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).