CS-405-T4539: Secure Coding

Professor Brian West

Carlos Aguirre

Southern New Hampshire University

April 22, 2021

# Implementing a security code standard helps the any project to remain consistent in its development and security features regardless of which member of the team is working on the part of code that will be pushed into the project's main branch. A project will be safeguarded from both internal and international threats to the system if it has a high and consistent security standard.

# The "Don't leave security to the end" approach suggests that security measures should not be developed towards the conclusion of the project's development. Ignoring this practice may result in a problem with the project itself, as well as a risk to the project's security owing to faulty code. Based on the scope and the safety set of code, the safety areas and the complete project may not be compatible, necessitating a team restarting the project to accommodate the security parts of code required in the project.

# I was able to witness how threats are analyzed and evaluated, the dangers are then classified into various threat levels. Teams can organize their time rectify and create defenses against these specific sorts of threats to safeguard the project from security risks, financial overruns, and time management by being able to categorize the many types of danger levels.

# Systems security features must continue to advance in this new era to combat the rising threat of assaults. To preserve the cash and security of the data in these firms, zero-trust regulations are being integrated into systems and databases for private companies and/or individual accounts.

# These regulations demand that triple A policies and encryption techniques be accessed so that even workers may see the data. Over time, these security rules have evolved from a "fortress" to defend the organization from outside dangers to a "labyrinth" design to safeguard the system by limiting access to those with authorization keys.

# Because a security system and an attacker both grow over time by their own successes and failures against one other, a security policy must be able to adapt and update over time to counteract the adapting and updating of assaults. With more data being kept in the digital world, the number and consistency of assaults will continue to rise over time, and developers must be ready to adjust their products' security measures to prevent existing and future attacks.

# References:

# What is secured coding? Retrieved from: <https://www.perforce.com/blog/sca/what-secure-coding>