Thesis Project Portfolio

Enhancing Code: Refactoring and Adding Type Hints

(Technical Report)

Replacing Passwords for a More Secure World

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Matthew Beck

Spring, 2024

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

My thesis portfolio presents two disjoint papers, my technical report and STS research. Although the two research papers focus on different problems, the research presents information on how technology interacts with organizations and society alike.

The technical report aims to address individual organizations in how they manage their code repositories and how bad practices affect an organization's developers. As companies continue to grow, their code repositories grow with them. With this growth, inefficiencies and errors are introduced through duplication of code and human oversight. This results in a reduction in efficiency for developers and increases the likelihood for more errors to occur. In the technical report, I analyze how code can be made more efficient and secure for developers. I present this analysis through my work as a software engineer intern this past summer. The first aspect of the report focuses on adding type hints to my team's code repository. This allows developers to use auto completion and check if the code that they are producing and using is type-safe. The second aspect of my technical report focuses on refactoring code. This process mainly consisted of removing duplicate code within the repository while maintaining the overall functionality. Additionally, this involved making the common functions being used more efficient. This resulted in developers spending less time looking for the correct code function to use and created a more cohesive development process across the team.

During my time at my internship, I reviewed thousands of lines of code with the hope of making the code more efficient and secure for the other developers on my team. I was able to accomplish this, however there still remains code that needs to be reviewed within the repository I was working in. Additionally, the problem discussed is not isolated to this code repository. The company itself has multiple code repositories and there are a multitude of companies that have legacy code that should be refactored and have type hints added.

Cyberattacks are increasing each year with a common target of the password-based authentication methods most people use. It is increasingly clear that additional security methods are in order which ultimately may lead to an alternative to passwords. In past years, there have been additional security measures added such as push notifications on mobile devices. However, since these measures have a foundation of knowledge-based information such as passwords, they are still susceptible to attack. Through my STS research, I examine what a shift towards passwordless authentication may look like and the social factors and implications that must be thoroughly considered to have a successful implementation. I begin by detailing the security risk that these password-based systems pose. Then, I use the Unified Theory of Acceptance and Use of Technology to analyze the different social components involved when deploying a new authentication system. This theory poses four key determinants which I argue must be met for each stakeholder group if the deployment of a new authentication system is to be successful. This led me to contend that the IT management teams, developers and users are the most important stakeholders to be considered. Finally, I explore a previous shift in authentication methods, how the key determinants were addressed, and what that may mean for the future shift to passwordless authentication.

The STS research is the first step needed to replace password-based systems. My findings of the social factors that need to be considered in the deployment of a new authentication system provides information of who should be considered when developing alternatives to passwords. This leads to the need for continued research on the technologies being developed and how they fulfill the expectancy determinants discussed. Passwordless authentication has not been fully implemented, this presents the warrant of my research as well as the limitations. Some of the social factors discussed are speculative and may not be fully understood until the implementation process actually begins.