Software & Supply Chain Assurance:

Enabling Enterprise Resilience through Security Automation, Software Assurance and Supply Chain Risk Management

Joe Jarzombek, PMP, CSSLP
Director for Software & Supply Chain Assurance
Stakeholder Engagement & Cyber Infrastructure Resilience
Cyber Security & Communications
Public-Private Collaboration Efforts for Security Automation, Software Assurance, and Supply Chain Risk Management
DHS Cybersecurity and Communications

Responsible for enhancing security, resiliency, and reliability of the nation's cyber and communications infrastructure; actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm strategic assets.

Works to prevent or minimize disruptions to our critical information infrastructure in order to protect the public, the economy, government services, and overall security of the United States by supporting a series of continuous efforts designed to further safeguard federal government systems by reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats.

As the Sector-Specific Agency for the Communications and Information Technology (IT) sectors, CS&C coordinates national-level reporting consistent with the National Response Framework, and fulfills the mission through its five divisions:

- Office of Emergency Communications (OEC)
- Network Security Deployment (NSD)
- Federal Network Resilience (FNR)
- National Cybersecurity & Communications Integration Center (NCCIC)
- Stakeholder Engagement & Cyber Infrastructure Resilience (SECIR)
Interdependencies Between Physical & Cyber Infrastructures: Addressing Considerations for Resilience, Reliability, Safety, & Security

-- Need for secure/resilient software and authentic parts
Increased risk from supply chain due to:

- Increasing dependence on commercial ICT for mission critical systems
- Increasing reliance on globally-sourced ICT hardware, software, and services
  - Varying levels of development/outsourcing controls
  - Lack of transparency in process chain of custody
  - Varying levels of acquisition ‘due-diligence”
- Residual risk passed to end-user enterprise
  - Counterfeit products
  - Tainted products with malware, exploitable weaknesses and vulnerabilities
- Growing technological sophistication among our adversaries
  - Internet enables adversaries to probe, penetrate, and attack us remotely
  - Supply chain attacks can exploit products and processes throughout the lifecycle
DHS Software & Supply Chain Assurance Strategy

Enable Automation

Support Response

Outreach & Collaborate

Influence Policy

Influence Standards

Manage Software & Supply Chain Risks

Security Automation, Requirements Analysis & Risk Modeling

Support, Response, Outreach & Collaborate

Policy decisions influence tool design

Tools allow standards and policies to work

Standards are implemented by tools

Policies implement standards

Standards are a foundation of good policy

US Fed D/A Mgmt & IT Acquisition

ITU-T CYBEX

ISO/IEC JTC1

The Open Group

NIST Spec Pubs SP800-161 & 53

Stakeholder Engagement and Cyber Infrastructure Resilience
Defects, Counterfeits & Tainted Components

Mitigating exploitable risks attributable to non-conforming constructs in ICT

- Enable ‘scalable’ detection and reporting of defective, counterfeit and tainted ICT components
- Leverage/mature related existing standardization efforts
- Provide Taxonomies, schema & structured representations with defined observables & indicators for conveying information:
  - Authenticity
  - Counterfeit
  - Defect
  - Tainted constructs:
    - Malicious logic/malware (MAEC),
    - Exploitable Weaknesses (CWE);
    - Vulnerabilities (CVE)
  - Attack Patterns (CAPEC)
- Catalogue Diagnostic Methods, Controls, Countermeasures, & Mitigation Practices

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

*Text demonstrates examples of overlap
Mitigating Risks Attributable to Exploitable Software and Supply Chains

Enterprises seek comprehensive capabilities to:

- Avoid accepting software with **MALWARE** pre-installed.  

- Determine that no publicly reported **VULNERABILITIES** remain in code prior to operational acceptance, and that future discoveries of common vulnerabilities and exposures can be quickly patched.

- Determine that exploitable software **WEAKNESSES** that put the users most at risk are mitigated prior to operational acceptance or after put into use.

- Determine that components traversing thru Supply Chain are not Counterfeit or Defective and have not been Tainted

---

MAEC  
CVE  
CWE
Challenges in Mitigating Risks Attributable to Exploitable Software, Counterfeits & Supply Chains

Several needs arise:

- Need internationally recognized standards to support security automation and processes to provide transparency for informed decision-making in mitigating enterprise risks.
- Need comprehensive diagnostic capabilities to provide sufficient evidence that “code behavior” can be understood to not possess exploitable or malicious constructs.
- Need scalable means for detecting & reporting counterfeits.
- Need ‘Assurance’ to be explicitly addressed in standards & capability benchmarking models for organizations involved with security/safety-critical applications.
- Need rating schemes for ICT/software products and supplier capabilities.
ICT/software security risk landscape is a convergence between “defense in depth” and “defense in breadth”

Enterprise Risk Management and Governance are security motivators

Acquisition could be considered the beginning of the lifecycle; more than development

Software & Supply Chain Assurance provides a focus for:
- Resilient Software and ICT Components,
- Security in the Component Life Cycle,
- Software Security in Services, and
- Supply Chain Risk Management (mitigating risks of counterfeit & tainted products)
Risk Management (Enterprise ↔ Project): Shared Processes & Practices ↔ Different Focuses

- **Enterprise-Level:**
  - Regulatory compliance
  - Changing threat environment
  - Business Case

- **Program/Project-Level:**
  - Cost
  - Schedule
  - Performance

Who makes risk decisions?  
Who “owns” residual risk from tainted/counterfeit products?

* “Tainted” products are those that are corrupted with malware, or exploitable weaknesses & vulnerabilities that put users at risk
https://buildsecurityin.us-cert.gov/swa

Provides resources for stakeholders with interests in Software Assurance, Supply Chain Risk Management, and Security Automation

https://buildsecurityin.us-cert.gov

Focuses on making security a normal part of software engineering
Software & Supply Chain Assurance: Enabling Enterprise Resilience through Security Automation, Software Assurance, and Supply Chain Risk Management

Joe Jarzombek, PMP, CSSLP
Director for Software & Supply Chain Assurance
Stakeholder Engagement & Cyber Infrastructure Resilience
Cyber Security & Communications