Software & Supply Chain Assurance:

Mitigating Risks Attributable to Exploitable ICT / Software Products and Processes

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

Homeland Security

Enabling Enterprise Resilience through Security Automation, Software Assurance and Supply Chain Risk Management
Homeland Security
National Defense
Commerce & Standards

General Services

Public-Private Collaboration Efforts for Security Automation, Software Assurance, and Supply Chain Risk Management

Next SSCA WG 2-4 June 2015 at MITRE in McLean, Virginia
Gaining confidence in ICT/software-based cyber technologies

- Dependencies on technology are greater than ever
- Possibility of disruption is greater than ever because hardware/software/services vulnerable
- Loss of confidence alone can lead to stakeholder actions that disrupt critical business activities
Interdependencies Between Physical & Cyber Capabilities – Convergence of Safety, Security and Resilience Considerations

In an era riddled with asymmetric cyber attacks, claims about system reliability and safety must include provisions for built-in security of the enabling software.

High Reliance on ICT/Software

Built-in Security enables Resilience

Critical security controls aligned with mission
Automated continuous diagnostics and mitigation
Assurance relative to Trust

Managing Effects of Unintentional Defects in Component or System Integrity

Managing Consequences of Unintentional Defects

Managing Consequences of Attempted/Intentional Actions
Targeting Exploitable Constructs, Processes & Behaviors
Exploitable Software Weaknesses (CWEs) are exploit targets/vectors for future Zero-Day Attacks
Software Assurance Addresses Exploitable Software:
Outcomes of non-secure practices and/or malicious intent

Exploitation potential of vulnerability is independent of “intent”

EXPLOITABLE SOFTWARE

Unintentional Vulnerabilities

Defects

Intentional Vulnerabilities

Malware

‘High quality’ can reduce security flaws attributable to defects; yet traditional S/W quality assurance does not address intentional malicious behavior in software

*Intentional vulnerabilities: spyware & malicious logic deliberately imbedded (might not be considered defects)

Software Assurance (SwA) is the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the life cycle.*

*From CNSS Instruction 4009 “National Information Assurance Glossary” (26APR2010)
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
  - Defective and 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
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 determines ‘fitness for use’ for ‘technically acceptable’ criteria?
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
Software-related Expectations for 2015

- Major breaches will be enabled by unpatched known vulnerabilities over 2 years old;
- Chained attacks and attacks via third-party websites will grow;
- Vulnerable web applications will remain easiest way to compromise companies;
- SQL Injection and XSS will constitute more frequent and dangerous vector of attacks;
- Third-party code and plug-ins will remain the Achilles heel of web applications;
- Server misconfigurations will continue to be a top source of vulnerability;
- Many vulnerabilities will be exploited in devices and systems that cannot be patched;
- Most software will be composed third party & open source (often unchecked) components;
  - Primary causes of exploited vulnerabilities will be software defects, bugs, & logic flaws;
  - Application logic errors will become more frequent and critical;
- Mobile apps will constitute a growing source of attack vectors, especially since many (in rush to release) won’t be adequately tested for known vulnerabilities prior to use;
- Software testing and lifecycle support will gain importance, especially with experienced teams that apply ‘test kits’ of multiple tools and methods – no single automated security tool or method will be effective.
SSCA Focus on Tainted Components

*Mitigating risks attributable to exploitable non-conforming constructs in ICT*

“Tainted” products are those that are corrupted with malware, or exploitable weaknesses & vulnerabilities that put users at risk

- Enable ‘scalable’ detection and reporting of tainted ICT components
- Leverage/mature related existing standardization efforts
- Provide Taxonomies, schema & structured representations with defined observables & indicators for conveying information:
  - Tainted constructs:
    - Malicious logic/malware (MAEC),
    - Exploitable Weaknesses (CWE);
    - Vulnerabilities (CVE)
  - Attack Patterns (CAPEC)
- Catalogue Diagnostic Methods, Controls, Countermeasures, & Mitigation Practices
- Publicly reported weaknesses and vulnerabilities with patches accessible via National Vulnerability Database (NVD) sponsored by DHS & hosted by NIST

*Text demonstrates examples of overlap*
Reduced Visibility, Understanding, and Control
SP 800-161, Supply Chain Risk Management for Federal Information Systems and Organizations

- Building on existing NIST Guidance
- Ability to Implement and Assess
- System Development Life Cycle
- Threat Scenarios & Framework
- ICT SCRM Plan

Multitiered Organizational Risk Management

Security Controls

SP 800-39

Risk Assessment

SP 800-30

SP 800-53r4

National Institute of Standards and Technology
Software Assurance (SwA) Pocket Guide Series

SwA in Acquisition & Outsourcing
• Software Assurance in Acquisition and Contract Language
• Software Supply Chain Risk Management and Due-Diligence

SwA in Development *
• Risk-based Software Security Testing
• Requirements and Analysis for Secure Software
• Architecture and Design Considerations for Secure Software
• Secure Coding and Software Construction
• Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses
* All include questions to ask developers

SwA Life Cycle Support
• SwA in Education, Training and Certification

SwA Pocket Guides and SwA-related documents are collaboratively developed with peer review; they are subject to update and are freely available for download via the DHS Software Assurance Community Resources and Information Clearinghouse at https://buildsecurityin.us-cert.gov/swa (see SwA Resources)
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 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
joe.jarzombek@hq.dhs.gov

Mitigating Cyber-Physical Risk Exposures Attributable to External Dependencies on ICT Supply Chain Components and Services