# 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

# Table of Contents

## Sociotechnical Synthesis

The main focus of both my STS research paper and technical report is to investigate the impact of applying the design thinking paradigm in the development of cybersecurity products, especially that of authentication systems to verify the identity of users. Although the topics of these papers are very similar, there are a couple of important distinctions. Firstly, the technical report primarily details the practical benefits of this paradigm, whereas the STS paper explores how design thinking may affect social imbalances in cybersecurity. Another difference is that the technical report goes more in-depth about how software engineers can be educated on design thinking principles, and it proposes modifications to the curriculums of cybersecurity courses at the university level.

In the technical report, I performed a meta-study to explore how design thinking concepts have been used to combat and prevent cyber attacks. I looked into existing systems related to threat modelling and the security features of smart homes in order to determine how the stages of design thinking process resulted in more robust and technically-sound software solutions. I also researched proposals for authentication systems that are developed through design thinking and how these systems might influence cybersecurity if properly implemented. Also, I considered how students might benefit from being educated about this paradigm. The technical report is concluded with an explanation of what the incorporation of design thinking in cybersecurity education might look like and what potential advantages it has. There is also a brief look into future project ideas that I could carry out in order to confirm my own theories.

As for the STS research paper, I focused on the social and ethical issues surrounding the current techniques used to develop authentication software. Integrating ideas from Langdon

Winner's theory of whether artifacts have politics, I discussed how discriminatory aspects of society may be reflected by the innate nature of some biometrically-based products, and how the design thinking process has the potential to minimize such harmful effects. To do this, I compiled texts that describe how members of marginalized groups have been prevented from being able to fully experience and benefit from particular authentication systems. I then discuss how Winner's theory may apply to such systems and what they say about our society's values. There is also a detailed look at past case studies in which researchers have successfully applied design thinking concepts in the development of cybersecurity systems and how the results of their experiments indicated that this concept really could help promote accessibility and fairness.

# EVALUATING THE POTENTIAL OF INTRODUCING DESIGN THINKING IN CYBERSECURITY EDUCATION

CS 4991 Capstone Report, Spring 2022

Samreen Azam
Computer Science
The University of Virginia
School of Engineering and Applied Sciences
Charlottesville, Virginia USA
sa3tnc@virginia.edu

**Abstract**

Because of its nature of prioritizing human needs and experiences, I wanted to investigate whether incorporating the design thinking paradigm could enhance students' understanding of cybersecurity concepts. I conducted a meta-study in which I looked into several published works about authentication software as well as design thinking usages in engineering. Based on the knowledge I gained from my research and from two of my CS courses, I determined that design thinking would be valuable to include in cybersecurity-related curriculums as it does positively influence the development process for authentication software and mitigates the impact of human errors that may undermine such systems. Going forward, I am interested in planning and developing an authentication application for students, in accordance with the principles of design-thinking, to draw a more detailed conclusion.

## 1. Introduction

Students at many universities depend upon websites and software that utilize authentication services. These services are in place to verify a user's identity and prevent an outsider from accessing their account and personal information. At the University of Virginia in particular, students are all expected to use multifactor authentication software in which they must provide confirmation through a personal, external device when attempting to log into their individual student accounts. As the need for more robust cybersecurity measures continues to grow, the design thinking paradigm may provide some insight on how to better accommodate users through these systems.

Design thinking refers to the methodology of developing design concepts in a way that emphasizes human-centric needs and interactions [1]. 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 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 [2]. 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 authentication systems. Hence, the primary aim of this technical report is to examine existing research and explain why it is useful to teach about the design thinking process in tandem with authentication software at the University of Virginia.

## 2. Review of Studies

Research regarding user-centric approaches to engineering new cybersecurity solutions has become more prominent in recent years. A new perspective of threat modelling that highlights the significance of design thinking reflects how this paradigm may play a role within the development of prevention techniques to reduce cyber-attacks [3]. This paper outlines how, in the context of developing risk-prediction software for a company, the process of empathizing with the client and maintaining a thorough understanding of their predominant concerns is an integral component of identifying vulnerabilities within their system. Moreover, the human-centric approach also takes possible intruders and their behaviors into account. As a result, the developers can evaluate potential threats with even more accuracy.

The way in which design thinking encourages redefining problems and challenging their constraints is also regarded as beneficial in better comprehending these systems. The author states that this is because design thinking's cyclicity allows for larger problems to effectively be broken down into subproblems that can be investigated in greater depth. The documentation produced after testing prototype solutions to these problems will in turn aid in once again redefining the scope of these problems and forming new ideas of solving them.

A conceptual model proposed in a sustainability journal advocating for smart homes, including their security measures, details the shift from solely technology-driven perspectives to more user-focused methods of developing solutions [4]. The authors discuss the benefits of the rapid prototyping stage of design thinking and how the process is revisited as the cycle continues, asserting that such methods are vital to generating creative solutions and being able to apply them in broader situations.

In addition, the authors argue that the tools that contribute to the operations of a smart home, such as monitors, sensors, and device authenticators, should be developed with the human users' needs, desires, and capabilities as the main factor of motivation and design inspiration. In their study, the authors designed six varying manifestations of a smart home system after analyzing what potential residents would want from such a system. They discovered that among these variations, residents rated the perceived level of security the highest for the systems that were developed through design thinking methods that emphasize the users' needs. An example would be voice-powered appliance automation and access control. Users felt safer and more satisfied when they were certain that their devices could differentiate between unique voices and only respond to those authorized to utilize them.

The next work is a proposal for an authentication system based on human psychological behaviors and our reactions to objects in our environment [5]. In this system, users arrange images of random objects or interact with them in other ways that imply a

personal preference or unique pattern of thought. A user's identity is verified upon interacting with the objects in the same manner as they did during their initial encounter. The assumption is that users' reactions and behaviors toward these objects would not change, so there is no need for users to rely on their memory or an external system as they typically would with other types of authentication software. This system is aimed to solve problems that current, commonly-used authentication methods supposedly might not. One such problem would be shoulder-surfing attacks, a social engineering technique in which an outsider acquires personal information by physically viewing their victim's screen or keypad. The logic is that even if someone were to view the user's screen, it would be difficult to recall all of the information, and the attacker would struggle to gain access since they are unlikely to have the same natural reactions toward the objects. This method also eliminates the need for external tokens to authenticate a user, which is beneficial as these tokens are susceptible to theft or loss. If implemented correctly, this proposed algorithm demonstrates how placing focus on human behaviors while developing authentication software can enable us to bypass our natural limitations and strengthen security.

## 3. Curriculum Recommendations

Due to the human user being the entity most vulnerable to risks in a cybersecurity system, incorporating design thinking methods could be a step in the right direction to strengthen these systems. As the design thinking paradigm can benefit the development of authentication software, I recommend that cybersecurity courses, especially introductory courses taught at the university level, cover this topic and delve further into how human experiences affect authentication and verification services. Many curriculums discuss social engineering and the human user being a major vulnerability of cyber systems already, but this can be further explained by including design thinking principles and how they are implemented.

For instance, students could work on projects that utilize design thinking techniques, such as conducting initial interviews and collecting feedback from stakeholders to determine the course of development, in order to synthesize cybersecurity software. Other assignments could focus on the ethical issues of existing systems, such as how the exclusionary nature of biometrically-based software can lead to inaccuracies. Encouraging discussion-centric exercises, such as presentations, debates, and Socratic seminars, in which students share their stances on cybersecurity topics and case studies, are also recommended.

## 4. Expected Outcomes

Based on the perspectives and information presented in the studies, I believe that these curriculum ideas will help students to learn how to think about and empathize with human experiences in a software-related context. In the long run, I believe that educating students about this topic will lead to an increase in the incorporation of design thinking strategies on a professional level. My understanding is that the influence of design thinking principles will minimize discriminatory aspects of authentication services. Because developers would be putting in more effort to understand different groups of people, this could also help prevent microaggressions and social inequalities. Furthermore, I expect this to lead to an uptick in more personalized and efficient cybersecurity products.

## 5. Future Work

If given the opportunity, I wish to work on a complex authentication service in which I iterate through multiple cycles of the design thinking process. Moreover, a useful experiment would be to directly compare two types of development styles by working with two teams that create an authentication system, where design thinking is utilized by one group and not used by the other. In doing so, I could collect data that would either support my conclusions about the benefits of using design thinking in cybersecurity or cause me to rethink and repurpose my curriculum recommendations.

## References

[1] Rikke Friis Dam and Teo Yu Siang. "5 Stages in the Design Thinking Process." (2 January 2021). The Interaction Design Foundation. Retrieved from https://www.interaction-design.org/literature/article/5-stages-in-the-design-thinking-process.

[2] "IBM X-Force Threat Intelligence Index."(23 Feb. 2021). IBM. Retrieved from https://www.ibm.com/security/data-breach/threat-intelligence.

[3] Suman De. A Novel Perspective to Threat Modelling using Design Thinking and Agile Principles". (2020) Sixth International Conference on Parallel Distributed and Grid Computing.

[4] Flavio Martins et al. "Design thinking applied to smart home projects: A user-centric and sustainable perspective." (2020). Technical Scientific Center, Pontifical Catholic University of Rio de Janeiro. Retrieved from https://doi.org/10.3390/su122310031.

[5] Ratna Deepthi Dasika and Sujanavan Tiruvayipati. "A Novel Authentication System Using Human Behaviour against Objects." International Journal of Advanced Research in Computer Science and Software Engineering 4, 6 (1 June 2014).

# 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.

# 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

Daniel Graham, 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.

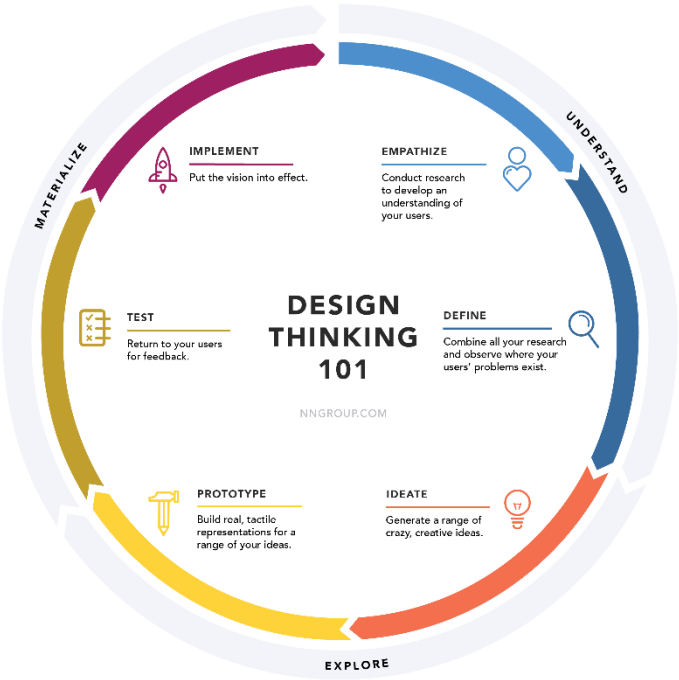


*Figure 1: The cyclical nature of design thinking. (Source: 'Design Thinking 101', Nielsen Norman Group, https://www.nngroup.com/articles/design-thinking.)*

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.