EVALUATING THE POTENTIAL OF INTRODUCING DESIGN THINKING IN CYBERSECURITY EDUCATION

(Technical Paper)

DESIGN THINKING IN THE CONTEXT OF DEVELOPING USER AUTHENTICATION MECHANISMS

(STS Paper)

A Thesis Portfolio in STS 4600
Presented to the
Faculty of the School of Engineering and Applied Science
Of the University of Virginia, Charlottesville, Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

Samreen Azam

Spring 2022

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

Daniel Graham, Department of Computer Science

Rosanne Vrugtman, Department of Computer Science

Joshua Earle, Department of Engineering and Society

DESIGN THINKING IN THE CONTEXT OF DEVELOPING USER AUTHENTICATION MECHANISMS

Introduction

As both the complexity of and demand for technological solutions continue to rise, the necessity for strengthened security measures to protect these systems in turn grows as well. Cyber attacks have become a frequent, daily occurrence, and any person that interacts with any type of virtual device is, to varying degrees, vulnerable to such attacks. Without appropriate security measures and recovery systems, numerous individuals, 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. The advancement of these kinds of tools is vital 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” is 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. Essentially, 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.

It would be a misstep to discuss the importance of designing stronger cybersecurity systems with the human users’ needs at the forefront without reflecting upon the various social impacts and ethical concerns that exist within this realm. The collection, management, and application of sensitive information are intrinsic aspects of cybersecurity, and for this reason, there are several social risks and responsibilities to consider. As such, the principal aim of this research paper is to explore the major controversies and concerns that arise when developing tools for authentication and to discuss their significance in the hopes that it may assist engineers in ameliorating cybersecurity products.

STS Frameworks and Methodologies

Langdon Winner’s theory of whether artifacts contain politics reminds me of reasons why the design thinking paradigm may be beneficial in addressing the current issues in the development of authentication systems. Winner’s theory discusses the importance of evaluating the social and/or economic system in which a technological artifact is embedded within (Winner, 1980). It explains that the arrangements of technical systems are manifestations of “forms of order”. A system may be intentionally designed for some social impact, such as ostracizing a particular group in favor of another. Winner also describes that not all political qualities of artifacts are the result of actively malicious intents, but rather due to neglect and ignorance brought about by societal norms. I believe these points relate to my interest in investigating the social ramifications of current authentication technologies and the techniques used in their development. If there are indeed politics embedded in authentication services, then design thinking concepts could be adopted to restructure their development processes and minimize any resulting political disadvantages. As a result, I integrated Winner’s theory in my discussion of the significance of design thinking in cybersecurity. Specifically, I considered this perspective when researching how personal data is collected, evaluated, and applied when creating user authentication products. This was done to understand whether there are aspects of cybersecurity products and development processes that inherently represent social hierarchies or imbalances, and if there are such qualities that, are a reflection of the developers’ beliefs. Perhaps, with a better understanding of the politics these technologies display and how they impact society, engineers will be able to effectively reframe problems to put the needs of people at the forefront and optimize cybersecurity products in such a way that reduces inequalities and other ethical dilemmas.

As for methodologies, I carried out my research by analyzing documents that detail common techniques used when developing authentication services and how people are able to interact with these services. I have explored what conditions or disabilities people may have that could affect their experience with these systems as well as what can be done to facilitate the usage of these systems. It was also beneficial to take a look at primary resources such as case studies and interviews related to the role of design thinking in cybersecurity. This meta-study has provided insight on how technologies developed through design thinking have historically influenced users and whether there is any evident indication of it being able to limit barriers caused by social imbalances.

Navigating Ethical Obstacles Presented by Cybersecurity Products and Techniques

Cybersecurity products, such as identification services and surveillance systems, tend to operate by gathering and interpreting information regarding unique, personal traits**.** The implications of misidentification and identity theft, as well as the issue of 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. An instance of this would be, in an attempt to access a website to apply for unemployment benefits, the failure of the facial recognition software used by that website to identify a person caused the individual's account to be frozen (Bass and Donnan, 2022). This same software had been known to have poor recognition abilities toward people with darker skin; rather than an issue of incompetency in programming or other technical skills, this actually leads to the question of underlying neglect by the developers or even underlying political biases they might harbor about race influencing the design process. Facial recognition algorithms, similar to most other forms of artificial intelligence, are based upon pattern recognition and machine learning. If the developer does not actively attempt to expose the algorithm to diverse types of faces at the start of its learning, then it is unlikely that the product will register certain groups of people as humans. Ultimately, this becomes an innate aspect of the software that indicates the lack of representation of marginalized groups in technology.

Moreover, there are concerns regarding accessibility through these mechanisms. Quite frequently, cybersecurity systems employ authentication services derived from biometrics. For context, “biometrics” refers to the application of statistical methods to the collection and analysis of biological data, and it is a building block for technologies like retina scans and fingerprint identification (“What Is Biometry?”, 2002). In biometrics, the focus placed on physiological and behavioral traits could become problematic if the vast extent of biological and lifestyle variances 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. In addition, people with voice tremors have struggled to engage with identification technologies operated by voice recognition (Schwartz et al). Aging can also bring about changes in a person’s fingerprints as well, which would pose a problem upon being tested based on the original fingerprint sample. Thus, the failure to consider multiple 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. Software systems that depend on fingerprint scanning pose a problem for people who either do not have fingers or have a skin disease that affect the pads of their fingers. For instance, individuals with the rare condition adermatoglyphia do not have the small ridges on the pads of their fingers, palms, and feet that make up a unique fingerprint (“Adermatoglyphia”, 2020). Thus, they cannot be identified via dermatoglyphs. Another denomination for adermatoglyphia is the "immigration delay disease" due to the struggle that people with this condition face when attempting to enter countries that require fingerprint scanning upon arrival. Also, 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. To look at this in terms of Winner's theory, the inherent lack of usability for these systems is a representation of how disabled people are commonly excluded from fully participating in society, whether it is done deliberately or unknowingly. 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. Although this technology does not seem to be political by nature, it can be manipulated to cause harm. For this reason, 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.

It is clear that in order to use design thinking to work toward optimal cybersecurity solutions, there should be thorough research efforts to break down barriers in accessibility and to mitigate the probability of data exploitation. In many situations, software engineers are presented with the question of whether it is even feasible to make something completely accessible or risk-free with our current technology. There may even be tradeoffs between usability and productivity, so developers need to determine whether or not a sacrifice has to be made for the sake of efficiency.

Related Studies in Cybersecurity and Design Thinking

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 published in the *Journal of Modern African Studies*. It 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, the author 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 she 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.

Moreover, another case study 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). Its purpose was to demonstrate how individual psychological factors are responsible for most violations in securing cyberspace. To do so, a series of interviews were conducted to examine people's experiences with cybersecurity in the workplace. The participants were categorized as either *I.T.* or *Non-I.T.* to separate those with a background in information technology from other employees; I believe it would have been valuable to also include where on the corporate hierarchy the *IT* participants fell under in order to better grasp the differences between their needs and experiences. The authors 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. They concluded that the process enabled them to determine which psychological qualities were most likely to influence security, such as a person's password management abilities and attitudes toward privacy, as well as what can be done to improve upon these behaviors and beliefs. Based on this, they created a handbook for internet users in the workplace to stay informed about how to avoid making mistakes that endanger their data; feedback on this prototype was used to redefine their research question and to develop a better product, a clear example of cyclicality of design thinking.

Similar to the aforementioned text, another primary resource that portrays 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. A common concern was found to be the fear of accidentally modifying a setting when using a touch-based system, resulting customers in opting for in-person, cash transactions whenever possible. This information was used to design behavioral experiments in which participants tried out an audio-controlled online banking application. Their observations of the participants' reactions to the prototype helped them decide which features needed to be included or reworked. They noted that the rapid prototyping was important to represent scalability and optimization features. It was also reportedly useful for understanding how this software can be tested in such a manner that reflects the real world.

Discussion

The objective of this paper has been to assess whether design thinking concepts are useful to incorporate in the development of authentication systems. By exploring the current social issues entangled in both the development processes and the aftereffects of these technologies through the lens of Winner's theory of the innate political identity of artifacts, it is apparent to me that the user-centric nature of the design thinking paradigm can help break down these barriers. Many of these issues are the consequences of power imbalances brought about by social divisions, and the emphasis on human experiences and empathy that is encouraged by design thinking can surely address them. Additionally, recent studies in the development of cybersecurity products have shown that, when design thinking plays a role in the process, there are positive effects in the accessibility and efficiency of these systems. With the needs of the human participants at the forefront of development, these studies showed that design thinking techniques can improve the quality of life for marginalized groups. It is my hope that these factors encourage software developers, as well as other types of engineers, to apply design thinking in their work and to seek to educate others about its impact.

Works Cited

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.

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

Winner, Langdon. “Do Artifacts Have Politics?” *Daedalus*, vol. 109, no. 1, The MIT Press, 1980, pp. 121–36, http://www.jstor.org/stable/20024652.

Bass, Dina, and Shawn Donnan. “How Did ID.me Get Between You and Your Identity?” Bloomberg.com, Bloomberg, 20 Jan. 2022, https://www.bloomberg.com/news/features/2022-01-20/cybersecurity-company-id-me-is-becoming-government-s-digital-gatekeeper.

“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.

“Adermatoglyphia” *MedlinePlus*, U.S. National Library of Medicine, 18 Aug. 2020, https://medlineplus.gov/genetics/condition/adermatoglyphia/#synonyms.

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.