Creating a password authentication protocol that protects user data even during server compromise

Improving the efficacy of employee cybersecurity awareness training

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
Maven Kim

October 27, 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

Kent Wayland, Department of Engineering and Society

Shangtong Zhang, Department of Computer Science

General Research Problem: Combating the Human Factor in Cybersecurity

How can the human error element of cybersecurity be mitigated to alleviate the severity and frequency of cybersecurity breaches?

The internet controls society. Due to the advent of COVID-19 and social distancing, almost every company, government, and school has incorporated the internet into their infrastructure in some way. It has revolutionized the way we interact and work and has massively benefitted the world, but it is also a source of vulnerability and weakness. Hackers can exploit security flaws in institutional network infrastructure and steal the data of millions of people. They can sell data, hold it ransom, and steal people's identities or bank account information for immense financial gain. In 2022, internet crime victims lost 4.2 billion dollars to cybersecurity breaches, which are estimate to occur every 44 seconds. The general public is beginning to understand the severity of these cyber-attacks, with 78% of consumers worldwide expressing concern about the privacy of their data (Norton, 2021).

Even though a growing number of people are worried about the threat of being hacked, they still may not necessarily follow the best cybersecurity practices, or may simply not be concerned enough to take action. For example, a survey by LastPass showed that although 91% of people know that reusing passwords is a security risk, two in three people still use the same passwords across multiple accounts. Additionally, 42% of people say that "a password that's easy to remember is more important than one that is very secure." Considering that around 82% of data breaches that occurred in 2021 were due to some form of human error, human nature and the human factor must be taken into account when it comes to cybersecurity (Verizon, 2021).

In order to mitigate the human element in cybersecurity, I propose two projects. For my technical project, I implemented an asymmetric password authenticated key exchange protocol called OPAQUE during my internship at Amazon over the summer. For my STS research project, I will analyze and determine what can be done to improve consumer cybersecurity awareness.

Technical Topic: Creating a password authentication protocol that protects user data even during server compromise

How can a password authentication protocol be built to maximize protection of customer data while considering customer convenience?

During my summer internship at Amazon, I worked with the AWS Cryptography team on the Nitro Enclaves OPAQUE project (NEO). I implemented a password authenticated key exchange protocol called OPAQUE using Amazon Web Services' (AWS) Nitro Enclaves. This project was conceptualized when Amazon Ring reached out to the AWS Cryptography team. Amazon Ring is a home security company known for its unique video doorbell, which allows users to remotely use security cameras and other smart devices through their phones. Ring encrypts and stores the video footage from these devices on AWS servers. It is very important for Ring to not only ensure that the data is cryptographically secure, but also ensure that customers can trust the security of their cryptographic systems.

On January 13, 2021, Ring announced that it would be providing opt-in end-to-end encryption (E2EE) for its customers. With E2EE, only the user has the cryptographic key that can be used to decrypt and access the video recorded by his or her devices, meaning Ring would have no way of accessing these user data. However, an issue with the current protocol is that it

relies on randomly generated 10-word passwords, which are needed to guarantee the security of the system (Ring, 2021). Remembering these long passwords is very inconvenient, and most customers prefer to use passwords that are much weaker but easier to remember. In fact, some of the most frequently used passwords worldwide include 123456 and the word "password" itself (Stouffer, 2021). Thus, this project attempts to maximize both customer convenience and security by taking the onus of protecting user data from the consumer. Only the customer should have access to the video data, but they shouldn't have to remember or write down a 10-word password to do so.

My project used Nitro Enclaves, which are isolated computing environments almost completely separated from the Internet that can only communicate with outside services through specified channels. These enclaves combined with the OPAQUE protocol provides forward secrecy and hides passwords from the server during both registration and authentication. Thus, even if the server were to be compromised, either by a hacker or a malicious actor from within the company, they would not be able to steal any user data. OPAQUE is also capable of safely encrypting user data with an export key generated by the protocol, which is only known by the client. This protocol would provide all of the benefits of E2EE without the hassle of remembering a 10-word password.

To build NEO, I first needed to conduct background research on the OPAQUE protocol, as well as learn how to create code that can interact with AWS applications and Nitro Enclaves. After my onboarding, I designed the client and the server that would be communicate using OPAQUE. Specifically, I drew diagrams mapping out what information would be passed between the client and the server during registration and authentication. I then used a template

Nitro Enclaves application as well as the information I learned from my onboarding to code my design in Python.

The project I built over the summer only involved a single server communicating with a single client. In order for OPAQUE to be usable by a company like Ring, the scale of my project must be increased and many NEO servers would be needed, and parallelization would be needed so that many users could authenticate at the same time. However, the scope of this would simply be too great for an internship project, and it would not be possible to accomplish this given the timeframe of my internship. To ensure my code could be further developed by other software engineers, I uploaded it to Amazon's codebase with detailed documentation of its functionality. I also created a script that set up the necessary software and automatically ran the OPAQUE registration and authentication server.

STS Topic: Improving the efficacy of employee cybersecurity awareness training

How can we better educate employees about cybersecurity threats and prevent bad behavioral practices that lead to cybersecurity breaches?

Although OPAQUE maximizes security without compromising on customer convenience, it cannot protect user data when passwords are stolen or credentials are leaked. Cybersecurity threats can not only be targeted at the security systems built by companies, but also at the people who work there. Hackers, for example, can send seemingly innocuous emails to employees, called phishing emails, that can trick them into providing their credentials. These types of attacks, called social engineering attacks, are surprisingly effective. Data collected from

a phishing simulation tool created by Proofpoint, a security company, showed a 20% failure rate for phishing scams that involved email attachments (Proofpoint, 2022).

Some companies have taken steps to educate their employees regarding these issues. They have integrated cybersecurity awareness training in some fashion, whether it be through the onboarding process or simply requiring employees to complete the training. However, these trainings can easily end up being ineffective. Employees simply may not value the training to be worthwhile, or may think it is boring or a waste of time. Additionally, if the training is infrequent or a requirement that can be completed relatively quickly, the information may not be absorbed.

In a study conducted by Back and Guerette (2021), the researchers tested whether cybersecurity education would increase or decrease the likelihood of university employees "falling for" a phishing email. Surprisingly, they found that employees who received the education were moderately more likely to click the fake link in the email than those in the control group.

Even if employees are aware of the importance of good cybersecurity workplace practices, this may not necessarily lead to sustainable behavioral outcomes. An article by Alshaikh and Adamson (2021) states that basic cybersecurity awareness training only drives short term change, and doesn't result in any sustainable behavioral differences in employees. In fact, they found that over half of cybersecurity breaches are caused by an employee not complying with the policies created to increase awareness. The authors argue that a more holistic approach is necessary, one that directly targets the attitudes and beliefs of the employees instead of simply providing information. To do this, a cybersecurity culture must be built, so that employees can internalize what they have learned.

An article by Cheng and Wang (2022) illustrates steps that companies can take to create a culture of cybersecurity. The authors state that the security policy of company must be tailored to particular role that each employee has within in a company. For example, a manager must have a stricter cybersecurity training than a lower ranked employee, since he or she is more likely to handle a higher volume of more sensitive information. Companies should also make awareness trainings human-centric and require employees to sign an acknowledgement stating that they truly understand the importance of the information they were taught. These trainings must also be frequent and readily accessible.

Although the literature has established a need for a culture of cybersecurity, the specific protocols and information taught to employees is not well established in literature. To further investigate how a culture of cybersecurity can be established, I will interview employees from a variety of different companies, such as tech companies and even those employed to UVA. These interviews will help me understand the type of cybersecurity culture, or lack thereof, in a variety of different companies, as well as the type of cybersecurity awareness training these companies employ. I will analyze how these different protocols influenced the behavior of the interviewees. I will also use the Internet to find blog posts about employers incorporating cybersecurity awareness training, and learn about the results they had.

Conclusion

From my STS research topic, I hope to better understand how people's behavior can be influenced through cybersecurity awareness training. This is an important subject because although people can be taught and know the importance of cybersecurity, they still may not take the necessary steps to ensure the security of the data they interact with. Additionally,

cryptographic protocols, such as OPAQUE, can only do so much to limit the human element in cybersecurity. Thus, alleviating human error through the lens of changing human behavior is a potential way to most effectively mitigate cybersecurity breaches.

References

2021 NORTON CYBER SAFETY INSIGHTS REPORT GLOBAL RESULTS. Norton. (2021, May). Retrieved October 28, 2022, from https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing, 25*(5), 829–841. https://doi.org/10.1007/s00779-021-01551-2

Back, S., & Guerette, R. T. (2021). Cyber Place Management and Crime Prevention: The Effectiveness of cybersecurity awareness training against phishing attacks. *Journal of Contemporary Criminal Justice,* 104398622110016. https://doi.org/10.1177/10439862211001628

Cheng, E. C. K., & Wang, T. (2022). Institutional strategies for cybersecurity in Higher Education Institutions. *Information, 13*(4), 192. https://doi.org/10.3390/info13040192

DBIR report 2022 - summary of findings. Verizon Business. (2022). Retrieved October 27, 2022, from https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

Proofpoint. (2022). *Enterprise cybersecurity solutions, services & training | Proofpoint US*. Retrieved October 28, 2022, from https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf

Psychology of passwords: How to password hygiene reduces your password security risk. LastPass. (2020). Retrieved October 27, 2022, from https://www.lastpass.com/resources/ebook/psychology-of-passwords-2020

Ring. (2021, July 13). *Ring encryption whitepaper 2021-07-13 - assets.ctfassets.net*. Retrieved October 28, 2022, from https://assets.ctfassets.net/a3peezndovsu/5ihit68yvJLf0IJ2dOHfuO/b9063f50382bbf3e143173bbf49e9781/Ring_Encryption_Whitepaper_2021-07-13.pdf

Stouffer, C. (2021, December 8). *Password security: How to create strong passwords in 5 steps*. Norton. Retrieved October 27, 2022, from https://us.norton.com/blog/privacy/password-security

Stouffer, C. (2022, September 1). *115 cybersecurity statistics + trends to know in 2023*. Norton. Retrieved October 27, 2022, from https://us.norton.com/blog/emerging-threats/cybersecurity-statistics