

ISSEA TIMES



Spring 2008 Edition

April 2008
Volume 5, Issue 2

Welcome to ISSEA!

The International Systems Security Engineering Association (ISSEA) was formed in 1998 to further industry acceptance of security engineering as a discipline. The early days of the association were focused on developing the System Security Engineering Capability Maturity Model (SSE-CMM), and gaining ISO approval of the SSE-CMM as an alternate assurance technique in the ISO framework.

Today, ISSEA focuses on security engineering activities across all phases of the system life cycle. ISSEA monitors standards committees, and works within the international community to define a common vocabulary for security and assurance activities. ISSEA maintains a library of base practices and tailored key process attributes that accommodate security engineering in the context of system engineering activities.

The standards landscape is ever-changing. Security Engineering impacts:

- System assurance practices
- Enterprise compliance processes
- Software Development practices
- Requirement Verification and Validation and
- Operations and maintenance functions

Security Engineering supports the Enterprise Governance Functions. In a world where new design processes and architectures are developed daily, ISSEA provides a compass to help the enterprise build a sound security engineering practice.

INSIDE THIS ISSUE

Welcome to ISSEA!	1
ISSEA Conference: Save the Date	1
Call for Papers	2
International Standards Update	3
Outreach Committee	3
Making Life Simple	4
Great Finds: Web Sites to Visit	5
Contacting ISSEA	6

ISSEA CONFERENCE:

SAVE THE DATE

OCTOBER 21-24, 2008

CHICAGO ILLINOIS, USA

Chicago Hilton(312) 922-4400
720. S Michigan Ave; Chicago, Illinois 60605

JOIN US IN THE WINDY CITY!

ISSEA hosts an annual conference to promote experiential learning and sharing about security engineering implementation activities. The Outreach and Awareness Committee invites interested practitioners or students in industry, government, and academia to share and contribute their knowledge to grow the knowledge base of security engineering.

This year's theme is:

Assurance and the Enterprise Life Cycle:
exactly what is it,
who is the audience for it?
and how is it applied in practice?

The conference offers attendees an intimate forum to discuss the state of the practice. engineering processes and standards.

Please see *Call for Papers on Page 2*

Call For Papers, Panels & Presentations

Submission Due Date: June 1, 2008

Submit to: Angela Morgan, AMorgan@ewa.com

About The Conference:

The ISSEA Conference is intended to further the Association's mission of advancing the field of systems security engineering by presenting an outstanding educational program on the latest developments and critical issues in the field. Open to all members and the general public, this conference provides a forum for the exchange of knowledge and ideas for security professionals from around the world. In addition, the event is an excellent networking opportunity. The Program Committee invites you to submit original papers, presentations, and panel proposals to be considered for inclusion in the 8th Annual ISSEA Conference. This year's theme is: **Assurance and the Enterprise Life Cycle: exactly what is it, who it is for and how can it be used?**

Submissions should include:

- Title
- 250 word topic abstract
- Type of presentation
- If panel or debate, please provide suggested participants list
- Author(s), organization affiliation,
- Point of contact, phone number, and e-mail address.
- If the presentation has been previously presented or published, indicate when and where.
- Estimated duration of presentation (30, 45, 60 minutes)
- Release for Publication and Copyright: Authors are responsible for obtaining government or corporate releases for publication. Written releases will be required for all papers to be published. Papers developed as part of official U.S. Government duties may not be subject to copyright. Papers that are subject to copyright must be accompanied by written assignment for multi-media publication to ISSEA.

Topics Sought:

The conference is particularly interested in papers, presentations, or panels that address the areas of:

- Systems security engineering best practices (Examples, Case studies, Tools and techniques)
- Security metrics
- Development and implementation methodology
- Application of security engineering and process metrics
- Gained through process maturity
- Alternate means of achieving assurance
- Conducting SSE-CMM appraisals
- Objective profiles developed for specific user communities
- Relationship between security and privacy
- Systems engineering practices specifically designed for privacy systems
- Impact of privacy laws on security engineering practices
- Risk assessment methodologies
- Secure systems development, integration and application security
- Security management as it relates to security engineering
- Assurance and its contribution to Governance
- Assurance Cases and Risk Management
- Security-Enhanced Supply Chain Risk Management
- Software Assurance
- Security Measurement and the Assurance Case
- Security Process Improvement Methods and Techniques
- Enabling Informed Security Risk Management Decision Making
- Systems Security Engineering Best Practices for Security and Privacy
- Related Emerging and Evolving Standards

STANDARDS UPDATE

ISSEA Technical Officer

As usual there is a lot going on in the world of International Standards. ITU-T's security standards and references web database continues to be updated and is gaining in reputation and recognition. If you have not yet looked at this resource, I strongly suggest that you take a look, it is 15 minutes well spent, go to <http://www.itu.int/ITU-T/studygroups/com17/ict/index.html> .

The 27000 series of standards continues to mature and expand with new elements being added to the set at regular intervals, see the SC 27 Catalogue for more details. Of particular interest to ISSEA members is the work commencing on Application Security in Working Group 3, and the work on Secure Systems Design in Working Group 3. ISSEA is actively participating in the Secure Systems Design work and monitoring the Application Security project.

The portfolio of products produced by SC 27 continues to grow and expand, with new items being added at regular intervals. A great resource to keep abreast of what is happen is the SC 27 Catalogue, which is updated every 6 months, and contains a one page summary of every SC 27 project. The Catalogue can be found at <http://www.jtc1sc27.din.de/sce/SD7> .

Another standards group of interest to ISSEA members is SC 7 Systems and Software Engineering. They are currently developing a revised standard on Systems and Software Assurance, ISO/IEC 15026. ISSEA is contributing to this work to help ensure that 15026 does not conflict with work in the security area such as ISO/IEC 21827, 15443, 15408, 19791, etc, etc. ISSEA plans to continue to contribute to this work.

That's all for now folks, have a great winter, best wishes from the world of Standards.

Papers, Presentations, and Panel Proposals are due to the ISSEA Secretary by 1 June 2008!

OUTREACH AND AWARENESS

In the spirit of advancing systems security engineering as a defined and measurable discipline, ISSEA is collaborating with other initiatives to get the word out and promote mature security capability among system and software developers.

ISSEA members attend most major software, security, and systems engineering conferences. The event calendar includes:

RSA - April 7- 11 San Francisco CA
<http://www.rsaconference.com/2008/US/Home.aspx>

Systems and Software Technology Conference (SSTC) - April 29- May 2, 2008 Las Vegas, Nevada
<http://www.sstc-online.org/home.cfm>

DHS -[Software Assurance Forum \(May 2008\)](http://www.buildsecurityin.us-cert.gov/daisy/bsi/events.html)
[5/6/08]
May 6-8 in McLean, Virginia.
<https://buildsecurityin.us-cert.gov/daisy/bsi/events.html>

4th World Congress for Software Quality
September 15-18, 2008 Bethesda, Maryland
<http://www.asq.org/conferences/wcsq/>

Resources to Simplify Life

Build Security In

Build Security In (BSI) contains and links to best practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development. BSI content is based on the principle that software security is fundamentally a software engineering problem and must be addressed in a systematic way throughout the software development life cycle.

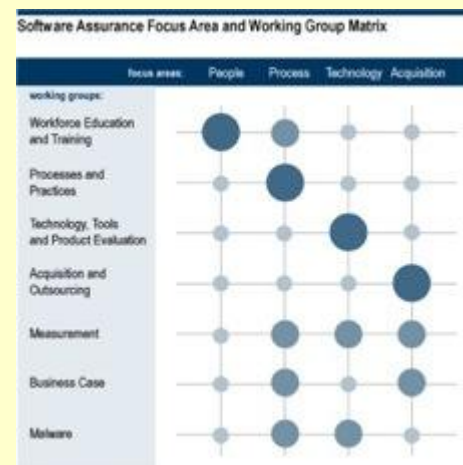
Build Security In is a project of the [Software Assurance](#) program of the Strategic Initiatives Branch of the National Cyber Security Division (NCSA) of the U.S. Department of Homeland Security. The Software Engineering Institute (SEI) was engaged by the NCSA to provide support in the Process and Technology focus areas of this initiative. The SEI team and other contributors develop and collect software assurance and [software security](#) information that helps to create secure systems.”

SWA Community of Practice Portal

As part of the DHS risk mitigation effort, the Software Assurance (SWA) Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development of trustworthy software products with predictable execution, and to improve diagnostic capabilities to analyze systems for hidden vulnerabilities. In an effort to support and sustain these efforts, the Software Assurance Community of Practice Portal is providing a collaborative venue for stakeholders to share and advance techniques and technologies relevant to software security.

The SWA framework encourages the production, evaluation, and acquisition of better quality and more secure software, providing focuses in these four areas:

- **People:** Education and training for developers and users
- **Process:** Sound practices, standards, and practical guidelines for the development of secure software
- **Technology:** Diagnostic tools, cyber security R&D and measurement
- **Acquisition:** Specifications and guidelines for acquisition and outsourcing



CERT Resiliency Engineering Framework

“The framework is an industry-agnostic process improvement model for organizations that want to actively manage operational resiliency and improve their security, business continuity, and IT operations management capabilities.” The framework is the result of a three year collaboration between CERT and the Financial Services Technology Consortium. To learn more about FSTC and to explore participating in the ongoing project visit the [FSTC web site](#) or download the document at http://www.cert.org/resiliency_engineering/.

Great Finds: Web Sites to Visit

Software Acquisition Materials buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/acquisition.html

Software Assurance in Acquisition: Reducing Risks to the Enterprise, v1.0 (procurement guide - <https://buildsecurityin.us-cert.gov/daisy/bsi/resources/dhs/908.html>);

State-of-the-Art Report on Software Project Management for Software Assurance <https://buildsecurityin.us-cert.gov/daisy/bsi/resources/dhs/906.html>

Defense in Depth buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/347.html

SWA Common Body of Knowledge with Guiding Security Principles (curriculum development guide, updated Oct 2007) at <https://buildsecurityin.us-cert.gov/swa/people.html>

Securing the Software Lifecycle: Making Application Development Processes - and Software Produced by Them - More Secure, v2.0 (developer's guide, update available mid-Feb 2008)

Practical Measurement Guidance for SwA and InfoSec, v1.0 (Measurement Guide to support information needs; draft update available Jan 2008);

National Vulnerability Database nvd.nist.gov
Repository of vulnerability management, security measurement, and compliance information

Common Attack Pattern Enumeration and Classification (CAPEC - <http://capec.mitre.org>)

Common Weakness Enumeration (CWE - <http://cwe.mitre.org>) with links to the National Vulnerability Database - <http://nvd.nist.gov/nvd.cfm>.

IATAC <http://iac.dtic.mil/iatac/>

“IATAC provides the specialized knowledge you need to develop network defenses rapidly and cost - effectively”

State-of-the-Art Report on Software Security Assurance
<http://iac.dtic.mil/iatac/download/security.pdf>

IA Newsletter http://iac.dtic.mil/iatac/IA_newsletter.jsp

DID YOU KNOW?

Academic Institutions Can Join ISSEA FREE Of Charge? For details send email to slindquist@ewa.com

Contacting ISSEA:

Sarah Lindquist,
ISSEA Relations Coordinator
13873 Park Center Road,
Suite 200
Herndon, VA 20171

E-Mail:
slindquist@ewa.com

Web Site:
www.issea.org

Making Security Measurable

<http://measureablesecurity.mitre.org>

MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through **enumerating** baseline security data, providing standardized **languages** as means for accurately communicating the information, and encouraging the sharing of the information with users by developing **repositories**.

The other activities and initiatives listed here have similar concepts or compatible approaches to MITRE's. Together all of these efforts are helping to make security more measurable by defining the concepts that need to be measured, providing for high fidelity communications about the measurements, and providing for sharing of the measurements and the definitions of what to measure.”

ISSEA
13873 Park Center Road,
Suite 200
Herndon, VA 20171

