Replacing Passwords for a More Secure World

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Matthew Beck

Spring 2024

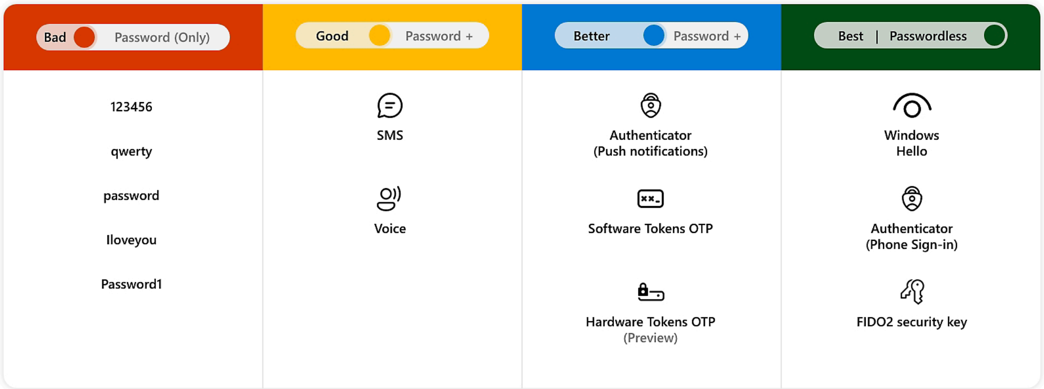
On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Caitlin D. Wylie, Department of Engineering and Society

Introduction

Microsoft's Digital Defense Report details how, in April 2023, there were approximately eleven thousand password attacks per second (Microsoft Defense Report 2023). Malicious actors can gain access to a user's sensitive information, such as their address and social security number when a password is stolen. Users tend to believe that their information is secure since the majority of web-based authentication systems make use of passwords. However, passwords are severely vulnerable to cyberattacks. In a survey commissioned by Forbes Advisor, the market research company, OnePoll, has found that forty-six percent of the two thousand Americans polled have had their password stolen in the past year (Haan, 2024). This is why an alternative to passwords is needed.



Bad Password (Only)	Good Password +	Better Password +	Best | Passwordless
123456	SMS	Authenticator (Push notifications)	Windows Hello
qwerty	Voice	Software Tokens OTP	Authenticator (Phone Sign-in)
password		Hardware Tokens OTP (Preview)	FIDO2 security key
lloveyou			
Password1			

Figure 1: Microsoft Diagram Comparing Authentication Methods

Applications have begun to shift away from passwords to increase the security level of their authentication system. Most authentication technologies deployed fall within the better password category of Figure 1. For example, the University of Virginia currently uses a push notification to a mobile device to authenticate an user's login. Popular authentication methods, such as the one being used by the University, are systems that are foundationally still password-based authentication systems. Therefore, they are still vulnerable to an array of attacks such as phishing and brute force attacks (Parmar et al., 2022). Ultimately, a shift towards passwordless authentication is necessary. Cyberark, an information security company, defines passwordless authentication as any method of authenticating the use of a technology system that does not require the user to input a text-based password or security questions (Cyberark, 2023). Passwordless authentication takes many different forms, such as hardware tokens or biometric methods such as facial, voice or retinal scanning. The different methods of passwordless authentication each have distinct advantages and disadvantages associated with them. However, the benefit of increased security is present in all of the methods. It is crucial to better understand the social factors that contribute to the deployment and use of authentication technologies to transition away from passwords.

The Unified Theory of Acceptance and Use of Technology (UTAUT) can be applied to better understand how a new authentication system can be deployed. UTAUT was published in 2003 in the MIS Quarterly and authored by four academics from different universities across the nation with a background of business and management. UTAUT describes four key determinants for the acceptance and use of technology: performance expectancy, effort expectancy, social expectancy, and facilitating expectancy (Venkatesh et al., 2003). The analysis provided in this paper speculates what a shift towards passwordless authentication may look like. The next sections of this paper explore each of the determinants, what stakeholders they affect, and how each expectancy can be met if a shift towards passwordless authentication were to occur. The end of the paper will examine a past shift in authentication systems to MFA, how the expectancy were or were not addressed, and what similarities and differences expected with a shift to passwordless authentication.

Performance Expectancy

The users of a new authentication system should believe that the technology will help them achieve their tasks and provide an improvement to their productivity. Performance expectancy is defined as, “the degree to which an individual believes that using the system will help him or her to attain gains in job performance” (Venkatesh et al., 2003, p. 447). This ranges from individuals believing that the system will make their job easier, increase their job performance, or result in themselves spending less time doing routine tasks. Analyzing each stakeholder group and how performance expectancy can be met for each group is important since replacing authentication will affect an array of different stakeholders.

Information technology (IT) leaders should believe that the use of a new authentication system will help them achieve their job of maintaining a security posture at their organization. Cybersecurity remains to be one of the largest challenges faced by IT decision makers (Dayton, 2021). These decision makers are more likely to implement a new authentication system if they view it as a way to help protect themselves and their organizations from future data breaches.

Next we should consider the developers of the technology itself and the applications that will make use of the technology. The developers need to believe that users will be able to be authenticated in a timely and safe manner by replacing passwords. Private information leaks are becoming more prominent as developers use private information during the development process in their day-to-day operations. Replacing passwords can help developers maintain a more secure posture allowing them to focus on their actual work and become more productive (Stiefel, 2023).

The users need to believe using this technology will help achieve their goals and job requirements. Ultimately, the user will spend less time authenticating themselves when they try to use the system. Additionally, users are less likely to be routinely rejected from being authenticated. Users are unable to make mistakes or forget their password when trying to authenticate themselves since there is no password that users need to remember.

Effort Expectancy

The amount of effort needed to use a new system should not be higher if the replacement of the existing password-based authentication systems is to be successful. Effort expectancy is defined as, "the degree of ease associated with the use of the system" (Venkatesh et al., 2003, p. 450). This can be how easy it is to learn how to use the system or interact with the system. In terms of replacing an authentication system, the effort may be higher, especially upon initial use, which becomes a barrier to replacing password systems. The IT management and the users of the technology must be examined when considering the effort expectancy of replacing the password-based authentication system.

The IT decision makers within organizations should believe that the use of an alternative to passwords will require little to no increase in the effort required. In terms of passwordless authentication systems, the cost-per-user of this system remains low and compatible with server and browser sides. Additionally, these systems are all well documented while remaining non-proprietary technology (Bonneau et al., 2012). This information leads to the belief that the implementation of a different authentication method will not require extensive effort. However, any significant change to a system that is used daily will have an increased amount of effort upon its initial use. This is a major drawback of any systematic change and replacing authentication systems will not be different. Effort expectancy can still be met even though there is an expected increase in effort, especially for the IT decision makers . IT decision makers are expected to be required to deploy a lower amount of effort in relation to the maintenance of non-password based systems. These teams will not have to deal with password resets when an user forgets their password and will be less likely to deal with security breaches of their organization's information systems.

Users should believe that it will not require an increase in effort to learn or to use a new authentication method. The key difference between passwords and passwordless authentication is that passwords rely on a knowledge-based secret that can be forgotten or stolen. Passwordless authentication can use the same key for different applications which removes the burden from the user of memorizing a different secret for each application. Subsequently, users have to take the time to recover their passwords if they forget them. Alternatives to passwords can eliminate this problem. Similar to that of the IT decision makers, it would be naive to think that upon the initial deployment of a new system that there would not be an increase in effort associated with the use of the system. However, effort expectancy can still be met as the effort related to using an alternative to passwords should require less effort in the long-term use of the system.

Overall, effort expectancy is a difficult determinant to identify when dealing with the replacement of authentication methods. The initial use of the system will require an increase in effort for both IT teams and users. However, this is the case for any change to a major IT system. The benefit in terms of effort expectancy for both stakeholders is derived from the long term use of the system.

Social Expectancy

Social expectancy is crucial to understand in order to deploy a new authentication system successfully. Social expectancy is defined as, "the degree to which an individual perceives that important others believe he or she should use the new system" (Venkatesh et al., 2003, p. 451). The social influence deals with if family, friends, co-workers or senior management believe that you should be using this system. According to Venkatesh et al. (2003), the leading factor in social influence, in relation to the acceptance and use of technology, is subjective norms. Subjective norms relate to the opinions of others about a certain individual or system. Venkatesh et al. (2003) believes that people are more likely to accept and use a technology if their peers believe that they should be using the technology and will judge them if they do not use the technology. However, this is not the only thought when it comes to social influence revolving around technology. In *Social influence on technology acceptance behavior: self-identity theory perspective* (Younghwa et al., 2006), the authors conducted a study finding that self-identity plays a larger role within the influence of an individual to use a technology when compared to subjective norms. Both academic papers were written before the explosion of social media, which is a crucial component to factor in when considering the next generation of technology users. It is necessary to consider the roles that both subjective norms and self-identity play when considering the acceptance and use of technology. It is imperative to consider the different stakeholders that are affected by replacing an authentication system in terms of social expectancy in addition to considering the roles of both subjective norms and self-identity .

Subjective norms and self-identity have an interdependent relationship where the self-identity of one stakeholder can increase the influence of subjective norms in another group. The first group to consider are the IT management teams. It is paramount that the social expectancy is thoroughly understood for the IT management teams, since they will be at the forefront of deciding whether or not a new authentication system is deployed. Self-identity can play a major role for this stakeholder as many of these decision makers' self-identity is committed to making the best decision, not only for themselves, but also their entire organization. If the decision makers believe that the performance expectancy and effort expectancy are satisfied in replacing their authentication system, they will be more likely to implement it as a way to fulfill their self-identity. The self-identity aspect of social expectancy has direct ties with the former two determinants discussed. Subjective norms can also begin to play a role once the self-identity aspect is reached. When dealing with the technology industry, the organization will want to be at the forefront of the technology. If IT decision makers see other leading organizations begin to implement a new authentication system, they will begin to feel the need to implement the technology themselves. One way to think about this relationship is to consider the top technology organizations. If the IT leaders at Apple decide that it is in their best interest to implement a new authentication system, then they may do so. Google may see that Apple has deployed a new authentication system and begin to question whether they should implement a new authentication system. If both Apple and Google then implement a new system, Microsoft will likely decide to implement a new system themselves to ensure that they are not falling behind their competitors. It is important to consider the IT decision makers as a stakeholder, as they will ultimately be the ones to decide whether or not the system is deployed within their organizations. However, it is also imperative to consider the actual users of the system and how social expectations can be met.

The users of the authentication systems are another stakeholder that are influenced by self-identity and social norms. The self-identity of the users are similar to that of the IT decision makers. The users will most likely believe that it is in their self-interest to use the system if they believe that the performance expectancy and effort expectancy of a new authentication system are met. Subjective norms play a larger role for users. The user will likely feel social pressure and begin to use an alternate system to passwords if their co-workers begin to use an alternative.

Facilitating Expectancy

Facilitating expectancy is a crucial aspect of implementing a new authentication system. Following the Unified Theory of Acceptance and Use of Technology, facilitating expectancy is the final determinant to be examined. Facilitating expectancy is defined as, "the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system" (Venkatesh et al., 2003, p. 453). The determinant is about believing the resources and knowledge are readily available to use the system. Venkatesh et al. (2003) examine facilitating expectancy and its relationship with the determinant of effort expectancy. Organizational structure and support should be in place for users when a system is deployed to achieve facilitating expectancy. It is important to consider effort expectancy when seeking to achieve facilitating expectancy. It is clear through examining the relationship between facilitating and effort expectancy, that if effort expectancy is not met, facilitating expectancy cannot be met. The users should believe that a minimal increase of effort is required to use the new system for effort expectancy to be achieved . This does not forgo the continued need for support from developers of the technology and the users' management team where if the users encounter any issues with the new technology, training and advice will be provided in a quick and simple manner that maintains a low effort expectancy of the users.

There is a hierarchy of need when considering the stakeholders for facilitating expectancy. The direct users of the technology are the focus, as they will need facilitating support from not only their management team, but also the developers of the technology. The management team should have facilitated support and training from the developers of the technology for them to provide proper support to their employees. It is imperative for the developers of the technology to provide the support needed to both the direct users and the management teams involved.

The users are limited in their need to provide facilitating support with facilitating support rooted in management teams and the developers of the authentication technology. One example of users providing facilitating support that may prove fruitful is aiding their co-workers and colleagues with the use of the technology. There exists extensive literature surrounding the benefits of peer education. In an academic paper by Velez et al. (2011) published within the Journal of Agricultural Education, they detailed the role that peer instruction plays in increasing a student's engagement and the effectiveness of learning from someone without authority over oneself. This paper, like other peer instruction literature, focuses on classroom spaces and the relationships between classmates and the teacher with the students. This idea may be extended to workplaces and other settings where authentication systems are deployed. The burden placed upon the management groups and developers decreases with users supplying facilitating support to other users. The management teams and developers must still provide support to the users for them to be comfortable in assisting others.

The organizational structure will play a crucial role in the feasibility of the implementation when a new authentication system is deployed. It is important for organizations to provide facilitating support to the users when using the new system. Forbes released an article in 2021 detailing different ways to help employees adapt to new technology. The overall approach can be summarized through three facets: training, incentivize, and communication. First, the organization should have a training system in place that will correctly teach the users how to use the authentication system. The expert panel within the article published in Forbes

(2021) details that training should come in a variety of forms. Such forms may include online, in person or tutor based training. Next, incentives should be in place to encourage users to learn the new authentication system. Placing incentives within the training process will encourage users to become more active within their training and willing to participate. Lastly, it is crucial that the organizations communicate with their employees. These organizations should communicate why a new authentication system is being deployed and how it is going to be deployed. Additionally, the employees and users of the system should feel that they have some voice within the deployment process for their organization. Educating users on the why and how and helping them feel heard will encourage them to learn the system and understand its importance.

The most important stakeholder to be considered when discussing deploying new authentication systems are the developers of the technology. The organizations will not be able to support the users of the system if developers fail to provide support to the organizations deploying their systems. The direct users of a new authentication system will be unable to provide support to their co-workers and friends if the developers fail to provide support. Overall, if the developers of the authentication systems fail to provide facilitating support, facilitating expectancy will fail and the feasibility of deploying a new authentication system diminishes.

Developers provide facilitating support in a variety of ways, many of which are similar to those presented in the discussion about organizational teams. Developers may provide online videos and in person demonstrations to facilitate the learning process. This may involve developers leading training sessions at organizations deploying their system. This allows the developers to provide hands-on support to users. Additionally, developers should provide extensive documentation about the authentication system. This documentation serves as a resource for organizations and end users. It is important to consider the challenges that may be associated with documentation. Since technology is a fast paced, evolving environment, documentation quickly becomes out-of-date and subsequently less useful. Forward and Lethbridge (2002) from the University of Ottawa highlight concerns surrounding the importance of maintaining relevant documentation. However, this paper also includes how outdated documentation can still prove useful. Outdated documentation can create a line of communication between the developers, organizations and end users. Developers of an authentication system should provide a line of communication that goes beyond documentation. This communication may be primarily used by the organizations deploying the new system for support on issues and concerns that are not addressed by the documentation.

Facilitating expectancy of the stakeholders should be considered for a new authentication system to be successfully implemented. Evidence shows that end users receiving facilitating support from organizations and developers of the technology are more engaged and accepting of the authentication system. Active communication between organizations, developers and end users helps create a culture of acceptance among users.

The Implementation of Multi-Factor Authentication

A future shift to passwordless authentication can be more readily understood by examining the past shift from passwords to multi-factor authentication (MFA). MFA is an authentication system that is built on top of the existing password authentication systems. It requires users to input the correct password and then use a text message, email, or authenticator application, such as DUO, to authenticate that it is themselves logging into the system. Strata is an authentication company that published a blog post detailing the challenges faced by MFA

(Strata, 2022). Each of the four determinants can be examined using the challenges detailed within the blog post.

There is a direct relationship between the satisfaction of facilitating and performance expectancy. The first expectancy needed to be met is facilitating expectancy. Organizations must provide enough education to the users of MFA by being transparent with the implementation plan. Satisfying the facilitating expectancy will result in less difficulties of adaptation and decrease the overall implementation time. Performance expectancy is more likely to fail with a longer implementation time as it increases the productivity loss (Strata, 2022). The satisfaction of social expectancy is derived directly from the leaders of the organizations implementing MFA. Strata claims that leadership must be the biggest advocates for MFA if they want their employees to use it. MFA often fails the effort expectancy determinant as many users find it mundane to take another step to authenticate themselves. MFA complicates the login process which adds user friction (Strata, 2022). This is the most prevalent feedback when dealing with MFA, leading to some users even disabling MFA.

A similar transition of passwords to MFA can be expected of the shift to passwordless. Facilitating, performance, and social expectancy will most likely follow the pattern shown in the previous shift. Organizations must educate their employees and be transparent throughout the implementation process. This will help satisfy performance expectancy by preventing a loss of productivity. Social expectancy will be met with leadership pushing for passwordless authentication and supporting the implementation As in the shift to MFA. The biggest difference between the shift to MFA and to passwordless authentication lies with effort expectancy. The largest complaint of MFA is that it adds an additional step to the login process; passwordless authentication would remove this step and make the authentication process easy for the user.

Conclusion

The existing password authentication systems present serious security risks, so an alternative is needed. While it is critical to deploy an alternative to the existing password authentication ,challenges should be considered. Using the Unified Theory of Use and Acceptance of Technology, these potential challenges can be analyzed. Application of the four determinants of performance, effort, social and facilitating expectancy is useful in the introduction of a new authentication system. New research considering the relationship between the satisfaction of the determinants discussed and the development of alternatives to passwords can be generated. This will result in a more secure cyberspace for all of us.

References

Bonneau, J., Herley, C., Oorschot, P., and Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *2012 IEEE Symposium on Security and Privacy*, San Francisco.

Dayton, D. (2021, March 23). *Challenges of Information Technology Management in the 21st.Century*. Work. https://work.chron.com/challenges-information-technology-management-21st-century-28780.html

Forbes Expert Panel. (2021). 13 practical ways to help employees adapt to new technology. *Forbes.*

Forward, A. and Lethbridge, T. (2002). The relevance of software documentation, tools and technologies: a survey. In Proceedings of the 2002 ACM symposium on Document engineering (DocEng '02). Association for Computing Machinery, New York, NY, USA, 26–33. https://doi.org/10.1145/585058.585065

Haan, K. (2024, February 5). America's password habits: 46% report having their password stolen over the last year. *Forbes.* https://www.forbes.com/advisor/business/software/american-password-habits/

Microsoft. (n.d.). *Microsoft Digital Defense Report*. Microsoft Threat Intelligence. Retrieved February 2024, from https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

Parmar V., Sanghvi H. A., Patel R., and Pandya A. (2022). A comprehensive study on passwordless authentication. *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Erode, India. pp. 1266-1275, doi: 10.1109/ICSCDS53736.2022.9760934.

Passwordless authentication. (n.d.). Microsoft. Retrieved March 26, 2024, from https://www.microsoft.com/en-us/security/business/solutions/passwordless-authentication#diagram-cta-popup

Passwordless authentication. CyberArk. (2023, December 11). h0ttps:/ /www.cyberark.com/what-is/passwordless-authentication/

Stiefel, A. (2023, November 29). *Developer secrets keep leaking. can we stop the flood?: 1password*. 1Password Blog. https://blog.1password.com/exposed-developer-secrets-gitguardian/

Strata. (2022, November 7). *How To Avoid Top 10 MFA Implementation Challenges - Strata.io*. Strata Identity. Retrieved April 30, 2024, from https://www.strata.io/blog/app-identity-modernization/top-10-mfa-implementation-challenges-how-to-avoid-them

Velez, J., Cano, J., Whittington, M. S., and Wolf, K. J. (2011). Cultivating change through peer teaching. *Journal of Agricultural Education*, *52*(1), 40–49. https://doi.org/10.5032/jae.2011.01040

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Younghwa Lee, Jintae Lee, and Zoonky Lee. (2006). Social influence on technology acceptance behavior: self-identity theory perspective. *SIGMIS Database 37.* https://doi.org/10.1145/1161345.1161355