USER EXPERIENCE DESIGN IN CLOUD-BASED NETWORKING SOFTWARE ONBOARDING

ANALYSIS OF FACTORS LEADING TO THE FACEBOOK DATA BREACH IN 2021

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 Systems Engineering

By
Mackenzie Nguyen

December 9, 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

Benjamin Laugelli, Department of Engineering and Society

Gregory Gerling, Department of Engineering Systems and Environment

Introduction

Cybersecurity and the protection of personal data on the internet is an important concept to be taken seriously in any situation. The amount of data breaches in the recent years has increased to as much as 68% each year and there is no reason to foresee a decline in the near future with the steady emergence of cutting-edge technology (Fowler, 2022). When implementing software or new features into a system, the set up and maintenance of it is crucial to maximize the value and capabilities of the system (Couey, 2021). More specifically, it is just as important to follow user experience design principles when designing software setup instructions as it is to have the system in place to combat security threats and hackers.

In my technical project, my capstone team and I will improve on the current onboarding design for a cloud-based networking system by creating a more efficient and understandable navigation for users to successfully automate their network. With this redesign, there will be confirmation provided to indicate setup was done correctly and securely which will reduce the likelihood of cybersecurity threats. For my STS project, I will explore the Facebook data breach of 2021 and the different factors that contributed to it such as the individuals in charge of creating the flawed features against the hackers.

With this research, I will gain a stronger understanding of the roles these opposing actors have against and for each other. In executing a technical project along with support from my STS research, I will better understand the external and internal factors that lead to data breaches in an overall attempt to reduce the likelihood of cybersecurity threats for all. Protecting user data and security is a sociotechnical concept that requires attention from both technical and social sides. In the following, the technical project findings combined with the STS project research will provide data to support and address ways to better protect user data on the internet.

Technical Project Proposal

Cloud-based networking is a type of IT infrastructure implemented into an organization and used to support network capabilities such as hosting data to be centrally located in the cloud (Lee 2014). It is more important to focus on the setup and implementation of software to ensure it is done correctly and accurately rather than focusing on using the software itself (completesol_admin, 2021). For that reason, my technical project consists of a complete redesign of the onboarding system for a cloud-based networking software. The overall goal is to optimize a user's onboarding experience with an improved and organized workflow. The end result will be a platform that is simple and guided enough for any typical user to follow and successfully set up the software. In order to address the lack of a clear onboarding process, the organization that provides the software service has been working on creating a visual user's journey map to outline and diagram the actions a user takes to setup the software. In the diagram, key actions are defined along with sub-steps, challenges, and desired outcomes. From this diagram, we can identify gaps that indicate there is a lack of guidance and mapping for certain actions/tasks.

Setting up this networking software is a complicated process for novice users as it requires precise technical expertise that prevents them from fully understanding and implementing the product to its full potential. The main issues with the current design arise from a lack of feedback to confirm the setup was successful, an unclear workflow around navigating through tasks, and the inability to benefit from all the features the product offers. In general, users have no way of knowing if they have set it up correctly which results in a lack of security and data protection. Without improvements to the current onboarding process, the organization providing this service will lack competitiveness in the market for networking support if they are

unable to provide a product that fits their clients' needs with ease. With a redesign, customers will be more inclined to use their product across more of their organizations and recommend it to other organizations as well. Furthermore, it is extremely important for information and data to be secure or else there is a high risk for cyber threats.

A complete redesign of the current onboarding system must occur to ensure a secure and successful networking system implementation. The improved system will promote a personalized setup where users are guided into completing the various tasks necessary to configure the system in a strategic yet straightforward method. In turn, this will create a more efficient and easier way to understand navigation flow without overlooking and/or misusing impactful features. With our main focus to explore and improve user experience of the product, we will be using human machine interface concepts along with user interface design principles. In doing so, we will see how the system can best be redesigned in order to suit the specific needs and abilities of the user. This project will be completed over the course of 2 semesters in SYS 4053 and SYS 4054 in a team of six students. While collecting data, we will not only speak with professionals who are experts in the onboarding process, but also conduct user interviews to gain the perspective from both ends of the technical expertise spectrum. Through exploring the current onboarding process that a user must follow, we will be able to identify gaps in our solution.

STS Project Proposal

Without a doubt, Facebook is the largest and most popular social networking site at the moment. In gaining traction throughout the past several years, Facebook fell vulnerable to data breaches and security threats with the vast amount of data they have access to. In April 2021,

Facebook suffered from one of its largest data breaches where private information from 533 million Facebook users was posted to a public online forum (Ghosh, 2021). The data included full names, emails addresses, phone number, date of birth, and other personal identifiable information Facebook had access to (Ghosh, 2021). The hackers obtained this confidential data by exploiting a feature on Facebook that allowed users to import contacts to find friends (Newman, 2021). Some might argue the Facebook data breach occurred because Facebook lacked proper security and prevention methods in order to identify, if not prevent, it from occurring in the first place. The source of the data breach came from a bug in the code that was easy to hack (Newman, 2021). Facebook diverted blame to the hackers and malicious actors instead of admitting their mistakes. (Haskell-Dowland, 2021).

The media puts the spotlight and blame on the hackers; however, it is just as important to consider and analyze other actions in this situation such as those that built the software that was weak enough to fall victim to a data breach in the first place (Carr, 2020). This factor is commonly overlooked as we are quick to blame the individuals who took action rather than those behind the scenes who brought the software into existence to be tampered with. There exists no regulation or federal law requiring organizations that collect personal information through the internet to ensure the security of the data is protected (Linebaugh, 2018). However, these internet companies have an obligation under FTC federal consumer protection laws to not engage in "unfair or deceptive acts or practices" (Linebaugh, 2018). Without addressing this major data breach, Facebook faces serious legal obligations to notify affected individuals, which they failed to do so under justification that the information leaked was not extremely sensitive (Bowman, 2021).

I will use Actor-Network Theory (ANT) to analyze the factors that led to the Facebook data breach of 2021. I propose the data breach happened on account of the hackers' malicious intent along with the poor development of one of Facebook's features that allowed hackers to get access to private user data. In order to get to the root of the problem, I will look at the intent and actions of the ones developing the feature that was hacked into instead of just solely at the hackers. Using this concept, I will investigate the Facebook data breach to identify preventative measures that can be taken when setting up and implementing software in the first place. ANT focuses on a technology network formed by network builders made up of both non-human and human actors with a common goal in mind (Cressman, 2009). Specifically, I will identify and analyze technical and social actors as they have the most prominent influence and presence in the Facebook data breach. I will utilize media articles to view the incident in different perspectives along with academic articles and sources that analyze data breaches and the factors that contribute to them. I will examine sources specifically about the Facebook data breach of 2021 along with other major data breaches that have occurred throughout history to find differing external factors that contributed specifically to the Facebook incident.

Conclusion

The challenge of cybersecurity and data protection can be addressed after engaging in my technical project and diving into research with my STS project. In the technical project, my team and I will produce a user journey map, low-fidelity prototype, and high-fidelity prototype that will be presented to the client throughout the fall semester and will be iterated upon after feedback from the client. The prototypes will be presented as wireframes along with a simulation that enables customers to verify their setup and ensure it will work as intended. Overall it will

result in a combined end-to-end setup and verification experience for the solution. Research conducted through my STS project will result in a stronger understanding about the social and technical factors that led to the Facebook data breach of 2021.

In identifying how users behave and respond to the current onboarding process and protocols to implement cloud-based networking into their system, we can work to address and identify these gaps and areas of improvement that can be made to the design. The technical project will work to validate that the software is setup correctly so that the system and organization's information is secure. On the other hand, the STS project focuses more on identifying external factors that lead to cyber threats which will consequently guide us into determining how to prevent them.

References

Bowman, E. (2021, April 9). *After data breach exposes 530 million, Facebook says it will not notify users.* NPR. https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users

Carr, R. (2017, October 11). *Data breach accountability and responsibility: Who gets blamed for data breaches?* Zettaset. https://www.zettaset.com/blog/data-breach-accountability-and-responsibility-who-gets-blamed-data-breaches/

Cressman, D. (2009, April). *A brief overview of Actor-Network Theory: Punctualization, heterogeneous engineering & translation*. https://summit.sfu.ca/item/13593

completesol_admin. (2021, September 6). *Why software installation services are so important.* Completesol. https://www.completesol.com/blog/2021/09/06/why-software-installation-services-are-so-important/

Couey, C. (2021, April 23). *5 Critical steps for your software implementation plan.* Software Advice. https://www.softwareadvice.com/resources/software-implementation-plan/#:~:text=Proper%20implementation%20will%20maximize%20the,risking%20lost%20time%20and%20money

Fowler, B. (2022, January 24). *Data breaches break record in 2021.* CNET. https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/

Ghosh, S. (2021, April 5). How Facebook's recent data breach affect its users. *The Hindu.* https://www.thehindu.com/sci-tech/technology/internet/explainer-how-facebooks-recent-data-breach-affect-its-users/article34324019.ece

Haskell-Dowland, P. (2021, April 6). *Facebook data breach: what happened and why it's hard to know if your data was leaked.* The Conversation. https://theconversation.com/facebook-data-breach-what-happened-and-why-its-hard-to-know-if-your-data-was-leaked-158417

Lee, G. (2014). *Cloud networking: understanding cloud-based data center networks.* Elsevier. https://learning.oreilly.com/library/view/cloud-networking/9780128007280/B9780128007280000011.xhtml

Linebaugh, C. D. (2018, October 25). *What legal obligations do internet companies have to prevent and respond to a data breach?* Congressional Research Service. https://crsreports.congress.gov/product/pdf/LSB/LSB10210/2

Newman, L. H. (2021, April 6). What really caused facebook's 500m-user data leak? *WIRED.* https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/