Software Assurance (SwA) Program

SwA: Strategic Overview

Project Description: Promotes software security and resilience via enhanced processes & diagnostics; enables public-private collaboration focused on reducing exploitable software weaknesses and addressing means to improve capabilities that routinely develop, acquire, and deploy resilient software products.

Goals & Objectives:

- **Goal 1: Software Security Automation and Measurement**
  Objective: Enable the automation of software security risk mitigation and enhance software security diagnostic capabilities and test criteria.
- **Goal 2: SwA technology and process transition**
  Objective: Transition software assurance technologies and processes into standards and maturity models suitable for voluntary adoption through collaboration with government agencies, industry stakeholders and relevant standards bodies.
- **Goal 3: Software Security Education**
  Objective: Integrate software security content into relevant education and training programs.
- **Goal 4: Public-Private Collaboration**
  Objective: Provide the public-private collaboration infrastructure for the SwA Community of Practice via SwA Forums, working groups, websites, and SwA outreach in public journals, presentations, etc.

SwA: Strategic Overview (cont.)

Current Capabilities:

- Lead programs enabling software security automation and measurement through common schemas: Common Vulnerabilities & Exposures (CVE) , Open Vulnerability & Assessment Language (OVAL), Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration & Classification (CAPEC), Malware Attribute Enumeration Characterization (MAEC)
  - CVE and OVAL provide information feeds for Security Content Automation Protocol (SCAP), National Vulnerability Database (NVD), and Threat Alerts by US-CERT and others.
  - CWE provides common reporting for static code analyzers; used to prioritize CVEs in the Common Vulnerability Scoring System
- Collaborate with NIST, NSA, international standards organizations, and tool vendors to create standards, metrics and certification mechanisms from which tools can be qualified for software security verification.
- Host interagency SwA Forums, Working Groups and training to provide public-private collaboration in advancing software security and providing publicly available resources (journals/guides/on-line resources).
- Provide input and criteria for leveraging international standards and maturity models used for process improvement and capability benchmarking of software suppliers and acquisition organizations.

Planned Capabilities:

- Evolve software security formalization efforts of the respective schema and programs for CWE, CAPEC and MAEC with Cybersecurity Observables to enable software security automation & measurement.
- Provide repository and on-line resources of SwA material suitable for use in education and training.
- Quantify how the use of SwA processes and tools contribute to enterprise security.
- Enhance relevant standards (through collaboration) to address needs for software security and provide rating schemes and processes to certify applications are conformant with the applicable standards.
- Provide lessons-learned on the use of Assurance-related Reference Models supporting process improvement and benchmarking of organizational capabilities in terms of software security.

Capability Gaps/Needs:

- Insufficient staffing and inadequate design-to-budget program funding to deliver capabilities in near term

Legal authorities/regulations supported (NSPDs, HSPDs, etc.):

- The National Strategy to Secure Cyberspace (2/14/03)

SwA: Performance Measures

- Continue to link to Department Goals/Objectives:
  - QHSR Goal 4.2 “Promote Cybersecurity Knowledge and Innovation” to ensure that the Nation is prepared for the cyber threats and challenges of tomorrow.
  - Enable partners and citizens to secure their part of cyberspace;
- Focus on providing measures for capability & capacity, along with measures for advancing adoption for SwA:
  - Software Security Automation and Measurement
    - Enable automation of software security measurement and risk mitigation;
    - Enhance software transparency and security diagnostic & measurement capabilities
  - SwA Technology and Process Transition
    - Develop/publish SwA practices for process improvement and capability benchmarking;
    - Transition SwA practices into standards and maturity models suitable for voluntary adoption
  - SwA Education & Training
    - Develop & publish software security content & curriculum courseware;
    - Integrate software security content into relevant education and training programs
  - SwA Outreach & Public-Private Collaboration
    - Provide outreach & public-private collaboration infrastructure for SwA Community of Practice;
    - Increase use and awareness of SwA resources available for voluntary adoption

SwA: Performance Measures (proposed changes)

Focus on Providing Capability & Capacity and Advancing Adoption

Software Assurance (SwA) Goal Title	Department Goal/Objective	Objective: provide capability and advance adoption	Performance Measures	Output/Outcome/ Uptake	Goal for FY11	Results new (by quarter) and total	Explanation of Results
Software Security Automation and Measurement	Enable partners and citizens to secure their part of cyberspace; QHSR Goal 4.2						
		Enable automation of software security measurement and risk mitigation					Enable security automation, measurement & reporting for cyber ecosystem
			# of updates of CVE & OVAL				Provide info feeds for SCAP, NVD & threat alerts
			# of updates of CWE & CAPEC schema				Provide updates for common weaknesses and common attack patterns
			# of updates of MAEC schema & code behavior obserables				Provide updates for malware enumeration (and language/formats for code behavior & observables)
			# of IDs released for CVE, CWE, etc	new (in the quarter) & total			CWE IDs represent root causes and enable prioritization of CVE/CVSS
			# of updates to rating/reporting & labeling schemes for SW products				Provide common reporting formats for use in software supply chain and SwA Market Place
		Enhance software transparency and security diagnostic & measurement capabilities					Enhance effectiveness & comprehensiveness of software security test & diagnostic capabilities, and provide SW rating/ reporting schemes/labels
			# of tools or services adopting CVE, OVAL, CWE, CAPEC, MAEC	new (in the quarter) & total			Track community uptake of relevant technologies

Draft Sample without numbers for output/outcomes/uptake or results

SwA: Performance Measures (proposed changes)

Focus on Providing Capability & Capacity and Advancing Adoption for SwA

Objective: Provide capability & capacity and advance adoption	Performance Measures	Output/ Outcome / Uptake	Goal for FY 11	Results new (by quarter) and total	Explanation of Results
Enable automation of software security measurement and risk mitigation					Enable security automation, measurement & reporting for cyber ecosystem
	# of updates of CVE & OVAL				Provide info feeds for SCAP, NVD & threat alerts
	# of updates of CWE & CAPEC schema and CWSS				Provide updates for common weaknesses and common attack patterns and CWSS
	# of updates of MAEC schema & cyber observables				Provide updates for malware enumeration (and language/formats for cyber observables)
	# of IDs released for CVE, CWE, etc	New in quarter& total			CWE IDs represent root causes and enable prioritization of CVE/CVSS
	# of updates to rating/ reporting & labeling schemes for products				Provide common reporting formats for use in software supply chain and SwA Market Place

Draft Sample without numbers for output/outcomes/up take or results

SwA: Performance Measures (proposed changes)

Focus on Providing Capability & Capacity and Advancing Adoption for SwA

Enhance software transparency and security diagnostic & measurement capabilities					Enhance effectiveness & comprehensiveness of software security test & diagnostic capabilities, and provide SW rating/ reporting schemes/labels
	# of tools or services adopting CVE, OVAL, CWE, CAPEC, MAEC, CybOx, CVSS, CWSS	new (in the quarter) & total			Track community uptake of relevant technologies and scoring systems
	# of visitors to websites for CVE, OVAL, CWE, CAPEC, MAEC				track community uptake of relevant technologies (on quaterly basis)
	# of NIST 800 & 500 series Special Pubs & interagency reports using CVE, OVAL, CWE, CAPEC, etc				Track community uptake of relevant technologies
	# of international standards, consortia guides & best practices using CVE, OVAL, CWE, CAPEC, etc				Track community uptake of relevant technologies
	# of static analysis tool evaluations, specs, reports; publications				Track community uptake of relevant technologies
	# participating in rating/ reporting/ labeling schemes for SW				Track community uptake of relevant technologies

NIST Special Publications:

SP800-36	CVE
SP800-40	CVE, OVAL
SP800-42	CVE
SP800-44	CVE
SP800-51	CVE
SP800-53a	CVE, OVAL, CWE
SP800-61	CVE, OVAL
SP800-70	CVE, OVAL, CCE, CPE, XCCDF, CVSS
SP800-82	CVE
SP800-86	CVE
SP800-94	CVE
SP800-115	CVE, CCE, CVSS, CWE
SP800-117	CVE, OVAL, CCE, CPE, XCCDF, CVSS
SP800-126	CVE, OVAL, CCE, CPE, XCCDF, CVSS

Draft Sample of community uptake without numbers for output/outcomes/up take or results

NIST Interagency Reports:

NISTIR-7007	CVE
NISTIR-7275	CVE, OVAL, CCE, CPE, XCCDF, CVSS
NISTIR-7435	CVE, CVSS, CWE
NISTIR-7511	CVE, OVAL, CCE, CPE, XCCDF, CVSS
NISTIR-7517	CVE
NISTIR-7581	CVE
NISTIR-7628	CVE, CWE

FDCC

SCAP™

EMAP

SwAAP

SwA: Performance Measures (proposed changes)

Focus on Providing Capability & Capacity and Advancing Adoption for SwA Technology and Process Transition

Develop/publish SwA practices for process improvement and capability benchmarking					Produce and publish publicly available free resources, suitable for voluntary adoption
	# of resources and updates to relevant standards and maturity models				provide content for standards, maturity models, and rating schemes for capabilities of software supply chain
	# of on-line resources provided for community use				Publish publicly available free resources, including pocket guides, technical papers and articles in journals
Transition SwA practices into standards and maturity models suitable for voluntary adoption					Provide support to transition SwA technologies and processes into standards and maturity models suitable for voluntary adoption
	# of standards and models using SwA practices				Track international and national uptake of relevant processes, practices, and frameworks to guide process improvement and benchmark capabilities
	# of quarterly downloads of key SwA documents				Track community uptake of relevant material
	# of quarterly uses of relevant material				Track community uptake of relevant material

SwA: Performance Measures (proposed changes)

Focus on Providing Capability & Capacity and Advancing Adoption for SwA Education and Training

Develop & publish software security content & curriculum courseware					Through SwA Curriculum project, continue to develop and refine software security content and courseware
	# of curriculum-related resources				Provide content for others to use
Integrate software security content into relevant education and training programs					Provide assistance in transitioning the use of SwA content into education and training programs
	# of education & training programs adopting SwA content				Track community uptake of relevant material
	# of industry and consortia programs adopting use of SwA content				Track community uptake of relevant material
	# of SwA training sessions offered				Track community uptake of relevant material

SwA: Performance Measures (proposed changes)

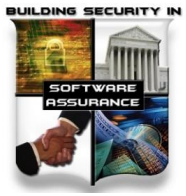
Focus on Providing Capability & Capacity and Advancing Adoption for SwA Outreach and Public-Private Collaboration

Provide outreach & public-private collaboration infrastructure for SwA Community of Practice					Provide public-private collaboration infrastructure for SwA Community of Practice via SwA Forums, working groups, websites, and SwA outreach in public journals, presentations
	# of SwA collaboration events producing deliverables for community use				Produce deliverables via SwA Forums and Working Groups; collaborate with agencies, academia, industry stakeholders and relevant standards bodies
	# of SwA outreach events and public presentations				Take message/resources to other conferences; includes hiring opportunities
	# of articles in relevant journals				Provide content in non-DHS journals; Includes hiring opportunities
	# of website updates				Provide on-line resource available for free download

SwA: Performance Measures (proposed changes)

Focus on Providing Capability & Capacity and Advancing Adoption for SwA Outreach and Public-Private Collaboration

Increase use and awareness of SwA resources available for voluntary adoption					Track community uptake of relevant resources
	# of quarterly downloads of key journals with SwA content				Track community uptake of relevant resources
	# of quarterly downloads of key material on SwA websites				Track community uptake of relevant resources
	# of participants in SwA events (quarterly)				Track community uptake of relevant resources
	# of unique visitors to SwA websites (quarterly)				Track community uptake of relevant resources



Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

Incident Management

CPE/ OVAL/ ARF

CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE

CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF

CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAEC

CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS/ XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE

ESIP

SCAP

TAAP

EMAP

ITAP

Operations Security Management Processes

Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation

CWE/CAPEC/ SBVR/CWSS/ MAEC/OVAL/ XCCDF/CCE/ CPE/ARF

SwAAP

Development & Sustainment Security Management Processes

INTERNET

Router

DMZ

Firewall

Web Servers

Application Servers

Database Systems

INTRANET

DNS Server

Mail Server

Web Servers

Desktop Systems

Desktop Systems

Desktop Systems

Desktop Systems

Operational Enterprise Networks

CVE/CWE/CVSS/CCE/CCSS/ OVAL/XCCDF/ CPE/CAPEC/MAEC/SBVR/CWSS/CEE/ARF

Enterprise IT Change Management

ERAP

CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/SBVR/CWSS/CEE/ARF

Centralized Reporting

ECAP

Enterprise IT Asset Management