Michigan Technological University

CS5760: HCI Usability Testing

Spring 2024

Balancing Usability and Security of Popular Authentication Methods

Aditya Patil

ABSTRACT

This paper explores the critical balance between Usability and Security across popular authentication methods, employing Norman's Human-Computer Interaction principles as a theoretical framework. It conducts a comparative analysis of passwords, biometric, token-based and multi-factor authentication, highlighting their strengths and weaknesses concerning affordances, signifiers, feedback, constraints, and synthesizability. The study emphasizes the trade-offs designers face when implementing these methods in various contexts, such as college libraries, home IoT systems, corporate repositories, and hospital records. Recommendations are provided for optimizing user experience without compromising security, aiming to guide future authentication system designs towards more user-centered approaches. This work contributes to the ongoing discourse on enhancing both the security and usability of authentication methods to accommodate diverse user needs and security requirements.

INTRODUCTION

Usability has always been a key focus of Software design since the introduction of Consumer Applications. Designers have often focused on modeling the product according to their target Users and have also sought to ensure that they get a good experience while using the application. Similarly, Security has also been a focus while designing Consumer Applications to ensure compliance with the various Regulations with NIST, PCI-DSS, HIPAA and GDPR just to name a few. The universal focus of Security has always been on ensuring Confidentiality, Integrity and Availability(CIA) Triad for the users and Authentication has been one of the primary methods of achieving this for a long time now. However, the interplay between usability and security in authentication methods is a critical area of concern, as these methods serve as the primary gateway to personal and sensitive information. This paper leverages Donald Norman's principles of Human-Computer Interaction (HCI) to examine the delicate balance between usability and security within popular authentication methods. Through a comparative analysis of passwords, biometric authentication, multi-factor authentication (MFA), and token-based authentication, this study sheds light on how each method aligns with or diverges from Norman's design principles, including affordances, signifiers, feedback, constraints, and synthesizability.

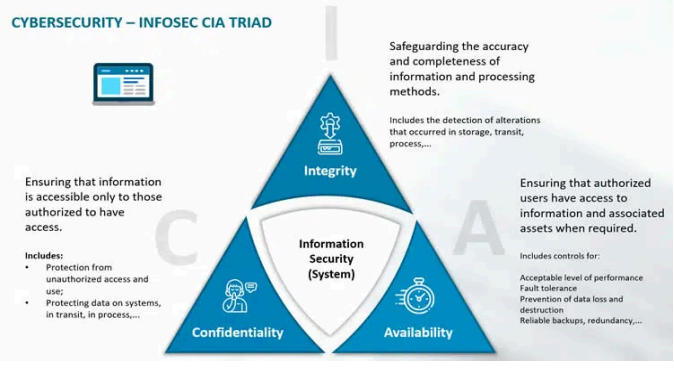


Figure 1: The CIA Triad

AUTHENTICATION

According to NIST, Authentication refers to the verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system[2]. Currently, Authentication is implemented in systems using various methods and they can be broadly classified as follows:

- Knowledge Based (Something you know): E.g. Username-Password login.

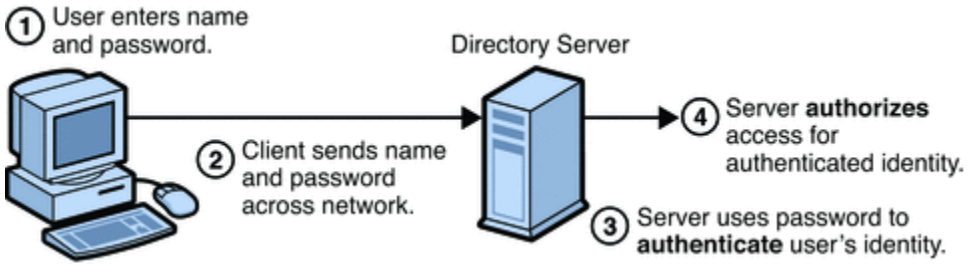


Figure 2: Password authentication

- Token Based(Something you possess): E.g. NFC Tags, RSA SecurID Tokens.

Figure 3: NFC Tag being used

- Biometric (Something you are): E.g. Fingerprint, Iris scan, Voice recognition.

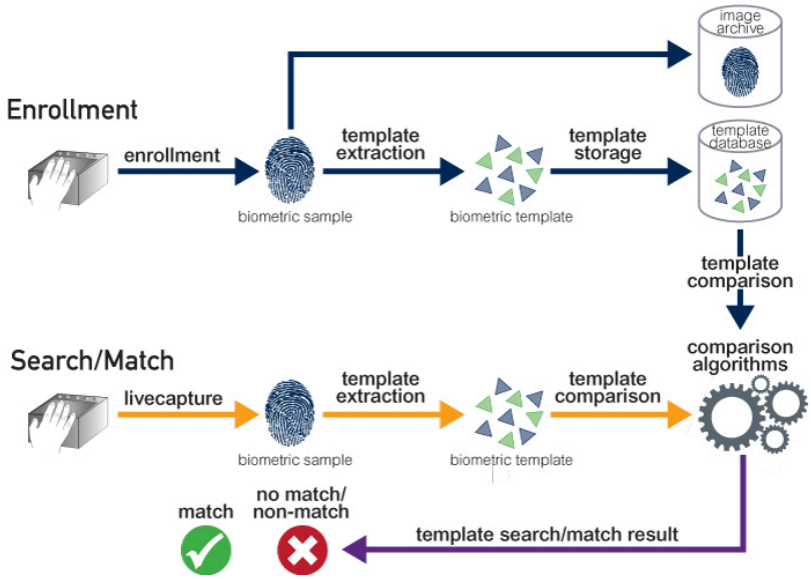


Figure 4: Biometric authentication process

- Behavioral (Something you do): E.g. Keystroke patterns, Gait.

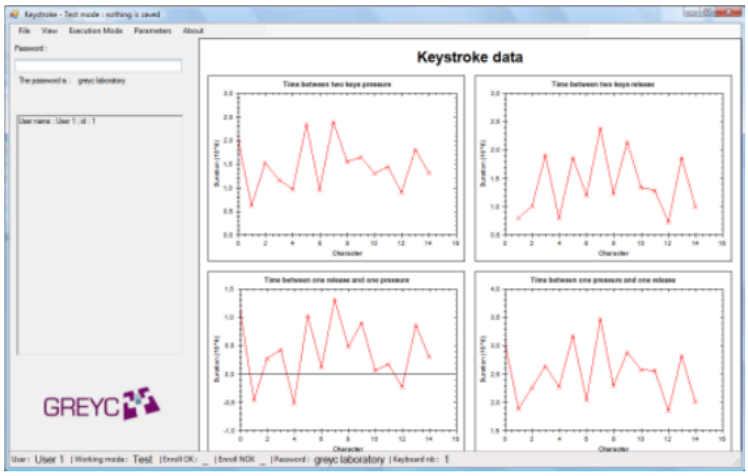


Figure 5: Keystroke data Obtained using GREYC software[1]

ANALYSIS OF AUTHENTICATION METHODS

This study shall focus on the analysis of some common authentication methods and their quality from a User Experience perspective.

1. **Password based authentication**

   Password based authentication is the single most popular type of authentication method currently deployed across the world with 88% of organizations using it as their primary authentication method[4][5]. Analyzing this method through the lens of Norman's six usability principles—affordances, signifiers, mappings, feedback, constraints, and synthesizability—provides a nuanced understanding of its strengths and weaknesses.

   Strengths

   - Affordances: Passwords inherently afford privacy and security, allowing users to access systems or information through the action of entering a secret known only to them. This direct relationship between the action (typing a password) and the outcome (gaining access) is clear.
   - Signifiers: The password field in interfaces is a well-understood signifier. It indicates where users should enter their password, often accompanied by icons (such as a lock) or text cues, guiding the user's action toward secure access.
   - Feedback: Most systems provide immediate feedback upon entering a password, such as a success message or redirecting to the secured area for correct entries, or an error message for incorrect ones. This feedback loop is crucial for correcting mistakes and confirming successful authentication.

Weaknesses

- Constraints: While intended to enhance security (e.g., requiring a mix of characters, numbers, and symbols), constraints on password creation can lead to poor usability. Users often struggle to remember complex passwords, leading to frustration or the use of insecure practices like writing passwords down, which can compromise security.
- Mappings: The relationship between the password chosen and the security outcome is not always clear to users. People may not understand how the complexity of their password affects its security, leading to the selection of weak passwords that are easy to remember but easily compromised.
- Synthesizability: Users' synthesizability of password-based authentication can vary significantly, with some not understanding the importance of complexity or the risks of reusing passwords across sites. This lack of understanding can lead to behaviors that compromise both the security and effectiveness of password-based systems.

2. **Biometric authentication**

Facial recognition and Fingerprint recognition are the two most widespread biometric authentication methods with Fingerprints having a wider acceptance than Facial recognition[6]. Since the working principles of Biometrics are different from Passwords, they demonstrate different Usability properties.

Strengths

- Affordances: Biometric systems afford a natural and intuitive means of authentication. The user's action (e.g., touching a fingerprint sensor, looking at a facial recognition camera) is closely tied to the outcome of authentication, leveraging physical characteristics that are always with the user.
- Feedback: Biometric systems typically provide immediate feedback. For example, a fingerprint scanner may light up upon touch, and systems often display messages or visual cues indicating successful recognition or the need to retry, helping users understand the authentication status quickly.
- Constraints: Biometric authentication naturally constrains access to those who possess the required biometric trait, effectively limiting unauthorized access. This built-in constraint enhances security without the need for users to remember complex passwords or carry additional tokens.

Weaknesses

- Signifiers: The effectiveness of signifiers in biometric systems can vary. While the presence of a fingerprint scanner or facial recognition camera may be apparent, the exact manner in which the user needs to present their biometric data (e.g., angle of a finger, eye positioning for iris recognition) may not always be clear, potentially leading to errors or frustration.
- Mappings: The direct mapping between the biometric input and the outcome (access granted or denied) is clear, but users may not always understand how their biometric data is processed or stored, raising concerns about privacy. The opaque nature of these processes can create mistrust or confusion.
- Synthesizability: Users might have varying ideas of how secure biometric authentication is. Some may overestimate the security, believing biometric data to be infallible, not recognizing the potential for false positives/negatives or data breaches. These misconceptions can affect user behavior and trust in the system.

3. **Token based authentication**

Due to inherent flaws in Password based authentication and newer developments in encryption technology, Token based authentication was introduced in 1986 with the patented RSA SecurID product[7]. Initial tokens provided a One Time Password(OTP) that would change after a set interval, however newer OTP generation protocols enabled authentication through cell phones and email, making it more accessible. Near Field Communication(NFC) and Radio Frequency ID(RFID) also made it possible to implement tokens on physical devices like tags and cards, making the system more accessible.

Strengths

- Affordances: Physical tokens clearly afford carrying and using wherever necessary, making the act of authentication tangible and straightforward. Digital tokens, through apps, afford convenience by utilizing devices users already carry, such as smartphones.
- Feedback: Token-based systems typically provide immediate feedback. For hardware tokens, this might be the display of a new OTP. For software tokens, feedback can include visual cues on the app or notifications.
- Constraints: Tokens effectively constrain access to those who possess them, adding a layer of security by requiring something the user has. This constraint makes unauthorized access more difficult compared to knowledge-based methods like passwords.

Weaknesses

- Signifiers: The indication of what to do with the token, especially in the case of hardware tokens, might not be clear to all users, especially those with lower technological literacy.
- Mappings: The relationship between having the token and gaining access might be conceptually clear (having the token allows access), but the underlying mechanism can be less intuitive for some users.
- Synthesizability: Users might struggle with understanding how tokens enhance security. Misplacing a token can lead to access issues, and users might not always grasp the importance of the token or how to manage it securely (e.g., not sharing it or keeping it safe).

4. **Multi-factor authentication**

After analyzing the various advantages and disadvantages of the prevalent authentication methods, Multi-factor authentication(MFA) was introduced. It refers to using any of the existing authentication methods combined with the others. Incidentally, increasing the number of authentication methods and integrating them into a singular process increases the cost of implementation but it significantly increases the security of the system. The most common type of MFA is Two-Factor Authentication(2FA) as it provides a healthy balance between Cost and Security.

Strengths

- Affordances: MFA systems afford a higher level of security by utilizing multiple authentication factors, clearly indicating that more than one step is necessary for access. The use of familiar elements like passwords, mobile phones, or fingerprints leverages existing user behaviors and expectations.
- Feedback: Effective MFA systems provide immediate and clear feedback at each step of the authentication process. Users receive prompts or messages indicating the success or failure of each authentication factor, guiding them through the process.
- Constraints: MFA introduces beneficial constraints that significantly enhance security by making it more difficult for unauthorized users to gain access. These constraints are not arbitrary but directly tied to improving security outcomes.

Weaknesses

- Signifiers: The process and requirements of MFA may not be adequately signified, especially for users unfamiliar with the concept. Users may be unclear about what actions are required, in what order, or the importance of each step, leading to confusion or errors.

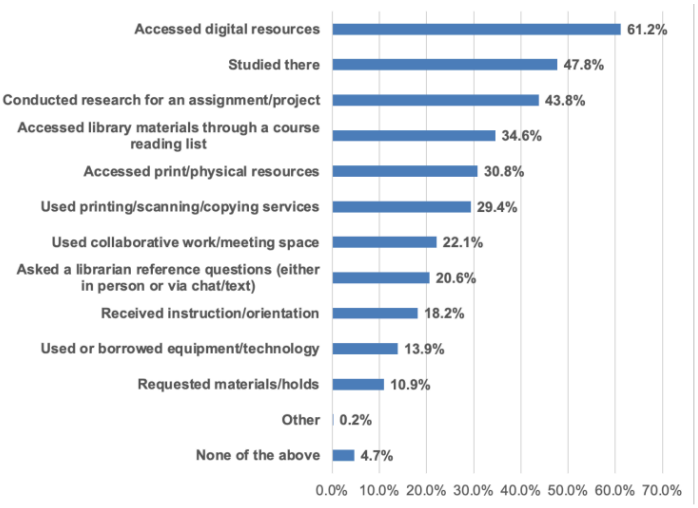
- Mappings: The relationship between actions required by the user (entering a password, using a token, providing a fingerprint) and the outcome (access granted) can become complex in MFA systems. This complexity can obscure the direct cause-and-effect relationship, making the system less intuitive.
- Synthesizability: Users may struggle with imagining the model of MFA, not fully understanding why multiple steps are necessary or how each factor contributes to overall security. This can lead to frustration or resistance, especially if the process is seen as overly cumbersome.

APPLICATION OF AUTHENTICATION METHODS

Based on the Usability analysis of the selected Authentication methods, this paper aims to explore the application of these methods to some popular use cases taking into account the criticality of the system, its target user base, the tech-literacy of the users and the overall perception of the method.

Use Cases

1. College Libraries:
   Most College Libraries are used by Students and Professors. This demographic regularly accesses the library for digital resources and gathering required academic materials for study[10].



n=402

Figure 5: Interaction of Respondents with College Library[10]

As a result, implementation of Passwords is sufficient to protect the resources however if the Library network is not isolated from the rest of the Campus, implementation of 2FA is a valid choice since the Users have sufficient literacy and awareness about the importance of additional security even if the resources become less accessible.

2. Home IoT networks:
   Automation using Home IoT is a quickly growing market and the emergence of many “Smart” devices exemplifies this. A typical Home IoT setup consists of Smart Lights, Door Cameras, Garage doors and other devices which can be controlled remotely or through mobile apps. It has been observed however that a significant number of these devices have security vulnerabilities including lack of authentication, lack of encryption and insecure firmware[11].

Vulnerability	Reference	Risk CIA
Insecure web interface	[16]	I
Insufficient authentication	[17][18]	C
Insecure network services	[19][20]	I, D
Lack of transport encryption/integrity verification	[21][22]	C, I
Privacy issues	[23][24]	C
Insecure cloud interface	[25][26]	I
Insecure mobile interface	[27][28][29]	I, D
Insufficient security settings	[30][31][32]	I
Insecure software/firmware	[33]	I
Poor physical security	[34][35]	C,I,D

Figure 6: Vulnerabilities in Home IoT devices[11]

A lot of these vulnerabilities can be mitigated by implementing Passwords on the devices and basic encryption for transit data. The method is simple and comes with very little additional cost for the manufacturers while not significantly compromising with the usability of the device.

3. Corporate Repositories:
   Corporate Repositories are meant to host proprietary code and are accessed by the development team in various capacities. Hardware/Software token is the most feasible technique applicable to this scenario because it is usually provided as a Federated Identity Management(FIdM) service by third-parties, which offloads the task of security from the actual development team.
   In terms of usability, it does not have much of a negative impact since the development teams possess a good knowledge about the need of these security measures and are compliant with the security policies.

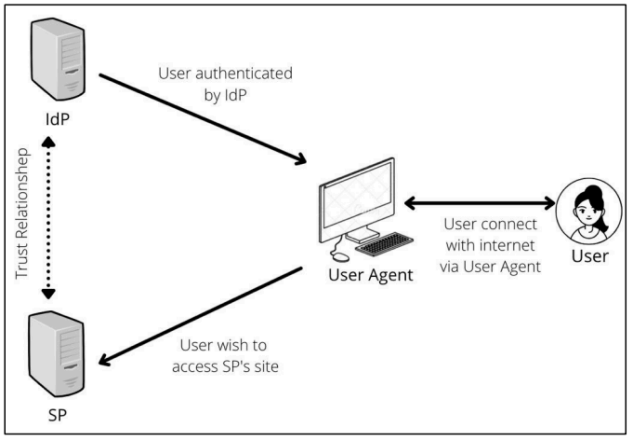


Figure 7: FIdM Components

4. Hospital Records:
   Hospital Records are a challenge from both Security perspective and Usability perspective. The Security challenge arises from the fact that they are protected by Government regulations like HIPAA in the United States and therefore require some mandatory protection mechanisms for compliance. On the other hand, the people with access to these systems are mostly Health professionals and patients who have a wide range of technological literacy. To tackle this situation, MFA implementation should be practiced, however the second factor beside Passwords can be something more intuitive like Biometrics, which are usable by a variety of people while giving good security[1].

CONCLUSION

Considering the various advantages and drawbacks of popular authentication methods, it is suggested to implement the more complicated authentication methods like Tokens and MFA when the User base has a higher technological literacy while Biometrics are a good technique for a balance between Usability and Security for the general public. Password authentication should still be considered a default scheme in most scenarios due to its ease of implementation and can be provided as a backup in case the other methods cannot be used in a particular instance.

REFERENCES

[1] Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J. J. (2013). A review on authentication methods. Australian Journal of Basic and Applied Sciences, 7(5), 95-107.

[2] https://csrc.nist.gov/glossary/term/authentication

[3] Komarova, A., Menshchikov, A., Negols, A., Korobeynikov, A., Gatchin, Y., & Tishukova, N. (2018). Comparison of authentication methods on web resources. In Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry"(IITI'17) Volume 1 (pp. 104-113). Springer International Publishing.

[4] Specops 2024 Breached Password Report

[5] https://specopssoft.com/our-resources/most-common-passwords/

[6] S. H. Katsanis et al., "U.S. Adult Perspectives on Facial Images, DNA, and Other Biometrics," in IEEE Transactions on Technology and Society, vol. 3, no. 1, pp. 9-15, March 2022, doi: 10.1109/TTS.2021.3120317.
keywords: {Biometrics (access control);DNA;Instruments;Fingerprint recognition;Face recognition;Dentistry;Privacy;DNA;ethics;face recognition;law;privacy;technology social factors},

[7] Method and apparatus for synchronizing generation of separate, free running, time dependent equipment, by Kenneth P. Weiss (1985, Nov. 27) U.S. Patent 4 885 778 [Online]. Available:https://ppubs.uspto.gov/dirsearch-public/print/downloadPdf/4885778

[8] Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five {two-factor} authentication methods. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (pp. 357-370).

[9] Forget, A. (2013). A world with many authentication schemes (Doctoral dissertation, Carleton University).

[10] "College Student Library Usage Survey Report", ProQuest 2022, https://s3.amazonaws.com/ImageCloud/Research/2022/College%20Student%20Library%20Usage%20Report%20Final.pdf

[11] L. Ayavaca-Vallejo and D. Avila-Pesantez, "Smart Home IoT Cybersecurity Survey: A Systematic Mapping," 2023 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2023, pp. 1-6, doi: 10.1109/ICTAS56421.2023.10082751.

IMAGES

Figure 1: https://www.i-scoop.eu/cybersecurity/cia-confidentiality-integrity-availability-security/

Figure 2: https://docs.oracle.com/cd/E19424-01/820-4811/6ng8i26ag/index.html#gdzej

Figure 3: https://static1.makeuseofimages.com/wordpress/wp-content/uploads/2021/06/person-using-iPhone-NFC-payment.jpg

Figure 4: https://www.aware.com/wp-content/uploads/2015/07/wab_biometric-processes.jpg

Figure 5: https://s3.amazonaws.com/ImageCloud/Research/2022/College%20Student%20Library%20Usage%20Report%20Final.pdf , Pg. 20

Figure 6: L. Ayavaca-Vallejo and D. Avila-Pesantez, "Smart Home IoT Cybersecurity Survey: A Systematic Mapping," 2023 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2023, pp. 1-6, doi: 10.1109/ICTAS56421.2023.10082751.

Figure 7: Aldosary, Maha and Alqahtani, Norah, A Survey on Federated Identity Management Systems Limitation and Solutions (May 27, 2021). International Journal of Network Security & Its Applications (IJNSA) Vol.13, No.3, May 2021, Available at SSRN: https://ssrn.com/abstract=3869295