Department of Homeland Security
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
HOME
ABOUT
ICSJWG
INFORMATION PRODUCTS
TRAINING
FAQ
Control Systems
Home
Calendar
ICSJWG
Information Products
Training
Recommended Practices
Assessments
Standards & References
Related Sites
FAQ
More Advisories
Print
Tweet
Send
Share

**Advisory (ICSA-16-348-05)**

Siemens S7-300/400 PLC Vulnerabilities

Original release date: December 13, 2016

**Legal Notice**

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

**OVERVIEW**

Zhu WenZhe from Beijing Acorn Network Technology has identified password leak and denial-of-service vulnerabilities in Siemens' S7-300 and S7-400 programmable logic controllers. Siemens has released Security Advisory SSA-731239 with advice to mitigate these vulnerabilities.

These vulnerabilities could be exploited remotely.

**AFFECTED PRODUCTS**

Siemens reports that the vulnerabilities affect the following versions of SIMATIC PLC family:

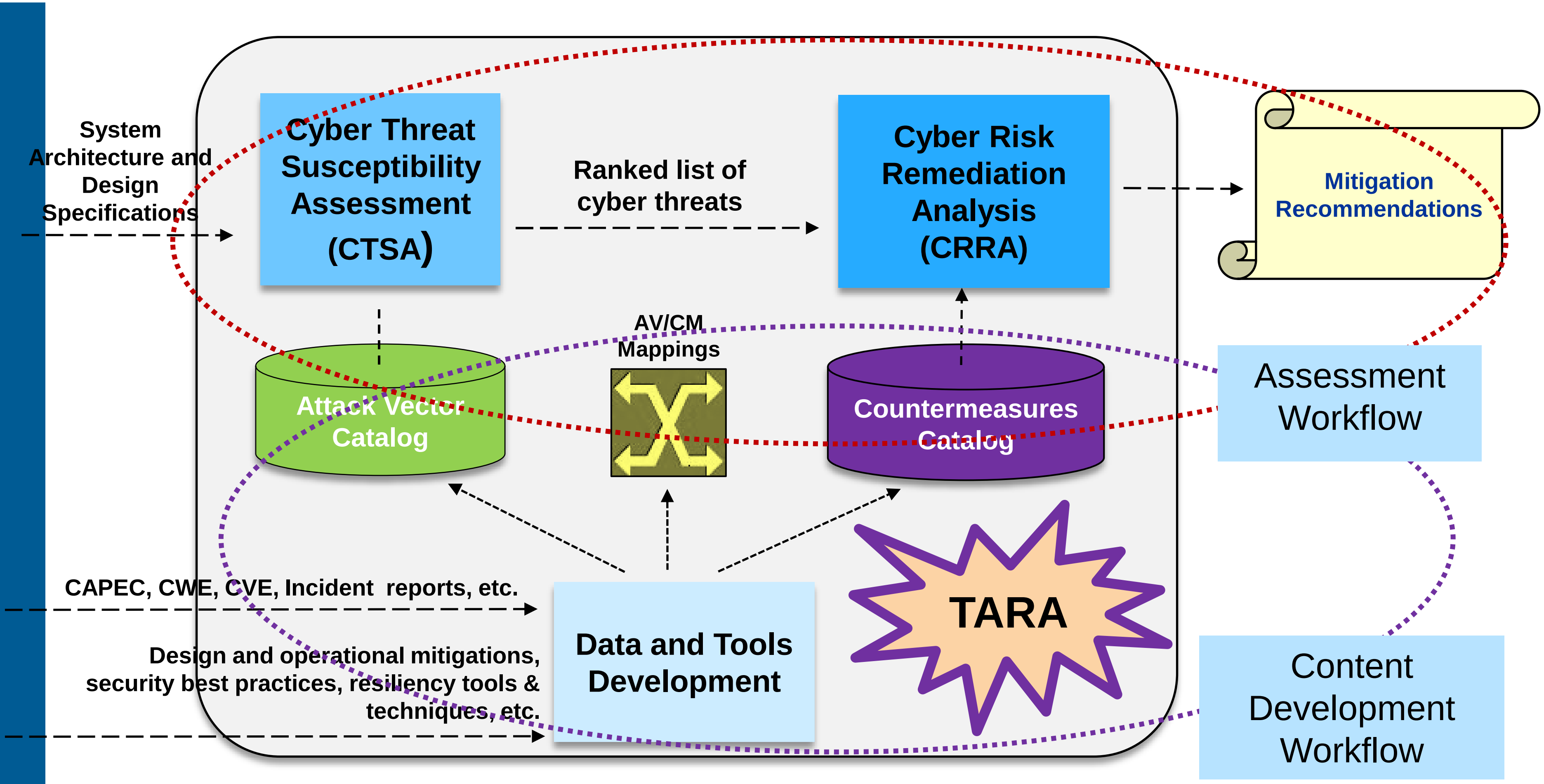
https://ics-cert.us-cert.gov/

# The TARA Assessment Methodology

# Threat Assessment & Remediation Analysis (TARA)

- **MITRE-developed methodology to identify and assess cyber threats and select countermeasures effective at mitigating those threats**
  - Leverages catalog of Attack Vectors (AVs), Countermeasures (CMs), and associated mappings
    - Use of catalog ensures that findings are consistent across assessments
  - Uses scoring models to quantitatively assess AVs and CMs
    - AVs ranked by risk, providing a basis for effective triage
    - CMs ranked by cost-effectiveness, providing a basis for identifying optimal solutions
  - Delivers recommendations
    - Allows programs to make informed choices on how best to improve a system’s security posture and resilience

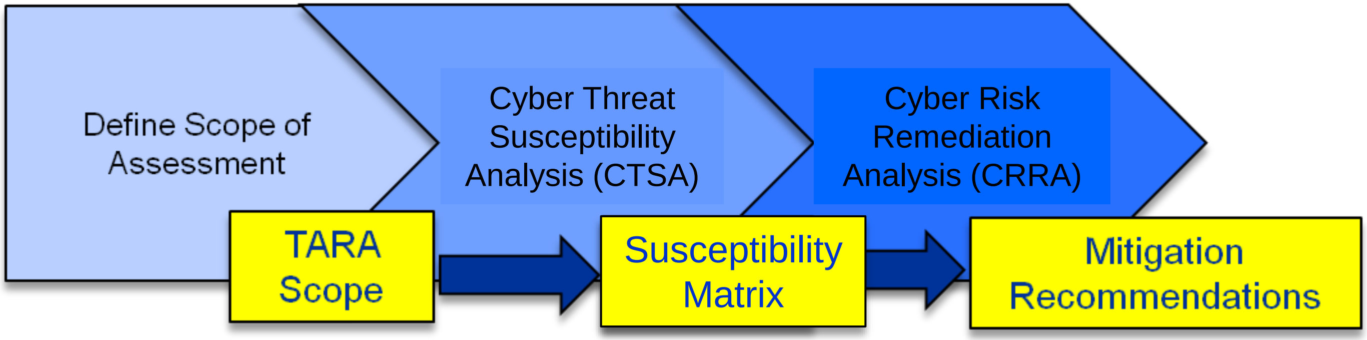
# TARA Methodology Workflows


System Architecture and Design Specifications
Cyber Threat Susceptibility Assessment (CTSA)
Ranked list of cyber threats
Cyber Risk Remediation Analysis (CRRA)
Mitigation Recommendations
AV/CM Mappings
Attack Vector Catalog
Countermeasures Catalog
Assessment Workflow
CAPEC, CWE, CVE, Incident reports, etc.
Design and operational mitigations, security best practices, resiliency tools & techniques, etc.
Data and Tools Development
TARA
Content Development Workflow

*Workflow – Sequence of connected activities that produce useful work*

# Phases of a TARA Assessment

Objective is to identify and assess cyber threats and select countermeasures effective at mitigating those threats


Define Scope of Assessment
Cyber Threat Susceptibility Analysis (CTSA)
Cyber Risk Remediation Analysis (CRRA)
TARA Scope
Susceptibility Matrix
Mitigation Recommendations

The evaluation target(s)

The range of threats to be assessed

The adversary

The phase of the system acquisition lifecycle

Verify assessment scope with sponsor

Model the target

Perform catalog search to identify candidate AVs

Eliminate implausible AVs

Define a scoring model to rank plausible AVs

Construct the Susceptibility Matrix

Select AVs to mitigate

Use mitigation mappings to identify candidate countermeasures (CMs)

Eliminate implausible CMs

Define a scoring model to rank CMs

Select the best CM solution set

Develop well-formed recommendations

# TARA Assessment Products

## Susceptibility Matrix

*Provides a ranked list of cyber threats, mapped to components of the evaluation target*

| Attack Vectors | | Risk Score | Shopping cart | | | |
|---|---|---|---|---|---|---|
| AV ID | AV Name | | Browser | Database | Web Server | Email App |
| T000049 | Buffer Overflow | High | X | X | X | X |
| T000014 | Accessing, Intercepting, and Modifying HTTP Cookies | Moderate | X | | | X |
| T000050 | Forced Integer Overflow | Moderate | | X | | |
| T000071 | SOAP Array Overflow | Moderate | | | X | |
| T000052 | Inducing buffer overflow to disable input validation | Low | | X | | X |
| T000170 | Attack through shared data | Low | X | | X | |

***Answers the questions: Where and how is my system most susceptible?***

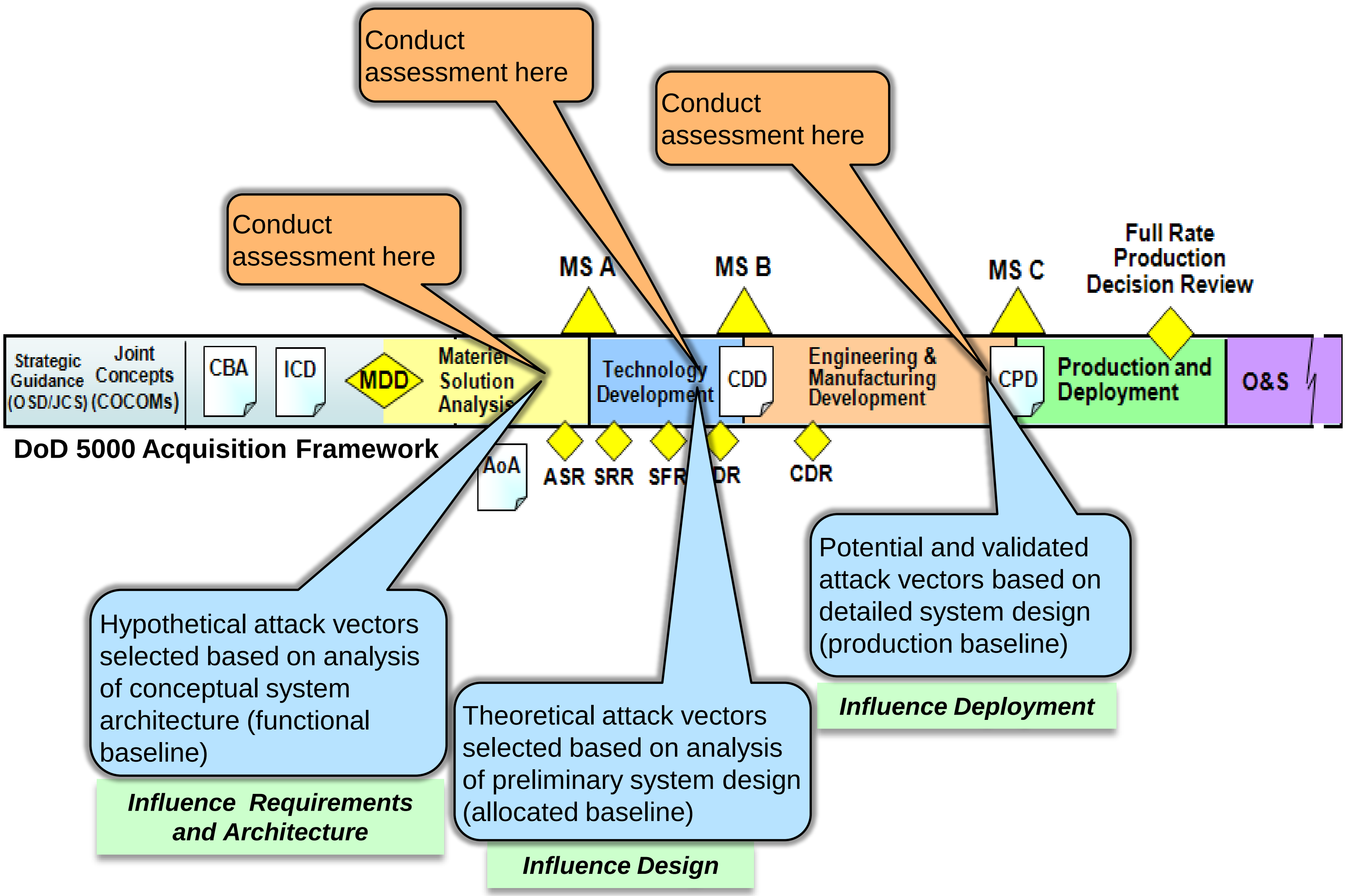
## Solution Effectiveness Table

*Provides a ranked list of countermeasures, mapped to cyber threats, and identifies the preventative or mitigating effect each countermeasure provides*

| Countermeasure (CM) | | Scoring | Effect (by Attack Vector ID) | | | | | |
|---|---|---|---|---|---|---|---|---|
| CM ID | Name | U/C Ratio | T000014 | T000049 | T000050 | T000052 | T000071 | T000170 |
| C000134 | Select programming languages that minimize software defects | 75 | | PM | PM | PM | | |
| C000117 | Apply principle of least privilege | 67 | | | | | RM | RM |
| C000093 | Merge data streams prior to validation | 50 | | | | PM | | |
| C000096 | Use vetted runtime libraries | 50 | | PH | | | PH | |
| C000047 | Encrypt session cookies | 33 | PH | | | | | |
| C000051 | Use digital signatures/checksums | 33 | PH | | | | | |
| C000132 | Use sandboxing to isolate running software | 25 | | | | | | PM |
| | TOTALS | 333 | 2 | 2 | 1 | 2 | 2 | 2 |

***Answers the questions: How are my threats mitigated and where are the gaps?***

# Threat-informed Systems Analysis for Acquisition Programs


MS A
MS B
MS C
Full Rate Production Decision Review
Strategic Guidance (OSD/JCS)
Joint Concepts (COCOMs)
CBA
ICD
MDD
Materiel Solution Analysis
Technology Development
CDD
Engineering & Manufacturing Development
CPD
Production and Deployment
O&S
AoA
ASR
SRR
SFR
PDR
CDR

DoD 5000 Acquisition Framework

Conduct assessment here

Conduct assessment here

Conduct assessment here

Hypothetical attack vectors selected based on analysis of conceptual system architecture (functional baseline)

***Influence Requirements and Architecture***

Theoretical attack vectors selected based on analysis of preliminary system design (allocated baseline)

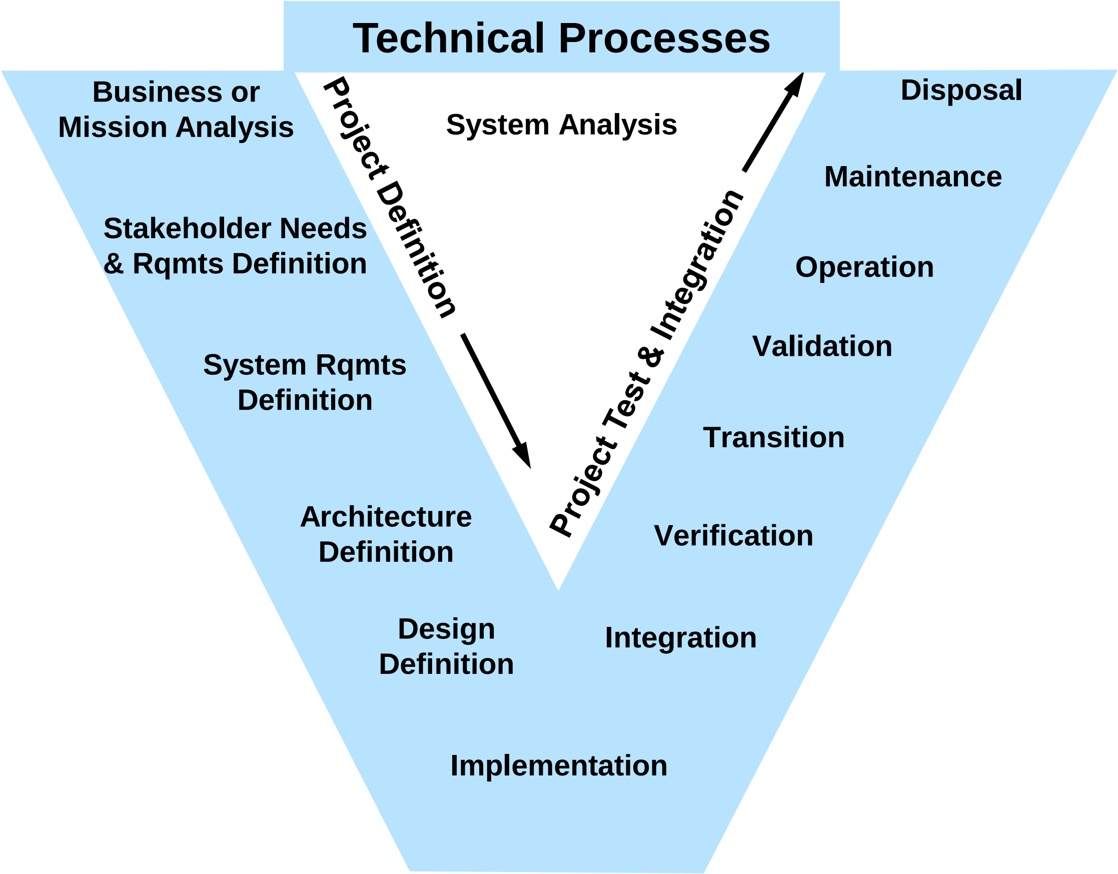
***Influence Design***

Potential and validated attack vectors based on detailed system design (production baseline)

***Influence Deployment***

# System Life Cycle Processes

The Systems Engineering “Vee” Model



ISO/IEC/IEEE 15288, System life cycle processes, 2015-05-15

## Agreement Processes

- Acquisition
- Supply

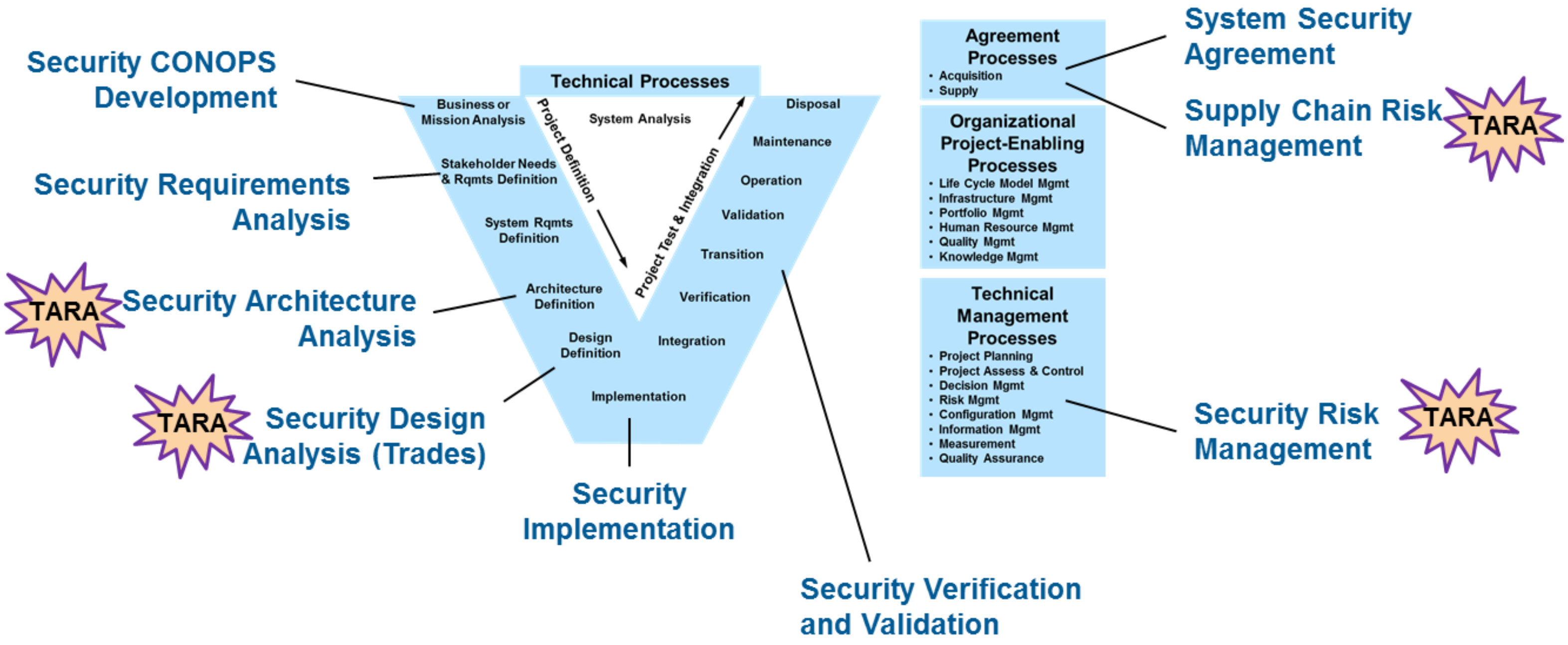
## Organizational Project-Enabling Processes

- Life Cycle Model Mgmt
- Infrastructure Mgmt
- Portfolio Mgmt
- Human Resource Mgmt
- Quality Mgmt
- Knowledge Mgmt

## Technical Management Processes

- Project Planning
- Project Assess & Control
- Decision Mgmt
- Risk Mgmt
- Configuration Mgmt
- Information Mgmt
- Measurement
- Quality Assurance

# Systems Security Engineering (SSE) Framework



Security CONOPS Development

Security Requirements Analysis

TARA Security Architecture Analysis

TARA Security Design Analysis (Trades)

Security Implementation

Security Verification and Validation

Technical Processes

Business or Mission Analysis

Stakeholder Needs & Rqmts Definition

System Rqmts Definition

Architecture Definition

Design Definition

Implementation

Integration

Verification

Transition

Validation

Operation

Maintenance

Disposal

System Analysis

Project Definition

Project Test & Integration

Agreement Processes
- Acquisition
- Supply

Organizational Project-Enabling Processes
- Life Cycle Model Mgmt
- Infrastructure Mgmt
- Portfolio Mgmt
- Human Resource Mgmt
- Quality Mgmt
- Knowledge Mgmt

Technical Management Processes
- Project Planning
- Project Assess & Control
- Decision Mgmt
- Risk Mgmt
- Configuration Mgmt
- Information Mgmt
- Measurement
- Quality Assurance

System Security Agreement

Supply Chain Risk Management TARA

Security Risk Management TARA

## Applications of TARA in the SSE Framework

- Security architecture analysis / threat model development
- Countermeasure selection (trade)
- Cyber risk assessments
- SCRM assessments

# What’s Next?

- **TARA has been used to conduct cyber risk assessments for DoD acquisition programs since 2010**
  - Changes in the methodology can lead to different kinds of assessments and assessment artifacts
  - Changes to the underlying data model and/or technical content make possible assessments on different kinds of systems

- **Decision support for cyber incident analysis and response is a form of risk assessment conducted in an operational context**

- **Adaptation of TARA to support operational risk assessments**
  - Changes in how catalog data is selected and evaluated
  - Catalog content specific to nuclear reactor safety and control systems
  - Taxonomies that facilitate navigation within large sets of data

# Backup Slides

# Assessing Countermeasure Effects

**The following table provides guidance for assessing the effect a countermeasure has on a given attack vector**

| **Countermeasure Effect** | ***Tends to be…*** | | |
|---|---|---|---|
| | **Prevent** | **Detect** | **Respond** |
| *The countermeasure disrupts the attack's sequence of activities* | X | | |
| *The countermeasure eliminates condition(s) necessary for the attack to occur* | X | | |
| *The countermeasure facilitates detection of conditions leading to an attack* | X | X | |
| *The countermeasure reduces the likelihood of the attack being successful* | | | X |
| *The countermeasure minimizes the extent of damage or disruption* | | | X |
| *The countermeasure facilitates rapid recovery/reconstitution after the attack occurs* | | | X |
| *The countermeasure facilitates forensic analysis and/or attribution following an attack* | | X | X |