HUMAN FACTORS IN CYBERSECURITY: A USABILITY APPROACH TO THE AUTHENTICATION PROBLEM

Introduction

While the term ‘cybersecurity’ may conjure up an image of security technicians frantically typing on a keyboard trying to fend off a sophisticated computer virus, we must not forget the importance that everyday people have on securing computer systems. In fact, the number one cause for data breaches are weak and stolen credentials [6]. More than 50% of ransomware attacks originate through “user-initiated actions such as clicking on a malicious link […] or visiting a compromised website” [2]. Clearly, the ways in which users interact with a system are as important in protecting it as the technical safeguards put in place. What’s the point of installing a firewall or utilizing encryption if an employee leaves his password written down and in plain view? While technical vulnerabilities should be addressed, companies also need to understand the way their employees affect the security ecosystem. This is especially true for the authentication problem: verifying the identity of a user trying to access an information system.

Possible Solutions

There are many approaches to improving the cyber hygiene of non-technical employees. These include security training, enforcing security policies, or fostering a security culture such as by encouraging a zero-trust model. However, many of these approaches have their limitations. Too much security awareness training may actually be counterproductive. Training bombardment, desensitization, and over-simulation can make users feel overconfident about their ability to discern phishing emails [12]. While training can provide knowledge, it may not

necessarily translate to behavior unless people are nudged in the right direction [4]. A 2016 study by NIST found that fatigue related to users' security decisions led to "a sense of resignation, loss of control, fatalism, risk minimization, and decision avoidance" [1]. Overexposure to technical terminology, security icons embedded in interfaces, and safety tools can lead to "security fatigue" [1]. For example, the term 'multi-factor authentication' may seem daunting to a novice user who doesn't fully appreciate the importance of such a fundamental protection mechanism. Users may also develop a perception about security being a built-in feature of a system and neglect safety practices, thus leading to learned helplessness.

There is, however, a superior approach that circumvents fatiguing decision making and costly security training programs. Good usability can be leveraged for "seamless protection while enhancing user experience" [10]. Security solutions that involve usable user interfaces can help reduce the number of unsafe ways a system can be used by making it easy to do the right thing. There is a common misconception that security and usability come at a tradeoff [10]. However, when done correctly, users can achieve security goals with little to no interface friction. For instance, one-tap push notifications are much faster and less tedious at solving the problem of multi-factor authentication than one-time password algorithms where the user needs to input a six digit password within a 30 second time window. The purpose of this paper is to make a case for usability as the most efficient way of tackling the authentication problem.

Usability in Authentication

Broadly speaking, there are four authentication areas where usability can be used to improve security: password management, multi-factor authentication, secondary authentication

mechanisms for reestablishing access, and mobile and biometric authentication. While each of these areas could be addressed through employee training or password policies, a usability approach will be most efficient at increasing security while not hindering the user experience.

Password Policies: Usernames and passwords have historically been the traditional method for authentication. However, as people need to remember more and more passwords, users reusing, sharing, or choosing weak passwords become real concerns. It's important to not underestimate the insecure workarounds users will find to avoid password management [9]. While company policy may require employees to choose a password that is, for example, 8-16 characters long and includes one upper case letter, a number, and a special character, these passwords are not easy to remember and only incentivize users to write them down. Forcing employees to change their passwords every couple of months encourages them to choose a slight variation of their old password. Instead of using training or policies to achieve higher password security, companies should instead adopt a usability approach. One such avenue is the use of password managers. These tools allow users to store all of their passwords in an encrypted database whose key is the only piece of information employees need to memorize. Password managers allow users to select secure machine-generated passwords while reducing the likelihood of relying on insecure workarounds [9]. Password managers can also provide users with a sense of password strength, help automatically reset passwords, and help users autofill passwords across different platforms. It's typically faster for someone to copy-paste a password from a password manager than it is to type it out in full. As long as incorporating a password manager into the security strategy is easier for users than any alternative, it will prove more efficient at elevating authentication security.

Multi-Factor Authentication (MFA): When evaluating the effectiveness of MFA, there are several factors to consider. These include login time, setup difficulty, perceived increased in security, and availability of the second factor [5]. While pre-generated codes and time-based one-time passwords (TOTP) are easy to set up, they have longer login times. Security keys require users to have access to a physical USB device for authentication. Pre-generated codes don't provide a sense of increased security since they are oftentimes seen as just a second password that can also be guessed [5]. On the other hand, push notifications for approving or denying login attempts are easy to set up, have fast login times, and rely on smart phone devices which most users have regular access to. Furthermore, MFA Push apps typically have a 'Remember Me' option that requires the second factor only be used to validate login attempts once for a limited amount of time. Considering the pros and cons of all these options, a company may require its employees enroll in some method of MFA. Nevertheless, company policies and training may be insufficient to ensure the selected method is adequately used. If employees leave a list of pre-generated codes or their security key next to their desk for convenience, unauthorized logins are more likely. However, the usability-focused approach of Push apps reduces the difficulty of MFA while naturally incentivizing users to use it correctly. This is because most people have their phones on them at all times. Either way, the usable approach is the most efficient one.

Secondary Authentication Mechanisms: When a user forgets his login credentials, the conventional way of resetting a password has been by answering security questions. These questions typically need to be memorable, consistent, confidential, and specific. However, they are easy targets for social engineering, and provide less security than one might think. Security questions typically have a low recall rate by users and a higher-than-expected guess rate by

attackers. For example, an attacker has a 19.7% chance of guessing an English-speaker's answer to the question "What is your favorite food?", while the same user would only have a 22% success rate at recalling the answer to the question "What is your library card number?" [3]. This is due to the fact that easy-to-remember questions are less secure while hard-to-remember questions are not usable. An approach often taken by companies is to simply pile on more security questions in hopes that the user will be able to answer a certain number of them correctly. Unfortunately, this reduces both security and usability. Users may provide fake answers in order to adhere to strict system defined questions. Worse still would be to allow users to write their own questions. As such, NIST no longer recognizes security questions as a valid form of secondary authentication. [3] Users should instead resort to authentication methods that are just as strong as primary authentication mechanisms. This highlights the importance of strong MFA. It's worth noticing that approaching this issue from a usability standpoint quickly revealed why security questions are not a good idea.

Mobile and Biometric Authentication: Mobile devices pose a unique problem to authentication since users need to unlock them multiple times a day and typically in a kinetic context (e.g., while walking or distracted). Problems specific to mobile devices include typing a password on a small screen, not knowing what characters have been typed so far, dealing with small user interfaces, as well as various usability concerns for people with disabilities. Common solutions to these problems are using PINs instead of passwords, lock screen patterns, and biometric solutions such as fingerprint scanning or facial recognition [11]. However, many of these solutions are prone to spoofing attacks while only providing a similar or reduced level of security as compared to fully developed computer authentication mechanisms. This is inevitable but has typically been accepted given the physical constraints of mobile devices and biometric sensors.

In cases like these, usability may be the only way of increasing security. For example, using emails instead of usernames, automatically logging out inactive users, allowing logins through external accounts, and using a device's built-in authentication mechanisms are all ways of elevating security through good usability. No amount of employee training or company policies could establish natural incentives for typing a long password on a small keyboard or interacting with an interface designed for a computer on a smartphone. User-adaptive and usable approaches are most appropriate for mobile authentication.

Children as a Case Study for Usable Authentication

As our dependence on technology rises, a generation of children are growing up with computers being a part of their daily lives. This makes children a population worth investigating for authentication safety, practices, and perceptions. A 2021 study [8] showed that while children are aware of privacy, access, and safety being key properties of passwords, their knowledge didn't directly translate to safe behaviors. Many children started sharing and reusing passwords when they reached high school age, early symptoms of bad habits. While this study concludes with a "call for cybersecurity education" [8], improving usability through good user interfaces and password management would also help address these concerns. For instance, children reported incorporating personal information into their passwords. A usable approach to solving this would be to nudge users to select strong but memorable passwords during password creation instead of relying on complexity requirements. An interface that makes it easy for the user to choose a usable password would be more efficient at improving security than trying to reinforce positive behavior through technical understanding. This is particularly true for children, who may struggle to understand concepts such as 'password entropy' or 'dictionary attacks'. In fact,

children seem to think of passwords in terms of vague concepts like ‘information’, ‘safe’, and ‘stuff’ [8]. This mirrors, in a way, the way adult employees need to abstract security away from whatever task requires them to authenticate themselves. In much the same way that visiting a website doesn’t require the user to type an IP address or understand the DNS protocol, so too should users not be required to understand the intricacies of password creation and management for safe authentication. As previously mentioned, this could lead to security fatigue and information overload. Instead, a helpful password interface can achieve all the desired goals for both children and adults while following natural human behavior more closely. Yet again, the usable approach is demonstrably better.

Limitations

While usability is certainly an outstanding and effective way of improving authentication security, it does come with its drawbacks. Firstly, being able to design a usable system from scratch involves having direct access to the software being used as well as UI and UX designers and programmers. This may not always be feasible if third-party software is being used or if the costs of hiring such staff would make it prohibitively expensive. Nevertheless, its benefits should be realized to the fullest extent that resources permit. Additionally, software solutions don’t exist isolation and must be considered within the context they’re being used. A usability approach may be optimal for non-technical employees but may prove less efficient in the context of a cybersecurity firm run by security-aware professionals. The weakest-link principle must also be used when determining which improvement areas to prioritize. Investing in usable authentication may be worth the cost to a business who deals with thousands of customers who need to be authenticated but may not be as important to a business who deals with fewer users.

Conclusion

Efforts at improving security in the authentication space should be directed at usability. As demonstrated in this paper, this approach provides a high return on investment while achieving the same goals as other approaches (i.e., training, policy enforcement), oftentimes more effectively and with less burdensome side effects. As the section on secondary authentication mechanisms reveals, approaching a problem from a usability standpoint can reveal insights that would otherwise have been difficult to arrive to. Usability may sometimes be the only way of improving security as explored in the section on mobile authentication. The prevalence of passwords and the complex relationships people have with them is best addressed through usable approaches than by enforcing complexity requirements. This is all to say that usability provides a source of incentives that naturally align with the way we interact with computer systems. A large part of combating human factors in cybersecurity revolves around tilting the scales so that it's easier for people to adopt the more secure approach. It's time for companies and organizations to invest in usability and reconsider the ways their current authentication mechanisms are being promoted.

References

[1] B. Stanton, M. F. Theofanos, S. S. Prettyman and S. Furman, "Security Fatigue," in *IT Professional*, vol. 18, no. 5, pp. 26-32, Sept.-Oct. 2016, doi: 10.1109/MITP.2016.84. Available: https://ieeexplore.ieee.org/document/7579112.

[2] Center for Internet Security, “Ransomware: Facts, Threats, and Countermeasures”, *Center for Internet Security,* 2022. [Online]. Available: https://www.cisecurity.org/insights/blog/ransomware-facts-threats-and-countermeasures.

[3] E. Bursztein and I. Caron, “New Research: Some Tough Questions for ‘Security Questions’”, *Google Security Blog,* May 21, 2015. Available: https://security.googleblog.com/2015/05/new-research-some-tough-questions-for.html.

[4] J. Giddens, “Rethinking Communication in The Cybersecurity Space”, *Cyber Empathy,* October 18, 2022. Available: https://cyberempathy.org/episodes/rethinking-communication-in-the-cybersecurity-space.

[5] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, “A Usability Study of Five Two-Factor Authentication Methods”, *Brigham Young University,* August 12, 2019. Available: https://www.usenix.org/system/files/soups2019-reese.pdf.

[6] L. Irwin, “The 5 Most Common Causes of Data Breaches”, *IT Governance,* April 28, 2022. Available: https://www.itgovernance.eu/blog/en/the-most-common-causes-of-data-breaches-and-how-you-can-spot-them

[7] M. Theofanos and S. Pfleeger, "Guest Editors' Introduction: Shouldn't All Security Be Usable?" in IEEE Security & Privacy, vol. 9, no. 02, pp. 12-17, 2011. doi: 10.1109/MSP.2011.30. Available: https://www.computer.org/csdl/magazine/sp/2011/02/msp2011020012/13rRUxBa5lL.

[8] M. Theofanos, Y. Choong, and O. Murphy, “’Passwords Keep Me Safe’- Understanding What Children Think about Passwords”, *Usenix Association,* August 11, 2021. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/theofanos.

[9] National Centre Cybersecurity Centre, “Password Administration for System Owners”, *National Centre Cybersecurity Centre,* November 19, 2018. Available: https://www.ncsc.gov.uk/collection/passwords/password-manager-buyers-guide.

[10] P. Hesse, “Usability vs Security – The Myth That Keeps CISOs Up at Night”, *Tech Accord,* September 3, 2020. Available: https://cybertechaccord.org/usability-vs-security-the-myth-that-keeps-cisos-up-at-night/.

[11] P. Dmytro, V. Cherniakova, P. Kolesnichenko et al., “Behavior-Based User Authentication on Mobile Devices in Various Usage Contexts”, *EURASIP J. on Info. Security,* 2022. Available: https://doi.org/10.1186/s13635-022-00132-x.

[12] S. Poremba, “Your Security Awareness Training Isn’t Working”, *Techstrong,* October 11, 2022. Available: https://digitalcxo.com/article/your-security-awareness-training-isnt-working/.