Supply Chain Information Exchange:
Non-conforming & Authentic Components

Joe Jarzombek

Director for Software and Supply Chain Assurance

Stakeholder Engagement & Cyber Infrastructure Resilience

Homeland Security

Agenda

- Purpose
- Overview
- Community of Interest
- Environment
- Opportunities
- Methodology
- Leveraging Structured Representations to Support Consistency and Automation
- Next Steps

Homeland Security

Purpose

- Elicit Stakeholder Collaboration for Security Automation efforts associated with Supply Chain Risk Management:
  - Standardize taxonomies for component conformance to specifications and authenticity
  - Develop standard information sharing mechanisms, such as a “Supply Chain Observable eXpression” language and associated data dictionary

Homeland Security

Overview

- The USG and industry partners are working toward solutions to reduce counterfeit information and communications technology (ICT) supply chain risks.
- The USG and industry partners need a scalable means to report and detect ICT supply chain risks attributable to counterfeits, defects, and tainted components (i.e. non-conforming components/parts).
- Existing structured representations can be leveraged to support consistency and automation of reporting and detecting non-conforming components/parts.

Homeland Security

Community of Interest

- There are multiple government, industry, and associations who are engaged in counterfeit taxonomies and anti-counterfeiting, at large. Below are a sample of said entities:

Government	Industry	Academia and Associations
• MDA • DLA • FAA • US Navy • US Army • CBP • ICE • and many others	• SMT • BAE • Honeywell • American Electronic Resource	• Center For Hardware Assurance and Security Engineering (CHASE) • SAE • CALCE University of Maryland • ERAI • AIA • IDEA

Homeland Security

Community of Interest (example)

- CHASE strives to unite commercial, academic and government expertise to enhance the nation's hardware assurance and security. Their current and past project sponsors include:

Industry

Government

Homeland Security

Community of Interest

- What communities have databases for identifying non-conformant components?
  - **Government-Industry Data Exchange Program (GIDEP)**: Cooperative activity between USG and industry participants to reduce resource expenditures by sharing technical information.
  - **Joint Deficiency Reporting System (JDRS)**: Cross-service, web-enabled automated tracking system across the Aeronautical Enterprise. designed to initiate, process and track deficiency reports from the Warfighter through the investigation process.
  - **ERAI, Inc**: Privately held global information services organization that monitors, investigates and reports issues affecting the global semiconductor supply chain.
  - **Product Data Reporting and Evaluation Program (PDREP)**: Product Quality Deficiency Report for the Department of the Navy.
  - **Suspected Unapproved Parts (SUP) Program**: Used by the Federal Aviation Administration (FAA).

Homeland Security

Community of Interest

- What entities currently have counterfeit taxonomies?
  - University of Connecticut Center for Hardware Assurance, Security, and Engineering (CHASE)
  - SAE Standards AS5553 “Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition”
  - Department of the Navy’s Product Data Reporting and Evaluation Program (PDREP) Product Quality Deficiency Report
  - Department of Energy Annual Counterfeit Report

Homeland Security

Environment

- Departments' and Agencies' (D/A's) counterfeit management programs vary in approach and maturity.
- There are a number of counterfeit databases that are not used to their fullest potential (e.g., GIDEP).
- Various definitions and characterization of counterfeits across the USG complicates the issue (e.g., many quality assurance procedures reflect existing counterfeit standards, but are not explicitly counterfeit guidance).
- The level of sophistication for testing counterfeits varies across D/As.
- The verification of data entered into counterfeit databases and confidence level for testing techniques are unclear.
- Not all D/A's approaches to counterfeits have uniform reporting procedures.
- The majority of D/As may prioritize the inspection of suspect counterfeit items based on factors that include mission criticality.

Homeland Security

Opportunities

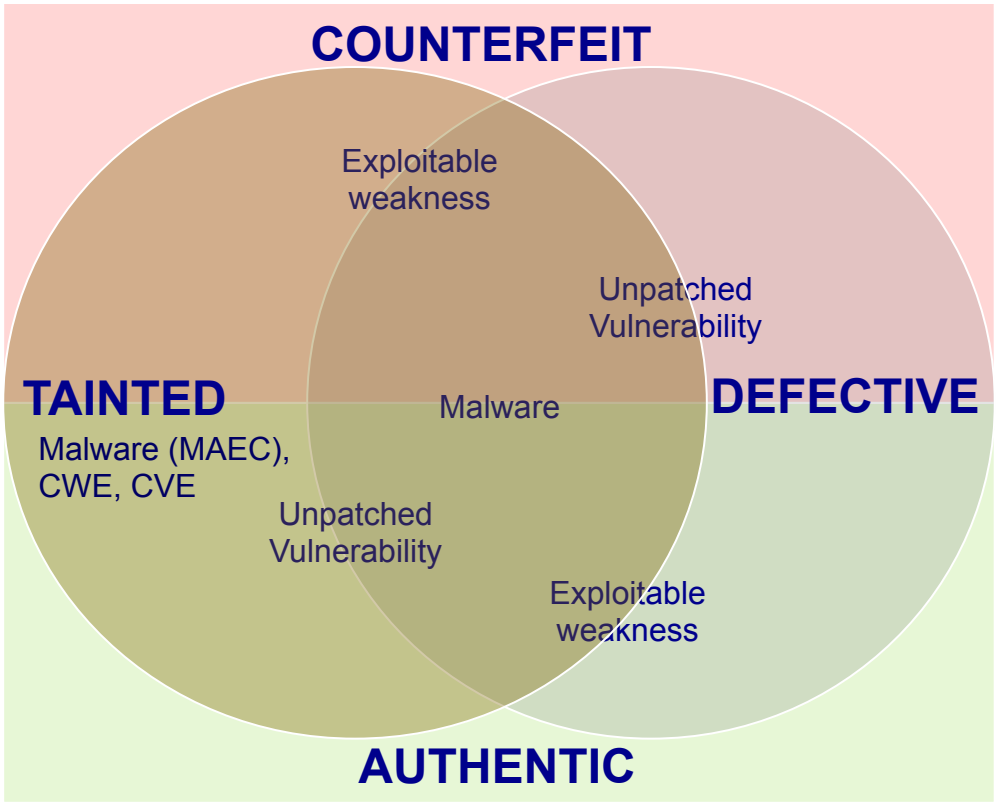
- **Need for a common language for communicating and interacting within the USG (among D/A's) and with industry**
- **Need for sharing information on authentic components**
  - Facilitates research into and detection of non-conforming items
- **Need for sharing information on non-conforming components**
  - Ability to create repository of searchable data for identification, trend analysis, etc.
- **Need to reduce test cost and time**
  - Ability to reduce the cost of testing, reporting, and maintaining counterfeit-free components
- **Need to encourage OCM-level anti-counterfeiting techniques**
  - Most economical method to add track and trace capability to a chip
- **Need to establish mechanisms and test flows to benchmark the testing techniques and counterfeit ICs**

Homeland Security

Methodology

Taxonomy for Conforming & Non-Conforming Components/Parts

- Catalogue Methods for Detection, Testing, and Anti-Counterfeiting
- Build Taxonomies for determining:
  - Authentic components
  - Counterfeit components
  - Defective components
  - Tainted components containing malware (MAEC, exploitable weaknesses (CWE), and known vulnerabilities (CVE)
- Define Observables
- Leverage existing structured representations to 'scale' detection & reporting of counterfeits



Components can become tainted intentionally or unintentionally throughout the supply chain, SDLC, and in Ops & sustainment

*Text demonstrates *examples* of overlap

Homeland Security

Leveraging Structured Representations to Support Consistency and Automation

After defining 'observables' for each type of non-conformant component (including defective and tainted components), the following enumerations, languages, and schemas would be used to specify extensions that cover counterfeits, authentic components, and defects. These enumerations include:

- **CVE** to reference vulnerabilities in defective or tainted components (http://cve.mitre.org/)
- **CWE** to represent weaknesses leading to defective or tainted components (http://cwe.mitre.org/)
- **MAEC** to represent characterization of malicious logic in tainted components (http://maec.mitre.org/)
- **CAPEC** to represent approaches in the Counterfeiting taxonomy (http://capec.mitre.org/)
- **CybOX** to represent observable characteristics for detection/determination of non-conformant components (http://cybox.mitre.org/)
- **STIX** to represent non-conformant patterns, Anti-counterfeiting approaches and other threat context (http://stix.mitre.org/
- **TAXII** to enable sharing of actionable cyber threat information across organization and product/service boundaries (http://taxii.mitre.org/)

Homeland Security

Next Steps

In moving forward, need to leverage support from engaged stakeholders and harmonize existing counterfeit taxonomies to ensure automation efforts align with industry, academia, and government-wide approaches.

- Formalize taxonomies for conforming and non-conforming parts
- Build-and maintain catalogue of detection & anti-counterfeiting methods and establish mechanisms and test flows to benchmark techniques
- Test ability to create automated tools for observables and identify gaps in existing enumerations and languages
- Specify extensions that covers counterfeits, authentic components, and defects
- Specify relevant data dictionaries to serve as clear description of the expressivity needed (including identifying and filling the gaps between CybOX and SCOX).
- Ensure “XXXX-as-a-Service” supply chain risks are addressed in moving to the Cloud for software, IT, platform, communications and data services
- Ensure automation efforts reduce test cost and time

Homeland Security

Homeland Security

Background

Leveraging Structured Representations to Support Consistency and Automation

Common Attack Pattern Enumeration and Classification (CAPEC)

- **Community effort targeted at:**
  - Standardizing the capture and description of attack patterns
  - Collecting known attack patterns into an integrated enumeration that can be consistently and effectively leveraged by the community
  - Gives you an attacker's perspective you may not have on your own

- **Where is CAPEC today?**
  - http://capec.mitre.org
  - Currently 386 patterns, stubs, named attacks

Homeland Security

Leveraging Structured Representations to Support Consistency and Automation

Common Attack Pattern Enumeration and Classification (CAPEC)

- The CAPEC structure can be used to characterize common approaches to counterfeiting and tainting.
- Can represent attacker behavior, observables, skills or resources required, mitigations, etc.
- For example, in the draft Counterfeit Taxonomy the Counterfeit/ Alteration/Inserted Malware entry already has a brief CAPEC pattern (CAPEC-441 Malicious Logic Inserted Into Product).
- Current CAPEC Supply Chain Attack taxonomy could easily be modified with the results of the taxonomy work here to refine and extend its value to anti-counterfeiting and SCRM.

Homeland Security

Leveraging Structured Representations to Support Consistency and Automation

Cyber Observable eXpression (CybOX)

- Cyber Observable eXpression (CybOX) is a standardized language for encoding and communicating information about cyber observables (http://cybox.mitre.org)
- A ***measurable event*** or ***stateful property*** in the cyber domain
  - Some measurable events: a registry key is created, a file is deleted, an http GET is received, …
  - Some stateful properties: MD5 hash of a file, value of a registry key, existence of a mutex, …
- CybOX provides **Expressivity**:
  - Very flexible -- can express both instances and patterns
  - Large number of objects defined and is user-extensible
  - Each object has a rich set of (optional) properties
  - Object patterns can be expressed as arbitrary Boolean expressions using AND, OR, NOT and at the field level with a range of patterning conditions

Homeland Security

CybOX™

Leveraging Structured Representations to Support Consistency and Automation

Cyber Observable eXpression (CybOX)

- CybOX can be leveraged to explicitly specify the observable patterns for what “counterfeit” and what “real” look like
  - These patterns could then be used within Indicators of what to look for and as adornments to relevant CAPEC attack patterns
- CybOX can also be used to capture actual “instantial” observations of observable properties
  - This could support the capture of test/inspection results
- Capturing the patterns and the “instantial” results in the same language simplifies the ability to match against the patterns

Homeland Security

CybOX™

Leveraging Structured Representations to Support Consistency and Automation

Cyber Observable eXpression (CybOX) for SCRM/Anti-Counterfeiting

- CybOX currently contains ~80 defined Objects including objects that can convey some of the relevant properties (Product, Device, etc.) for the SCRM/Anti-Counterfeiting use cases
- The core of CybOX is built to provide basic "observable" expressivity independent of specific Objects or Actions.
  - Because of this, it can easily be extended with new Objects or Actions
- CybOX is/will continue to be primarily focused on Cyber Domain
  - This does not mean that it can not be leveraged as a basis for other domain-specific representations
  - CybOX is a common schema shared among MAEC (for Malware), CAPEC (for Attack Patterns), CEE (Events), and Digital Forensics
- The SCRM/Anti-Counterfeiting community could define its own domain-specific language based on CybOX to enable characterization of all relevant observable properties

Leveraging Structured Representations to Support Consistency and Automation

Cyber Observable eXpression (CybOX) for SCRM/Anti-Counterfeiting

- The CybOX Product Object currently captures Name, Vendor, Version, Edition, etc.
- The CybOX Device Object currently captures Manufacturer, Model, Serial Number, etc.
- A wide range of other Objects cover much of the digital landscape.
- SCRM-specific Object could easily derive from these objects and add structures for characterizing things like packaging, anti-tamper, hardware-specific properties, etc.
- New Objects could also be created for non-CybOX, SCRM-specific constructs like Chip, Circuit, Boards, etc.

Homeland Security

Leveraging Structured Representations to Support Consistency and Automation

Structured Threat Information eXpression (STIX™)

- Structured Threat Information eXpression (STIX™) is a collaborative community-driven effort to define and develop a standardized *language* to represent structured cyber threat information. See http://stix.mitre.org/
  - The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible.
  - All interested parties are welcome to participate in evolving STIX as part of its open, collaborative community.
  - It is NOT a sharing program, database, or tool …but supports all of those uses and more

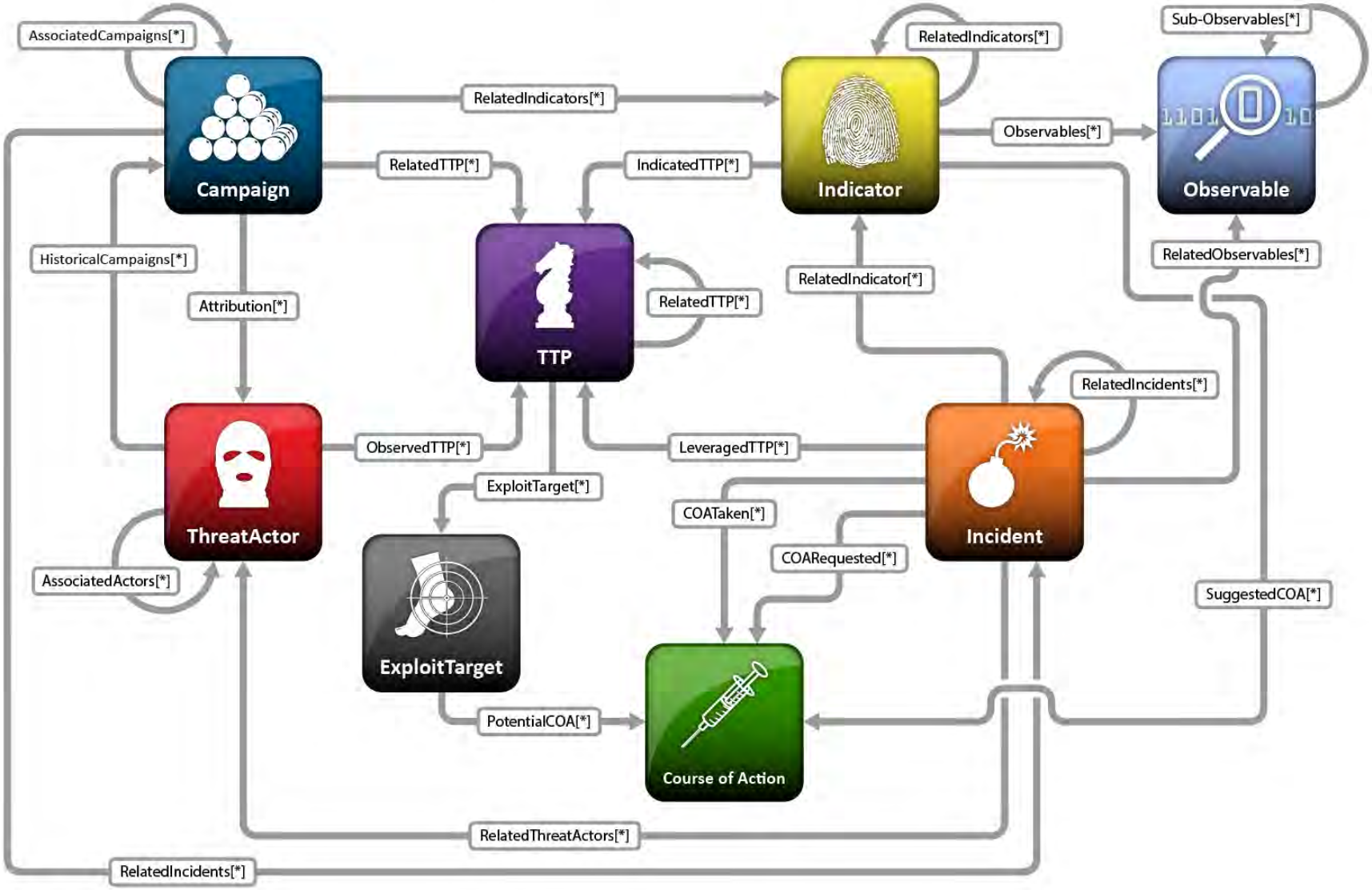
- Trusted Automated eXchange of Indicator Information (TAXII™) is the main transport mechanism for cyber threat information represented as STIX. Through the use of TAXII services, organizations can share cyber threat information in a secure and automated manner.

- Supports
  - Clear understandings of cyber threat information
  - Consistent expression of threat information
  - Automated processing based on collected intelligence
  - Advance the state of practice in threat analytics

Homeland Security

STIX™
Structured Threat Information eXpression

Structured Threat Information eXpression (STIX) v1.0 Architecture



Leveraging Structured Representations to Support Consistency and Automation

Structured Threat Information eXpression (STIX™)

- Leveraging Indicators to represent targeted patterns of concern (i.e. what to look for)
- Leveraging CVE & CWE within Exploit Targets to convey underlying issues in processes and products
- Leveraging CAPEC within TTP to convey counterfeiting and tainting approaches and give context to Indicators
- Leveraging Incidents to characterize instances of counterfeiting/tainting
- Leveraging Threat Actors to convey parties doing counterfeiting and tainting
- Leveraging Courses of Action to convey anti-counterfeiting approaches and taint/defect mitigations

Homeland Security

Leveraging Structured Representations to Support Consistency and Automation

Structured Threat Information eXpression (STIX™) Usage Example for SCRM

- Incident
  - Acme router found with counterfeit/altered malware-injected OS code
- Indicator
  - Immediately deploy Indicators with pattern for specific hash of the OS code
- COA
  - Test all such deployed routers for the Indicators
  - Remove all tainted routers from operations and submit for forensic analysis
  - Investigate supply chain provenance to detect how code was injected
- TTP
  - CAPEC-447: Malicious Logic Insertion into Product Software during Update
- Exploit Target
  - CWE-494: Download of Code Without Integrity Check

Homeland Security

Leveraging Structured Representations to Support Consistency and Automation

Structured Threat Information eXpression (STIX™) Usage Example for SCRM

- COA
  - Integrate integrity check into router software update process
- Threat Actor
  - Through forensic/incident analysis a commercial proxy for a certain nation state is identified as the culprit
- Campaign
  - Through cross-incident and TTP analysis, a campaign is discovered with this Threat Actor using similar TTP to target a particular set of victims on not limited to Acme routers
- Indicator
  - More general Indicators are developed and deployed to targeted victims that are not specific to the particular Acme tainting

Homeland Security