Secure Software Programming Practices and Development

Date: December 13, 2023

Presented by: Nitin Sukhija (Slippery Rock University of Pennsylvania)

(The slides are available under “Materials from the Webinar” in the above link.)

Q. Can you comment on the impacts to users of Science DMZ?

A. Users of ScienceDMZ need to be aware of risks in collaboration and optimizations, especially tampering of data which can lead to loss of scientific fidelity of data.

Q. I experienced personal financial damage from someone spoofing an AWS admin, first via email (I failed to inspect the email headers in my panic), then by my dialing an included, spoofed toll free phone number, requesting “reimbursable” funds in the form of gift cards to help trace hypothetical server security leaks. How can that be addressed using STRIDE?

A. We can implement various mitigation techniques,such as the principle of least privilege and staff training/ Fuzz testing, to address different categories of threat that can be identified using the STRIDE modeling technique.

Q. This presentation seems to be primarily targeted at maintainers of systems, and it contains great advice on that topic. However, how does that filter down to say, a graduate student with minimal experience, time and funding who just needs to run some code for their work?

A. (Erik Palmer) In my experience working with security teams, the information is organized and presented in a way very consistent with today’s presentation. Personally, I see value as a software developer gaining insight into the way someone from a security background approaches the problem of software security. My understanding is that Nitin will walk through some examples which will help to explain how the security framework can be applied to more specific aspects of a piece of software.

Q. Do you - or do you plan to - collaborate with those in trustedci.org?

A. Yes,definitely, there are many workshops offered by trustedCI and I will be glad to collaborate.

Q. (Alfred Tang) STRIDE and DREAD are developed by Microsoft. Do they work on Linux? If not, what are some alternatives for Linux?

A. STRIDE and DREAD are frameworks for categorizing and prioritizing security issues. They are not software tools, and therefore do not depend on the operating system. So they equally apply to Linux and any other software or operating system.

Q. What are the best security practices for software repositories such as Spack, PyPI, Anaconda that contain potentially malicious software but are made so easy to install and run on user's behalf?

A. Using STRIDE for categorizing types of threats and using Static and Dynamic testing techniques especially in controlled environments using common vulnerabilities (CVE) will help to identify malicious functionality.