“Prototype Software Assurance Framework: Introduction and Overview” by Christopher Alberts and Carol Woody

CS 540 Advanced Software Engineering

Victor Hazlewood, CISSP
victor@utk.edu

19 February 2024

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Overview

- CMU Software Engineering Institute
- Software Supply Chain issues
- Software Assurance defined
- A Proposed Solution…
- Describing the Prototype Software Assurance Framework

Carnegie Mellon University (CMU)
Software Engineering Institute (SEI)

- The SEI and CMU is a Federally Funded Research and Development Center (FFRDC)
  - a nonprofit, public–private partnership that conducts research for the United States government. One of only 10 FFRDCs sponsored by the U.S. Department of Defense (DoD), the SEI conducts R&D in software engineering, systems engineering, cybersecurity, and many other areas of computing, working to introduce private-sector innovations into government.
- SEI Publications: https://sei.cmu.edu/publications

Software Engineering Supply Chain Issues

- Dr. Mockus mentioned **software supply chain** in the context of World of Code research benefits
- ? "~~A chain~~ Software is only as strong as its weakest link" ?
- Investigated SW supply chain security in SEI publications
- Came across:
  The Measurement Challenges in Software Assurance and Supply Chain Risk Management
  I will refer to this as "Measurement Challenges"

Software Engineering Supply Chain Risks

- “Measurement Challenges” says
  “Software supply chain risk has increased exponentially since 2009 when the Heartland Payments System breach [Lewis 2015] made the issue newsworthy “
- Heartland Payments System was breached in May 2009 due to a SQL injection attack that allowed 100 million credit and debit cards to be stolen
- Once they gained access to the network, the attackers planted sophisticated packet-sniffing tools and malware to detect and steal sensitive payment card data flowing over the retailers' networks[1]

1 - https://www.computerworld.com/article/2527185/sql-injection-attacks-led-to-heartland--hannaford-breaches.html

Software Engineering Supply Chain Issues

- Recent events in 2020 and 2021, such as, SolarWinds and Log4j show the scale of disruption from a third-party software supplier can be massive

Two Examples:

- **Solarwinds software update platform, Orion, compromised**

  Solarwinds, a network monitoring product used by 300,000 customers, uses the Solarwinds Orion software update platform to allow customers to update their software. Orion was compromised allowing malicious code to be introduced. **DHS issued Emergency Directive 21-01[2]**

- **Log4j critical vulnerability: CVE-2021-44228 score 10.0 critical**

  Apache Log4j 2.0-beta9 through 2.15.0 JNDI features used in configuration, log messages, and parameters is vulnerable. Attacker who can control log messages/parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled

- There is also the '23 MoveIt breach affecting National Student Clearinghouse?

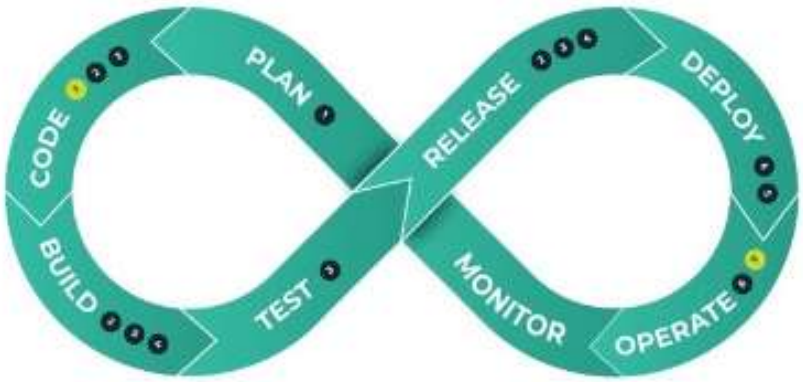
2 - Emergency Directive 21-01 https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise

Software Assurance

- Software assurance is defined as:

  a level of confidence that software will function as intended and will be free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the software acquisition lifecycle

A Proposed Solution?... Introducing a Prototype Software Assurance Framework

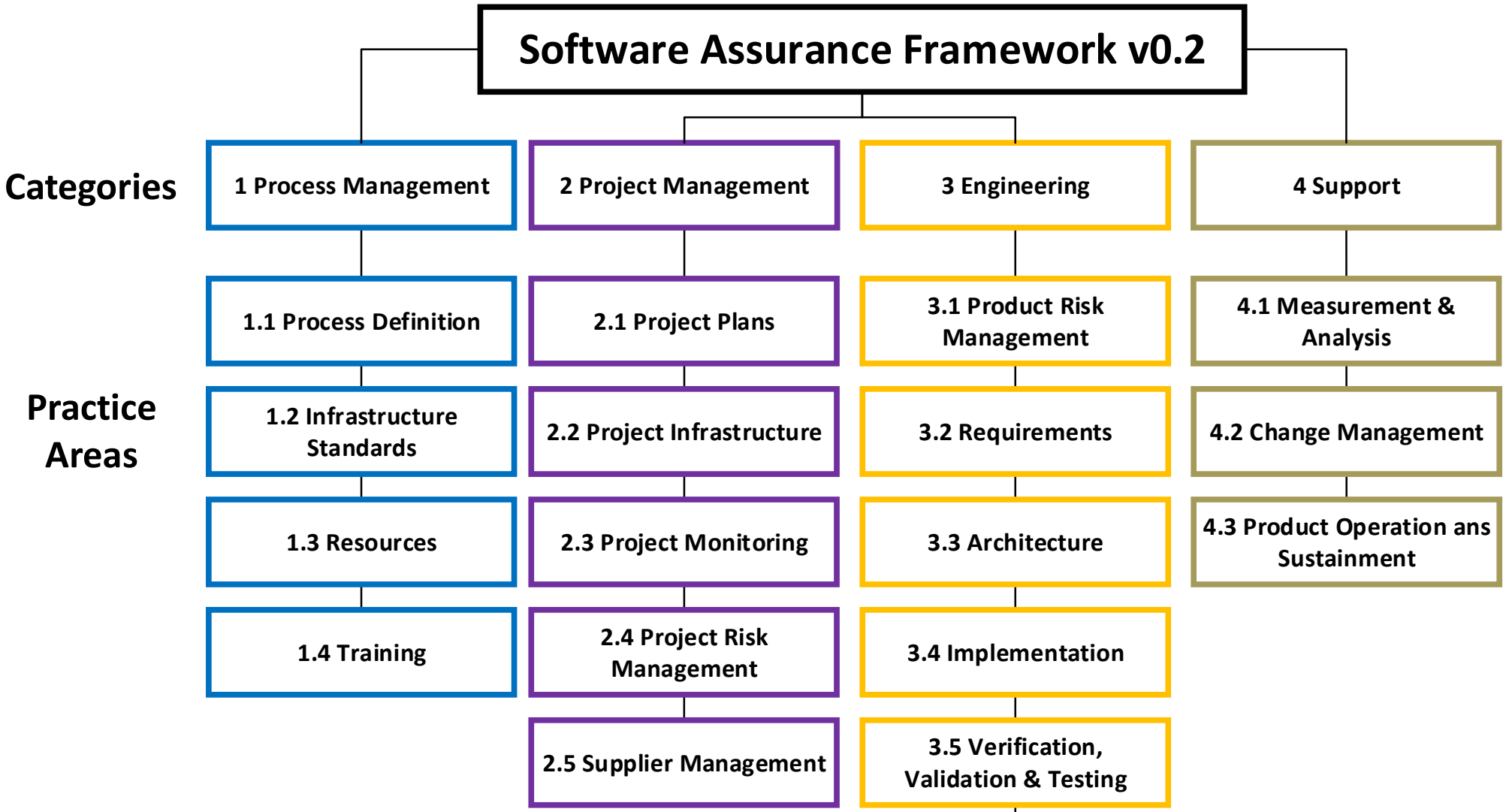


- Field experiences of SEI staff indicate that few programs currently implement effective cybersecurity practices early in the software development or acquisition lifecycle

- Researchers from the SEI started cataloging the cybersecurity practices needed to acquire, engineer, and field software systems that are acceptably secure and provide this paper
- Prototype Software Assurance Framework (SAF): Introduction and Overview Note: paper added to CS540-24/papers
- The SEI paper introduces the **Software Assurance Framework** that can apply across the acquisition lifecycle and supply chain

Software Assurance Framework

- As organizations become more dependent on software:
  - Software is more complex, so risk is on the rise
  - Costs must be controlled: address SW security risks early!
- SAF defines a set of cybersecurity practices orgs & programs should apply across the SW lifecycle and supply chain (acquire, engineer, operate)
- The SAF helps to:
  - establish confidence in the program's ability to acquire software-reliant systems that are secure, and
  - reduce the cybersecurity risk of deployed software-reliant systems
- SAF v0.2 is a working prototype rather than a complete body of research



For each Practice Area think of applicability related to
- acquiring software
- developing/engineering software
- deploying/operating software

Software Assurance Framework

- Overall there are:
  - Four categories
  - Nineteen Practices Areas
  - Seventy-six security practices

Samples Practices

Category	Area	Practice	Artifacts
1 Process Management	1.4 Training	1.4.1 Provide security awareness training for program personnel (including vendors, contractors, and outsources workers).	Project Training Plan Training Products Vendor Contracts and Service Level Agreements
		1.4.2 Provide role-based security training for technical staff (including vendors, contractors, and outsources workers).	Project Training Plan Training Products Vendor Contracts and Service Level Agreements
		1.4.3 Track completion of security training activities.	Program Status Reports

Category	Area	Practice	Artifacts
2 Project Management	2.3 Project Monitoring	2.3.1 Monitor the progress of the project's cybersecurity tasks.	Program Status Reports
		2.3.2 Monitor project compliance with cybersecurity policies, laws, and regulations.	Program Compliance Documents
		2.3.3 Conduct independent cybersecurity reviews of project tasks.	Independent Review Results

Sample Practices

Category	Area	Practice	Artifacts
3 Engineering	3.7 Deployment	3.7.1 Obtain security sign off for system release.	Assessment and Authorization Plan
		3.7.2 Obtain the authority to operate in a production environment (i.e. accept residual cybersecurity risk to operations).	Assessment and Authorization Plan
		3.7.3 Protect the code during transport and installation.	Deployment Policy
4 Support	4.1 Measurement and Analysis	4.1.1 Define and improve cybersecurity measures.	Program Plan Program Status Reports
		4.1.2 Collect and analyze cybersecurity measures.	Program Plan Program Status Reports
		4.1.3 Store cybersecurity measurement data appropriately.	Program Data Repository

Conclusions & Future Work

- **Conclusions**
  - The SAF provides a collection of cybersecurity practices that can apply across the SW lifecycle and supply chain.
  - Similar to NIST SP 800-53 security controls but more focused for process & project mgmt., engineering, and support (for deployment)
- **Future Work**
  Read Exploring the Use of Metrics for Software Assurance to determine methods for effectively implementing the SAF

Q&A

Thank you, next…