Towards a standard approach to supply chain integrity

Claire Vishik

September 2013

Draws from:

- ENISA's report on this topic
  - **Slawomir Gorniak**, European Network and Information Security Agency
  - **Demosthenes Ikonomou**, European Network and Information Security Agency
  - Contributors:
    - **Scott Cadzow**, Cadzow Communications Consulting
    - **Georgios Giannopoulos**, European Commission – Joint Research Centre
    - **Alain Merle**, LETI France
    - **Tyson Storch**, Microsoft
    - **Claire Vishik**, Intel
    - http://www.enisa.europa.eu/media/news-items/new-report-on-supply-chain-integrity-launched
- CSRA Report on research priorities in supply chain for cyber-physical systems
  - Coordinators: Nadya Bartol, UTC; and Jon Boyens, NIST
  - Available at: http://www.cybersecurityresearch.org/

SCI (Supply Chain Integrity) Definitions

A **supply chain** is a system of organizations, people, technology, activities, information and resources involved in developing or producing a product or service from supplier or producer to customer

Integrity is the extent to which consistency of actions, values, methods, measures, principles, expectations and outcome is achieved

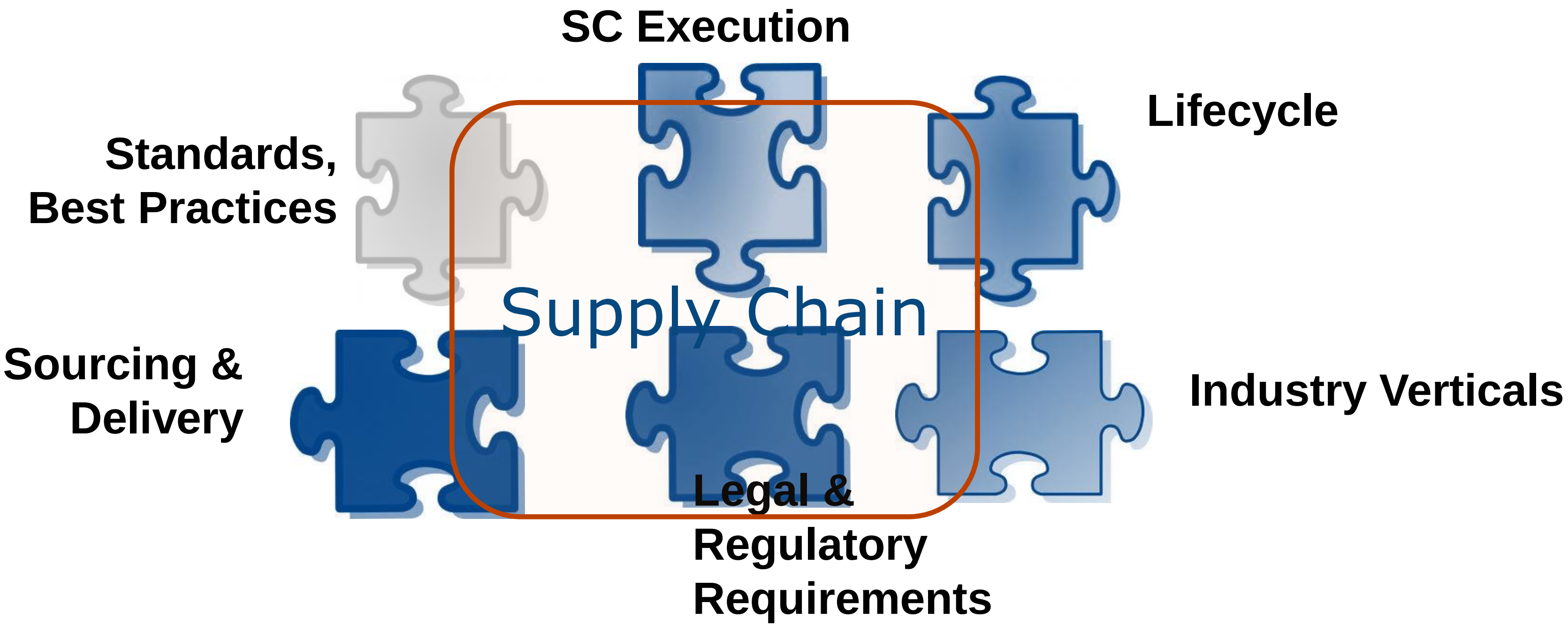
SCI (Supply Chain Integrity):

--Not a binary all or nothing term

--Can be improved, by, e.g. going directly to trusted manufacturer, and deteriorates when un-vetted links are introduced

--Best practice: authorized distribution framework

Supply Chain Puzzle



Some Key Issues (including gaps)

- Complexity of the space
- Trust, Claims & Evidence
- Harmonization of global requirements
- Coordinated framework for commonalities
- Understanding of operational context
- Broadly applicable approaches to analysis and mitigations
- Metrics and test tools

Background for SCI (Supply Chain Integrity)

The goal of supply chain integrity in the ICT domain is to ensure that ICT products meet the intended specifications

Threat Analysis

- Multiple diverse threats (context dependent, but a canonical list would improve understanding)
  - Typology of threat agents is as important as typology of threats
  - Prioritization of threats by probability and impact is necessary

Remedies

- Mitigations are also context dependent
- Co-design approaches could be used in practice and in standardization
- Decision support strategies for remedies based on the typologies of threats and threat agents could be an important area of standardization

Example: Cyber-Physical Systems

Suggested research priorities focus on understanding context and finding commonalities

Specific context

- Longer term use
- Focus on mission rather than security

Available best practices

- Telecom
- Aerospace

Short term goals

- Describe context and existing best practices
- Develop supplier reliability methodologies
- Develop testing tools

Long term goals

- Build secure architectures for CPS
- Develop next generation analytics
- Determine treatment of legacy systems and protocols

From CSRA report

SCI Landscape by Focus

Numerous related standards exist, but their mutual dependencies are still weak.

Origins

- ISO/IEC 27036: Guidelines for Security of Outsourcing

Delivery & Governance

- Several ANSI and NIST standards
- ISO/IEC 15288 (lifecycle)

Processing & Configuration

- RFID supply chain applications (SC31 in ISO)
- Risk Modeling pilot (iNEMI)
- Data Exchange pilot (HDPUG)

Integrity

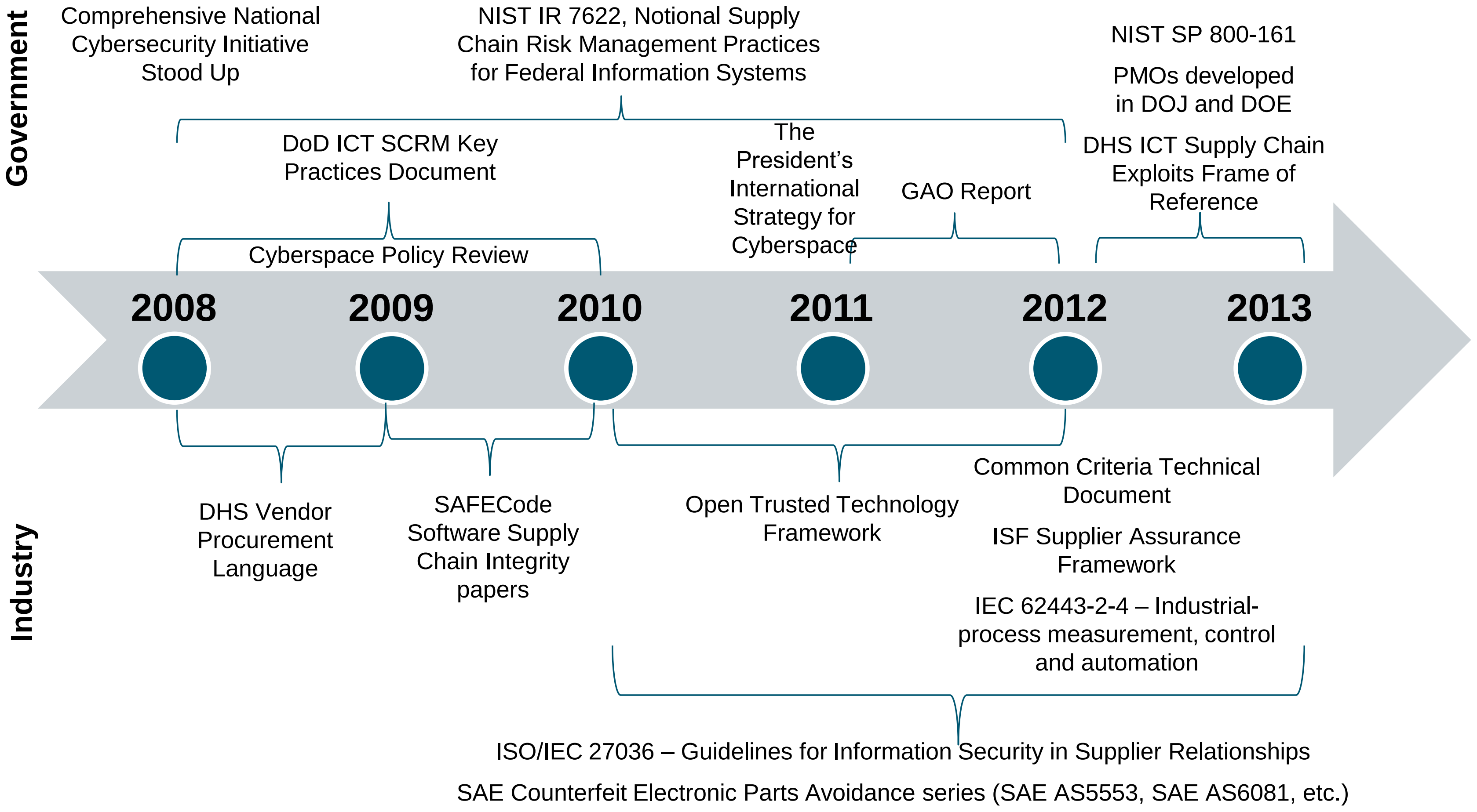
- N10656: Update to ISO 27002: Security Techniques
- Open Trusted Technology Framework

Verification & Checks

- Fraud Controls and Countermeasures
- SEMI T20: Traceability (semiconductor industry)

Some activities

From CSRA report, Bartol & Boyens



Government

Comprehensive National Cybersecurity Initiative Stood Up

NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems

NIST SP 800-161

PMOs developed in DOJ and DOE

DHS ICT Supply Chain Exploits Frame of Reference

DoD ICT SCRM Key Practices Document

The President's International Strategy for Cyberspace

GAO Report

Cyberspace Policy Review

2008

2009

2010

2011

2012

2013

DHS Vendor Procurement Language

SAFECode Software Supply Chain Integrity papers

Open Trusted Technology Framework

Common Criteria Technical Document

ISF Supplier Assurance Framework

IEC 62443-2-4 – Industrial-process measurement, control and automation

ISO/IEC 27036 – Guidelines for Information Security in Supplier Relationships

SAE Counterfeit Electronic Parts Avoidance series (SAE AS5553, SAE AS6081, etc.)

Industry

SCI Landscape by Involvement

Numerous related efforts ar under way, but it is too early to look at aggregation

Standards Bodies

- NIST, ANSI. JTC1,OASIS, ISO, other

Industry & Research Efforts

- ISF, Open Group, SafeCode, NASPO (North American Security Products Organization), iNEMI (International Electronic Manufacturing Initiative), HDPUG (High Density Packaging User Group International, Inc.), DARPA, FP7, other

Industry Segments

- Software, hardware, retail, aerospace, technology manufacturing, pharmaceuticals, other.

Geography

- Europe, US, China, India, Japan, other

Some Gaps to be Addressed

Technology, Process

- Real time integrity checks and awareness
- New integrity technologies to strengthen supply chain
- Evaluation tools & approaches, including approaches to composition

Risk Analysis, Metrics

- Approaches for broader contexts
- More general purpose techniques and models
- Broadly applicable metrics
- General understanding of evidence

Standards

- Numerous light or exploratory efforts, no large scale coordinated work
- No forum for multi-domain multi-disciplinary discussion
- No big picture

Some Recommendations: Areas of Focus

Technology, Process

- **Improved trust models**
- **New approaches to assurance**
- **Technology solutions (e.g., to counterfeiting)**
- **Improved evaluation & integrity checking**

Standards, Policy

- **Global policy assessment**
- **Taxonomy of the space**
- **Coordinated SCI framework**
- **Broadly applicable and efficient standard development**

Practice

- **Universally recognized best practices**
- **Collaboration mechanisms to assess and evaluate existing best practices**
- **Harmonized legal and evaluation framework**
- **Metrics and threat analysis tools**

Thank you

- Questions?