25th anniversary
annual INCOSE
international symposium
Seattle, WA
July 13 - 16, 2015

Guidance for Working Group Maintenance of the Systems Engineering Body of Knowledge (SEBoK), with Systems Security Engineering Example

Logan Mailloux (Air Force Institute of Technology) - Logan.Mailloux@afit.edu
Rick Dove (Paradigm Shift International) - dove@parshift.com
Cheryl Garrison (Northrop Grumman Corporation) - Cheryl.Garrison@ngc.com
Ryan Biondo (WPL, Inc.) - Ryan.biondo@wpli.net

30 minute presentation, 10 minute Q&A

Authors

Logan Mailloux, CSEP, CISSP, is a Major in the USAF and is a PhD Candidate at the Air Force Institute of Technology. He has served the USAF as a cyber operations expert responsible for planning and executing global network defense exercises, documenting and training computer security best practices, performing test and evaluation of information technologies, and supporting distributed model and simulation infrastructure. He leads the SEBoK effort for the Systems Security Engineering working group.

Rick Dove is an INCOSE Fellow and chairs the INCOSE Systems Security Engineering working group. He is CEO of Paradigm Shift International, conducting R&D in agile security concepts and prototypes.

Ryan Biondo, CSEP, CISSP, is a Senior Systems and Security Engineer with WPL, Inc. He has 11 years experience as a Systems Engineer in the areas of radar, satellite communications, and cryptographic design and operations.

Cheryl Garrison, CSEP-ACQ, Northrop Grumman Corporation, has held positions in Software Engineering design, development and test for commercial Air Traffic Control systems as well as classified satellite, airborne and ground station programs for the US Army and Air Force.

Abstract

Maintenance of the Systems Engineering Body of Knowledge (SEBoK) has been accepted by INCOSE and others. Within INCOSE the responsibility to update and maintain the SEBoK is assumed by relevant working groups.

Working groups are populated with volunteers, each with limited participation time, special interests, and individual motivations.

Maintenance teams in one period may have different views of what should be covered by the SEBoK than those in other periods.

Therefore, it is beneficial, and perhaps even necessary, for working groups to facilitate a cohesive approach for maintaining SEBoK content.

In this paper, we offer guidance for working groups to maintain SEBoK materials employed by the Systems Security Engineering (SSE) working group's recent experiences.

WG Operating Principles

Objectives:

– Leverageable fundamentals rather than niche practices & recommendations.

– Applied rather than theoretical research.

– In-demand knowledge products for the practitioner.

– Embraceable knowledge products (joy in usage).

– Testing and refinement to verify efficacy.

– Socialization and facilitated-assimilation of results.

Project execution:

- **Clear project objectives, customers, and plans.**
- **Recruit core members with passionate interest driven by personal value.**
- **Effective project leadership.**
- **Firm deliverable dates.**
- **Frequency & Momentum – project-progress meetings weekly.**
- **Knowledge-development and remote collaboration tools.**
- **Incrementally releasable deliverables.**
- **Reflective process learning.**
- **Oversight progress facilitation.**

Reality:

- **People work on what they want to work on, but we attempt to guide.**

Internal WG Guidance Document

The Systems Security Engineering (SSE) WG first wrote, reviewed, and approved an internal guidance document to govern WG maintenance activity.

Predicated on dynamics applicable to all INCOSE working groups:

- working group membership is transient, subject to different views, understandings, and perhaps, favorite interests as volunteers rotate;
- SEBoK maintenance submission is open to all contributors, i.e., submissions can be made by anyone;
- IEEE Computer Society has also been requested to accept responsibility for SEBoK topics
  (we offered to collaborate on mutual guidance doc, TBD);
- Knowledge is evolving rapidly, adding new reference material to an already rich knowledge base - particularly true for SSE; and
- specialty-engineering-focused contributions run the risk of poor understanding with concepts and vocabulary unfamiliar to SEs.

SEBoK Intention

The SEBoK is intended to provide timely coverage of SE topics and emerging issues,

including a vetted listing of primary and secondary references the systems engineer can visit for more details on a particular subject.

The SEBoK is intended to be industry and domain neutral,

“useful to systems engineers anywhere,” and

“aims to inform a wide variety of user communities about essential SE concepts and practices”

(SEBoK Authors, 2014).

Background

Article Format and Size. Each article is posted as an individual webpage with a discussion of the subject topic, limited to 2,000 words.

Primary references are the Authors' and Editors' recommendations on the "most important" literature for a given topic.

The recommendation is that each article should have three to five primary references, with firm limits being no less than two and no more than ten.

Goal: if a SEBoK user were to read both the article and the listed Primary References, he or she would have a firm grasp on the principle concepts related to the subject.

This implies the Primary Reference list should be comprehensive and assessable to the systems engineer, yet limited in number.

Initial Approach

SEBoK Purpose: to "provide a widely accepted, community-based, and regularly updated baseline of SE knowledge [to] strengthen the mutual understanding across the many disciplines involved in developing and operating systems" (SEBoK Authors, 2014).

We set out to build a mutually beneficial foundation to facilitate development of authoritative SEBoK SSE content and foster collaboration with key stakeholders, such as INCOSE, IEEE, SERC, and other participants such as the National Defense Industrial Association (NDIA).

Initial Objectives

1. **Establish guidelines to maintain the SEBoK SSE content**
   - ❑ **Review and update the SEBoK SSE content on an annual basis**
   - ❑ **Review and update the entire SEBoK for security associations and references**
2. **Institute an authoritative Primary Reference list for systems engineers**
3. **Institute a comprehensive Secondary Reference list for systems engineers**

Early Start

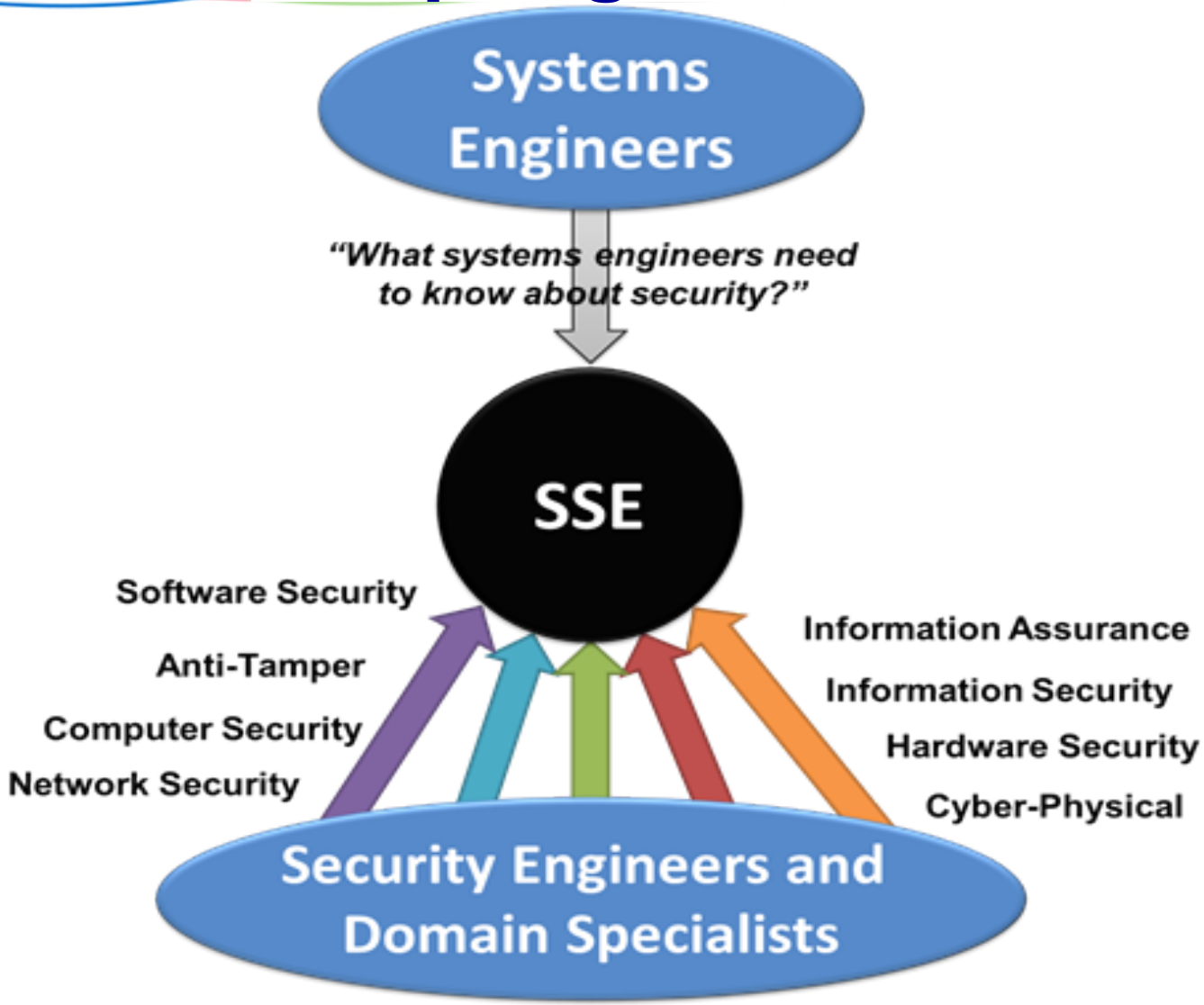
Each member of the maintenance team had a different view of what constituted primary reference material. This was challenging.

So, considered using the Certified Information System Security Professional (CISSP) ten domains of security.

But they address Information Technology (IT) security requirements, and don't provide systems engineers the necessary understanding of system security within other systems of interest.

Thus, the team attempted to identify references that covered security responsibilities and domains more holistically, with emphasis on references that discussed multiple security domains in totality, and not dedicated to a single domain (e.g., software, hardware, networks, etc.).

Adopting a Focus



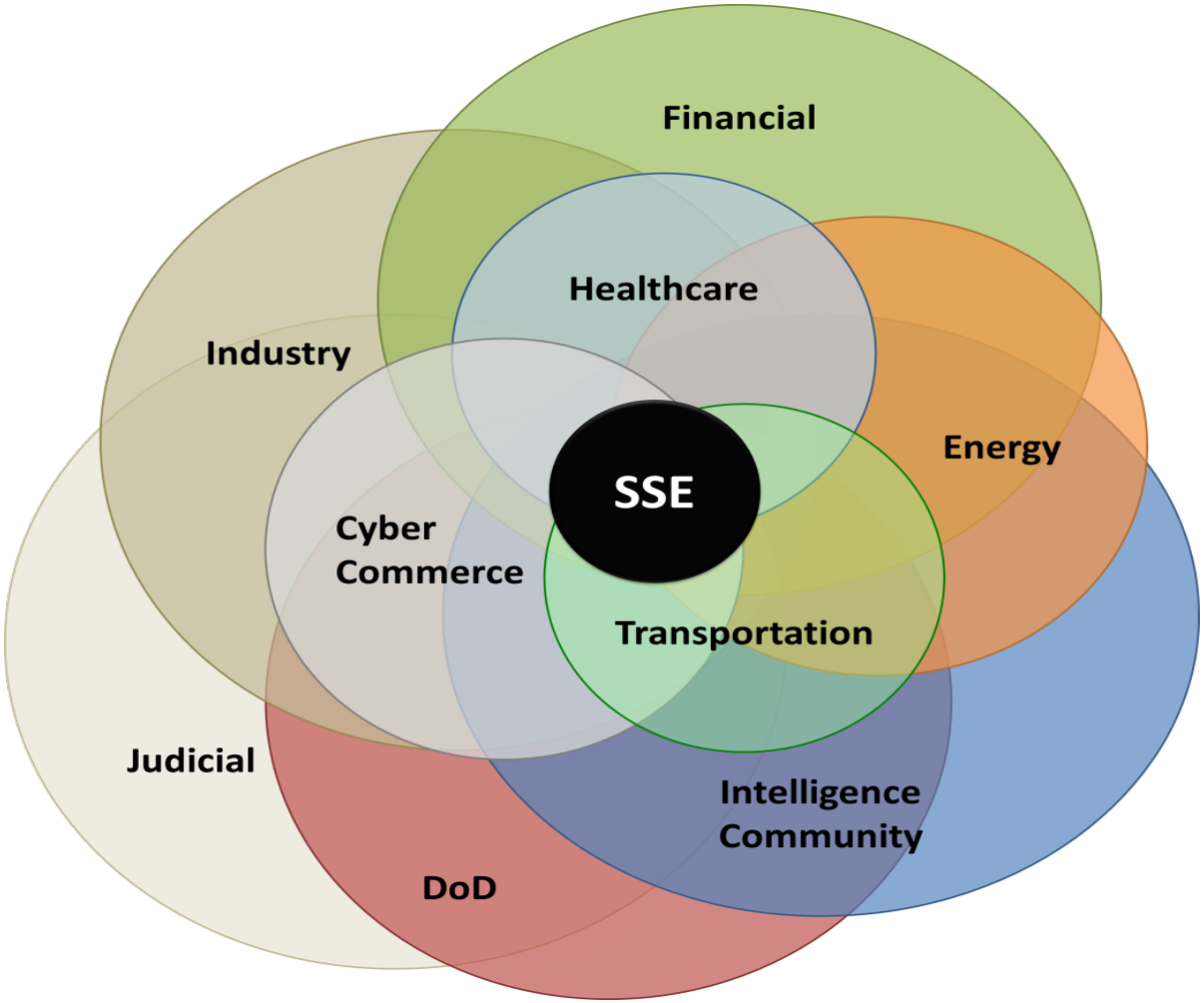
Adopted the internationally accepted life cycle approach of ISO/IEC 15288 Systems and Software Engineering – System Life Cycle Processes standard (ISO/IEC, 2011; ISO/IEC, 2010; ISO/IEC, 2011).

Speaking to SEs

LIFE CYCLE STAGES	PURPOSE	DECISION GATES
CONCEPT	Identify stakeholders' needs Explore concepts Propose viable solutions	Decision Options • Execute next stage • Continue this stage • Go to a preceding stage • Hold project activity • Terminate project
DEVELOPMENT	Refine system requirements Create solution description Build system Verify and validate system	
PRODUCTION	Produce systems Inspect and test	
UTILIZATION	Operate system to satisfy users' needs	
SUPPORT	Provide sustained system capability	
RETIREMENT	Store, archive or dispose of system	

Areas of Interest to Systems Engineering

Team chose an SE approach which is not industry specific nor focused exclusively on IT implementations.



Criteria for Primary References

- Considers system life cycle – Each reference should address one or more defined life cycle stages.
- Depth and breadth across foundational and specialty security domains – Ensure a comprehensive understanding of security knowledge is conveyed to the systems engineer.
- Accessibility for an interested audience – Ensure primary references are readily available and suitable for dissemination to a broad set of systems engineers with a wide range of applicable industries and associated technological implementations.
- Timely – Ensure primary references are recent and relevant with fresh insights into a constantly changing security environment.
- Recognized as an authoritative source – Identify primary references published from reputable sources, acknowledged industry experts, recognized standards, or accepted best practices, each with an established “high pedigree.”

Also – References should be acceptable and appreciated by the International Community.

Justifying Primary References

6. Anderson, R. 2008. Security Engineering: A Guide to Building Dependable Distributed Systems. 2nd ed., Wiley. Retrieved 8-Sep-2014 from http://www.cl.cam.ac.uk/~rja14/book.html.

Considers system life cycle: The Anderson text is particularly helpful in developing a detailed understanding of the security environment. While this text is not written for systems engineers nor life cycle specific, it highlights security considerations for a number of distributed systems from a practical implementation viewpoint.

Depth and breadth across foundational and specialty security domains: Covers a wide range of security topics with many supporting implementation discussions.

Accessibility for an interested audience: Available for purchase worldwide at a nominal fee and available free online. The Anderson text is a fascinating tomb of knowledge and practical examples for understanding SSE. Free online chapters ease the intimidating size of text and make it available to a wide international audience.

Timely: Updated and expanded edition published in 2008 (second edition).

Recognized as an authoritative source: Ross Anderson is a widely recognized leader in the security field and his book is acknowledged as the seminal text for security engineers. His book is the most comprehensive source text available for security engineering at the time of this writing.

Primary References

1. Anderson, R.J. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Ed. New York, NY, USA: John Wiley & Sons. Accessed October 24, 2014 at http://www.cl.cam.ac.uk/~rja14/book.html
2. DAU. 2012. "Defense Acquisition Guidebook (DAG): Chapter 13 -- Program Protection." Ft. Belvoir, VA, USA: Defense Acquisition University (DAU)/U.S. Department of Defense (DoD). November 8, 2012. Accessed October 24, 2014 at https://dag.dau.mil/
3. ISO. 2008. "Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)," Second Edition. Geneva, Switzerland: International Organization for Standardization (ISO), ISO/IEC 21827:2008.
4. ISO/IEC. 2013. "Information technology — Security techniques — Information security management systems — Requirements," Second Edition. Geneva, Switzerland: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2013.
5. Kissel, R., K. Stine, M. Scholl, H. Rossman, J. Fahlsing, J. Gulick. 2008. "Security Considerations in the System Development Life Cycle," Revision 2. Gaithersburg, MD. National Institute of Standard and Technology (NIST), NIST 800-64 Revision 2:2008. Accessed October 24, 2014 at the Computer Security Resource Center [1]
6. Ross, R., J.C. Oren, M. McEvilley. 2014. "System Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems." Gaithersburg, MD. National Institute of Standard and Technology (NIST) Special Publication (SP) NIST SP 800-160:2014 (Initial Public Draft). Accessed October 24, 2014 at the Computer Security Resource Center

Results of 2014 IW Meeting Review.

Team suggested the socialization and consideration of the following recommendations across SE and SSE communities for review, refinement, and acceptance:

- ❑ Agreement to the described approach as a collaborative tool for updating and maintaining the system security of SEBoK.
- ❑ Endorsement of the primary reference list.
- ❑ Endorsement of the secondary reference list.
- ❑ Propose the development of a new primary reference document: an SE security standards and practices roadmap, so the systems engineer can more effectively navigate security standards, guidelines, and best practices.

These four items were agreed upon, resulting in submission to the SEBoK. Minor updates and secondary references were also made.

The last item was taken into consideration as a follow-on project as part of a future security primer for systems engineers.

The team was able to share the project with other interested individuals and gain feedback more quickly because the decision making rationale was documented.

Summary

We all learned that establishing a common foundation and investing time into formalizing a maintenance approach was necessary to complete even the most fundamental of tasks (i.e., developing a Primary Reference list).

The initial development of an internal white paper was a necessary effort to facilitate agreement on how the team would proceed with identifying and recommending SEBoK Primary and Secondary References and maintenance of SSE content.

The team identified a shortage of system security literature written with a distinct SE perspective, and limited formalized guidance available to describe "What the systems engineer needs to know about security?" Therefore, the project team suggests the expansion of the SEBoK SSE site content and the development of additional SE-oriented system security materials to aid system engineers in understanding, assigning, and managing system security responsibilities.

Team leadership is of key importance. We fortunately found a PhD candidate motivated to cover breadth of security issues relevant to Systems Engineers.

Maintaining momentum is of key importance. The team has a telecon weekly.