NDIA Systems Engineering Division

NDIA System Security Engineering Committee

August 2019

Holly Dunlap
Raytheon
NDIA SSE Committee Chair
Holly.Dunlap@Raytheon.com

Cory Ocker
Raytheon
NDIA SSE Committee Co-Chair
Cory.Ocker@Raytheon.com

Agenda

- **Summary of the Committee Status & Accomplishments June – August**
- **Highlight Key Projects & Engagements**
- **Review Agenda for August SSE Committee Meeting**
- **IEEE NDIA INCOSE System Security Symposium 2020 Status Update**

SSE Committee April – June Summary

- **OSD Cyber Resilient Weapon System (CRWS) Work Shop, Aug 6-8**
  - Objective: Identify, describe, and provide rationale for data items to provide confidence about the cyber-security, cyber survivability, and cyber resilience of weapons systems, with focus on
    - Derivation of security requirements
    - System design
    - Systems analysis
- **Supported Industry Security Focused Review of Draft OUSD A&S Software Acquisition Pathway Policy and Guidance**
- **Critical Program Information (CPI) Assessment & Identification Guide Workshop 6/5/2019**
  - Comments from workshop incorporated into CPI Assessment and Identification Guide (CAIG) and sent out to attendees for program use
- **AF SSE Acquisition Guidance v 1.4**
  - USAF provided updated policy as well as comment adjudication matrix for committee review

OUSD A&S SW Acquisition Pathway – Key Security Concerns

- The new process needs to be integrated into the Systems Engineering process. A new model describing this integration and how it ties to 5000.02 would be valuable.
- The document does not adequately address architecture and specifically security within the architecture.
- Security is framed in a way of compliance; to reach Approval to Operate is not to reach a secure system.
- As many of our products are systems of systems, a holistic appreciation of all security specializations (Cyber, IA, AT, SSE, SwA, SCRM) is necessary; Compliance to RMF Controls only buys a minimum level of assurance and doesn't adequately cover the security specialties in an integrated risk managed trade space.
- The focus on DevSecOps will contribute significantly to the concept of continuous ATO, but the document omits the need for Application level cybersecurity.
- Importance of MVCR security requires elevation, fielding a 'minimum' introduces environmental, intended use, and configuration control concerns. A greater definition of a sustainment support community is necessary.

OUSD A&S SW Acquisition Pathway – Key Security Concerns

- The push to ‘leverage enterprise services’ and the level of interaction with the test strategy seems to ignore embedded systems.
- With the shift from monolithic requirements to more agile methodology, cost estimation will be a problem. The top recommendation cited to improve cost estimates is to "define the team size and makeup", which is great for defining how much will be spent but a poor way to determine how much the work should cost. This also assumes a dedicated workforce with the right skills are available. This may work for top priority programs but will be challenging to scale to all programs with the gap in talent.
- While the idea of user testing of an MVP allows for flexibility in terms of capability and design, security is best designed into the architecture from the onset, major revisions may lead to vulnerabilities.
- The flexibility of CNS/UA/MVP is an exciting prospect, but firm high-level requirements are necessary to drive core architecture.
- Lessons learned include the short story incremental development and review cycles are good but the traditional major reviews are still needed to ensure the big picture isn’t lost while focusing on detailed iterative developments.
- Security and software assurance within the supply chain is currently a gap and needs to be addressed. The SCRM discussion focusses on the OS. There’s lots of COTS/FOSS components in the platform and infrastructure to track, as well as the tools in the pipeline.

NDIA SSE Committee Participation in the OUSD A&S SW Acquisition Policy and Pathway Review

Chair: Holly Dunlap, Raytheon **Co-chair: Cory Ocker, Raytheon**

Attendees:

Gerry Ourada LMC
Kenneth Nidiffer – SEI
Brian Cohen – IDA
Charles Miller – RTN
Nick Shouse – USAF CROWS
Tom Hurt – OSD
Holly Dunlap – RTN
Colton Sundstrom – RTN
Michael O'Grady – NGC
Jennifer Barzeele – RTN
Goeff Draper – L3
Fred Jones – RTN
Rhonda Henning – L3
Teresa Moyer – AF TSN
Cory Ocker – RTN

Didn't participate in the meeting, but provided comments:

John Catrone – RTN
Peter Francis – RTN
Rick LaRowe - RTN
Preston Frazier – NGC
Carol Woody – SEI
Richard Massey – Boeing

Comment Resolution Matrix Received:

SEI
RTN
Northrup
Boeing
Harris / L3

System Security Engineering Committee Meeting Agenda

8/22/2019 2:00 PM – 5:00 PM EST,

Location: Telecon Only

Call in information: (877)336-1275 Access Code: 3019886

Agenda:

- **Welcome and Committee Update – Holly Dunlap**
- **OSD Overview – Melinda Reed**
- **Draft Software Acquisition Pathway policy and Business Decision Guidance Update - TBD**
- **Navy Cybersafe - CDR Salvia, NAVAIR 4.0**
- **USAF Acquisition Guide Update – USAF CROWS Representative**
- **CRWS Outbrief - Michael McEviley, MITRE**
- **System Security Symposium 2020**

IEEE NDIA INCOSE
System Security Symposium
April 6-9, 2020

SYSTEMS SECURITY
symposium

The IEEE-INCOSE-NDIA Systems Security Symposium seeks research papers and application studies that focus on the development of secure, safe, and resilient systems. This symposium attempts to address the convergence of cybersecurity, safety, and engineering with interest in the effective application of security principles, methods, and tools to complex systems such as cyber-physical systems, autonomous systems, transportation vehicles, medical devices, large IoT systems, and other systems of interest. Preference will be given to papers and case studies that bridge theory to practice.

SUBMISSION DETAILS

Theory & Methods

Papers or Extended Abstracts addressing novel ideas, theoretical issues, technology, methodology, or detailed studies. These academic-oriented papers will be peer reviewed and prioritized according to their contribution.

Cases & Practical Experiences

Papers presenting practical ideas, lessons learned, and real-world achievements. Papers are reviewed for relevance but not necessarily academic contribution.

Papers and extended abstracts of both categories will be peer reviewed. Papers will be published in the proceedings with an 8-page maximum. Extended abstracts (typically 3-5 pages) will not be published, but will be available to the conference attendees. Student papers are encouraged in both categories.

All submission details are available on the IEEE-INCOSE-NDIA SSS 2020 Submission Portal at

https://2020.ieeesystemssecuritysymposium.org

SYSTEMS SECURITY
symposium

IEEE NDIA INCOSE
System Security Symposium
April 6-9, 2020
http://www.ieeesystemssecuritysymposium.org

Key Dates

Special Sessions & Tutorial Proposals Deadline	Initial Deadline	Acceptance Notification & Feedback to Authors	Final Draft Paper Deadline
Wed, Jul 31st, 2019	Fri, Aug 30th, 2019	Thu, Oct 31st, 2019	Wed, Jan 15th, 2020

Systems Security Symposium 2020
Topics

- Systems Security Work Focused on Advancements in Theory, Practice, and Education
- Engineering of Safe, Secure, and Resilient Systems
- Examples of Mission/Systems Assurance and Assurance Cases
- Model Based Engineering focused on Security, Safety, Trust, Resiliency
- Affordable and Scalable Approaches to Hardware, Software, Firmware Assurance
- Novel Architecture Design and Analysis Examples or Trade-Space Studies
- Trust of Complex Systems with Emphasis on Cyber-Physical Systems
- Security considerations for machine learning / artificial intelligence
- Large-Scale DevSecOps and Agile Approaches for System Development
- System Security Design Considerations for Cloud Environments
- Verification, Validation, and Evidences for Secure System Development
- Extensions of Formal Methods to System-Level Evaluation
- Cybersecurity in Manufacturing and Supply Chains
- Case studies to include automotive, transportation, space, and others
- Cyber-Physical System Event Detection, Investigation, Forensics, and Malware Analysis
- Tailored Risk Management Approaches for Large Complex Systems
- Attack/Defense Modeling, Simulation, and Characterization
- Techniques for Cyber Risk Buy Down in Legacy Systems, Infrastructure, and Enterprises
- Policy, Ethical, Legal, Privacy, Economic, and Social Issues

IEEE NDIA INCOSE
System Security Symposium
April 6-9, 2020

SYSTEMS SECURITY
symposium

General Chair
Bob Rassa
IEEE Systems Council
RCRassa@Raytheon.com

Technical Program Chair
Holly Dunlap
NDIA
Holly.Dunlap@raytheon.com

Technical Program Co-Chair
Beth Wilson
INCOSE
wilsondrbeth@aol.com

Technical Program Committee:
Steve Holt
IEEE Systems Council
smdholt@gmail.com

Kathleen Kramer
IEEE Aerospace & Electronic Systems Society
kramer@sandiego.edu

Tom McDermott
Systems Engineering Research Center
tmcdermo@stevens.edu

Melinda Reed
OUSD (R&E)
melinda.k.reed4.civ@mail.mil

Logan Mailloux
United States Air Force
Logan.mailloux@us.af.mil

For Information Contact:
Shelby Lussier
slussier@conferencecatalysts.com

Location
Marriott Crystal Gateway
Crystal City, VA, USA

SUBMISSION DEADLINES
~~July 31, 2019~~
Special Sessions & Tutorial Proposals

~~August 30, 2019~~
Initial Manuscript & Abstract Deadline

October 31, 2019
Acceptance Notification

Extended Deadlines by 30 days