Kris Marchevka

Professor Gudivada

CS-499-Computer Science Capstone

9/20/2025

Milestone 2 Narrative

For this enhancement I chose CS-405 Secure Coding Module 5 Encryption program from the June to mid-August term. It originally used a repeating-key XOR function to encrypt and decrypt a file, it was very simple and showed off the basic concepts of encryption. It had some weaknesses like using assert for error checks as I’ve mentioned before. It also operated in text mode only and wrote the encryption key into the output file.

I selected this item because it clearly illustrates an improvement to insecure code and reflects professional coding and design practices by using AES-256 for encryption for example. I also added PBKDF2 with a random salt for key derivation as well as binary I/O for handling ciphertext which I proved in the command prompt. This shows I can write secure code as well as integrate external libraries at a professional level.

Yes, I believe I met the outcomes that I planned to meet in Module One. I showed that I could redesign the code using secure industry standard cryptography all the while improving maintainability and reliability. I don’t have any updates to my outcome-coverage plans as I believe I have met this enhancement requirement.

Upon reflection, at first I was considering writing my own algorithm but that was too much of a challenge and not expected of me. So instead, I used well established cryptographic libraries which gave me the experience to set up OpenSSL through vcpkg and ensured the code compiled using C++17. The issue I had at first was accidentally running C++14 which didn’t give me access to features like std::string\_view and std::optional, which had me wracking my brains a bit. To ensure it all worked I created a tamper check by changing a byte in the ciphertext and confirming that the decryption failed with an authentication error. Overall, this was quite the challenge generally but has now given me the future confidence in recognizing insecure coding patterns and allowing me to replace them with more modern, robust practices.