Connecting Academia and Practitioners to Address the Cyber Threat: one year later

Carol Woody, PhD

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0466

Agenda

Highlights of SSCA Workshop May 2018

Special Journal December 2018

Training for Acquisition

Next Steps

Highlights of SSCA Workshop May 2018

SSCA Workshop May 2018

Goal:

Identify what knowledge, skills, and abilities (KSAs) should be taught in formal education and training programs

Participants:

118 persons from industry (64) government (45) and academia (12)

Topics Explored:

What is the SwA/C-SCRM Problem

Recruiting and Retaining

Role of Education and Training

Needed KSAs for: IT/Cybersecurity Professionals, Software Developers, Cross-Domain, Supply Chain, General Users, Senior Leadership, Project/Middle Managers, Acquisitions

Software and Supply Chain Context

Anyone Can Write Software

From 1997 to 2012, software industry production grew from $149 billion to $425 billion

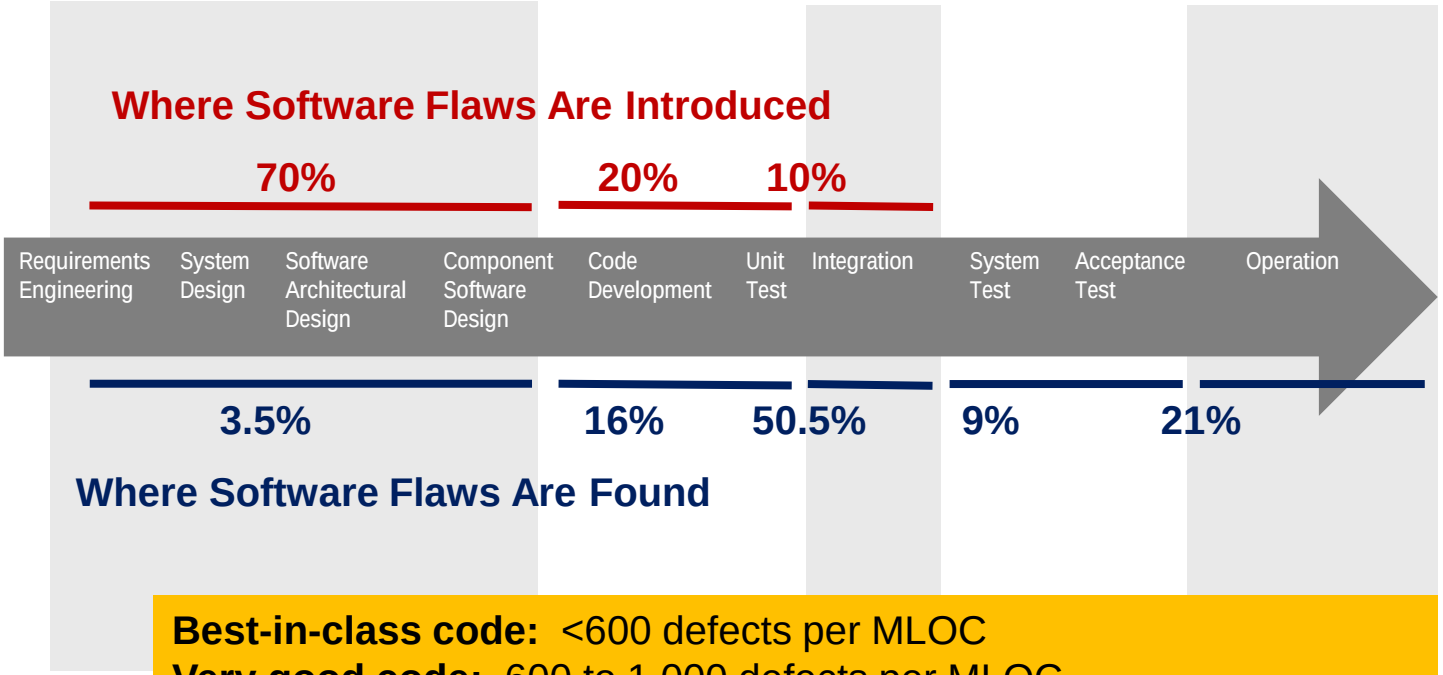
From 1990 to 2012, business investments in software grew at more than twice the rate of all fixed business investments; from 2010 to 2012, software accounted for 12.2% of all fixed investment, compared to 3.5% for computers and peripherals

How to Raise the Next Zuckerberg: 6 Coding Apps for Kids
http://readwrite.com/2013/04/19/how-to-raise-the-next-zuck-6-coding-apps-for-kids/

TYNKER: We Empower KIDS to Become Makers
https://www.tynker.com/

How and Why to Teach Your Kids to Code
http://lifehacker.com/how-and-why-to-teach-your-kids-to-code-510588878

All Software has Flaws

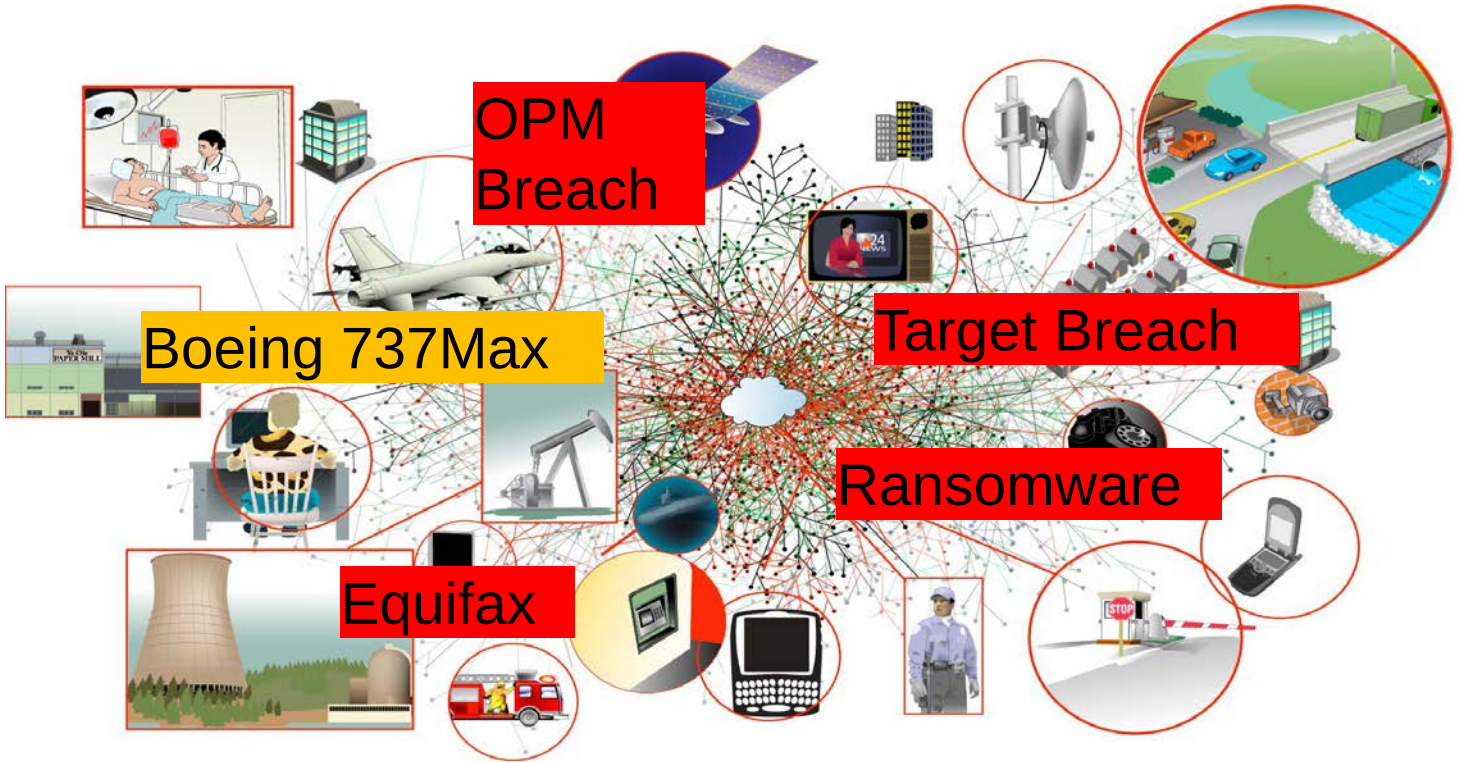


Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies

Best-in-class code: <600 defects per MLOC
Very good code: 600 to 1,000 defects per MLOC
Average quality code: 6,000 defects per MLOC

Up to 5% of defects are potential vulnerabilities

Software is Everywhere & Complex Supply Chains Add to Security Risk



Who Owns the Problem?

When Something Bad Happens Who Do We Blame?

It’s Acquisition’s Fault

1. Acquirers only care about cost and schedule
2. Acquirers do not require that the technology they purchase be resilient to cyber threats.
3. Acquirers do not test the technology to ensure it provides sufficient cyber resilience/software assurance.
4. Acquirers do not know how to require and test for cyber threats.
5. Acquirers do not care about the vendor’s supply chain, only that the vendor deliver as promised
6. Acquirers do not know how to verify a vendor’s supply chain

It’s Engineering’s Fault

1. Engineers do not consider all possible states of the system to build in sufficient cyber resiliency/software assurance.
2. Engineers only care about ensuring that safety and security compliance mandates are met
3. Engineers are not trained to understand and address cyber threats
4. Available tools are insufficient to help engineers find cyber threats

It’s the Developer’s Fault

1. Developers build a system to “pass the tests” and nothing more
2. Developers turn off as many flags as possible to not see problems
3. Available tools are inadequate (take too long, find too many false positives)
4. Developers do not know how to use the tools properly
5. Developers include whatever code they want and do not ensure it is from a reliable source

It’s Program Management’s Fault

1. Program Managers only care about cost and schedule
2. Program managers do not know how to budget for cyber threats so they don’t
3. Program managers do not provide the tools needed by engineers and developers when needed
4. Program managers do not know how to pick the right tools to address cyber threats
5. Program managers know security problems will not show up until sustainment which is someone else’s problem

It’s Security’s Fault

1. Security does not keep it’s compliance requirements current with cyber threats
2. Security runs the tools and tests and tells the developers things are broken but not what to fix
3. Security requires so much paperwork for an ATO that there is no time to fix real problems

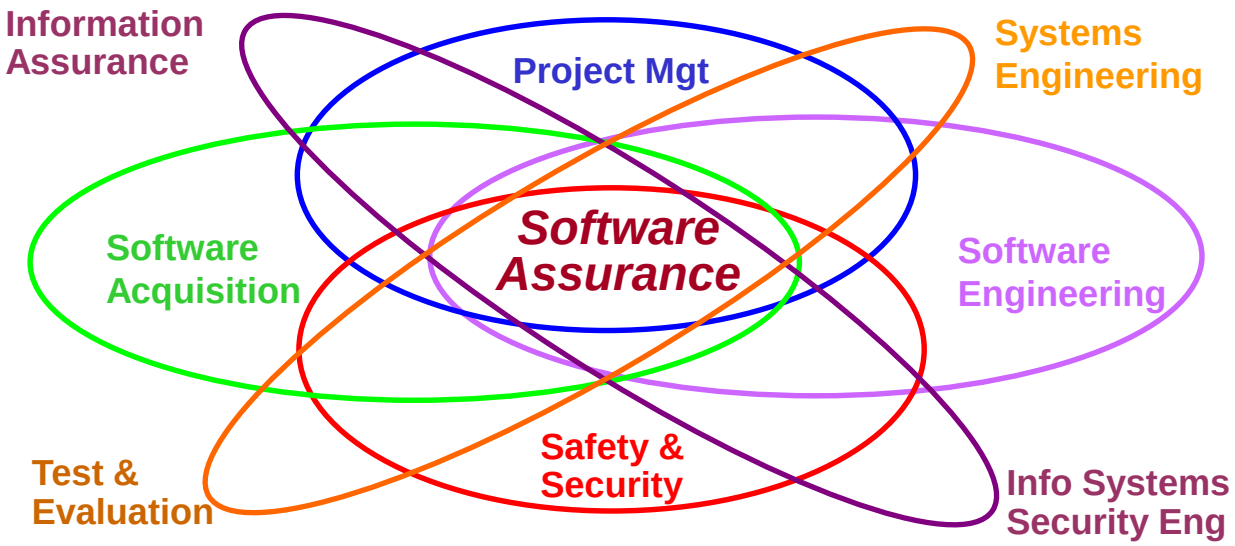
It’s Tool Builder’s Fault

1. Tools are too hard to run
2. Tools cost too much for what they provide
3. Multiple tools are needed but the vendors do not build their products to work together

It’s Senior Leadership’s Fault

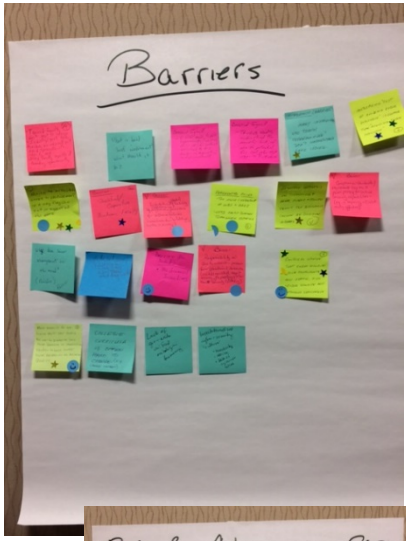
1. Policy is vague and unenforced
2. No funding is provided for new requirements
3. No one is responsible for software risk
4. There are penalties for delivering late and over budget but not for unacceptable cyber risk

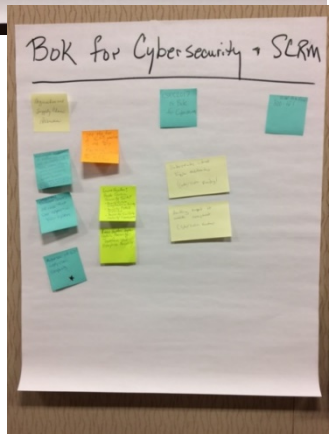
Contributing Disciplines

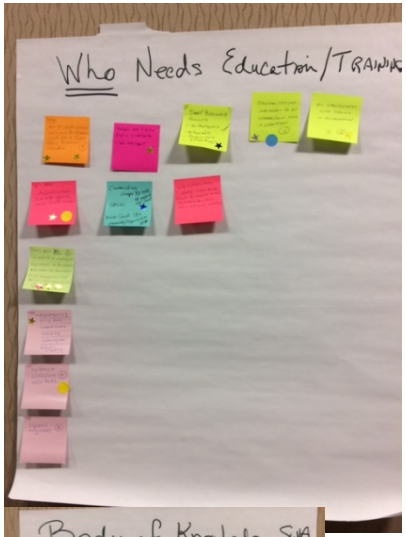


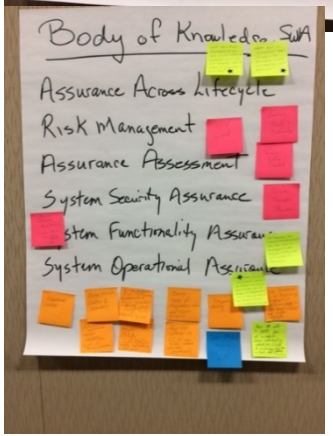
Everyone is part of the problem and needs to be part of the solution

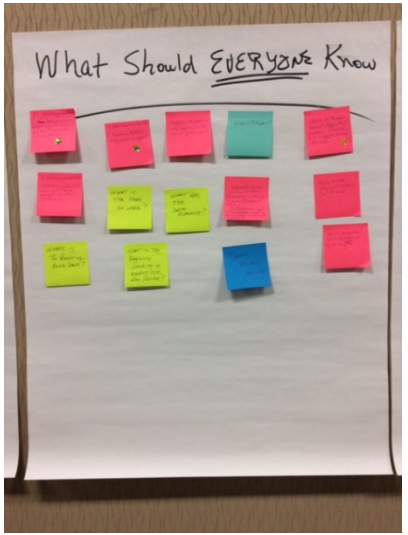
Shared Wisdom to Address the Problem(s)











Special Journal December 2018

Special Journal Published December 2018

Series: International Journal of Secure Software Engineering (IJSSE)

Special Journal Title:

Education and Training for Cybersecurity and Supply Chain Risk Management (SCRM)

Guest Editor: Carol Woody, Ph.D.

Abstract:

There is a noticeable gap in the current acquisition and engineering workforce's knowledge and skills and support resources with the right capabilities are brought in too late, if at all, to help address these challenges. Expanding the knowledge of decision makers and participants in system acquisition and engineering is a critical component in changing this situation, but how can we best prepare them for effectively addressing cyber security and SCRM in the jobs that they already perform? What they need to know and how they should go about learning remains unclear. In addition, how will they demonstrate that they have mastered these new capabilities?

Selected Articles - 1

Opinions of the Software and Supply chain Assurance Forum on Education, Training, and Certifications by Beatrix Boyens

Reports discussions with industry, academia, and government on efforts to clarify what knowledge is needed, who should have it, and how should they obtain it to better address today's cybersecurity and SCRM challenges.

A Case For Using Blended Learning And Development Techniques To Aid The Delivery Of A UK Cybersecurity Core Body Of Knowledge by David A. Bird and John Curry

Shares efforts underway in the UK to establish cybersecurity as a profession based on a knowledge framework that must span many existing silos in learning and development.

Selected Articles - 2

The Need for Higher Education in Cyber Supply Chain Security and Hardware Assurance by Brian Cohen and colleagues

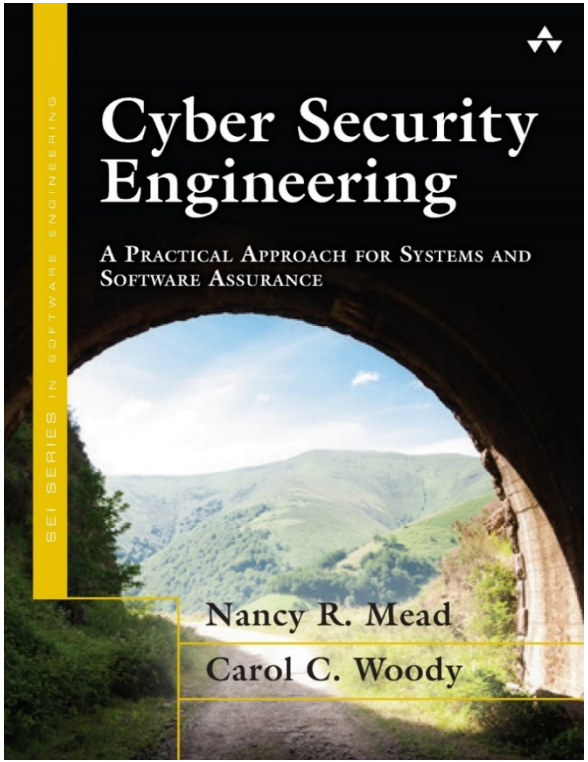
Describes why current academic programs teaching supply chain risk management need to focus more extensively on cyber aspects that emphasize hardware assurance.

Enhancing a SCRM Curriculum with Cybersecurity by Art Conklin and Chris Bronk

The steps taken to incorporate cybersecurity exemplars into an existing supply chain education program (hardware) are described.

Training for Acquisition

Textbook for the Current & Future Workforce



Released November 2016 as part of the SEI Book Series

For more information see https://insights.sei.cmu.edu/sei_blog/2016/10/seven-principles-for-software-assurance.html

Developed for SwA Curriculum

Courses on FEDVTE

Executive Course

Prepare executives to make informed decisions when acquiring or overseeing development of a security-critical software system

SCRM Awareness Course

SCRM for ICT acquisitions considers two kinds of malicious actions.

- Malicious supply chain events: counterfeits & tampering
- Malicious system events: a system weakness provides access to sensitive information, reduces the availability of an essential service, or affects data integrity.

SEI course development sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD)

CERT Cybersecurity Engineering and Software Assurance Professional Certificate

Released March 26, 2018

The program consists of five components

- Software Assurance Methods in Support of Cybersecurity Engineering
- Security Quality Requirements (SQUARE)
- Security Risk Analysis (SERA)
- Supply Chain Risk Management
- Advanced Threat Modeling

To learn more, visit https://sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=33881

SEI Publications for Acquisition

Available at:

www.sei.cmu.edu/go/cybersecurity-engineering

www.sei.cmu.edu

Samples:

- Woody, Carol; Ellison, Robert; & Ryan, Charles. *Exploring the Use of Metrics for Software Assurance.* CMU/SEI-2018-TN-004. Software Engineering Institute, Carnegie Mellon University. 2019. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=540881
- Ellison, Robert, et al, “Software Supply Chain Risk Management: From Products to Systems of Systems,” Software Engineering Institute, Dec 2010, https://resources.sei.cmu.edu/asset_files/technicalnote/2010_004_001_15194.pdf
- Ellison, Robert, et al. “Evaluating and Mitigating Software Supply Chain Security Risks,” Software Engineering Institute, May 2010, http://resources.sei.cmu.edu/asset_files/technicalnote/2010_004_001_15176.pdf

SEI Podcasts

Cybersecurity Engineering & Software Assurance: Opportunities & Risks

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=524351

1,700 downloads since September of last year

Predicting Quality Assurance with Software Metrics and Security Methods

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=473883

Next Steps

Visibility for the Problem; Promote Viable Solutions

Expanded Audiences:

Workshops at other conferences?

Other publications?

Expanded Training:

Delivery of public courses?

University curriculum offerings?

Other Ideas?:

Models for Acquisition to ensure the right KSAs are there at the right time

SEI Resources

Carol Woody, PhD

cwoody@cert.org

Web Resources

www.sei.cmu.edu/go/cybersecurity-engineering

www.sei.cmu.edu