SYNTHESIZING AN AUTHENTICATION SYSTEM TO EVALUATE THE IMPACT OF DESIGN THINKING

DESIGN THINKING IN THE CONTEXT OF DEVELOPING USER AUTHENTICATION MECHANISMS

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

Samreen Azam

November 1, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Joshua Earle, Department of Engineering and Society

Panagiotis Apostolellis, Department of Computer Science

DESIGN THINKING IN THE CONTEXT OF DEVELOPING USER AUTHENTICATION MECHANISMS

Introduction

As both the complexity of and demand for technological solutions continues to rise, the necessity for strengthened security measures to protect such systems in turn grows as well. Cyber-attacks have become a frequent, daily occurrence, and without appropriate security measures and recovery systems, numerous businesses and organizations face extreme losses. Implementing basic forms of verification is generally a given; having login credentials is a baseline expectation for most websites and applications, and multi-factor authentication is increasing in popularity as well. Many systems also employ authentication services derived from biometrics, such as facial recognition or fingerprint scanning ("What Is Biometry?", 2002). The advancement of these tools is essential to improve the protection of sensitive assets and data.

Devising more robust user authentication algorithms is an ongoing affair, and the design-thinking paradigm may inspire novel ideas in tackling this issue. Design thinking refers to the methodology of developing design concepts in such a way that emphasizes human-centric needs and interactions (Dam and Teo, 2021). It is an iterative and solution-based approach to planning out products in which designers seek to redefine problems by challenging their constraints and identifying new solutions. Additionally, design thinking centers on fostering a sense of empathy and having a full understanding of the users' interests and experiences; this is carried out through observing and interviewing the human actors associated with a problem. Ultimately, design thinking is a cyclical process of learning about the users' needs, specifying their issue, brainstorming possible ways to address it, generating prototypes, and testing those protypes. The

cycle continues on as new information collected from the testing stage helps engineers reevaluate the problem and work toward a more efficient solution.

It is critical to understand the needs and behaviors of clients and users when developing any type of cybersecurity product. Recent studies have reported that human-caused errors result in the majority of cybersecurity breaches (“IBM X-Force Threat Intelligence Index”, 2001). Due to its focus on the human experience, design thinking may prove to be a beneficial strategy in optimizing the verification of personal identities and facilitating access control. In turn, this would greatly enhance the overall data security and integrity for many systems. For this reason, the principal aim of this exploration is to link the fields of human-computer interaction and cybersecurity from the perspective of a student who has taken courses in both of these subjects. Specifically, there will be an emphasis on the concepts of design thinking and its potential impact on the development of user authentication technology.

Synthesizing an Authentication System to Evaluate the Impact of Design Thinking

In order to investigate how design thinking may potentially influence the development of cybersecurity systems, particularly user authentication services, the technical portion of the thesis portfolio will follow the planning and development of an application. This report will document the execution of each step of the design thinking cycle, in which two iterations at minimum will be carried out. Although a highly sophisticated system may not be feasible for one student to work on alone, a simple program that still requires particular credentials should be sufficient in illustrating the role design thinking plays in software development.

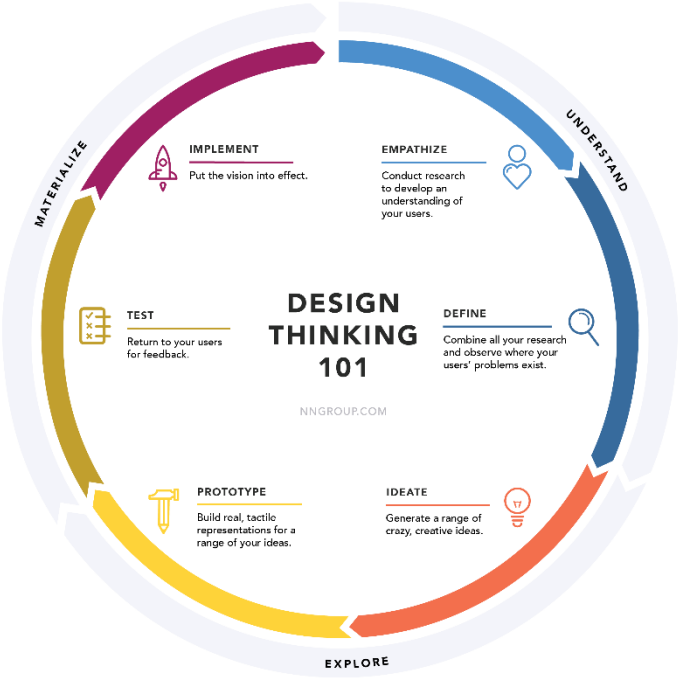

Figure 1: The cyclical nature of design thinking. (Source: 'Design Thinking 101', Nielsen Norman Group, https://www.nngroup.com/articles/design-thinking.)

The initial step would be to identify the users and garner an in-depth understanding of their needs. This can be done by conducting interviews or requesting them to fill out surveys. As an undergraduate, the most accessible userbase would be other students at the University of Virginia. They can be inquired about their typical schedules, what hurdles they are facing in relation to cybersecurity, and their experiences with authentication services. This data will assist

in empathizing with the future users of the system, as the design-thinking paradigm suggests, and determining a specific problem to solve. This problem definition should be framed with the users as the central subject.

The next task would be to formulate ideas to address the problem using a solution-oriented approach. Upon doing so, the development of the prototype will begin. This prototype will most likely only implement the key features of the proposed solution. Testing metrics could be based on user feedback upon interacting with the system, and the results of these evaluations will help in redefining the requirements of the system, thus leading to the start of the cycle once again.

Navigating Ethical Obstacles Presented by Cybersecurity Products and Techniques

It would be a misstep to discuss the importance of designing stronger cybersecurity systems without reflecting upon the many ethical concerns that exist within this realm. Hence, the STS-focused section of this portfolio will be an analysis of the social impacts of developing tools for authentication. Cybersecurity products such as identification services and surveillance systems tend to operate by collecting and interpreting information regarding unique, personal traits**.** The implications of misidentification as well as sacrificing privacy for the sake of security demonstrate why it is important to evaluate the needs of different human actors when using design thinking to optimize authentication mechanisms.

Moreover, there are concerns regarding accessibility through these mechanisms. In biometrics, the focus placed on physiological and behavioral traits could become problematic if the vast extent of human diversity is not properly taken into account. For example, in fingerprint scanning, people whose occupations require them to perform hard labor or work with harmful chemicals may end up with callouses that prevent accurate readings of their fingerprints in comparison to people who can afford to take better care of their hands. Aging can bring about changes in a person's fingerprints as well, which would pose a problem upon being tested based on the original fingerprint sample. Additionally, people with voice tremors have struggled to engage with identification technologies based on voice recognition (Schwartz et al). Thus, the failure to consider varying demographics in the design process hinders the accuracy of data acquired through biometrics. Furthermore, verification via biometrics may exclude people who lack a particular characteristic from accessing services. In one recent study, it was found that websites employing dynamic device positioning, a biometric technique that involves using the hands to set a device at a particular location relative to the face, had very low usability for people

with limited vision or dexterity. (Brink et al., 2020). Poor accessibility within such mechanisms have blocked people with disabilities or health conditions from being able to independently use websites for government resources and tax services as well. Thus, it is important to explore the ways in which these systems may influence different demographics in order to prevent unfair biases dominating the design of cybersecurity systems.

Another major concern would be the possibility of the information collected to develop authentication services to be maliciously exploited. Government organizations are known to keep massive databases of biometric data for the purposes of identifying criminals, employment verification, border security, etc. (Schwartz et al.). Private companies also manage similar databases to ease the process of accessing product and service information for consumers and employees. However, the abuse of such systems can lead to issues related to the creation of "deepfakes", a form of artificial intelligence that essentially copies the likeness of a person ("Misused Biometric Data Could Lead to More 'Deepfakes'", 2019). Such technologies may lead to serious violations of intellectual property and could encroach upon sensitive data. As a result, not only the development of these mechanisms, but also their management should be carefully designed with the safety and needs of the users in mind.

Foundational Texts and Primary Resources

A text that I feel has greatly enhanced my understanding of the impact biometrically-based security systems can have on societies would be a case study conducted by Alena Thiel. This study, published in the *Journal of Modern African Studies*, focuses on the push for more applications of data analysis in Ghana and how new identification technologies are emerging following recent breakthroughs in biometrics (Thiel, 2020). Over the course of several years, Thiel interviewed several types of stakeholders, such as civil rights activists, government officials, data scientists, and legal experts. Also, she spoke to citizens about how their daily lives had been affected by the implementation of new identification systems used by health registrars and police forces. Although Thiel ultimately concludes that these systems have overall favorable impacts and should continue to be developed, her interview notes also included significant criticisms presented by the citizens, such as a loss of confidence in the efficiency of the government. Due to Thiel's usage of data collected by other organizations, several of the works cited in this study are statistical reports from sources such as the World Bank and UNDP. Additionally, because of the text's exploration of the relationship these technologies have with governmental policies, Thiel also cites information from official documents published by the Ghanian government and other academic journals.

Moreover, another case study I found to be relevant to this topic is an investigation on the challenges in cybersecurity that working adults face and whether the design thinking process can provide adequate solutions to tackle such issues (Dorasamy et al., 2019). The authors' purpose was to demonstrate how individual psychological factors are responsible for most violations in securing cyberspace. To do so, they interviewed 20 people between the ages of 18 and 40 about their experiences with cybersecurity in the workplace. The participants' work background was

categorized as either “IT” or “Non-IT”; I believe it would have been valuable to also include which fields in particular the “Non-IT” participants were part of, as well as where on the corporate hierarchy the “IT” participants fell under. The authors also reported about how they utilized each stage of the design thinking process to determine potential solutions for the problems the participants were frequently dealing with. This report also primarily cites statistical reports, even more so than Thiel’s case study, published by globally-recognized organizations. Other types of referenced literature would be definitions of cybersecurity concepts from academic journals, mostly to provide some context about cyberattacks.

Similar to the aforementioned text, another primary resource that details the stages of the design thinking process within the domain of cybersecurity would be a recent case study about the accessibility of identification systems in online monetary transactions for the visually impaired in India (Manjunath et al., 2021). The authors spoke to residents of an institution for the blind, and reported what percentage of their population sample possessed the ability to read braille. Interviews were held in order to understand what problems the residents experienced when interacting with these systems. This information was used to design behavioral experiments in which participants tried out online banking applications. It appears to me that all the relevant stakeholders were involved in the process. Furthermore, the authors mainly referenced data collected by official treasuries as well as other published case studies that focused on developing technological solutions for the visually impaired.

Works Cited

"IBM X-Force Threat Intelligence Index." IBM, 23 Feb. 2021, https://www.ibm.com/security/data-breach/threat-intelligence.

Dam, Rikke Friis, and Teo Yu Siang. "5 Stages in the Design Thinking Process." *The Interaction Design Foundation*, 2 Jan. 2021, https://www.interaction-design.org/literature/article/5-stages-in-the-design-thinking-process.

"What Is Biometry?" *International Biometric Society*, The International Biometric Society, 31 Jan. 2002, https://www.biometricsociety.org/about/what-is-biometry.

Schwartz, Adam, et al. "Biometrics." *Electronic Frontier Foundation*, Electronic Frontier Foundation, https://www.eff.org/issues/biometrics.

Brink, Ronna ten, et al. "Usability of Biometric Authentication Methods for Citizens with Disabilities." *MITRE*, The MITRE Corporation, 25 Nov. 2020, https://www.mitre.org/publications/technical-papers/usability-of-biometric-authentication-methods-citizens-disabilities.

"Misused Biometric Data Could Lead to More 'Deepfakes'", International Association of Privacy Professionals, 19 Aug. 2019, https://iapp.org/news/a/misused-biometric-data-could-be-used-to-create-deepfakes/.

Thiel, Alena. "Biometric Identification Technologies and the Ghanaian 'Data Revolution'." *Journal of Modern African Studies*, vol. 58, no. 1, 1 Mar. 2020, pp. 115 - 136.

Dorasamy, Magiswary, et al., “Cybersecurity Issues Among Working Youths in an IoT Environment: A Design Thinking Process for Solution,” *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS),* 2019, pp. 1-6, doi:10.1109/ICRIIS48246.2019.9073644.

Manjunath, Akanksh A., et al. “Design Thinking Approach to Simplify Monetary Transactions for the Visually Challenged.” *British Journal of Visual Impairment*, Aug. 2021, doi:10.1177/02646196211032492.