# Journal: Portfolio Reflection

Jacob Burchett

CS 405

Professor Philomena Ogoh

2 March 2025

# Journal: Portfolio Reflection

As someone who has not yet had the opportunity to work in software development, this course provided new insights to me, in terms of security. While I understood the importance of security before this course, I now have a much better understanding of the importance of integrating security into the early phases of development rather than adding security measures later. Implementing security integration early into development allows for a more secure system overall while removing some of the complexity and unsustainability that adding these features later would lead to.

When discussing the cost-benefit of mitigation, you are referring to the cost of making a system more secure. Often, there is a balance between the two that can be charted to determine the appropriate level of security for the cost that should be implemented during development. Early integration of security leads to a more secure system that is more easily maintained but can also lead to increased cost.

Zero trust is a security model that states that no one whose identity has not been verified should be trusted on a network. There are subsections to this model that make up the whole. Least privilege is a principle that states users should only be given enough access to accomplish their specific tasks and no more. Microsegmentation is the process of dividing a network into smaller zones with separate access rules. Verification is the process of continually monitoring the activity of users and systems. Zero trust is set in place to protect the system itself as well as users.

As briefly discussed above, a proper risk assessment is crucial in the early stages of development in order to determine potential risk factors for a new system. Identifying vulnerabilities, potential attack routes, and security needs leads to a system that is more secure while also being easier to maintain.