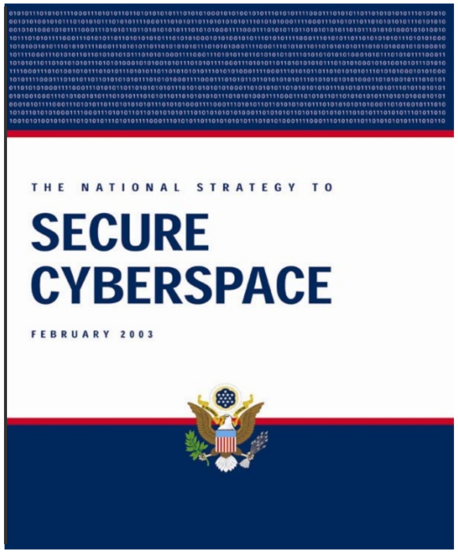
Software Assurance:

A Strategic Initiative of the U.S. Department of Homeland Security to Promote Integrity, Security, and Reliability in Software



THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

Collaboration through the Software Assurance Forum

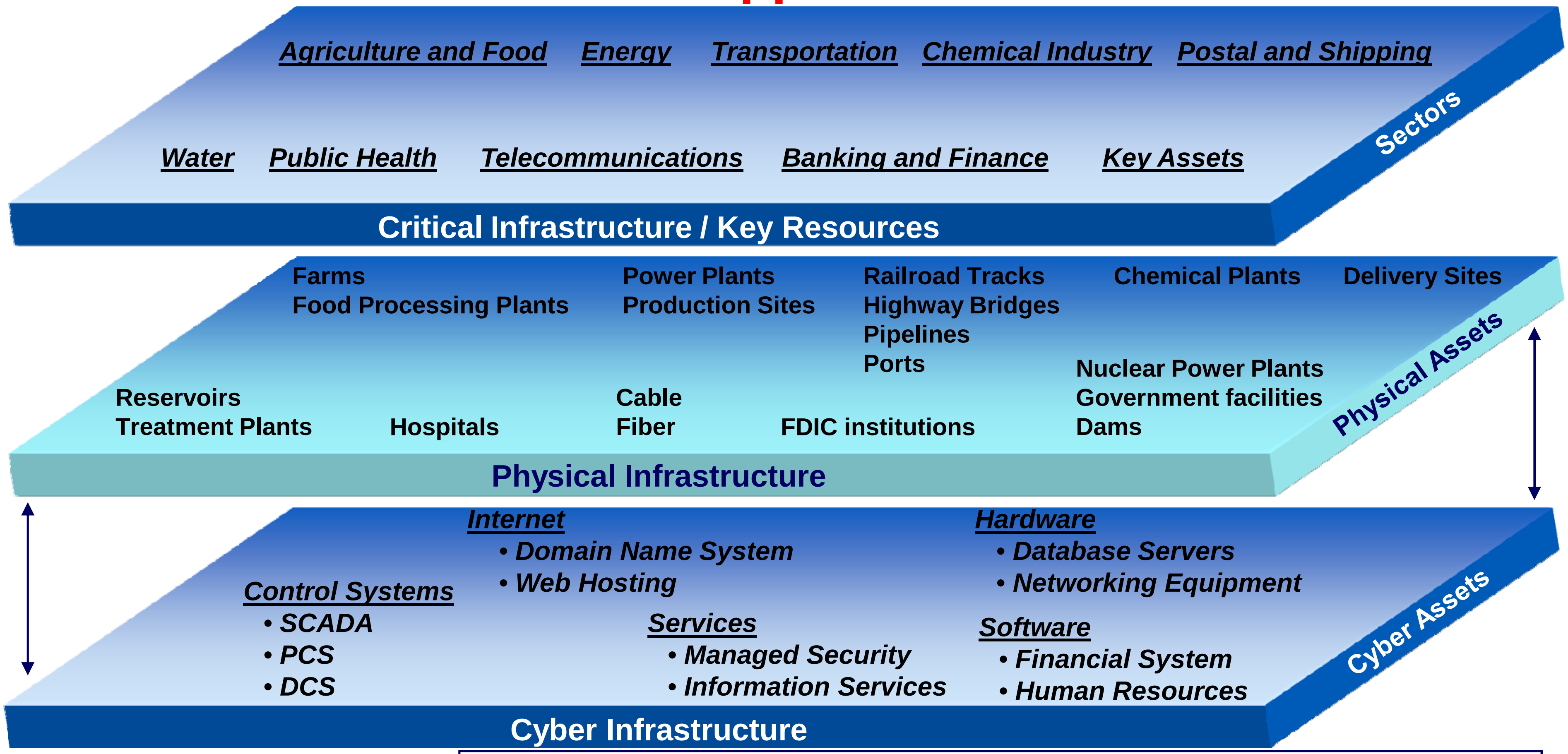
IEEE CS S2ESC ExCom
July 18, 2007

Homeland Security

Joe Jarzombek, PMP
Director for Software Assurance
National Cyber Security Division
US Department of Homeland Security

Cyberspace & physical space are increasingly intertwined and software controlled or enabled

Need for secure software applications *



Sectors

Agriculture and Food · Energy · Transportation · Chemical Industry · Postal and Shipping

Water · Public Health · Telecommunications · Banking and Finance · Key Assets

Critical Infrastructure / Key Resources

Physical Assets

Farms
Food Processing Plants

Power Plants
Production Sites

Railroad Tracks
Highway Bridges
Pipelines
Ports

Chemical Plants

Delivery Sites

Nuclear Power Plants
Government facilities
Dams

Reservoirs
Treatment Plants

Hospitals

Cable
Fiber

FDIC institutions

Physical Infrastructure

Cyber Assets

Internet
- *Domain Name System*
- *Web Hosting*

Hardware
- *Database Servers*
- *Networking Equipment*

Control Systems
- *SCADA*
- *PCS*
- *DCS*

Services
- *Managed Security*
- *Information Services*

Software
- *Financial System*
- *Human Resources*

Cyber Infrastructure

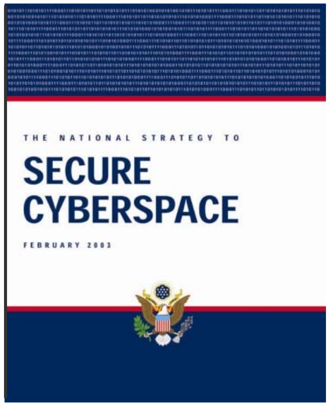
*** 75% of hacks occur at application level (Gartner, Dec 2005)**

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

DHS Software Assurance Program Overview

- Program based upon the National Strategy to Secure Cyberspace - Action/Recommendation 2-14:

  "DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development."



THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

- DHS Program goals promote the security of software across the development, acquisition and implementation life cycle
- Software Assurance (SwA) program is scoped to address:
  - **Trustworthiness** - No exploitable vulnerabilities exist, either maliciously or unintentionally inserted
  - **Predictable Execution** - Justifiable confidence that software, when executed, functions as intended
  - **Conformance** - Planned and systematic set of multi-disciplinary activities that ensure software processes and products conform to requirements, standards/ procedures

CNSS Instruction No. 4009, "National Information Assurance Glossary," Revised 2006, defines Software Assurance as: "the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner".

Homeland Security

DHS Software Assurance Program Structure *

- As part of the DHS risk mitigation effort, the SwA Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development of trustworthy software products and tools to analyze systems for hidden vulnerabilities.
- The SwA framework encourages the production, evaluation and acquisition of better quality and more secure software; leverages resources to target the following four areas:
  - **People** – education and training for developers and users
  - **Processes** – sound practices, standards, and practical guidelines for the development of secure software
  - **Technology** – diagnostic tools, cyber security R&D and measurement
  - **Acquisition** – due-diligence questionnaires, contract templates and guidelines for acquisition management and outsourcing

* July 28, 2006 statement of George Foresman, DHS UnderSecretary for Preparedness, before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, and International Security

Software Assurance (SwA) Forum and Working Groups …

… encourage the production, evaluation and acquisition of better quality and more secure software through targeting

People	Processes	Technology	Acquisition
Developers and users education & training	Sound practices, standards, & practical guidelines for secure software development	Security test criteria, diagnostic tools, common enumerations, SwA R&D, and SwA measurement	Software security improvements through due-diligence questions, specs and guidelines for acquisitions/ outsourcing

Products and Contributions

Build Security In - https://buildsecurityin.us-cert.gov and SwA community portal – http://.us-cert.gov/SwA

SwA Common Body of Knowledge (CBK) & Glossary
SwA Developers' Guide on Security-Enhancing SDLC
Systems Assurance Guide (via DoD and NDIA)

SwA-related standards – ISO/IEC JTC1 SC7/27/22, IEEE, OMG and CMM-based Assurance extensions

Software Security Assurance State of the Art Report

Practical Measurement Guidance for SwA/InfoSec

SwA Metrics & Tool Evaluation (with NIST) and SwA Ecosystem (with DoD, NSA, NIST & OMG) and NIST Special Pub 500 Series on SwA Tools

Common Weakness Enumeration (CWE) dictionary
Common Attack Pattern Enumeration (CAPEC)
Common Malware Enumeration (with ASC)

SwA in Acquisition: Mitigating Risks to Enterprise

Homeland Security

Links available via https://buildsecurityin.us-cert.gov

Bi-Monthly Working Groups & Semi-Annual SwA Forum:

Next WG sessions held 4-6 Dec 2007 – Next SwA Forum 2-3 Oct 2007

Typical Format	Tuesday	Wed	Thursday
Morning 9:00am - 11:30am	**Session 1:** *Technology, Tools & Product Evaluation Working Group*	**Plenary Session**	**Session 6:** *Processes & Practices Working Group on "Argument/Case"*
	Session 2: *Business Case Working Group*		**Joint Session 8:** *Measurement WG with another SwA WG*
Afternoon 1pm - 5pm	**Session 1:** *Technology, Tools & Product Evaluation Working Group*	**Session 4:** *Malware Working Group*	**Session 6:** *Processes & Practices Working Group on "Argument/Case"*
	Session 3: *Workforce Education & Training Working Group*	**Session 5:** *Acquisition Working Group*	**Session 7:** *Measurement Working Group*

Presentations from previous SwA WGs and Forums are on US-CERT Portal (https://us-cert.esportals.net/) under the appropriate Working Group in the Library folder. Access to WG folder is restricted to those who have participated in the WG. Contact DHS NCSD if you do not yet have access to the appropriate folders.

DHS SwA – People Focus

- Provide Guide to Software Assurance (SwA) Common Body of Knowledge (CBK)
  - Leverage standards and "best practices" serves as a framework to guide software-related curriculum development
  - Addresses three domains: "acquisition & supply," "development," and "post-release assurance" (sustainment)
  - Draft v1.1 distributed on 25 Sep 2006 for review and comment; being used by early adopters in graduate level courses in secure coding/programming and NDU Information Resource Management College (IRMC) CISO Certificate Program course on SwA
  - Using common definitions from relevant standards; in collaboration with NSA/IA , updating SwA Glossary – several SwA definitions also found on-line via wikipedia.org
- Plans:
  - Next SwA CBK update with "guiding security principles" mapping to be released Sep 2007
  - Link to Common Weakness Enumeration and Common Attack Patterns - Dec 2007
  - Develop pilot training/education curriculum consistent with CBK in conjunction with early adopters for distribution by September 2008
  - Link with relevant tests, eg., SANS Secure Software Programming Assessment *
  - Provide input to IT Security Essential Body of Knowledge (EBK)

Tuesday, Aug 14 in Washington DC Secure software programming tests – one on Secure Java and one on Secure C

DHS SwA – Process Focus

- Provide Software Assurance (SwA) Developers' Guidance
  - Provided practical guidance via "Build Security In" on US-CERT web site with regular updates based on feedback from stakeholders
  - Provided developers guide, "Securing the Software Lifecycle: Making Application Development Processes – and Software Produced by Them – More Secure" v1.2
  - Collaborate with DoD "Systems Assurance" Guidebook
  - Work with IEEE CS S2ESC, ISO/IEC JTC1 SC7/SC27/SC22, OMG, CNSS, & NIST to recommend changes to national/ international standards related to SwA
- Plans:
  - Continue to provide periodic updates to https://buildsecurityin.us-cert.gov
  - Evolve developers' guide, draft v2 in Sep 2007 reflecting new organization and references to related work
  - In collaboration with federal agencies, standards bodies, industry and academia:
    - provide draft guidance for specifying 'assurance case/arguments' from which to base claims about the safety, security and dependability of software – draft to be released September 2007 for review and comment
    - provide recommended changes to national and international standards on programming languages, software testing and software assurance
    - provide recommendations to Capability Maturity Models (CMMs) for Assurance

DHS SwA – Technology Focus

- Provide SwA Technology Lifecycle Support Guidance
  - Sponsor work with NIST to inventory and measure effectiveness of SwA tools
  - Sponsor public-private work to provide a common dictionary of software weaknesses (CWE) - primarily those that can be discovered by tools
  - Published common attack pattern enumeration & classification (CAPEC) with 101 attacks from which to understand resilience of software relative to abuse and misuse
  - Provide SwA Measures to support decision making throughout the software lifecycle
  - Provided draft SwA Landscape document, including organizing mechanisms for SwA ecosystem infrastructure, from which to clarify and specify interfaces and interoperability among various SwA initiatives – input to Sw Security Assurance State of the Art Report
  - NIST Special Pub 500-268, “Source Code Security Analysis Tool Functional Spec”
- Plans
  - NIST Special Pub 500-269, “SwA Tools: Web Application Scanner Functional Spec”
  - NIST Special Pub 500-270, “Source Code Security Analysis Tool Test Plan”
  - In collaboration with NIST, provide a Test Case Generator from which to evaluate SwA tool compatibility and effectiveness – demonstrated in March 2007
  - In Sep 2007 provide update draft v1.0 SwA Measurement Guide, “Practical Guidance for Software Assurance and Information Security Measurement”

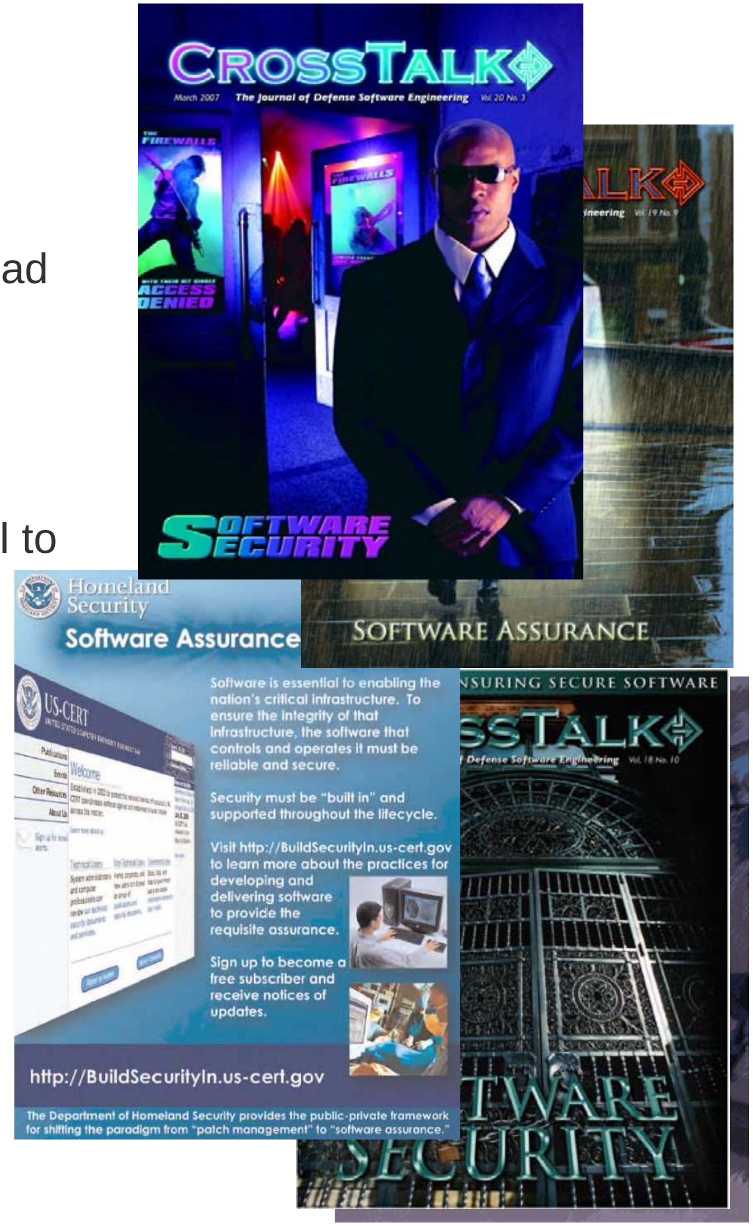
A SwA Ecosystem Demonstration was held the evening of March 7, 2007 during the OMG SwA Workshop and included a demo of the Test Case Generator being co-sponsored by DHS and NIST.

DHS SwA – Acquisition Focus

- Provide Software Assurance (SwA) Acquisition Guidance
  - Provided draft Acquisition Management guidance focused on enhancing supply chain management through improved risk mitigation and contracting for secure software
    - Collaborated on “due diligence” questionnaires for RFI/RFP and source selection decision making
    - Drafted templates and sample statements of work / procurement language for acquisition and evaluation based on successful models
  - Collaborated with agencies implementing changes responsive to the Federal Acquisition Regulation (FAR) IT security provisions of FISMA when buying goods and services and new core competency of “Software Acquisition Management” identified by Federal CIO Council’s IT Workforce Committee
  - Released acquisition guide, draft v1.0, “Software Assurance (SwA) in Acquisition: Mitigating Risks to the Enterprise” in March 2007 for review and comment
- Plans:
  - Release acquisition guide, “Software Assurance (SwA) in Acquisition: Mitigating Risks to the Enterprise” for public review and comment in Sep 2007

DHS Software Assurance Outreach Services

- Co-sponsor bi-monthly SwA WG sessions and semi-annual Software Assurance Forum for government, academia, and industry to facilitate the ongoing collaboration -- next Oct 2007
- Sponsor SwA issues of CROSSTALK (Oct 05, Sep 06, Mar 07); provide SwA articles in other journals to "spread the word" to relevant stakeholders
  - March 2007 issue on "Software Security"
  - May 2007 issue on "Software Acquisition"
  - Sep 2007 issue on "Service Oriented Architecture"
- Provide free SwA resources via "BuildSecurityIn" portal to promote relevant methodologies
- Launch http://us-cert.gov/SwA for Software Assurance Community of Practice (Summer 07)
- Provide DHS Speakers Bureau speakers
- Support efforts of consortiums and professional societies in promoting SwA



Homeland Security

Software Assurance

Software is essential to enabling the nation's critical infrastructure. To ensure the integrity of that infrastructure, the software that controls and operates it must be reliable and secure.

Security must be "built in" and supported throughout the lifecycle.

Visit http://BuildSecurityIn.us-cert.gov to learn more about the practices for developing and delivering software to provide the requisite assurance.

Sign up to become a free subscriber and receive notices of updates.

http://BuildSecurityIn.us-cert.gov

The Department of Homeland Security provides the public-private framework for shifting the paradigm from "patch management" to "software assurance."

INPUT TargetVIEW

Homeland Security

Security in the Software Life Cycle:
Informed development and supply chain management

- Enhance existing processes, methods and technologies to help specify, design, implement, configure, evaluate, & sustain software that is able to:
  - Resist or withstand many anticipated attacks.
  - Recover rapidly and mitigate damage from attacks.
- Keys to secure software:
  - A security-enhanced software development life cycle process -- includes practices and technologies that help developers root out and remove exploitable defects (e.g., weaknesses and vulnerabilities) and increase the likelihood that such defects will not be introduced in the first place.
  - A security-enhanced acquisition / out-sourcing life cycle process -- includes practices that address risks associated with the software supply chain (including due-diligence practices that assist in mitigating risk exposures posed by software and suppliers)

Functional Correctness must be exhibited even when software is subjected to hostile conditions; therefore, claims about system reliability, integrity and safety must include provisions for built-in security of enabling software

What if…

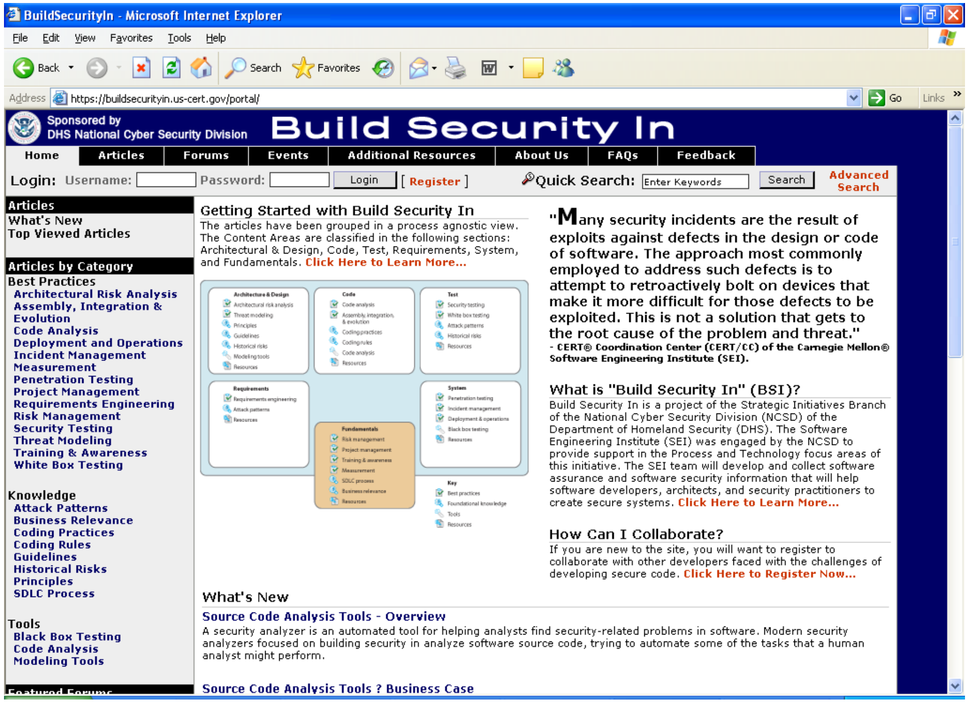
- **Government, in collaboration with industry / academia, raised expectations for product assurance with requisite levels of integrity and security:**
  - Helped advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities and weaknesses;
  - Promoted use of methodologies and tools that enabled security to be part of normal business.
- **Acquisition managers & users factored risks posed by the supply chain as part of the trade-space in risk mitigation efforts:**
  - Information on suppliers' process capabilities (business practices) would be used to determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software.
  - Information about evaluated products would be available, along with responsive provisions for discovering exploitable vulnerabilities, and products would be securely configured in use.
- **Suppliers delivered quality products with requisite integrity and made assurance claims about the IT/software safety, security and dependability:**
  - Relevant standards would be used from which to base business practices & make claims;
  - Qualified tools used in software lifecycle enabled developers/testers to mitigate security risks;
  - Standards and qualified tools would be used to certify software by independent third parties;
  - IT/software workforce had requisite knowledge/skills for developing secure, quality products.

SwA Working Group Sessions every two months – Next 4-6 Dec 2007
Next SwA Forum 2-3 Oct 2007 at Hilton, McLean, VA

See http://us-cert.gov/SwA for SwA Community of Practice (August 2007)

Several SwA documents to be released for public review at SwA Forum

http://buildsecurityin.us-cert.gov



Articles
What's New
Top Viewed Articles

Articles by Category

Best Practices
- Architectural Risk Analysis
- Assembly, Integration & Evolution
- Code Analysis
- Deployment and Operations
- Incident Management
- Measurement
- Penetration Testing
- Project Management
- Requirements Engineering
- Risk Management
- Security Testing
- Threat Modeling
- Training & Awareness
- White Box Testing

Knowledge
- Attack Patterns
- Business Relevance
- Coding Practices
- Coding Rules
- Guidelines
- Historical Risks
- Principles
- SDLC Process

Tools
- Black Box Testing
- Code Analysis
- Modeling Tools

Featured Forums

Getting Started with Build Security In

The articles have been grouped in a process agnostic view. The Content Areas are classified in the following sections: Architectural & Design, Code, Test, Requirements, System, and Fundamentals. **Click Here to Learn More...**

"Many security incidents are the result of exploits against defects in the design or code of software. The approach most commonly employed to address such defects is to attempt to retroactively bolt on devices that make it more difficult for those defects to be exploited. This is not a solution that gets to the root cause of the problem and threat."
- CERT® Coordination Center (CERT/CC) of the Carnegie Mellon® Software Engineering Institute (SEI).

What is "Build Security In" (BSI)?

Build Security In is a project of the Strategic Initiatives Branch of the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS). The Software Engineering Institute (SEI) was engaged by the NCSD to provide support in the Process and Technology focus areas of this initiative. The SEI team will develop and collect software assurance and software security information that will help software developers, architects, and security practitioners to create secure systems. **Click Here to Learn More...**

How Can I Collaborate?

If you are new to the site, you will want to register to collaborate with other developers faced with the challenges of developing secure code. **Click Here to Register Now...**

What's New

Source Code Analysis Tools - Overview
A security analyzer is an automated tool for helping analysts find security-related problems in software. Modern security analyzers focused on building security in analyze software source code, trying to automate some of the tasks that a human analyst might perform.

Source Code Analysis Tools ? Business Case

Opportunities for more explicit linkage and collaboration with other groups

Homeland Security

Joe Jarzombek, PMP
Director for Software Assurance
National Cyber Security Division
Department of Homeland Security
Joe.Jarzombek@dhs.gov
(703) 235-5126