

1 PURPOSE

Recent data breach cases and industrial control system incidents call attention to the inadequacy of current approaches to systems security [1, 2]. Each case presents more compelling evidence of the potential economic impact of cybersecurity threats. Each case adds to the recognition that security cannot be assumed to be provided by existing standards. Vast amounts of sums have been directed toward systems security solutions [3, 4]. Yet there is no theoretically proven method of deciding on what that money should be spent on; and no new paradigms have evolved to guide management decisions toward practical security solutions [5, 6].

To date, systems security curriculum has mostly concentrated on technology issues involved in implementing security standards. They have not focused on any other means to measure systems security. Although one textbook attempted to model enterprise security using the Zachman enterprise architecture framework [7], that attempt did not result in any comprehensive way to model or measure the security of any given system. Even textbooks that combine security and systems engineering principals emphasize the mindset of the security engineer rather than suggest any innovative methods, tools, and procedures with which to approach systems security engineering [8, 9]. The result is that security engineers use checklists to ensure their work is complete rather than validate that systemic security requirements are addressed. Most security engineers do not have the background in systems engineering required to approach a security problem holistically.

Holistic system views of verification and validation is the forte of the systems engineer [10]. However, when it comes to cybersecurity, systems engineers typically cede the responsibility to the security profession. Making the point well [11]: “When you ask an engineer to make your boat go faster, you get the trade-space. You can get a bigger engine but give up some space in the bunk next to the engine room. You can change the hull shape, but that will affect your draw. You can give up some weight, but that will affect your stability. When you ask an engineer to make your system more secure, they pull out a pad and pencil and start making lists of bolt-on technology, then they tell you how much it is going to cost.”

One reason that this situation is prevalent is that systems engineers have not considered it a problem. Systems engineers are taught to divide system requirements into two partitions: functional and non-functional requirements, or capabilities and characteristics. Capabilities always take precedence over characteristics, and security is classified as a characteristic [12]. One otherwise scholarly and astute textbook [13] on systems engineering refers to security as “related to system attributes that enable it to comply with regulations and standards.” It is far easier to blame security standards bodies for the outcome of a poor security design than to take responsibility for “building security in [14].” Where security is directly addressed in systems engineering literature, it is circularly defined as a process to ensure security concerns are covered, rather than as a core system requirement [15, 16].



INCOSE System Security Engineering Working Group Charter

As security practitioners search for workable solutions to the ever-more-complex maze of criminal and terrorist threats they encounter, the trend should be to escape from best practices checklists and return to core systems engineering methods, processes, and tools. However, as noted, most security engineers have no experience with these methodologies, and these methodologies have traditionally obscured security requirements. As long as systems engineers do not consider security a functional requirement, it will not be likely to rise to the top of the implementation checklist, because processes for managing system development lifecycles prioritize functional requirements over nonfunctional requirements. The situation is that security practitioners are not getting help at the design stage, and new approaches to systems engineering will be needed to meet the growing need for secure systems.

This working group believes that system engineering cannot succeed without accepting core responsibility for enabling and facilitating effective system security – partly in system requirements, partly in system trade space recognition, but mainly in system thinking applied to concepts of operations and systems architecture. Sustaining system functionality in the face of intelligent determined attack requires self preservation capabilities that adapt and evolve with intelligence, proactive innovation, and strength of community equal to the adversary as a minimum. This requires full system awareness and adaptability, and system-of-system relationships. Security engineering alone cannot accomplish this.

It is fitting for INCOSE to tackle Next Generation Security, as the issues are leading edge systems engineering issues: architecture, systems of systems, self organizing systems, security tradeoffs with human factors, systems thinking – things that are typically high level integrated-system SE issues.

2 GOALS

- Goal: Establish the responsibility for security within Systems Engineering with effective system security accepted and practiced as a fundamental goal of system engineering.
- Goal: Instigate self-sustaining cross- community involvement between systems engineers, security engineers, and system security standards.
- Goal: Establish exemplar profiles of system security concepts for next generation security.
- Customer(s)/Stakeholder(s): Systems engineering educators, systems engineering process and standards developers, DoD systems engineering acquisition procedure developers, systems engineering leaders and managers., customers of systems that require effective security, systems engineers, and security engineers.

3 SCOPE

This WG will address and foster system design concepts, system engineering processes, enabling support (such as standards and certifications), and community understanding and acceptance; all relative specifically to next generation system security characterized principally as self organizing, innovative, evolutionary, and harmonious in at least equal effectiveness as the system-adversarial communities.

4 SKILLS AND EXPERTISE REQUIRED

Required are skills and expertise in cyber security, physical security, system engineering processes, systems architecture, complex adaptive systems, systems of systems, self organizing systems, natural systems, human and organizational behavior, value propositioning, and cross-community collaboration. Most important, however, is an engaged sense of mission, which is neither a skill nor an expertise, but rather an internal drive that shapes the acquisition and application of skill and expertise. This WG will pursue a phased approach to the acquisition of participants and cross-community collaborative involvement required to round out the necessary skill and expertise set. Earlier phases of WG activities will engage in definitional work and preliminary example development, laying groundwork to attract participants with the breadth of necessary skills and expertise to achieve the goals.

5 MEMBERS, ROLES AND RESPONSIBILITIES

Names of key members and their responsibilities.

- Chair: Rick Dove
 - o The Chair shall build consensus among the engaged membership as to appropriate goals and strategies for satisfying the purpose of the WG, and be responsible either directly or through delegation for acquiring and applying necessary resources to execute strategies in pursuit of goals.
 - o The Chair shall initiate and lead at least one project at all times that supports the achievement of one or more WG goals.
 - o The Chair shall be responsible for status reporting to designated Tech Ops personnel.
 - o The Chair shall keep the WG membership participation page current for scheduled events, progress, work in process, and relevant supporting documents.
- Co-chair: Jennifer Bayuk
 - o The co-chair shall assist in the consensus building among the engaged membership as to goals and projects
 - o The Co-chair shall be responsible to act in the absence of the Chair.
 - o The co-chair shall initiate and lead at least one project at all times that supports the achievement of one or more WG goals.
- Chair and Cochair serve at the pleasure of the membership.
- Engaged Membership:
 - o Actively engaged in at least one project as lead or participant.
 - o Contributes in person or remotely in at least one of the two regular workshops each year.
- Membership:
 - o Names carried on the membership list at their request, entitling them to activity announcements and access to working group work-in-process web-pages and documents.

6 OUTCOMES (PRODUCTS/SERVICES)

- Outcome: Fundamental responsibility accepted within systems engineering for effective security established in SE processes and standards.



INCOSE System Security Engineering Working Group Charter

- Product: Profiles of actionable next-generation security structures and strategies. Short term deliverable.
- Product: Next generation security process integrated with system engineering processes. Mid term deliverable.
- Product: System security standards enabling and encouraging next generation innovative security concepts. Long term deliverable.

7 APPROACH

The general approach that will guide this WG/Initiative includes:

- The WG shall meet in working sessions during IW and IS sessions each year as a minimum, to advance project work in process and consider new projects. Live Meeting (or equivalent) shall be used to allow participation by members unable to attend sessions in person.
- Prime methods for raising awareness and displaying progress toward goals will include papers written by WG members and associates for relevant conferences and publication outlets, panel sessions at INCOSE and other appropriate conferences, and essays for INCOSE INSIGHT.
- Decision making will be done by engaged WG members toward achievement of the recognized goals of the WG, with the requirement that leadership for decision achievement is accepted and active. Decisions will be made twice yearly during IW and IS sessions as appropriate.

8 MEASURES OF SUCCESS

Overall measures of success for the WG include:

- The WG goals are mission oriented in an environment not yet broadly aligned with the goals. The prime measure of initial success will be recognition of security responsibility evidenced in appropriate changes to established system engineering processes.
- Active projects toward recognized WG goals is one indicative measure of success, with quality of active projects taking precedence over quantity.
- Quantity of “project engaged” membership is one indicative measure of success, with continual progress on each project being the measure of an acceptable number of engaged members.

9 RESOURCE REQUIREMENTS

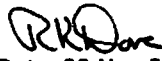
At the current early stage this WG has not identified any annual dollar (US) requirements to achieve goals. Infrastructure support from INCOSE is currently limited to Microsoft LiveMeeting. Human resources outside of INCOSE are anticipated as eventual requirements once initial groundwork is completed, and methods for identifying and obtaining such resources will await further development.

10 DURATION

This Charter will remain in effect until rescinded by the signatory or the signatory’s successor as WG Lead.

11 SIGNATURES

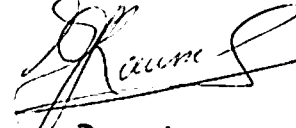
Enter the signature block of the submitter


Date: 22 Nov 2010

1st Level of Approval

Technical Director, INCOSE

Date


Aug 2011

2nd Level of Approval (Note this will be added by the INCOSE Technical Director when deemed appropriate.)

Chairman, INCOSE Board of Directors

Date

References:

1. McGlasson, L., *More Heartland-Related Fraud Detected*, in *Bank Information Security* 2010.
2. Fuhrmans, V., *Virus Attacks Siemens Plant-Control Systems* in *Wall Street Journal*. 2010.
3. Williams, C., *Cameron to spend £1bn+ on cyber security*, in *The Register*. 2010.
4. Cacas, M., *DHS outlines cybersecurity planning in Federal News Radio*. 2010.
5. Spafford, G., *Privacy and Security Remembrances of Thing Past*. Communications of the ACM, 2010. 53(8): p. 35-37.
6. Shipley, G., *Epic Fail*, in *Information Week*. 2010, UBM Techweb. p. 26-38.
7. Sherwood, J., A. Clark, and D. Lynas, *Enterprise Security Architecture*. 2005: CMP Books.
8. Anderson, R., *Security Engineering, Second Edition*. 2008: Wiley.
9. Bishop, M., *Computer Security, Art and Science*. 2003: Pearson Education.
10. Checkland, P., *Systems Thinking, Systems Practice*. 1999: John Wiley & Sons.
11. Example is attributed to Barry Horowitz, Munster Professor of Systems and Information Engineering and Chair at University of Virginia.



INCOSE System Security Engineering Working Group Charter

- 12. Buede, D.M., *The Engineering Design of Systems, Models and Methods*. 2009: Wiley.
- 13. Larson, W., et al., *Applied Space Systems Engineering*. 2009: McGraw Hill.
- 14. A phrase that, largely due to the community behind the site: <https://buildsecurityin.us-cert.gov/bsi/home.html>, has become synonymous with software security, but it is used here to refer holistically to any system of interest.
- 15. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), *Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM, ISO/IEC 28127)*. 2002.
- 16. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), *Systems and software engineering — Systems and software assurance — Part 2: Assurance case (ISO/IEC 15026)*. 2009.

Revision History

| <u>Date</u> | <u>Revision</u> | <u>Description</u> | <u>Author</u> |
|-------------|-----------------|--------------------|------------------------------|
| 22 Nov 2010 | 1.0 | Initial Draft. | Rick Dove and Jennifer Bayuk |
| | | | |
| | | | |
| | | | |