Software Assurance (SwA) in Education, Training & Certification

Pocket Guide v2.1

Robin A. Gandhi
Nebraska University Center on Information Assurance (NUCIA)
University of Nebraska at Omaha
What is a Pocketguide?

• Self-contained
• Concise
• Enumeration of resources
• Theme
• Living document
• Reprints and redistribution possible
• Fits in the coat pocket
SwA ETC Pocketguide Theme

• Educating the Educator/Trainer on available SwA resources

• Purpose:
  – Awareness resource for “getting started” in educating, training and sustaining a workforce capable of producing secure software
  – An “index” in to a vast amount of resources, tools, curricula, and certification and training opportunities for software assurance
Software Assurance (SwA) Pocket Guide Resources

This is a resource for getting started in educating, training and certifying a workforce to build secure software. It describes how to promote awareness of the engineering activities and knowledge areas needed to build software that operates as expected, free from vulnerabilities. It summarizes how to train exemptions and prevent vulnerabilities from being intentionally designed into the software or accidentally inserted at any time during its life cycle. To do so, this guide describes knowledge areas for software assurance, starting with the core areas of study and extending to sub-disciplines related to software security subject materials. It then presents lists of resources for accomplishing such study, including programs, tools, and books, with pointers to their use. Lastly, this guide describes the people who make up a security-conscious system development team, their education, titles, credentials, and standards. As part of the Software Assurance (SwA) Pocket Guide series, this resource is for information only. For details, see referenced source documents. For proper attribution, please include mention of these sources when referencing any part of this document.

This volume of the SwA Pocket Guide series focuses on enumerating education, training and certification resources. It identifies the most effective strategies to inject software assurance topics into existing higher education programs and workforce development programs.

At the back of this pocket guide are references, limitation statements, and a listing of topics addressed in the SwA Pocket Guide series. All SwA Pocket Guide resources and SwA-related documents are freely available for download via the SwA Community Resources and Information Clearinghouse at https://republicsecurity.us-cert.gov/swa.

Acknowledgements

The SwA community collaborates to develop SwA Pocket Guides. The SwA Forum and Working Groups function as a stakeholder meta-community that welcomes additional participation in advancing and refining software security. All SwA-related information resources are offered free for public use. The SwA community invites your input: please contact SoftwareAssurance@hsis.gov for comments and inquiries. For the most current pocket guides, refer to the SwA community website at https://republicsecurity.us-cert.gov/swa.

Members from government, industry, and academia comprise the SwA Forum and Working Groups. The Groups focus on incorporating SwA considerations into acquisition and development processes to manage potential risk exposure from software and from the supply chain.

Participants in the SwA Forum's Workforce Education and Training Working Group contributed to developing the material used in this pocket guide as a step in raising awareness on how to incorporate SwA topics in education, training, and certification of a knowledgeable workforce. One that is ready to perform engineering or technical activities that promote software assurance throughout the Software Development Life Cycle (SDLC).
Software Assurance?

- The \textit{basis for the belief} that software will work as expected
  - Claims, arguments, evidences that span the software lifecycle from cradle to grave
  - People, Process, Technology that enable us to promote assurances in the software that is mission and business critical
SwA Knowledge Areas and Efforts

Key Software Assurance Knowledge Areas and Efforts

**Processes and Practices**
- Enhancement of Development Lifecycle
- Integrating Security into the Software Development Lifecycle
- Requirements and Analysis
- Architecture and Design Considerations
- Risk-Based Security Testing

**Capacity Maturity Model Integration**
- Harmonizing and Extending existing Security Capability Maturity Models
- Mapping Assurance Goals and Practices to CMMI for Development

**Maturity Model**
- Building Security In Maturity Model (BSIMM)
- Software Assurance Maturity Model (SAMM)

**Key Practices for Mitigating Software Weaknesses**
- Secure Coding Standards (CERT)

**Measurement**
- Measurement Frameworks
- Practical Measurement Framework for Software Assurance and Information Security
- Acquisition Measurement
- Measurements Goals and Questions Lists

**Business Case**
- Making a Business Case for SwA
- Cost/Benefit Models
- Measurement
- Prioritization
- Process Improvement
- Globalization
- Organizational Development
- Case Studies and Examples

**Workforce Education and Training**
- Curriculum Guides
- Knowledge necessary to Develop Sustain, Acquire and Secure Software (SwABoK)
- State of the Art Reports (SOAR)
- Guidebooks (NASA, DACS)
- Reference Curriculum (MSwA2010, Undergrad outline)
- Security Principles and Guidelines
- Logical and in-depth organization of Principles and Guidelines
- Workforce Development and Improvement
- Competency and Functional Framework for IT Security Workforce (EBK)
- Workforce Credentials

**Technology, Tool and Product Evaluation**
- Making Security Measureable
- CWE, CVSS
- CVE, CCE, CPE, OVAL, CVSS
- Measuring Functionality and Capability of SwA Tools (SAMATE)
- Functional Specifications
- Test suites
- Tool Metrics

**Acquisition and Outsourcing**
- Security-Enhanced Software Acquisition and Outsourcing
- Reference Guide: SwA in Acquisition
- Practices to Enhance SwA in Purchasing
- Due diligence Questionnaires
- Sample Contract Provisions and Language
- Application Security Procurement Language
- Supply chain Risk Management
- Risk-based approach to Software Acquisition

**Malware**
- Malware Dictionaries
- Malware Attribute Enumeration and Characterization (MAEC)
- Novel Approaches to Malware
SwA Knowledge Areas and Efforts

**Workforce Education and Training**
- Curriculum Guides
  - Knowledge necessary to Develop Sustain, Acquire and Assure Secure Software (SwABoK)
  - State of the Art Reports (SOAR)
  - Guidebooks (NASA, DACS)
  - Reference Curriculum (MSwA2010, Undergrad outline)
- Security Principles and Guidelines
  - Logical and In-depth organization of Principles and Guidelines
- Workforce Development and Improvement
  - Competency and Functional Framework for IT Security Workforce (EBK)
  - Workforce Credentials

**Technology, Tool and Product Evaluation**
- Making Security Measureable
  - CWE, CWSS
  - CVE, CCE, CPE, OVAL, CVSS
- Measuring Functionality and Capability of SwA Tools (SAMATE)
  - Functional Specifications
  - Test suites
  - Tool Metrics
- Metamodels for Software Assets and Operational Environments
  - Abstract Syntax Tree Metamodel (ASTM)
  - Knowledge Discovery Metamodel (KDM)
  - Software Metrics Metamodel (SMM)

**Acquisition and Outsourcing**
- Security-Enhanced Software Acquisition and Outsourcing
  - Reference Guide: SwA in Acquisition
  - Practices to Enhance SwA in Purchasing
  - Due diligence Questionnaires
  - Sample Contract Provisions and Language
  - Application Security Procurement Language
  - Supply chain Risk Management
  - Risk-based approach to Software Acquisition

**Processes and Practices**
- Enhancement of Development Lifecycle
  - Integrating Security into the Software Development Lifecycle
  - Requirements and Analysis
  - Architecture and Design Considerations
  - Risk-Based Security Testing
- Capability Maturity Model Integration
  - Harmonizing and Extending existing Security Capability Maturity Models
  - Mapping Assurance Goals and Practices to CMMI for Development
- Maturity Model
  - Building Security In Maturity Model (BSIMM)
## Curriculum and Training Guides

### Table 1 – SwA Curriculum and Training Development Guides

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Relevant Documents and Links</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Security Assurance SOAR</td>
<td><strong>Volume II: Undergraduate Course Outlines.</strong> Mead, Nancy R. et al. SEI/CMU. <a href="http://www.cert.org/mswa/">http://www.cert.org/mswa/</a></td>
<td>Focuses on an undergraduate curriculum specialization for software assurance. Intended to provide students with fundamental skills for either entering the field directly or continuing with graduate level education. Last updated 2010.</td>
</tr>
</tbody>
</table>
## Table 2 – Workforce Development and Improvement

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Relevant Documents and Links</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| DoD 8570.01-M    | Information Assurance Workforce Improvement Program. Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer.  
http://www.us-cert.gov/ITSecurityEBK/                                                                                                      | Characterizes the IT security workforce and provides a national baseline of essential knowledge and skills that IT security practitioners should have in order to perform specific roles and responsibilities. Last updated September 2008. |
| Information Security Workforce Development Matrix Project – Information Security Systems and Software Development Professional Role | See Section Role Descriptions section, page 17, for materials from the matrix project developed by Federal CIO Council’s IT Workforce Committee and Information Security and Identity Management Committee.  
Contacts:  
http://www.cio.gov/committees.cfm/csec/3/cid/4  
http://www.cio.gov/committees.cfm/csec/3/cid/5                                                                 | This project produces role-based information security workforce development matrices. The matrices are one-page dashboards intended to establish a baseline across the Federal Government for staff engaged in information security work. This initiative provides a government-wide perspective on common information security roles. The ISS&SDP is one of 11 roles that have been identified to date. Each matrix contains a uniform framework, by performance level, describing the recommended competencies/skills, education, experience, credentials, and training for a particular role. The matrices provide guidance for federal agencies and do not replace OPM basic qualifications. |
# Strategies for Injecting SwA Knowledge

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Relevant Documents and Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree programs and specializations in SwA</td>
<td>Reference curriculums available from the Software Engineering Institute, Carnegie Mellon University can be used as recommendations for designing Masters of Software Assurance degree program and undergraduate curriculum specialization in software assurance. These reference curriculums are available at <a href="http://repository.cmu.edu/sei/3/">http://repository.cmu.edu/sei/3/</a> and <a href="http://repository.cmu.edu/sei/4/">http://repository.cmu.edu/sei/4/</a>. Graduate Certificates and Master Degree Concentrations at the Stevens Institute of Technology: <a href="http://dc.stevens.edu/academic-programs/software-assurance/">http://dc.stevens.edu/academic-programs/software-assurance/</a></td>
</tr>
<tr>
<td>Strategy</td>
<td>Relevant Documents and Links</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Stand-alone Courses      | New course offerings based on SwA knowledge areas complement existing Software Engineering courses. Examples: [http://www.cs.jmu.edu/sss](http://www.cs.jmu.edu/sss)  
                          | https://www.securecoding.cert.org/confluence/display/sci/S08+15392+Secure+Programming. Also: graduate-level Software Assurance courses that cover secure software engineering activities during the SDLC are offered at the University of North Carolina at Charlotte, and The University of Nebraska at Omaha. |
| Augmenting Existing Courses | The SwA CBK and State-of-the-Art reports are catalogs of secure software development practices, processes, and techniques that can be mapped to topics relevant to current curriculums. The identified gaps can then be filled using relevant materials. |
| Micro-Modules            | Problem-based learning exercises, in class workshops, or short talks to inject topics such as Misuse Cases and Assurance Cases into existing software engineering or information security courses. |
| Capstone and Class Projects | Software Engineering capstone courses or class projects which can be geared towards a security critical domain such as designing a software system for the Department of Defense, Cyber-physical systems or for a Credit Card transaction processing company. These domains will facilitate the exploration of security needs throughout the SDLC. |
| Online Courses           | The Adaptive Cyber-Security Training Online (ACT-Online) courses are available on the TEEX Domestic Preparedness Campus. Ten courses address three discipline-specific tracks. The targets are everyday nontechnical computer users, technical IT professionals, business managers and professionals. These courses are offered at no cost and students earn a DHS/FEMA Certificate of completion along with Continuing Education Units (CEU) at the completion of each course. [http://www.teexwmdcampus.com/index.k2](http://www.teexwmdcampus.com/index.k2) |
|                          | The CERT Virtual Training Environment (VTE) combines the components of traditional classroom training with the convenience of web-based training. Over 200 hours of course material focused around the technical, policy, and management implications of information security – including preparatory courses for commercial certifications, core skills courses, role-based courses for managers and technical staff, and vendor-developed courses. Open access is provided to individual DoD personnel (Active Duty, DoD Civilian and contractors) and members of the Federal Civilian Workforce through specific sponsorships from DISA, and DHS in conjunction with the Department of State Foreign Service Institute. Sponsored accounts can be requested at [www.vte.cert.org](http://www.vte.cert.org). Public access to many of the materials is provided through the VTE Library at [https://www.vte.cert.org/vteweb/Library/Library.aspx](https://www.vte.cert.org/vteweb/Library/Library.aspx) |
Tools and web resources that can be used in class to provide hands-on experience with SwA Concepts.

<table>
<thead>
<tr>
<th>Tool Name</th>
<th>Tool Description</th>
<th>Possible Classroom Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArgoUML</td>
<td>ArgoUML is the leading open source UML modeling tool and includes support for all standard UML 1.4 diagrams. It runs on any Java platform.</td>
<td>Misuse cases, security focused UML class diagrams and other documentation for class assignments and projects.</td>
</tr>
<tr>
<td>ASCE</td>
<td>ASCE supports the key assurance case notations: Goal Structuring Notation and Claims-Arguments-Evidence. Academic license available upon request at <a href="http://www.adelard.com/web/hnav/ASCE/index.html">http://www.adelard.com/web/hnav/ASCE/index.html</a></td>
<td>Assurance case documentation for class assignments and projects, Demonstration of worked examples used on real projects.</td>
</tr>
<tr>
<td>Burp Suite</td>
<td>Burp Suite is an integrated platform for attacking web applications. Located at <a href="http://www.portswigger.net/suite/">http://www.portswigger.net/suite/</a></td>
<td>Burp Suite allows the combination of manual and automated techniques to enumerate, analyze, scan, attack and exploit web applications.</td>
</tr>
<tr>
<td>CERT Secure Coding Standards</td>
<td>Secure coding standards for commonly used programming languages such as C, C++ and Java. Located at <a href="https://www.securecoding.cert.org">https://www.securecoding.cert.org</a></td>
<td>Online reference; examples of coding do’s and dont’s.</td>
</tr>
<tr>
<td>FindBugs™</td>
<td>A program which uses static analysis to look for bugs in Java code at <a href="http://findbugs.sourceforge.net/">http://findbugs.sourceforge.net/</a></td>
<td>Scan java code repositories for bugs; Introduction to static code checking activities.</td>
</tr>
<tr>
<td>Microsoft SDL Threat Modeling Tool</td>
<td>The Microsoft SDL Threat Modeling Tool allows software architects to identify and mitigate potential security issues early, when they are relatively easy and cost-effective to resolve. Located at <a href="http://www.microsoft.com/security/sdl/getstarted/threatmodeling.aspx">http://www.microsoft.com/security/sdl/getstarted/threatmodeling.aspx</a></td>
<td>Conduct student group workshops to discuss threats to various design alternatives, while suggesting possible mitigation strategies.</td>
</tr>
<tr>
<td>Tool Name</td>
<td>Tool Description</td>
<td>Possible Classroom Uses</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Olly Debug</td>
<td>OllyDbg is a 32-bit assembly level debugger for Microsoft Windows. Located <a href="http://www.ollydbg.de/">at www.ollydbg.de/</a></td>
<td>Emphasize binary code analysis and is particularly useful in cases where source is unavailable. Explain Buffer Overflows.</td>
</tr>
<tr>
<td>Pharos</td>
<td>Pharos is an open source proxy that traps all HTTP and HTTPS data between server and client, including cookies and form fields, which can be intercepted and modified. Located at <a href="http://parosproxy.org/index.shtml">http://parosproxy.org/index.shtml</a></td>
<td>Pharos can be used as an introduction to web application security assessment.</td>
</tr>
<tr>
<td>SAMATE Reference Dataset</td>
<td>The purpose of the SAMATE Reference Dataset (SRD) is to provide users, researchers, and software security assurance tool developers with a set of known security flaws. This will allow end users to evaluate tools and tool developers to test their methods. Located at <a href="http://samate.nist.gov/index.php/Main_Page.html">http://samate.nist.gov/index.php/Main_Page.html</a></td>
<td>A reference data set can be used in class to reflect upon known flaws in software.</td>
</tr>
<tr>
<td>Splint</td>
<td>Splint is a tool for statically checking C programs for security vulnerabilities and coding mistakes. Located at <a href="http://www.splint.org/">http://www.splint.org/</a></td>
<td>Static analysis code checking activities.</td>
</tr>
<tr>
<td>Valgrind</td>
<td>Valgrind is an instrumentation framework for building dynamic analysis tools. Located at <a href="http://valgrind.org/">http://valgrind.org/</a></td>
<td>Demonstrate dynamic analysis techniques to detect memory management and threading bugs, as well as detailed program profiling.</td>
</tr>
<tr>
<td>Vine</td>
<td>Provides an intermediate language that x86 code can be translated to for Static analysis. Located at <a href="http://bitblaze.cs.berkeley.edu/vine.html">http://bitblaze.cs.berkeley.edu/vine.html</a></td>
<td>Identify data flows analysis and conduct binary analysis.</td>
</tr>
</tbody>
</table>

### Web Resources

- [Google Code](http://google-gruvere-appspot.com)
## Books

### Table 5 – A List of SwA focused Books for Use in Education and Training

<table>
<thead>
<tr>
<th>Topic</th>
<th>Title and Publisher</th>
<th>Summary and Possible Use</th>
</tr>
</thead>
</table>
# Standards of Practice

<table>
<thead>
<tr>
<th>Standard</th>
<th>Source</th>
<th>Purpose</th>
</tr>
</thead>
</table>
Self Assessment: [https://buildsecurityin.us-cert.gov/swa/downloads/20100922_PRM_Practice_List_2 page.pdf](https://buildsecurityin.us-cert.gov/swa/downloads/20100922_PRM_Practice_List_2 page.pdf) | The Assurance PRM can be used to help organizations conduct a gap analysis of existing practices. The results of a gap analysis can be used to prioritize and track SwA implementation efforts. The Assurance PRM addresses assurance from executive to developer. |
| **BSIMM2: The Building Security In Maturity Model** | [http://bsimm2.com/](http://bsimm2.com/)                                 | Pronounced “bee simm” was created by observing and analyzing real-world data from thirty leading software security initiatives. The BSIMM can help you determine how your organization compares to other real-world software security initiatives and what steps can be taken to make your approach more effective. |
| **CERT Resilience Management Model**         | [http://www.cert.org/resilience/rmm.html](http://www.cert.org/resilience/rmm.html) | It has two primary objectives:  
1. Establish the convergence of operational risk and resilience management activities such as security, business continuity, and aspects of IT operations management into a single model.  
2. Apply a process improvement approach to operational resilience management through the definition and application of a capability level scale that expresses increasing levels of process improvement. |
# Workforce Credentials

## Table 7 – Certification and Training Opportunities

<table>
<thead>
<tr>
<th>Certification Authority</th>
<th>SwA Relevant Certificates</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE Computer Society</td>
<td>Certified Software Development Professional (CSDP)</td>
<td><a href="http://www.computer.org/portal/web/certification">http://www.computer.org/portal/web/certification</a></td>
</tr>
<tr>
<td>(ISC)²</td>
<td>Certified Secure Software Lifecycle Professional (CSSLP)</td>
<td><a href="http://www.isc2.org/csslp-certification.aspx">http://www.isc2.org/csslp-certification.aspx</a></td>
</tr>
</tbody>
</table>
Job Roles

• What kind of jobs can I get?
  – Jobs and career planning
    • http://www.sans.org/20coolestcareers

#18 - Security-savvy Software Developer*
"Kool, because this is VERY rare."

Job Description
The security-savvy software developer leads all developers in the creation of secure software, implementing secure programming techniques that are free from logical design and technical implementation flaws. This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacker.

#2 - System, Network, and/or Web Penetration Tester* - Top Gun Job
"You can be a hacker, but do it legally and get paid a lot of money!"
Role Descriptions

» **Cyber Software Assurance Developer/Integrator**
  
  » Experience with applying security activities within SDLC
  
  » Experience with security, including CSSLP, CISSP and SANS secure programming assessments
  
  » Experience with security standards, including SSE-CMM, NIST SPs, ISO 15408
  
  » Common Criteria, or client-specific software assurance guides. (Also see the section on “Standards of Practice”)

» **Software Assurance Engineer**
  
  » Provide technical leadership in all aspects of software assurance and computer systems engineering support
  
  » Lead and actively participate in the evaluation and analyses of activities related to all phases of the secure software life cycle from initial planning, requirements definition, design and development through integrated system testing and sustaining operations.
  
  » Responsibilities will also include the support of a wide range of technical and programmatic activities for program offices, including leading the review and assessment of software system architecture; system requirements and their allocation to lower level specifications; design, code and test activities; trade studies; COTS/GOTS products; reuse software; test tools; simulators; software verification and validation (V&V); and system test and integration. Support independent review efforts in analyzing and assessing system software and related development and testing activities.
**Information Security Systems & Software Development Professional (ISSSDP)**

- The Information Security Systems and Software Development Professional is responsible for secure design, development, testing, integration, implementation, sustainment, and/or documentation of software applications (web based and non-web) following formal secure systems development lifecycle processes and using security engineering principles.

- The following professional requirements form part of a broad Federal Government effort to identify and describe roles.

<table>
<thead>
<tr>
<th>Table 8– Credentials, Competencies and Skills by Performance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software Development</strong></td>
</tr>
<tr>
<td>Written &amp; Oral Communication</td>
</tr>
<tr>
<td>Creative Problem Solving</td>
</tr>
<tr>
<td>Information Security/Accurance</td>
</tr>
<tr>
<td>Critical Thinking and Analytical Skills</td>
</tr>
<tr>
<td><strong>Entry Level</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td><strong>Intermediate Level</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td><strong>Advanced Level</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

| **Software Engineering**                                     |
| Project/Program Management                                  |
| Leadership & People Management                              |
| **Entry Level**                                               |
| No                                                            |
| **Intermediate Level**                                       |
| Yes                                                           |
| **Advanced Level**                                           |
| Yes                                                           |

| Suggested Credentials in:                                   |
| Computer science/engineering                                |
| Database/information management                             |
| Information assurance/security                               |
| Software assurance/security                                  |
| Information systems management                              |
| **Entry Level**                                              |
| Associate’s Degree from an accredited program                |
| **Intermediate Level**                                       |
| Bachelor’s Degree from an accredited program                 |
| **Advanced Level**                                           |
| Master’s Degree from an accredited program plus 5 years’ experience |
Got Content?

• The pocket guide is a “work in progress”

• Plenty of opportunity to contribute content

• Join the Effort!
  – Your comments, suggestions, criticism/praise are all very welcome
Where to find the PocketGuide?

• [https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html](https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html)

• And many others...
Software Assurance Pocket Guide Series

The SWA Pocket Guide Series comprises free, downloadable documents on software assurance in acquisition and outsourcing, software assurance in development, the software assurance life cycle, and software assurance measurement and information needs. SWA Pocket Guides are developed collaboratively by the SWA Forum and Working Groups, which function as a stakeholder community that welcomes additional participation in advancing and refining software security. Your input on these documents is welcome; please use the feedback form. For general inquiries, please email Software.Assurance@dhs.gov.

- **SWA in Acquisition and Outsourcing**
  - Software Assurance in Acquisition and Contract Language
  - Software Supply Chain Risk Management and Due Diligence

- **SWA in Development**
  - Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses
  - Software Security Testing
  - Requirements and Analysis for Secure Software
  - Architecture and Design Considerations for Secure Software
  - Secure Coding

- **SWA Life Cycle**
  - Software Assurance in Education, Training & Certification

Future SWA Pocket Guides

---

**Software Assurance in Education, Training & Certification**

*Life Cycle Support Volume 1 - (Version 2.1, March 1, 2011)*

Current events related to cybersecurity encourage a fundamental shift in the way we think about educating and training a workforce prepared to address security issues in all phases of a software system. Software assurance education and training is aimed to ensure adequate coverage of requisite knowledge areas in contributing disciplines such as software engineering (including its many subdisciplines), systems engineering, project management, etc. to identify and acquire competencies associated with secure software. The primary audiences for this pocket guide are educators and trainers who can use this guide to identify resources to supplement their efforts as well as identify strategies to inject software assurance-related topics in the existing education and training programs.

8.5" x 11" version PDF file

Future SWA Pocket Guides
Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses

Development Volume II - (Version 1.3 May 24, 2009)
Common Weakness Enumeration (CWE) provides a standard means for understanding residual risks; enabling more informed decision-making by suppliers and consumers about the security of software. The 2009 CWE/SANS Top 25 Most Dangerous Programming Errors is a list of the most egregious programming errors that can lead to serious exploitable software vulnerabilities. The main goal for the Top 25 list is to stop vulnerabilities at the source by educating programmers on how to eliminate the most egregious programming errors before software is shipped. The list could be used as a tool for education and awareness that helps programmers prevent the kinds of vulnerabilities that plague the software industry. Software consumers could use the same list to help them to ask for more secure software, while software managers and CIOs could use the Top 25 list as a measuring stick of progress in their efforts to secure their software. This volume of pocket guide links the CWE’s with the common attacks that exploit these weaknesses, the resulting mission and business risks. It provides recommended practices for preventing the exploits in software.

8.5" x 11" version PDF File

Software Security Testing

Development Volume III - (Version 0.7 May 10, 2010)
Software security testing validates the secure implementation of a product thus reducing the likelihood of security flaws being released and discovered by customers or malicious users. The goal is not to “test in security,” but to validate the robustness and security of the software products prior to making them available to customers and to prevent security vulnerabilities from ever entering the software. This volume of the pocket guide describes the most effective security testing techniques, their strengths and weaknesses, and when to apply them during the Software Development Life Cycle.

8.5" x 11" version PDF File

Requirements and Analysis for Secure Software

Development Volume IV - (Version 1.0, October 5, 2009)
Comprehensive requirements are critical for successful system development, but all too often, requirements fail to explicitly consider security. As a result, systems meet the functionality but are rarely safe and consequently are the target of attacks. Systems which carefully document security requirements reduce the likelihood of successful attacks. Security requirements include functions that implement a security policy such as areas of access control, identification, authentication and...
Software Assurance in Acquisition and Contract Language

*Acquisition and Outsourcing Volume I – (Version 1.1 July 31, 2009)*

Integrating software security in the acquisition life cycle promotes the acquisition of secure software. This volume of the pocket guide includes sample SwA Request for Proposal (RFP)/Contract language. Buyers and evaluators of software and suppliers can gain security risk-based insight. They can put suppliers on notice that consumers are concerned about software security and the risks to their organizations that are attributable to exploitable software.

8.5” x 11” version PDF File

Software Supply Chain Risk Management and Due Diligence

*Acquisition and Outsourcing Volume II – (Version 1.2 June 16, 2009)*

Software security enhanced due-diligence is a critical element of software supply chain risk management. The focus of the volume is to increase awareness for the need to include software assurance and identify best practices in the acquisition of software. Due-diligence involves taking reasonable steps to ensure that software or a software-intensive system not only meets functional and technical requirements, but also addresses software assurance concerns. Buyers and evaluators of software and services can gain security risk-based insight. They can put suppliers on notice that consumers are concerned about software security and the risks to their organizations that are attributable to exploitable software.

8.5” x 11” version PDF File
Find me

• Robin A. Gandhi, Ph.D.
  Assistant Professor of Information Assurance
  University of Nebraska at Omaha

rgandhi@unomaha.edu

Voice: (402) 554 3363, Fax: (402) 554-3284

http://faculty.ist.unomaha.edu/rgandhi
Acknowledgement

• Joe Jarzombek for giving me the opportunity to lead this effort
• Members of the SwA WG on Education and Training for insightful comments, reviews and content (Dan, Carol, Nancy, Art)
• Susan Morris, Walter Houser, Dominick Chiriyan
• And many others...
Bonus Slides
Why Johnny Can’t write secure code?

• *Johnny, avoid these weaknesses.... Period!*
  – Common Weaknesses Enumeration (CWE)

• *Johnny...learn from your mistakes*
  – Common Vulnerabilities and Exposures (CVE)

• *Johnny...these are the ways of the bad guys*
  – Common Attack Patterns Enumeration and Classification (CAPEC)

• *Johnny...these are ways to develop secure code*
  – CERT secure coding guidelines
Poor Johnny!

45000+ CVE Vulnerabilities

CWE 650+ Weaknesses 1000+ Pages

Countless Do’s and Don’ts

CAPEC 300+ Attack Patterns
Using Semantic Templates to Study Vulnerabilities Recorded in Large Software Repositories
The Paradox we face!

Source Code Differences after the fix

Mailing list Discussions

Log of Changes

Bug tracking databases

Vulnerability Databases

Weakness Enumerations

Public Descriptions

The Apache HTTP Server Project

Apache httpd 1.3 vulnerabilities

This page lists all security vulnerabilities fixed in release Apache httpd 1.3. Each vulnerability is given a severity rating by the Apache security team - please note that this rating may vary from platform to platform. We also list the versions of Apache httpd affected by the vulnerability.

This page is created from a database of vulnerabilities originated by Apache Weekly. Please send comments or concerns about these vulnerabilities to the Security Team.

Features

• Apache httpd 1.3.42

• Fixed in Apache httpd 1.3.42

• Get Involved

• Bug tracking databases

• Vulnerability Databases

• Weakness Enumerations

• Mailing list Discussions

• Log of Changes

• Source Code Differences after the fix
Tangling of information in the CWE

• **CWE-119: Failure to Constrain Operations within the Bounds of a Memory Buffer**

  – The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer.

  – Certain languages allow direct addressing of memory locations and do not automatically ensure that these locations are valid for the memory buffer that is being referenced. This can cause read or write operations to be performed on memory locations that may be associated with other variables, data structures, or internal program data. As a result, an attacker may be able to execute arbitrary code, alter the intended control flow, read sensitive information, or cause the system to crash.
Tangling of information in the CWE

• CWE-120: *Buffer Copy without Checking Size of Input* ('Classic Buffer Overflow')
  
  – The program copies an input *buffer* to an output *buffer* without verifying that the size of the input *buffer* is less than the size of the output *buffer*, leading to a *buffer overflow*.

  – A *buffer overflow* condition exists when a program attempts to put more data in a *buffer* than it can hold, or when a program attempts to put data in a *memory area* outside of the boundaries of a *buffer*.

  – *Buffer overflows* often can be used to execute arbitrary code...

  – *Buffer overflows* generally lead to crashes
Buffer Overflow

WEAKNESS
- ACCESS AND OUT-OF-BOUNDS READ #125, #126, #127, #786
- ACCESS AND OUT-OF-BOUNDS WRITE #787, #788, #124
- FAILURE TO CONSTRAIN OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER #119
- IMPROPER-ACCESS-OF-INDEXABLE-RESOURCE #118

CAN-PRECEDE

RESOURCES/LOCATION
- STACK-BASED #121
- STATIC #129
- HEAP-BASED #122
- MEMORY-BUFFER #119
- BUFFER #119
- INDEX #466
- INTEGER #129
- INDEXABLE-RESOURCE #118

CAN-PRECEDE

CONSEQUENCES
- UNCONTROLLED MEMORY ALLOCATION #789
- INFORMATION LOSS OR OMMISSION #199 #221
- WRITE-WHAT-WHERE CONDITION #123
**WEAKNESS**

- **ACCESS AND OUT-OF-BOUNDS READ** #125, #126, #127, #786
- **FAILURE TO CONSTRAIN OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER** #119

**CONSEQUENCES**

- **WRITE-WHAT-WHERE CONDITION** #123

**CHANGE LOG ISSUE DESCRIPTION**

1. Off-by-one error in the toAlphabetic function in rendering/RenderListMarker.cpp
   - The math was slightly off here, and we wound up trying to access an array at index -1 in some cases
   - We need to decrement `numberShadow` rather than subtracting one from the result of the modulo operation
   - Line 105 decrement (`--numberShadow;`) and remove the subtraction of one in Line 106

**CHANGE LOG FIX DESCRIPTION**

- We need to decrement `numberShadow` rather than subtracting one from the result of the modulo operation

**CVE DESCRIPTION**

- Off-by-one error allows remote attackers to obtain sensitive information... or possibly execute arbitrary code

**CVE-2010-1773**

- Memory corruption in rendering...

**SOFTWARE-FAULT**

- **OFF-BY-ONE** #193
- **ACCESS AND OUT-OF-BOUNDS** #194 #195 #196
- **INCORRECT-BUFFER-SIZE-CALCULATION** #131
- **IMPROPER-INPUT-VALIDATION** #20
- **INCORRECT-CALCULATION** #682
Experiment

• The scenario...
  – A newbie programmer or occasional contributor to open source project
    • How much effort does it take to study a vulnerability and summarize lessons learned?

• 30 Computer Science students from a senior-level undergraduate Software Engineering course.
  – None to more than 5 years
  – No prior knowledge of semantic templates
Experiment

• $H_{10}$:
  – There is no reduction in completion time for subjects who use semantic templates compared to those who do not.

• $H_{20}$:
  – There is no improvement in accuracy of understanding of vulnerabilities for subjects who use semantic templates compared to those who do not.
Variables

• The experiment manipulated these *independent variables*:
  – **Group** - refers to the group assigned (1 or 2).
  – **Round** - refers to the experiment round (1 or 2).

• **Vulnerability ID** - the vulnerability under study (1-1, 1-2, 1-3, 2-1, 2-2, 2-3).
  – These self-reported *subject variables* were collected:
    • Programming skill level
    • *Reading comprehension and writing skill levels* - ability to read and write technical English documents.
Variables

• Dependent variables:
  – Time to complete assignment
  – CWE identification accuracy
  – Fault identification accuracy
    • a score (scale of 1-5) on the accuracy of the identification of the software fault that led to the vulnerability
  – Failure identification accuracy
    • a score (scale of 1-5) on the accuracy of the description of the nature of the vulnerability (the manifested problem, the resources impacted and the consequences)
Initial Results and Findings

Table 1: p-values of one-tailed t-tests for Time data

<table>
<thead>
<tr>
<th></th>
<th>Round 1</th>
<th>Round 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1-1)</td>
<td>0.3627</td>
<td>0.0001</td>
</tr>
<tr>
<td>(1-2)</td>
<td>0.5855</td>
<td>0.0030</td>
</tr>
<tr>
<td>(1-3)</td>
<td>0.1516</td>
<td>0.0015</td>
</tr>
</tbody>
</table>

p-values of one-tailed t-tests for CWE precision

<table>
<thead>
<tr>
<th></th>
<th>Round 1</th>
<th>Round 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1-1)</td>
<td>0.9281</td>
<td>0.1840</td>
</tr>
<tr>
<td>(1-2)</td>
<td>0.9957</td>
<td>0.6023</td>
</tr>
<tr>
<td>(1-3)</td>
<td>0.5344</td>
<td>0.0891</td>
</tr>
</tbody>
</table>

Table 1: p-values of one-tailed t-tests for CWE recall

<table>
<thead>
<tr>
<th></th>
<th>Round 1</th>
<th>Round 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1-1)</td>
<td>0.0683</td>
<td>0.0141</td>
</tr>
<tr>
<td>(1-2)</td>
<td>0.9481</td>
<td>0.0093</td>
</tr>
<tr>
<td>(1-3)</td>
<td>0.2286</td>
<td>0.0021</td>
</tr>
</tbody>
</table>

Time to completion (minutes) per vulnerability
Future Work

• Integrate with existing static and dynamic analysis tools to enhance reporting capabilities
  – Provide layers of guidance to a developer upon detection of a software flaw
  – Organize and retrieve knowledge of past vulnerabilities
  – Verify patch submissions

• Investigate project/developer specific coding errors and vulnerability fix patterns

• Other usage scenarios in the SDLC
Acknowledgement

- This research is funded in part by Department of Defense (DoD)/Air Force Office of Scientific Research (AFOSR), NSF Award Number FA9550-07-1-0499, under the title “High Assurance Software”
Thank you for your Attention