Essential Cybersecurity Measures in User Interface Design

Demontae T. Watson

Old Dominion University

IDS300W

Dr. Kat LaFever

June 17, 2024

Abstract

Given the increased risk of cyberattacks and data breaches in the modern digital environment, cybersecurity measures must be incorporated into user interface design. Strong cybersecurity measures are becoming more and more necessary in user interface design as technology develops. The aim of this research is to identify critical cybersecurity protections that should be integrated into user interface design in order to enhance security and combat cyberattacks. This research aims to identify the most important cybersecurity measures for efficient user interface design by looking at behavioral, technical, and design factors through the lenses of information security, psychology, and human-computer interaction.

Essential Cybersecurity Measures in User Interface Design

Introduction

When it comes to making sure digital systems are secure, user interface (UI) design is essential. It includes the creation of UIs that let users communicate with systems and software programs. User interface design must place a high priority on protecting confidential data, preventing unwanted access, and reducing potential security threats in the context of cybersecurity. This research explores the question: “What are the key cybersecurity measures in user interface design?” by integrating insights from three disciplines: Human-Computer Interaction (HCI), information security, and psychology.

Key terms that will be defined throughout the paper are Multi-factor authentication (MFA), Role-based access control (RBAC), and cross-site scripting (XSS). Each one of these terms have importance when explaining the security of UIs.

HCI is relevant as it focuses on creating interfaces that are both usable and secure, ensuring that security measures do not compromise user experience. This is important because when designing you must take in account user’s usability while also maintaining efficient security, which if not balanced correctly, could cause vulnerabilities.

Information security provides the technical framework and methodologies necessary to protect data and prevent breaches. This is just as important as the HCI as it is essentially the foundation of which cybersecurity measures are built upon in UI designing. Advances of cyber threats have to be met with new security features to best combat these cyber threats.

Psychology helps us understand how users perceive and interact with security features, enabling the design of interfaces that promote secure user behavior. This is essential as knowing how users think or make decisions when interacting with the UI, helps better design different features in a way that aligns with natural user behaviors and patterns, making them more likely to be used correctly.

Using this interdisciplinary approach, it will inevitably help form an answer of what cybersecurity measures should be taken when creating an UI. Although security is the main focus, you have to make sure the UI is user-friendly and compatible to all users. Without each of the three disciplines used (HCI, Information Security, and Psychology) it is not possible to gain the perspective needed to address cybersecurity challenges in UI designing.

Human-Computer Interaction

One of the primary challenges in UI design is balancing security and usability. A secure interface that is difficult to use can lead to user frustration and non-compliance with security protocols. There are multiple types of users like

> Nave users who is the person who has very little link with the system. Sophisticated users who are users that uses the system, and they are also comfortable in using that system. Specialized users who are users that are expert in using the system, administrating, and maintaining the system (Iftikhar, et al., 2018, p. 154).

To create user interfaces that are accessible to a majority of people and their skill levels, its important to understand these three different types of users. In other words, a UI for beginner users should provide clear instructions to avoid mistakes, while sophisticated users should have a more balanced focus with advanced features, they can use without it being too much, and finally, specialized users, who are advanced enough, may require a more technical and detailed features to best manage and maintain the system.

By understanding and addressing these different needs of each group of users, you are able to develop UIs that focuses on each user's needs being met. While although there are variables within the users, the UI type also matters. Command line and Graphical user interface (GUI) are two popular types of UIs. "Command line is the interface that allows the user to interact with the computer by directly using the commands" (Iftikhar, et al., 2018, p. 153). "Graphical user interface is the interface that allows the user to interact with the system, because this is user friendly and easy to use" (Iftikhar, et al., 2018, p. 153).

Information Security

While HCI focuses on the usability of UIs, it is important to maintain the security of the users through the UI. Information security does exactly this through multiple ways but we will focus on authentication/authorization mechanisms and passwords. One of the fundamental cybersecurity measures in UI design is the implementation of authentication features. Authentication is the process of verifying the identity of a user or system before granting access to resources.

In UI design, this often involves the use of authentication factors such as passwords and multi-factor authentication (MFA). Password-based authentication, while widely used, can be vulnerable to various attacks such as brute force attacks and password guessing. As such, user interface designers must consider alternative authentication methods such as biometric authentication (e.g., fingerprint or facial recognition) and MFA to enhance security. "With these schemes the reliance on passwords for the purpose of authentication keeps increasing, and the user friendliness of the process diminishes." (Choudharu, 2023). But this doesn't trump the usefulness of these biometric authentication methods.

> When we use biometric systems that will help to verify the users identity by physical biometrics such as fingerprint, palmprint, iris scans, and hand geometrics, Biometric system authentication can be more suitable than the traditional authentication systems because it is hard for most of the users to remember long passwords for various websites or carry all the smart cards the user needs (Debas, et al., 2023).

According to America's Cyber Defense Agency, strong passwords require at least 16 characters long, a string of mixed-case letters, numbers and symbols, and unique (Cybersecurity and Infrastructure Security Agency, n.d.). While this is the considered a strong password to the America's Cyber Defense Agency, most password requirements you'll encounter may only require 8 characters, numbers, and a symbol.

In addition to implementing authentication, user interface designers must adhere to secure coding practices to mitigate vulnerabilities and reduce the likelihood of exploitation by malicious actors. Secure coding encompasses principles such as input validation, output encoding, error handling, and secure communication protocols. By following secure coding practices, UI designers can minimize the risk of common web application vulnerabilities such as cross-site scripting (XSS), SQL injection, and insecure deserialization. Role-based access control (RBAC) and attribute-based access control (ABAC) are commonly used in UI design to manage user permissions and restrict unauthorized access to sensitive functionalities and data. UI designers must carefully implement access control mechanisms to ensure that only authorized users have access to specific features and data, thereby reducing the risk of insider threats and unauthorized data manipulation.

Psychology

Studying the human brain and behavior is a very complex subject, especially when mentioning the different factors that goes into how someone thinks. This is important for UI designers to understand because it directly impacts how users interact with security features and this is known as the User experience (UX). “UX design is a process that involves researching and analyzing the user and their behaviors in order to create an experience that helps to interact with the product” (Stadler, 2022).

Being a UX designer isn’t easy, research UX designers have to conduct requires them to learn more about the user which includes “the user’s lifestyle, habits, preferences, dislikes, anything else that distinguishes the user from the researcher, because if everyone were the same, there would be no need for research” (Stadler, 2022). This is essential to understand what the user needs are and this is done. This ties in with HCI as the user may focus more on security which surrenders usability, or if the user focuses on usability or convenience.

Now while learning about the user is mandatory, its also important to keep in mind how the people who conduct these cyber attacks on the users. One big and well known way these attacks occur is through what is known as clickjacking. “In a clickjacking attack, a malicious page is constructed such that it tricks victims into clicking on an element of a different page that is only barely (or not at all) visible” (Balduzzi, et al., 2010). For example, you could visit a fake website by entering the link in the URL incorrectly and you don’t realize. A big green popup that says “Play Game” appears, innocently, you press on it to visit the game. Little did you know, behind that “Play Game” button was an invisible iframe which could be anything from gaining control of your device to gaining information from your device.

Relevant questions using psychology that are useful for the UX designers and it’s users includes: What caused you to press on the button? What were the intentions of the attacker? Remember I mentioned it was a “big green popup”, according to Wen, “colors with higher lightness are often used in the interface to match the light background, prompting the user to click or continue browsing” (2021). This proves that the color of the UI is a factor designing UIs and more importantly catering to the UX. Unfortunately, in this case, this is being used against the user by advertising the invisible iframe with a bright green button that says “Play Game”.

Common Ground

Each discipline used: HCI, Information Security, and Psychology, bring their own unique aspects to what the key cybersecurity measures should be taken when designing UI. HCI focuses on making sure that the UI is comfortable for all levels of usage by it’s users. Meaning this wouldn’t focus solely on the security aspect of a UI, but explains the importance of taking the user’s skills into consideration to promote compliance with security. Information Security is where we get to the more technical side which focuses on the security needs of a UI instead of the user’s needs. Authentication and passwords are the most important aspects of information security as this is what will safeguard your information. Psychology helps explain user behavior. It explains what people interact with, why they interact with it, and how they interact with it. This is helpful so that the UX is positive and easier to abide by the security. Although this can be used against the user if they are unaware of the websites they are visiting.

Disciplinary Conflicts

Constructing a More Comprehensive Understanding or Theory

You gain a holistic solution to the challenges of cybersecurity in UI designing when combining each of the theories used. Each discipline brings its own aspects which fills any issues any UI designer could approach. With the disciplines used, you gain psychological insights, balance security and usability, understand the importance and success of MFA and learn how to balance each with each other.

In order to construct a more comprehensive understanding on the topic, it is important to identify each of the disciplines used and determine what's best based on the user. For example, if a UI design required a user to have a long password with numbers and symbols, MFA activation, phone number and email verification, this is an example of focusing solely on information security which could lead to non-compliance of the user, ultimately causing a vulnerability for the user. Same could be said if the UI is very simplistic with little to no security protocols, it ultimately makes the user vulnerable to cyber-attacks.

Reflecting on, Testing, and Communicating the Understanding or Theory

The theory in which this research is built on is that an effective UI must balance security and usability by using the principles from HCI, information security, and psychology. Reflecting on this, the research emphasizes that understanding user behavior (psychology), ensuring interface usability (HCI), and implementing different security measures including using MFA, password recommendations, and authentication methods (information security) are all critical components. For example, safe authentication solutions must be both effective in protecting user data and simple for users to comprehend and apply.

To test this theory, I asked a group of people to rate the UI of a popular website known as Twitch, if 1. the security features were clearly integrated, 2. if they had a good UX, and 3. if they felt safe putting their information in the website. Although the testing size was small, they are vary from age, usability of the website, and understanding of cybersecurity in UI. Twitch's login UI includes your username and password, and once you sign in, you are required to set up a two-factor authentication (2FA) and MFA whether you use another email, include a phone number, or use backup codes. Majority of the group agreed that the UI was clearly integrated and that they felt good about the website having their information, but they all said they did not have a good UX. Their response was "it was too much to just access the website". In other words, I found that requiring multiple security protocols is not the best way to secure a UI. Rather taking into account what the user is willing to do to secure their information is more important in this circumstance. By using the different disciplines, this is achieved.

While the focus of cybersecurity measures in UI design often revolves around technical and user behavior aspects, user training and awareness are equally important in mitigating security risks. UI designers should consider incorporating intuitive and informative security prompts, notifications, and educational materials within the UI to guide users on best security practices. Moreover, the design of UI should aim to promote a security-conscious mindset among users, encouraging them to exercise caution when sharing sensitive information and interacting with the system. This also includes complying with industry standards and regulatory requirements. Non-compliance can result in severe consequences, including financial penalties and reputational damage.

Conclusion

In conclusion, cybersecurity measures in UI design are not an easy task to take on. Creating UIs are multifaceted and requires you to consider multiple aspects including: authentication, user's needs, security needs, and the user's behaviors towards increased security protocols. By balancing each of these aspects, the question of "what are the key cybersecurity measures?" is answered as you are able to effectively cater to UX as well as maintaining a secure site. It's important to note that attackers are finding new techniques to attack users at a rapid rate therefore requiring new ways to defend against them.

References

Choudhary, A. R. (2023). Enhancing cybersecurity using a new dynamic approach to authentication and authorization. *Issues in Information Systems*, *24*(2).

Bishop, L. M., Morgan, P. L., Asquith, P. M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020, July). Examining human individual differences in cyber security and possible implications for human-machine interface design. In *International Conference on Human-computer Interaction* (pp. 51-66). Cham: Springer International Publishing.

Cybersecurity and Infrastructure Security Agency. (n.d.). Require strong passwords. U.S. Department of Homeland Security. https://www.cisa.gov/secure-our-world/require-strong-passwords

E. A. Debas, R. S. Alajlan and M. M. Hafizur Rahman, "Biometric in Cyber Security: A Mini Review," *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Bali, Indonesia, 2023, pp. 570-574, doi: 10.1109/ICAIIC57133.2023.10067017.

G. Wen, "Research on Color Design Principles of UI Interface of Mobile Applications Based on Vision," *2021 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, Dalian, China, 2021, pp. 539-542, doi: 10.1109/AEECA52519.2021.9574226.

Iftikhar, W., Malik, M. S. A., Tariq, S., Sultan, M. S., Ahmad, J., & Shareef, F. (2018). User Interface Design Issues In HCI. *International journal of computer science and network security*, *18*(8), 153-157.

Stadler, A. (1970, January 1). How psychology can be used to influence user behaviour in UI and UX Design. Theseus. https://www.theseus.fi/handle/10024/751168