What can an Acquirer do to prevent developers from making dangerous software errors?

OWASP AppSec DC 2012
April 5, 2012
Key questions

• Do acquirers know why they need include requirements for secure code?
• How do acquirers articulate the requirements for secure code?
• What standards and best practices exist to communicate expectations?
• What are the critical success factors for developers developing secure code?
• How do acquires know their requirements for secure code have been met?
• How should acquirers communicate with other stakeholders?
• Next Steps?
Technology is an integral part of our lives

IT and Communications products are assembled, built, and transported by multiple vendors around the world.
Acquirers of IT products and services trust that suppliers are addressing cyber security without validating.

<table>
<thead>
<tr>
<th>Prepare for the acquisition</th>
<th>Advertise the acquisition and select the supplier</th>
<th>Initiate an agreement</th>
<th>Monitor the agreement</th>
<th>Accept the product or service</th>
</tr>
</thead>
</table>

Product Development and Maintenance
- Requirements Management
- Design/Develop
- Test

47% do not perform acceptance testing of third-party code
30% do not use static analysis/manual code
27% do not practice secure design
19% do not carry out security requirement definition
46% use own development method, rather than SDL or CMM/CMMI
15% follow SDL
20% follow CMM/CMMI®
61% had no special incentive program to get developers and testers to work together
More than 70% do not measure developers with security related metrics

ROI was greater for those who employed a coordinated, prescriptive approach

Malicious actors are taking advantage of abundant opportunities to tamper with and sabotage products …

<table>
<thead>
<tr>
<th>What commonalities exist?</th>
<th>83% of victims were targets of opportunity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>92% of attacks were not highly difficult</td>
</tr>
<tr>
<td></td>
<td>86% were discovered by a third party</td>
</tr>
<tr>
<td></td>
<td>96% of breaches were avoidable through simple or intermediate controls</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How do breaches occur?</th>
<th>50% utilized some form of hacking</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>49% incorporated malware</td>
</tr>
<tr>
<td></td>
<td>(lower percentages included physical attacks, privilege misuse, and social tactics)</td>
</tr>
</tbody>
</table>

*Source – 2011 Verizon Data Breach Investigations Report*

… ultimately compromising system integrity and operations
SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

Joint Strike Fighter Extended Team – U.S.

Source: Lockheed Martin Aeronautics Company
SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

F-35 Extended Team –
International Industrial Participation

Source: Lockheed Martin Aeronautics Company

Global Development and Production
Key questions

- Do acquirers know why they need include requirements for secure code?
- How do acquirers articulate the requirements for secure code?
- What standards and best practices exist to communicate expectations?
- What are the critical success factors for developers developing secure code?
- How do acquires know their requirements for secure code have been met?
- How should acquirers communicate with other stakeholders?
- Next Steps?
Requirements for secure code are implicitly and not explicitly stated

Reliabile software that functions as promised
Software free from security vulnerabilities and malicious code
Ease of Integration & Configuration
Software conforms to Requirements & Industry Standards
Convenience & Ease of Use
Rich Feature Set

https://www.cioexecutivecouncil.com October 11, 2006 Press Release
“Document and track security flaws and flaw resolution”.

The Contractor certifies that at least one member of its staff assigned to this project working on any software code to be delivered under this effort has earned the Global Information Assurance Certification for Secured Software Programming or equivalent.

The government intends to modify the contract as National Institute for Science and Technology (NIST) SCRM guidelines and standards evolve, and the contractor shall update its SCRM Plan to include such modifications at no cost to the government.

What provisions are taken to ensure there is no malware on any hardware, firmware and/or software components?

Define your approach for Software Assurance

Present a plan for conducting security engineering/software assurance support
SOFTWAR E ASSURANCE FORUM
BUILDING SECURITY IN

Current DOD RFP Content Considerations

- Section A: Solicitation Contract Form
- Section B: Supplies or services and prices/costs

- Statement of Work (SOW)
- System Requirements Document (SRD)
  - Compliance and Reference Document List (CDRLs)

- Section D: Packaging and marking
- Section E: Inspection and Acceptance
- Section F: Deliveries or performance
- Section G: Contract administration data
- Section H: Special contract requirements
- Section I: Contract Clauses
- Section J: List of Documents, Exhibits, and other Attachments
- Section K: Representations, Certification, and Other Statements of Offerors
- Section L: Instructions, conditions, and notice to offerors
- Section M: Evaluation factors for award

SOW to Include, but not Limited to:
- Conduct of Criticality Analysis (CA)
  - Identification of mission-critical functions that may result in Level 1 or Level 2 protection failures
  - Identification of logic-bearing elements of Level 1/2 failures
- Demonstration of visibility into supply chain and Software Assurance (SwA) for critical components
- Update of CA results and Program Protection risks and mitigations at each SETR

SRD to Include, but not Limited to:
- Detect and record incidents; sends alert
- Prevent onset of threat/vulnerability that results in catastrophic or critical failure
- Return system to a normal operational state

CDRL DIDs to Include, but not Limited to:
- CA results 30 days before each SETR
- Design trade studies for selection of Level 1/2 logic bearing components
- Supply chain risk analysis for supplier selection

Section L, to Include, but not Limited to:
Request a description of Supply Chain Risk Management and SwA processes and techniques that will be used to achieve system protection and mission effectiveness

Section M, to Include, but not Limited to:
Evaluate proposed processes, including SCRM and SwA use in system specification and design, to mitigate threats and vulnerabilities to system mission effectiveness
Balancing risk when making trades

COST ($) vs. SCHEDULE (t) vs. PERFORMANCE (x)
“Defacto” security requirements in NIST 800-53 rev 3 do not explicitly require secure code

- AC-2 Account Management
- AC-3 Access Enforcement
- AC-4 Information Flow Enforcement
- RA-5 Vulnerability Scanning
- CM-7 Least Functionality
- SI-3 Malicious Code Protection
- SI-10 Information Input Validation
Draft NIST SP 800-53 rev 4 has SwA controls for low, moderate, and high systems

- AT-3 Security Training
- CM-3 Configuration Change Control
- CM-7 Least Functionality
- SA-3 System Development Life Cycle
- SA-4 Acquisition Process
- SA-11 Developer Security Testing
- SA-15 Development Process, Standards, and Tools
- SA – 16 Developer-Provided Training
- SA – 17 Developer Security Architecture and Design
Key questions

- Do acquirers know why they need to include requirements for secure code?
- How do acquirers articulate the requirements for secure code?
- What standards and best practices exist to communicate expectations?
- What are the critical success factors for developers developing secure code?
- How do acquirers know their requirements for secure code have been met?
- How should acquirers communicate with other stakeholders?
- Next Steps?
A majority of SwA best practices focus on developer-centric audiences from a security point of view.
Application Security resources are available through industry efforts and relationships with industry leaders.

Secure Coding Libraries
Secure Development Lifecycles
SwA Implementation Roadmaps

Contract Language
Acceptance Testing Resources

Open Source SwA Validation Tools

www.owasp.org
http://bsimm.com/BuildSecurityIn.us-cert.gov
www.microsoft.com/sdl
www.safecode.org
DOD Acquisition Reviews include Supply Chain Risk Management and Software Assurance.
Key questions

• Do acquirers know why they need include requirements for secure code?
• How do acquirers articulate the requirements for secure code?
• What standards and best practices exist to communicate expectations?

• What are the critical success factors for developers developing secure code?
• How do acquires know their requirements for secure code have been met?
• How should acquirers communicate with other stakeholders?
• Next Steps?
Success requires identifying the missing elements of change.
Understanding business goals, software assurance requirements and associated is critical

The Assurance PRM Is A Holistic Framework that connects CMMI and RMM to facilitate communication.

https://buildsecurityin.us-cert.gov/swa/proself_assm.html
Key questions

• Do acquirers know why they need include requirements for secure code?
• How do acquirers articulate the requirements for secure code?
• What standards and best practices exist to communicate expectations?
• What are the critical success factors for developers developing secure code?

• How do acquires know their requirements for secure code have been met?
• How should acquirers communicate with other stakeholders?
• Next Steps?
"The only man I know who behaves sensibly is my tailor; he takes my measurements anew each time he sees me. The rest go on with their old measurements and expect me to fit them."

- George Bernard Shaw

Source: www.CartoonStock.com
Robust measurement does not happen overnight and requires foundational capabilities in place to be effective.

**Softwar Assurance Forum**

**Building Security In**

---

**Robust measurement does not happen overnight and requires foundational capabilities in place to be effective.**

---

**Goal**

- **Prepare Foundation**
- **Develop Capability**
- **Use Capability**

**Efficiency/Effectiveness**

- **Add Essential Monitoring and Controls**
- **Develop Timeliness, Accuracy, Coverage**
- **Continuous Operational Monitoring Supports Response**
- **---**
- **Maintain, and Improve Security**

**Metric Type**

- **Implementation Metric**
- **Effectiveness Metric**
- **Impact Metric**

---

**Courtesy of Matt Coose, DHS**
Security control measures

- Percent of new systems that have completed certification and accreditation (C&A) prior to their implementation (NIST SP 800-53 Control: CA-6: Security Accreditation)
- Percent of employees who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior (NIST SP 800-53 Controls – PL-4: Rules of Behavior and AC-2: Account Management)
- Percent of the agency’s information system budget devoted to information security (NIST SP 800-53 Controls – SA-2; Allocation of Resources)

Security Control Measures address compliance with the end state of the system, but not the underlying processes, structures, and code
Measurement for secure code requires understanding code level attributes …

Vulnerability

• A (software) vulnerability is a collection of one or more weaknesses that contain the right conditions to permit unauthorized parties to force the software to perform unintended behavior (a.k.a. “is exploitable”)

• CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.

Weakness

• A (software) weakness is a property of software/systems that, under the right conditions, may permit unintended / unauthorized behavior.

• The Common Weakness Enumeration (CWE™) is a list of software weaknesses.

Source: [http://makingsecuritymeasurable.mitre.org/](http://makingsecuritymeasurable.mitre.org/) and DHS Software Assurance Program
From incident response teams we know that some vulnerabilities are exploited.

- Over 47,000 common vulnerabilities are documented and identified as a CVE.

Adapted from Richard Struse, DHS Software Assurance Program.
Industry vetted practices to AVOID common software weaknesses that can be exploited are available today.
Key questions

- Do acquirers know why they need to include requirements for secure code?
- How do acquirers articulate the requirements for secure code?
- What standards and best practices exist to communicate expectations?
- What are the critical success factors for developers developing secure code?
- How do acquirers know their requirements for secure code have been met?
- How should acquirers communicate with other stakeholders?
- Next Steps?
SwA requires multi-disciplinary collaboration

Without a common language we cannot communicate across disciplines

Source: https://buildsecurityin.us-cert.gov/swa/procrsrc.html
Business functions rely on accurate and reliable information from technology that functions as intended (and only as intended).

Adapted from: November 2009 SwA Forum-Evolution in SwA Processes Panel – David White, SEI
Operational impacts from threats to business functions can be understood by communicating software level vulnerabilities.
Today's environment requires an innovative way to look at the value and use of the software we develop and/or integrate.

http://www.ruggedsoftware.org/

The Rugged Software Manifesto

I am rugged... and more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

I recognize these things - and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

I am rugged, not because it is easy, but because it is necessary... and I am up for the challenge.
Key questions

• Do acquirers know why they need include requirements for secure code?
• How do acquirers articulate the requirements for secure code?
• What standards and best practices exist to communicate expectations?
• What are the critical success factors for developers developing secure code?
• How do acquires know their requirements for secure code have been met?
• How should acquirers communicate with other stakeholders?
• Next Steps?
Cyber security and software assurance standard development organization landscape
Targets building software that is inherently less vulnerable through improving the programming languages, or, at least, improve the usage of them in coding

A catalog of 60+ issues that arise in coding when using any language and how those issues may lead to security and safety vulnerabilities

Cross-referenced to CWE

Each discussion includes

- Description of the mechanism of failure
- Recommendations for programmers: How to avoid or mitigate the problem.
- Recommendations for standardizers: How to improve programming language specifications.

Courtesy of Jim Moore, MITRE
• Scope: This international standard covers information security in relationships between acquirers and suppliers to provide appropriate information security management for all parties. In particular, it also includes management of information security risks related to these relationships.

• The standard will be subdivided into the following parts:
  – Part 1 – Overview and Concepts
  – Part 2 – Common Requirements
  – Part 3 – Guidelines for ICT Supply Chain
  – Part 4 – Guidelines for Outsourcing
Initially based on DoD ICT SCRM Key Practices document and developed in close collaboration with the industry

Introduces the notion of supply chain players

- Acquirer - For this document, the acquirer is always a government agency (including those agencies taking on the role of integrator).
- Integrator – A third-party organization that specializes in combining products/elements of several suppliers to produce elements (information systems).
- Supplier – Third-party organization providing individual elements. *Synonymous with vendor and manufacturer; also applies to maintenance/disposal service providers*

Lays out pre-requisites of being able to address ICT SCRM challenge

States specific practices that are consistent with DoD guidance and ISO frameworks
SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.

White papers:
- Software Assurance: An Overview of Current Industry Best Practices
- Fundamental Practices for Secure Software Development
- Security Engineering Training: A Framework for Corporate Training Programs on the Principles of Secure Software Development
- Framework for Software Supply Chain Integrity
- Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain
Purpose
Identify and gain consensus on common processes, techniques, methods, product and system testing procedures, and language to describe and guide product development and supply chain management practices that can mitigate vulnerabilities which could lead to exploitation and malicious threats to product integrity.

Objectives
- Identify product assurance practices that should be expected from all commercial technology vendors based on the baseline best practices of leading trusted commercial technology suppliers
- Help establish expectations for global government and commercial customers when seeking to identify a trusted technology supplier
- Leverage existing globally recognized information assurance practices and standards
- Share with commercial technology consumers secure manufacturing and trustworthy technology supplier best practices
- Harmonize language used to describe best practices

What’s next?

• Continued collaboration to:
  – Reach and enable developers
  – Reach and enable executives
  – Develop and promote resources for us by developers and executives
• Participation in international standardization efforts
  – SC7 TAG intersections through your SC7 TAG
  – CS1/SC27
  – IEEE representative to the SC7 TAG
  – SC22
• Participation through the SwA Working Groups and Forum
• Stay Tuned …
Mr. Donald Davidson,
Chief, Outreach, Science & Standards
Trusted Mission Systems & Networks
TMSN / DoD CIO
Don.Davidson@osd.mil

Michele Moss
Lead Associate
Booz Allen Hamilton
moss_michele@bah.com