[no markings required]

DM24-0288
The Latest Work from the SEI

by Douglas C. Schmidt

As part of an ongoing effort to keep you informed about our latest work, this blog post summarizes some recent publications from the SEI in the areas of supply chain risk management, technical debt, large language models, quantum computing, acquisition, and trustworthiness in AI systems. These publications highlight the latest work of SEI technologists in these areas. This post includes a listing of each publication, author(s), and links where they can be accessed on the SEI website.

The Measurement Challenges in Software Assurance and Supply Chain Risk Management
by Nancy R. Mead, Carol Woody, and Scott Hissam

In this paper, the authors discuss the metrics needed to predict cybersecurity in open source software and how standards are needed to make it easier to apply these metrics in the supply chain. The authors provide examples of potentially useful metrics and underscore the need for data collection and analysis to validate the metrics. They assert that defining metrics, collecting and analyzing data to illustrate their utility, and using standard methods requires unbiased collaborative work to achieve the desired results.
Read the white paper.

Report to the Congressional Defense Committees on National Defense Authorization Act (NDAA) for Fiscal Year 2022 Section 835 Independent Study on Technical Debt in Software-Intensive Systems
by Ipek Ozkaya, Forrest Shull, Julie B. Cohen, and Brigid O'Hearn

A team from SEI conducted an independent study to satisfy the requirements of the Fiscal Year 2022 National Defense Authorization Act (NDAA) Section 835, Independent Study on Technical Debt in Software-Intensive Systems.

This report describes the conduct of the study, summarizes the technical trends observed, and presents the resulting recommendations. The study methodology includes a literature review, a review of SEI reports developed for program stakeholders, deep dives on program data from SEI engagements with Department of Defense (DoD) programs, and interviews conducted using the 10 study elements specified in Section 835(b).

The study concludes that programs are aware of the importance of managing technical debt. Furthermore, a number of DoD programs have established practices to actively manage technical debt. During this study, the DoD published several guidance documents that begin to include technical debt and technical debt management as an essential practice for successful software development. Study recommendations include that the DoD must continue to update policy/guidance and empower programs to incorporate technical debt practices as part of their software development activities while enabling research in improved tool support and data collection.
View the report.

[no markings required]

DM24-0288

Assessing Opportunities for LLMs in Software Engineering and Acquisition

By Stephany Bellomo, Shen Zhang, James Ivers, Julie B. Cohen, and Ipek Ozkaya

In this white paper, the authors examine how decision makers, such as technical leads and program managers, can assess the fitness of large language models (LLMs) to address software engineering and acquisition needs. They introduce exemplar scenarios in software engineering and software acquisition, and they identify common archetypes. The authors also describe common concerns involving the use of LLMs and enumerate tactics for mitigating those concerns. Using these common concerns and tactics, the authors demonstrate how decision makers can assess the fitness of LLMs for their own use cases through two examples.
Read the white paper.

The Cybersecurity of Quantum Computing: 6 Areas of Research

By Tom Scanlon

Research and development of quantum computers continues to grow at a rapid pace. The U.S. government alone spent more than $800 million on quantum information science research in 2022. Thomas Scanlon, who leads the data science group in the SEI CERT Division, was recently invited to be a participant in the Workshop on Cybersecurity of Quantum Computing, co-sponsored by the National Science Foundation (NSF) and the White House Office of Science and Technology Policy, to examine the emerging field of cybersecurity for quantum computing. In this SEI podcast, Scanlon discusses how to create the discipline of cyber protection of quantum computing and outlines six areas of future research in quantum cybersecurity.
Listen to the SEI podcast.

Read Tom Scanlon's blog post, which provides a technical deep dive into this work.

Connecting Stakeholders for DoD Software Systems

By Hasan Yasar

The Deputy Secretary of Defense approved and signed the Department of Defense (DoD) Software Modernization Strategy on February 1, 2022. This act initiated a transformative journey for the department to deliver robust software capabilities at the pace of evolving demands. Though system complexity and stakeholder decentralization often challenge our ability to securely deliver capabilities on time and on budget, fostering collaboration and facilitating open discussions about these challenges, strategizing, and devising actionable plans will be crucial to overcoming them. This webcast highlights how the **December 2023** DoD Weapon Systems Software Summit **features** in addressing these challenges and providing us an opportunity to collectively devise effective solutions.

Attendees

- gain an understanding for software modernization strategy
- discover challenging areas for DoD weapon systems
- observe and learn enablers for solving system complexity
- align your system's objectives with your software engineering practices
- gain insights from key talks and sessions

[no markings required]

DM24-0288

View the webcast.

Measuring the Trustworthiness of AI Systems
By Katherine-Marie Robinson, Carol J. Smith, and Alexandrea Steiner
The ability of artificial intelligence (AI) to partner with the software engineer, doctor, or warfighter depends on whether these end users trust the AI system to partner effectively with them and deliver the outcome promised. To build appropriate levels of trust, expectations must be managed for what AI can realistically deliver. In this podcast from the SEI's AI Division, Carol Smith, a senior research scientist specializing in human-machine interaction, joins design researchers Katie Robinson and Alex Steiner, to discuss how to measure the trustworthiness of an AI system as well as questions that an organization should ask before determining if it wants to employ a new AI technology.
Listen to the podcast.

Read the related SEI blog post, Contextualizing End-User Needs: How to Measure the Trustworthiness of an AI System, by Carrie Gardner, Katherine-Marie Robinson, Carol J. Smith, and Alexandrea Steiner.

Additional Resources

View the latest SEI research in the SEI Digital Library.
View the latest installments in the SEI Podcast Series.
View the latest installments in the SEI Webinar Series.