Department of Computer Science

Submitted in part fulfilment for the degree of BSc Computer Science

Enhancing E-Commerce Security: A Passwordless Approach

Michael Cavaciuti

06 May 2024

Supervisor: Roberto Metere

Acknowledgements

I would like to use this section to acknowledge and thank those who aided me in the successful completion of this dissertation. Whom have been exceptional in guiding me and encouraging me to stay focused on my academic goals. To my supervisor, Roberto Metere, I am sincerely appreciative for the invaluable guidance and support you have provided through this research. Ensuring I am able to hone my skills and present a piece of work that I am proud of. To my friends and family, who have with unwavering support, encouraged, and kept belief in me that I can use my abilities to complete this task. And my academic supervisor, Siamak F. Shahandashti, who has guided me these past four years to complete my undergraduate study. Providing insightful discussions into the realm of cybersecurity and ensuring I am at my best. Finally thank you to all those who read this dissertation.

STATEMENT OF ETHICS

In undertaking this dissertation, I have rigorously adhered to the ethical guidelines and privacy principles established by the university. Where research primarily involved the evaluation of passwordless authentication technologies and the use of synthetic data sets created specifically for the purpose of this study, ensuring that no real data was compromised. I also made extensive efforts to attribute and acknowledge the contributions of other scholars found in the public domain. Ensuring the prevention of plagiarism and associated consequences through clear cross-referencing to maintain academic integrity. The research was conducted independently, without the influence of third-party interests, as in alignment with ethical standards. Ensuring findings and recommendations are unbiased and solely intended to contribute to academic knowledge and practical applications in e-commerce security. This statement underscores my commitment to ethical research practices, the responsible use of information and the advancement of knowledge in the field of cyber security within e-commerce environments.

TABLE OF CONTENTS

TABLE OF FIGURES

Executive summary

This dissertation focuses on enhancing the security of e-commerce platforms by transitioning from traditional password-based authentication to passwordless schemes. It aims to highlight the vulnerability of password-dependent systems, proving the benefits of adopting passwordless authentication as a more secure alternative.

The primary goal is to explore the efficacy of passwordless authentication in improving security with the secondary aim of implementation without compromising user experience. This involves the integration and evaluation of FIDO2 and Magic Link technologies as part of a multi-factor authentication strategy. To achieve this, a thorough and comprehensive literature review is conducted to discuss the evolution and limitations of traditional authentication methods, from simple passwords to multi-factor authentication, emphasising the need for more secure and user-friendly alternatives. Furthermore, passwordless authentication technologies are discussed and evaluated, to create an understanding of the core principles they operate within. Using research into evaluation frameworks for authentication schemes, we aim to a provide clear evaluation of these technologies for their potential to enhance security and usability.

Following the extensive literature review, a mixed-method research approach for the methodology is adopted, combing theoretical and empirical analyses to develop and test a prototype of the passwordless authentication system: FIDO2 with Magic Link. This incorporated an insight into the details of cyber breaches and attacks experienced by online businesses, big and small, across the e-commerce platform. Furthermore, these discussions led to the integration of the proposed authentication mechanism within ASP.NET, a popular tooling for building large scale websites and services for e-commerce.

The implementation demonstrated a significant improvement in security by eliminating the risks associated with password theft and reuse by methods of Phishing, brute-force and other cyberattacks. The prototype’s success in integrating FIDO2 and Magic Link underscored the feasibility of passwordless authentication in real-world e-commerce settings. However, highlights the dependencies and challenges that come forth when removing a password in place of newer technology with unknown vulnerabilities. Through rigorous evaluation, it can be said in confidence that passwordless schemes will come to outdate the traditional passwords. However, due to limitations within the project, a usability study was unable to be conducted. For this reason, further research is recommended to address the usability aspects of passwordless authentication in solutions such as the proposed. As this will allow for exploration of additional security measures that can mitigate the identified vulnerabilities of this paper, as well as understand the process passwordless schemes will need to take for widespread adoption.

In conclusion, this study states that passwordless authentication, particularly through the integration of FIDO2 and Magic Link, offers a promising solution to the security challenges in e-commerce. Providing a more secure alternative to the traditional passwords by leveraging advanced cryptographic methods and reducing the reliance on user-generated passwords.

1 Introduction

Today the cybersecurity landscape is continuously evolving to address increasingly sophisticated threats against the protection of user data and system integrity. This active environment brings to light a critical vulnerability in traditional security: the conventional vulnerability of dependence on passwords. As a solution, passwordless authentication has emerged as a significant innovation, offering a promising alternative to password-based security.

This dissertation aims to address the issues and limitations of password-based security within the e-commerce platform of web activities. An increasingly targeted sector of our digital world as more user's toy with the prospect of market-shares. Passwordless alternatives have similarly become more prominent in recent years, being recognised by the World Economic Forum [] as a contributing factor to the transformation of future security and technology. To address these password-based challenges, this study presents an innovative strategy leveraging the capabilities of FIDO2 authentication, such as YubiKey, with the objective of rendering traditional passwords obsolete. Additionally, the research pursues Multi-Factor Authentication through the combination of TOTCs (Time-based One-Time Codes) within Magic Link technology to permit an authorised user using trusted third-party communication channels.

This dissertation is comprised of an in-depth literature review from traditional password to passwordless authentication, delving into the limitations of each as well as the potential surrounding its solutions. Following, the methodology describes the approach to developing and evaluating a prototype, drawing on the findings of the literature review; concluded by resulted testing and comprehensive discussions to summarise and contribute to the future of this field.

1.1 Motivation

The motivation behind this dissertation lies in the imperative to address the shortcomings inherent in conventional password systems within the context of e-commerce. Traditional password mechanisms, while prevalent, are riddled with vulnerabilities that render them susceptible to exploitation. These vulnerabilities range from issues like password reuse, brute force attacks and social engineering tactics. In the bustling ecosystem of e-commerce, characterised by diverse user interactions and transactions, the need for robust authentication systems becomes even more pronounced. Therefore, the primary motivation is to forge an authentication framework using passwordless capabilities that not only fortify security, but also streamline the user experience within e-commerce platforms.

1.2 Problem Scenario

Consider the scenario of an e-commerce platform, where users engage in numerous transactions, from purchasing goods to managing accounts; all with differing levels of confidential and sensitive data. For some, this is their livelihood or side-business; therefore, requiring complete confidence of system security to ensure only authorised personnel are permitted. Within this dynamic environment, traditional password-based authentication mechanisms are proving inadequate in safeguarding user accounts against evolving cyber threats: increasing pressure on the user to maintain strong complex password paradigms.

To confront this challenge, this dissertation endeavours to explore the realm of passwordless authentication; leveraging e-commerce as the testing ground to research and implement these emerging authentication paradigms in fortifying security and enhancing user experience.

1.3 Research Questions

The primary aim of this study will be to examine the relationship between usability and security within an e-commerce platform with the implementation of a passwordless multi-factor authentication mechanism. To achieve this goal, two schemes will be selected based on in-depth analysis of existing literature and technologies; a prototype built on this claim. The study will seek to answer the following questions:

- How can the integration of two-factor/multi-factor authentication enhance security without compromising user experience?
- How do passwordless schemes compare against traditional text-based passwords in terms of security?
- What new threats revolve around the use of passwordless authentication?
- How is the security and usability of authentication schemes measured?
- What are the potential risks associated with implementing the chosen authentication schemes into MFA, and how can it be mitigated?

2 Literature Review

This literature review seeks to provide valuable information to address the research question in the introduction. Achieved by delving into the development, implications and technological underpinnings of passwordless authentication within the cybersecurity framework. Understanding how passwordless authentication leverages advanced methods such as biometrics, security tokens and mobile device authentication; the importance of these methods in enhancing identity protection and examining the evolution of authentication to more secure and user-friendly mechanisms. Analysing good practices on passwordless technology evolution, benefits and challenges, this review shall contribute to the on-going discourse in improving cybersecurity practices with implications for future research and development in passwordless authentication.

2.1 Evolution of Authentication Methods

The journey of authentication methods has evolved significantly since its conception in the early 1960s to modern passwordless solutions. This evolution is marked by key developments and continuous efforts to balance security, usability and convenience.

Traditional Passwords: As evidenced in the paper by Morris & Thompson [1], the traditional password has significantly influenced the widespread adoption of password-based systems today. The paper details the history of design behind a password security scheme on a remotely accessed time-sharing system, emphasising the compromise between extreme security and ease of use. For context, as mentioned in the early 1960s at MIT, F. J. Corbato and his colleagues devised the first Compatible Time-Sharing System (CTSS) [2]. Which allowed multiple users to interact with a computer simultaneously, with each user being allocated a certain amount of time for usage. This system was secured using passwords and was a large step towards interactive computer systems.

The implementation [1] was designed for the UNIX time-sharing system as a response to observed attempts by an adversary to penetrate the system. The initial system incorporated a password file to contain / store the plaintext (actual) passwords of all users, which had to be heavily protected against unauthorised access. However, this approach was found to be vulnerable to a multitude of security lapses, such as accidental disclosure of the password file. Which is a key event described in the paper, with two administrative users operating on the file at the same time, resulting in the accidental disclosure of all passwords on all machines. To address this issue, the authors proposed an encryption-based solution, where only the encrypted form of a user’s password would be stored in the password file and the plaintext version discarded. The paper [1] goes on to discuss several improvements to the initial system, including the use of a slower encryption algorithm, encouraging the use of less predictable passwords and the introduction of "*salted passwords"* to increase the difficulty of finding individual passwords by inverting the encryption. These enhancements aimed to address the weaknesses identified in the original systems and make it increasingly difficult for unauthorised users to compromise passwords.

Over the years, password-based systems have become ubiquitous in various domains, often serving as the primary method for user authentication and access control. However, the reliance on passwords has introduced significant constraints, including the cognitive burden on users to memorise and manage multiple complex passwords, and the prevalence of easily guessable passwords through various attacks such as brute force and spray attacks due to human behavioural patterns.

Exploring advancements beyond traditional protocols, attempts were made to pivot towards more intuitive authentication methods, such as Graphical and Pattern-based passwords. Graphical passwords, as discussed by Biddle et al. (2012) [3] in their comprehensive study, have been a topic of research since 1999, *"proposed as alternatives to text-based password authentication"* [3]. These schemes utilise visual elements for password creation and recollection, leveraging the human ability to better remember and recognise images/patterns over text. This approach sought to improve memorability, usability, and security by diversifying the password domain. However, it remained as vulnerable as conventional passwords, burdening users with the need to remember specific contexts or patterns of an image.

Two-Factor and Multi-Factor Authentication: As digital security progressed, Two-Factor Authentication (2FA) was introduced as a critical component in the verification security, addressing the limitations inherent in traditional password-only systems. 2FA adds an additional layer of security for identifying a user; this dual-layer approach *"couples the representative data (username/password combination) with the factor of personal ownership, such as a smartcard or a phone"* [4]. Generating a one-time token that can be used to prove personal ownership of the account in question. More commonly today, a second factor is based on the user's biometric data, such as fingerprints or retinal identification [5]. Which leads into Multi-Factor Authentication (MFA). MFA builds upon the concept of 2FA, with the distinction of 2 or more factors for verifying a user's identity. Typically, there are three factors to consider with 2FA to MFA: Knowledge, Ownership and Biometric: with knowledge as something the user knows; ownership as something the user owns, and biometrics being intrinsic to the user (unique). By combining these factors, MFA provides "*a higher level of safety and can facilitate continuous protection of computing devices as well as other critical services from unauthorised access"* [4]. Despite being built upon the traditional password, this system widens the field for investigation into different verification methods of a user.

Notable Authentication: The concept of the three factor types to connect an individual with their established credentials, has paved the way for a multitude of authentication methods. Token Hardware Authentication (such as RSA SecurID Token), as discussed by Parmar et al. (2022) [5], is another form of authentication where a protection token is a hardware mechanism that can verify the owner, granting access to a system. These protection tokens offer a level of authentication similar to 2FA: giving a personal number to the device, to then produce a variety of tokens to be used to login. Pairing an item the user owns with something they know: Knowledge and Ownership factors.

Single-Sign-On (SSO) technology represents a significant evolution in authentication methods, as it offers a streamlined and efficient approach for users obtaining access across multiple services with a single set of credentials: *"allows users to authenticate safely using only one set of passwords for various apps and websites"* [5]. Built upon an arrangement of trust between service providers and an identity provider, SSO simplifies the authentication process, mitigating the need for users to remember multiple passwords. This centralised authentication mechanism, as detailed by Jan De Clercq (2002) [6], leverages an infrastructure where users authenticate once and gain access to all associated resources without the need for reauthorisation. SSO not only brought user convenience to the forefront, but it also addressed critical scalability and administrative challenges within large IT companies: facilitating the enforcement of consistent authentication policies across the enterprise. However, this also introduces a singular point of failure; if the SSO system is compromised, then an adversary has access to all connected services. Despite this, it is still considered a pivotal advancement in the authentication landscape, guiding traditional password methods towards more integrated and secure solutions.

The literature on One-Time Passwords (OTPs), including discussions by Parmer et al. (2022) [5] and works of Hsieh & Leu (2011) [7], highlight a continued evolution of authentication technologies. Providing a critical understanding of the trajectory of security mechanisms from static passwords to dynamic, context-sensitive authentication methods. OTPs offer a robust option for digital authentication, through the generation of a unique password for each login attempt or transaction. Typically, numerical or alphanumeric, the OTP becomes invalid after a single use or a short time period [5]. This temporary nature of OTPs makes them an effective tool against a range of cyber-attacks, including credential surfing and replay attacks. Many distinct types of OTPs exist, for example time and location-based schemes [7], taking advantage of technologies such as GPS.

Building upon the foundation laid by traditional and evolving authentication methods the direction of research towards passwordless authentication becomes increasingly clear. These methods, as discussed in the literature by Parmar et al. (2022) [5] and others, incorporate elements that align closely with the principles of passwordless authentication, utilising the factors of MFA, without relying solely on traditional passwords.

Biometric Authentication: The transition towards passwordless authentication is highlighted by a growing focus on biometrics, a key topic in the evolution of authentication technology. Biometrics leverages unique physical or behavioural characteristics such as fingerprints, facial recognition, and voice patterns to enhance both security and user convenience. This transition reflects the broader trends identified in the literature [5] towards more secure, user-friendly, and context-aware security measures.

Fingerprint recognition, as outlined in the literature by Parmer et al. (2022) [5], is a widely used biometric method, leveraging a user’s unique physiological attributes: the distinctive swirls and ridges of fingertips. This form of biometric authentication compares a user’s fingerprints against that pre-stored in the database to allow access. Found in the widespread market of electronics such as smartphones and computers, it is integrated into various industries illustrating the practical application of biometric technologies. It does, however, suffer from issues such as moisture or dirt that renders the technology ineffective, unable to identify a fingerprint.

In recent years, the domain of biometric authentication has seen significant enhancements, notably in facial recognition technology. Which creates a faceprint using hundreds of distinct measurements. Similar to fingerprint recognition, this technology has been widely adopted by smartphones and other devices detailing its ease of use and minimal setup, proving to be user-friendly. While this offers convenience, it also faces accuracy challenges due to variations in appearance and angles. Vocal identification follows a similar authentication path, where a voiceprint profile is created to authenticate, looking at unique mouth and throat shapes in conjunction with the sound characteristics of a user. However, this method can be affected by background noise and changes in the voice.

Further advancements in retinal and iris scanning, alongside behavioural biometrics like typing rhythms, are promising steps toward improved security and user convenience. Nevertheless, the practical application of retinal scanning is currently hindered by its need for sophisticated equipment, making it less accessible for everyday use. On the other hand, behavioural biometrics introduce an innovative security layer by examining unique patterns in individuals' behaviour, thus expanding the horizons of authentication technology. However, it is still in its infancy.

This trend of developing biometric authentication that includes both physiological and behavioural traits is part of a much wider trend towards increasingly sophisticated, context-aware, and user-friendly security measures. It is a continuous revolution in the technology of authentication driven by the dual goals of improving the security and user experience.

Passwordless Authentication: In the evolving landscape of digital security, the development of authentication schemes such as biometrics have led to more user-friendly and secure authentication methods through passwordless mechanisms. Among these, Magic Links have emerged as a notable solution, offering a blend of convenience and security through the themes of 2FA. This authentication scheme eliminates the need for a traditional password, and instead leverages a unique one-time-use link sent directly to the user's email address. This method not only simplifies the login process but also aims to enhance security by reducing risks associated with password theft and reuse.

Magic Link authentication operates on a simple, yet effective principle: firstly, the user inputs their email address into the service to start the process of log-in. The system would thereafter create a unique identification key or token, embedding it into a URL to be sent to the user's email address. The system retains the URL temporarily on the server, and when the user follows this link, they are directed back to the service where the server validates the token and grants access. Often through the use of longer lasting session tokens, and this not only makes the user experience easier, but also adds another layer of security due to the validation of email account ownership.

The literature reveals various implementations and considerations surrounding Magic Link authentication. Both the study by Parmar et al. (2022) [5] and another by Chowhan & Tanwar (2019) [8], outline the process and benefits of Magic Links, emphasising its simplicity and enhanced security as a passwordless method. These studies include the reduction of password-related vulnerabilities and increase in convenience for users. However, highlighting the new dependency on email security, as if the security of the user’s email account is compromised then so is the Magic Link scheme. The study by Matiushin & Korkhov (2021) [9], further supports the discussion found in the previous literature, as well as an implementation of this technology using Keycloak: *“an open-source software product that implements single sign-on technology.”* [9]. Through the combination of this technology with Magic Links, the study demonstrates a practical application and potential for enhancing security in distributed systems. And goes further to discuss the potential approach of WebAuthn and FIDO2 for a wider range of implementations.

Another concept of passwordless authentication presented in [5], is the One-Time Code transmitted via email or SMS. Based upon the previously discussed OTPs, a one-time code is a generated unique code for individual authentication attempts, therefore enhancing security and eliminating risks associated with static passwords. The literature review explores the implementation of OTCs via email and SMS, their advantages, and disadvantages, as well as their significance in passwordless mechanisms.

OTC authentication involves sending a unique, single-use code to the user’s email address or mobile phone upon entering a system. Similar to Magic Link authentication, this process validates the user’s ownership of the account through the use of an associated device/tool, thus granting them access. The simplicity and ubiquity of emails make this method highly user-friendly, with low-setup and maintenance costs. However, it is subject to the reliability of email delivery such as spam filters, server rejections and interception. And similarly, it produces a redundancy issue, where if an attacker gains access to a user’s email account, potentially all services are compromised. OTCs via SMS also introduce its own set of challenges: dependent on mobile network coverage and susceptible to phone loss or theft. The email and SMS, all as channels within the wider context of passwordless authentication, illustrate a paradigm shift to more dynamic single-use credentials which far fortify security through reduction of exposure to threats ascribed to traditional passwords. However, the efficiency and safety of these systems lie in the delivery channels' ability to protect and the enforcement of backup mechanisms. This suggests a multi-pronged approach with alternatives to be explored for authentication factors ranging from biometrics to cryptographic keys where OTCs represent a standalone and integrated component in MFA strategies.

As recently as 2018, the Fast Identity Online (FIDO) and World Wide Web Consortium (W3C) published an open authentication standard with the goal of a secure and user-friendly passwordless authentication scheme for web browsers. This scheme, known as FIDO2, provides a secure and passwordless method of authentication, employing public-key cryptography to enable users to access services safely and effortlessly. Further as the successor to the Universal Authentication Framework (UAF) and Universal 2nd Factor (U2F) protocols, FIDO2 supports the use of 2FA and MFA as well as single-factor authentication by tokens. From the literature by Kabir & Elmedany (2022) [10], a detailed overview of FIDO2's mechanics are explained: aided by *"two underlying technologies … FIDO Client-To-Authenticator Protocol (CTAP2.1) and W3C Web Authentication API … known as WebAuthn API"*[10], incorporating a process of two distinct phases: registration and authentication.

When a user decides to register an authenticator with a FIDO2-compliant service, defined as "relying parties (RP)" [10], a registration request is sent to the server. In response, the server sends a unique challenge (acting as a 'nonce') and handle. These are then used by the WebAuthn API, which "utilises strong asymmetric cryptography (like elliptic-curve, ECC or RSA) … to locally generate [a] pair of … public and private keys"[10]. The authenticator, which can be biometric-based and/or token hardware-based, stores its private key; then for evidence of genuine functionality, it returns to the browser a key ID, the public key and proof of device by signing the challenge. This data is sent forward to the RP where it undergoes validation using the public key against the signature, meaning if any tampering/mismatch occurred an error would be returned. Otherwise, the RP will store only the valid public key and key id.

Once the user tries to log into the RP, authentication is triggered. The RP requests a login challenge of the browser, relaying this challenge to the authenticator in question. Where the authenticator. The authenticator signs using its securely kept private key and sends back to the browser the signature of the challenge as well as user handle. Upon receiving this packet to the given RP, a check is performed: verifying using the associated public key and user handle that the signature is authentic. Thereby, once successful, will lead to granting access to the user. On mismatching signatures, access is denied, and an error message is generated by the RP when one attempts logging in incorrectly.

2.2 Evaluation Method of Passwordless Authentication

The approach used by Bonneau et al. [11] in their proposed evaluation method is fundamental and very extensive, addressing important issues of cybersecurity such as emerging threats and implications of passwordless authentication. The framework has a sophisticated methodology for evaluating web-based authentication methods by combining security, usability and deploy-ability aspects into one holistic evaluation model. This review will concentrate on the security benefits of the framework and how they relate to evaluating passwordless authentication technologies' resilience and efficiency.

Within security, the framework effectively evaluates authentication schemes using 11 factors (labelled S*)[11]. Threats such as physical (S1) and internal (S5) observation are discussed, highlighting the need for security against all forms of surveillance to ensure confidentiality and protection against spyware techniques. A common yet widely underrated attack for gathering information. Furthermore, targeted impersonation (S2) and phishing attacks (S7) are covered, stressing the need for a safeguarding mechanism to adequately distinguish between a user and imposter, despite an attacker’s knowledge or deceit.

In considering an attacker's capabilities, the framework addresses both throttled (S3) and unthrottled guessing attacks (S4); underlining the importance to withstand widespread and targeted brute-force attacks. Thereby, preserving security against a range of attack intensities. Building on the consideration of an attacker’s capabilities, the framework evaluates based on the prevention of information leaks (S6), resilience to theft (S8), dependence on third-party entities (S9), requirement for user consent (S10), and the capacity for unlink-ability (S11). This set of criteria aims to provide a holistic defence against a wide array of security challenges, ensuring a comprehensive safeguarding of user data and interactions within the digital environment.

The framework's ability to be effective is attributed to the integration of the security benefits with considerations of usability and deploy-ability. Recognizing that the most secure schemes must also be user-friendly and practically deployable, such as a scheme's defence against physical observation (S1) being balanced with usability aspects like not being memory intensive (U1) to prevent security from becoming a user obstacle. Similarly, the practical implementation of secure methods is vital for widespread effectiveness, considering deploy-ability such as: negligible cost per user (D2) and compatibility with a range of browser / applications (D4).

In conclusion, the framework presented by Bonneau et al. [11] offers a nuanced evaluation of web authentication schemes, centring on a broad range of security benefits while factoring in usability and deploy-ability. A balanced methodology that is crucial for developing and adopting authentication technologies for security, accessibility and feasibility across various contexts.

2.3 Security Threats within Authentication

To effectively assess passwordless authentication addressing its issues, it’s vital to understand the evolution of security threats and cybercrime in a digital age where passwords aren’t reliant. A well-known issue with computerised systems is its dependency on humans, with deception the highest risk factor to security. Social Engineering and Phishing make up for a vast quantity of cyber-related crimes, where fake links or discussions have granted attackers unauthorized access or restricted information, aiding in ransom attacks against companies and individuals.

Though this vulnerability to security cannot be changed, it’s imperative to be aware of when developing security schemes; linking with the critical consideration against the perpetual tug-of-war between security and usability, as discussed with Bonneau et al.’s framework [11]. Existing as a repulsive relationship, where enhancing one often comes at the expense of the other. The appeal of passwordless authentication is derived from its promise of improved usability and convenience for users. However, this leads to many risks with security particularly in part with the human factor of systems. Such as the common approach for services to provide passwordless authentication, while retaining the password-based method to allow for choice. Yet, this increases the number of potential vulnerabilities for accessing systems without mitigating the known issues of password-based sign-on.

Furthermore, systems incorporating Single/Social-Sign-On are centralising the login process by outsourcing authentication to a third-party, under the assumption that the user is the owner of the connected account or social network. While increasing usability, this runs the risk of a centralised point of failure, where if the account is compromised then all connected systems are too. Similarly, Magic Link schemes rely on email communication which is not considered a fully secure medium and can be easily intercepted. If an adversary gains access to a user’s email address, the potential to intercept a magic link and authenticate themselves rises significantly. Alongside these issues of single-point vulnerability, Magic Links and OTCs are susceptible to phishing attacks and social engineering: deceiving a user through illegitimate websites or communication requests, resulting in the loss of sensitive information and access to accounts.

The paper by J.Guan et al [12] provides a formal analysis of the FIDO2 (WebAuthn & CTAP2) protocols. The researchers developed a formal model using ProVerif to analyse security assumptions and goals of the technology. Their analysis revealed several critical security vulnerabilities with the assumption of channel communication and storage security. Through the presentation of these vulnerabilities and the associated attacks, the researchers proceed to detail recommendations to address these issues.

A key finding, that piqued my interest, was the failure to achieve strong authentication properties due to an authenticated Elliptic-Curve Diffie-Helman (ECDH) key exchange within the CTAP2 protocol. Proving to be susceptible to a man-in-the-middle attack within 2nd factor authentication scenarios with the Client PIN mechanism. Where if the assumption that "$\neg A[C]$" (denoting that an attacker cannot use a compromised authenticator to communicate with a client) is not satisfied then the current PIN and new PIN mechanisms are vulnerable; similarly, the reverse assumption "$\neg C[A]$" the PIN token can be intercepted. Using this scenario, the adversary can act as a bridge between FIDO Client and a FIDO Authenticator without the knowledge of either, exploiting the ECDH to create independent key pairings to decrypt and re-encrypt information while observing everything.

The researchers also discovered authenticator rebinding attacks, where an adversary can compromise a FIDO client on the victim's device, to bind the account to a malicious authenticator. Effectively impersonating the victim. Additionally, parallel session attacks were discovered inherited from the protocol's predecessor UAF, posing a significant security risk.

The overall analysis highlighted the critical importance of rigorous security evaluation for emerging technologies like FIDO2, furthering this discussion by presenting recommendations to address the issues discovered. Particularly within the unauthenticated ECDH negotiations, there should be verification of the validity of entities in CTAP2; confirming that the FIDO Authentication and Client in each session are identical to those used in the authentication registration and subsequent authentications.

2.4 Mitigation Strategies and Effective Technologies

In researching the multitude of threats against authentication technologies, mitigating the impact of human factors is crucial against vulnerabilities. A familiar approach, acting as the cornerstone of all company security, is continuous education to keep users informed of the secure practices within the password domain. Such as using highly complex random passwords; avoiding common phrases or personal information, in addition to utilising trusted password managers. Though not restricted to the educating of password practices, these efforts aim to also educate on communication security against phishing. However, despite this the human behaviour remains a significant weakness in security. Often choosing weak passwords, reused across multiple domains, or falling victim to phishing attacks.

Even with extensive training, humans will always be prone to error and can succumb to social engineering tactics. Moreover, enforcing stricter password policies can lead to user frustration and may encourage risky behaviour. Amid these challenges comes passwordless authentication, mitigating the burden on a user and overall mitigating the risk passwords possessed. As discussed in this literature review, passwordless authentication is promising adversary to the traditional password, with technologies such as FIDO2 being coined "The Kingslayer" [13]. Additionally, technologies like Magic Links, Single Sign-On (SSO) and more streamline the authentication process while enhancing security. Leveraging cryptographic protocols and device-bound authenticators to verify users' identities.

However, these solutions are not without their own set of challenges. Biometric data can be stolen or spoofed, compromising privacy and security, leading to a legion of attacks against single-factor biometric solutions. Similarly, single-factor usage of FIDO2 and similar protocols require physical keys susceptible to theft, granting instance access to an attacker with the correct environment. As well as, requiring compatible hardware that may not be universally supported, leading to immense costs that the industry is not ready to adopt. Furthermore, Magic Links and SSO introduce singular points of failure, where compromising one account can heed potential access across many services.

Hence it is imperative that these issues can be mitigated, preserving the level of cryptographic security they provide. For instance, from the paper by J. Guan et al [12], FIDO2 inherits the vulnerability of a man-in-the-middle attack when faced with prior compromised clients and authenticators within the unauthenticated ECDH key exchange. This vulnerability can be addressed for further verification of participating entities during the entire process, linking back to registration. With new technologies, we are yet to know all the exploits accompanied, however with a combination of authentication factors through MFA it is possible to create a system that bears the good of each technology. By requiring a user to provide multiple forms of verification, through the 3 factors (inherent, possessive, knowledge) such as biometric scanning on a physical security key coupled with a time-based or geolocation OTP, it would be deemed unworthy of the amount of dedication required to exploit all components. Significantly reducing the likelihood of a successful attack; with MFA safeguarding against deceptive tactics like phishing, as separate credentials are still required to compromise the solution. Partnered with the recommendations found in this literature review, it is possible to create a unique system aimed at high security with minimal to null compromise of usability for the end-user.

3 Methodology

This methodology aims to provide a description of the expected achievements of this dissertation. Focusing on the implementation of multi-factor authentication through the integration of FIDO2 and Magic Link. A combination that leverages FIDO2's cryptographic strengths and Magic Link's one-time usage to enhance security. An approach that is not only in direct response to the concerns highlighted in the introduction, but also setting a clear framework for the subsequent sections. Outlining the requirements and specifications essential for successful development and implementation, with the primary focus to investigate whether passwordless methods can outperform traditional password-based systems within security; secondarily maintaining / improving user convenience.

3.1 Research Approach

As discussed in the literature review, passwordless authentication mechanisms are sophisticated with inherent complexity building their security benefits. Given this, a mixed-method research approach was adopted incorporating both quantitative and qualitative analysis. Creating an in-depth analysis of existing literature, to aid in contextualising the challenges faced by the online world: particularly within e-commerce. As well as a comprehensive evaluation of passwordless solutions to understand their performance within security and the vulnerabilities addressed from currents solutions.

This mixed approach is highly appropriate, due to the harnessing of both quantitative and qualitative research strengths. Where quantitative methods provide objective data that can be analysed to assess the technical aspects of a solution for efficacy, reliability and scalability. Crucial for understanding the performance of a solution and identifying measurable trends. Whereas qualitative research enriches these findings by exploring the context within which these solutions are deployed. Together, these methodologies offer a more complete understanding of both the technical and human factors driving the success of passwordless solutions.

3.2 Analysis of Existing Solutions

The digitalisation of commercial business offers convenience but also presents significant security challenges, particularly regarding personal and financial information. A 2023 UK government survey highlights vulnerabilities, with 32% of businesses experiencing data breaches/attacks, predominantly in medium and large organisations. Resulting in an average cost of £1,100 for businesses of any size, and upwards of £4,960 for large businesses per breach [14]. Where a significant proportion of attacks are phishing related [Ap.1] at 79%.

This situation that is aggravated by reduced prioritisation of cybersecurity measures among smaller businesses due to economic pressures; thereby showing a growing push for adopting passwordless solutions to mitigate the risks associated with weak password practices and endless cyber hygiene requirements. To compare, the recent 2024 survey has seen 50% of businesses experiencing breaches/attacks: 70% of medium and 74% of large businesses [15]; a significant increase on the previous year.

The integration of FIDO2 standards with Magic Link technology will illustrate a promising approach, facilitating passwordless authentication of FIDO2 using unique cryptographic credentials, significantly reducing the risk of credential theft and immunity to phishing. Complemented with Magic Link technology, which enhances security through a one-time link sent to a user's email, utilising separate trusted communication channels to achieve multi-factor authentication. This combination not only aims to bolster security but also simplifies the user experience, promoting widespread adoption. Ensuring robust protection of transactions and user data against evolving cyber threats, providing a forward-thinking solution to critical vulnerabilities identified in the survey's findings on cyber hygiene and authentication practices [14/15].

3.3 Functional Requirements

User Registration: The user must provide unique required information to complete the registration process, where an account doesn't already exist; provided through account confirmation. Following this the successful registration of a FIDO2 standard device to create and store cryptographic credentials.

User Login: The user must provide the required information to complete the authentication process, the generation and retrieval of cryptographic credentials must be successful from a FIDO2 standard device. Simultaneously, the successful generation a TOTP magic link which is sent to the user's registered email through a trusted 3rd party service provider. Where the user must access this link, serving as an additional authentication factor, further securing the login process.

Sensitive Information Access: Using multi-factor authentication to access sensitive information, meaning both authentication schemes must be successful. Furthermore, through the implementation of strict security protocols with encrypted data transit and at rest; preventing eavesdropping.

FIDO2 Authentication: The FIDO2 compliant authentication scheme must support a range of devices: successfully registering and managing cryptographic credentials. Which cannot be replicated or reused for differing accounts, limiting the credentials stored by the service to prevent the impact of cybersecurity breaches.

TOTP via Email / Magic Link Authentication: Successfully integrate a secure, trusted 3rd party email service to transmit a generated TOTP Magic Link unique to the user that initiates the login/registration process. The TOTP must be implemented to expire after a designated period of time, to protect against replay-ability attacks; authenticate / verify a user for access to the service, preventing against unauthorised access. The TOTP must be encrypted in transmit to prevent eavesdropping.

3.4 Non-Functional Requirements

Security: The implementation of the proposed authentication mechanism must provide an appropriate level of security, complying with global standards: including GDPR for data protection. Where all data transmissions, including user credentials and sensitive information, must be encrypted; multi-factor authentication as mandatory requirement for accessing data.

Reliability: The authentication mechanism must be reliable, ensuring that the user is always able to access the service when successfully authenticated. As well as, ensuring data integrity, protecting against corruption and unauthorised modification.

Compatibility: The user must be able to access, register and authenticate across multiple devices and browsers, therefore the proposed implementation needs to be functional using multiple browsers and machines for testing.

Usability: An important factor in the adoption of passwordless mechanisms, meaning that the user should be able to successfully pass authentication with ease. Where the user interface is simplistic and user friendly; considered when designing the e-commerce service to demonstrate the authentication mechanism. However, this will not be at the forefront of this project and will act as a secondary target.

3.5 Hardware Specification

In terms of hardware, the project requires no specialized equipment, making it accessible and feasible for a wide range of users and businesses. The specified minimum hardware configuration ensures broad compatibility and ease of integration, which supports the adoption of the proposed authentication system. Below are the specified requirements and their implications:

- **Dual-core CPU or better:** This specification allows the system to function on widely available hardware, avoiding the need for high-performance computing resources.
- **8GB+ of RAM:** A modest memory requirement, making the system suitable for a vast range of existing machines. This inclusivity supports organisations and users with limited technology budgets, allowing for implementation without additional investments.
- **Ethernet connection or a Wi-Fi adapter:** Despite the artifact running on localhost, by supporting standard internet connectivity options for seamless integration with most network environments.
- **20GB of storage:** A minimal storage requirement, which accounts for a suite of tooling to be implemented on e-commerce websites, including database storage and transactions. This requirement can increase with the more data and functionality a website presents.
- **FIDO2 standard security key:** In order to use the FIDO2 authentication scheme, a security key is required. By incorporating FIDO2 standard security keys, this system will align with current best practices for secure authentication. Enhancing security by requiring physical hardware-based credentials that are resistant to many common cyber threats, including phishing and credential theft. However, a physical device is still inherently susceptible to theft, and therefore the proposed system will support biometric security keys too. USB-A ensures compatibility with a range of devices, with USB-C supporting future adoption.

3.6 Software Specification

- **Development environment:** Visual Studio 2022 for running and testing the prototype.
- **Operating System:** Windows 10 is currently used for deploying the prototype, with the potential for future migration
- **Email Service:** A trusted email service, in this case Google Email for transmission of TOTP magic link to user during authentication.
- **Knowledge of FIDO2 & TOTP generation:** For implementation of authentication technologies using required libraries discussed in Design.
- **HTML & CSS:** Knowledge of this is important for implementing the front-end of the web application, which users will interact with to begin authentication via a web browser.
- **Computer programming languages:** JavaScript, C# & SQL.

4 Design

This section will provide a detailed description of the prototype for implementing the chosen authentication mechanisms; including the requirements they satisfy.

4.1 Authentication Overview

A short recap of FIDO2, which is an advanced authentication standard developed by the FIDO Alliance and W3C. Primarily consisting of two components: The Client to Authenticator Protocol (CTAP2) and Web Authentication API (WebAuthn). CTAP2 enables external devices like security keys to interface with browsers and operating systems, facilitating user authentication; while WebAuthn allows users to log into online services using biometric or hardware-based authenticators. This combination enhances security by using cryptographic credentials that are unique to each site and protects user privacy by never sharing sensitive information, like biometrics, with servers.

Magic Link authentication is a simplistic user-friendly mechanism, already widely adopted for account confirmation processes, involving the generation and transmission of a TOTP via email to users to log into services. When a user requests access to a secure area, they request a magic link, which contains a TOTP which is time sensitive embedded in the URL with a short expiration period to protect against replay-ability. The user clicks the link as taken to a verification page, where the TOTP is checked and is correct is securely logged in without the need for a password. This method streamlines authentication, reducing password fatigue and enhances security with a unique token per session, that only the rightful email recipient can use.

Combining these authentication mechanisms significantly enhances security through a layered approach:

- **Layered Defence:** Offering dual protection, where even is one method is compromised, the other serves as a safeguard against unauthorised access. Adopting the popular concept of multi-factor authentication.
- **Reduced Phishing Risk:** FIDO2's hardware-based/biometric verification paired with the transient nature of magic links, greatly mitigates the risk of phishing attacks. Due to the need to simultaneously compromise both the physical device and email account: a notably difficult task.
- **Stronger User Verification:** By requiring access to a user's email and physical device, this method ensures robust user verification, enhancing the authentication integrity.
- **Enhanced Non-repudiation:** The use of cryptographic primitives to prove a user's identity, alongside a time-sensitive

OTP creates a strong audit trail. Not only preventing unauthorised access but also ensuring transactions are traceable directly to specific users.

- **Adaptive Security Measures:** The combination enables adaptive security, where sensitive actions like login require both authentication methods, while less critical transactions may need only one. This balances robust security with user convenience, minimizing friction.

The sequence in which the authentication methods are deployed can significantly impact both security and user experience. The “Security-First” approach incorporates FIDO2 as the initial authentication step, emphasizing security: requiring physical presence of a device with cryptographic primitives, making it a highly secure first barrier. The second barrier being the magic link.

The ”User-Convenience” approach, starting with the magic link aims to offer an effortless entry point for users, with the simple click of a TOTP URL. Arguably a less intimidating approach for users unfamiliar with hardware tokens, with the higher barrier of security being second. The benefits of each ordering strategy, as well as their potential drawbacks in security, warrant thorough evaluation to determine the most effective implementation. This evaluation will be further elaborated in a later section after comprehensive testing.

4.2 Technical Architecture

The authentication artifact for integrating FIDO2 and Magic Link technologies was developed within Visual Studio 2022, leveraging ASP.NET Core and Identity frameworks: structured using the Model-View-Controller architecture to ensure clean separation of concerns, enhancing maintainability and scalability. As the aim of this dissertation is to create an authentication scheme providing multi-factor passwordless authentication for e-commerce sites, it was deemed appropriate to use a standard and universally recognised framework for building our site.

The MVC architecture works using three components dedicated to independent operations: The Model represents user data and authentication status, as well as handling all data-related logic. Responding to the Controller component upon request with information added/retrieved from the SQL database. The Controller component enables communication between the View and Model components acting as an intermediary. It doesn’t handle data logic; instead instructs the Model, processing all business logic and requests from the browser, before interacting with the View component to render the final output. As alluded, the View component handles all UI logic of the application, generating a user interface and only interacting with the Controller component. [16]

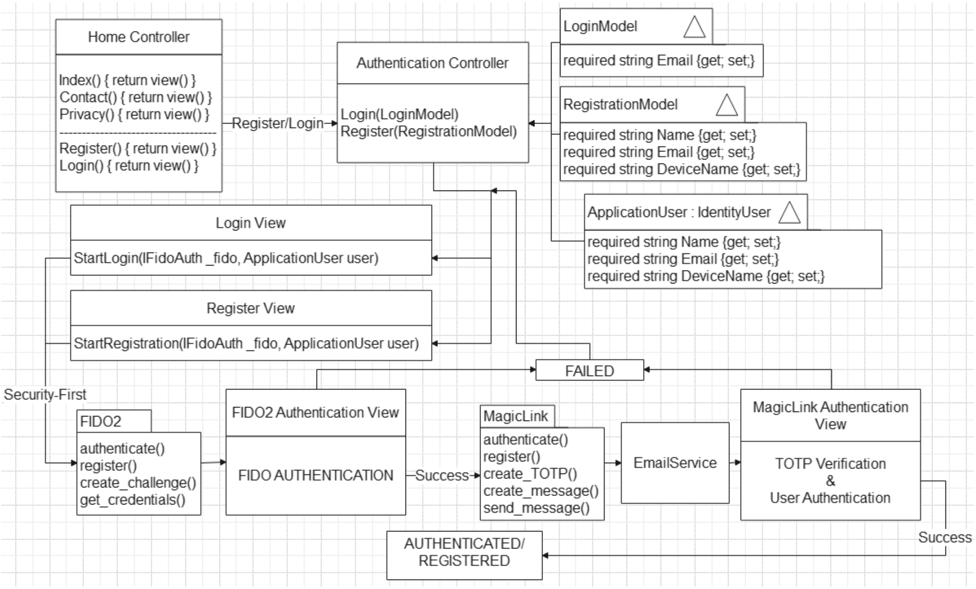

Home Controller
Index() { return view() }
Contact() { return view() }
Privacy() { return view() }
Register() { return view() }
Login() { return view() }
Register/Login
Authentication Controller
Login(LoginModel)
Register(RegistrationModel)
LoginModel
required string Email {get; set;}
RegistrationModel
required string Name {get; set;}
required string Email {get; set;}
required string DeviceName {get; set;}
ApplicationUser : IdentityUser
required string Name {get; set;}
required string Email {get; set;}
required string DeviceName {get; set;}
Login View
StartLogin(IFidoAuth _fido, ApplicationUser user)
Register View
StartRegistration(IFidoAuth _fido, ApplicationUser user)
FAILED
Security-First
FIDO2
authenticate()
register()
create_challenge()
get_credentials()
FIDO2 Authentication View
FIDO AUTHENTICATION
Success
MagicLink
authenticate()
register()
create_TOTP()
create_message()
send_message()
EmailService
MagicLink Authentication View
TOTP Verification
&
User Authentication
Success
AUTHENTICATED/
REGISTERED

Figure 1: MVC Skeleton

This architectural design ensures a clear separation of procedures, maintaining robust connections to an SQL Server that stores user information, such as *name*, *email address* and *id number*. An additional table is dedicated to storing cryptographic credentials associated with the registered FIDO2 device. This table is crucial for creating and verifying challenges to ensure the attempted users is rightful account holder. Furthermore, the architecture distinctly separates the Email Service, utilising an SMTP Client to transmit TOTP URLs, enabling users to authenticate seamlessly.

Taking the “Security-First” approach, the interactions between user, browser, FIDO2 device and architectural components are as follows:

Registration Process: Within the proposed authentication scheme, to begin registration the user must first interact with the site, navigating to the registration page from the site banner. Upon entering their basic information, such as name, email address and security key device name, the system will prompt the device registration of cryptographic credentials of the FIDO2 device [12]. Involving the connection of a FIDO2 compatible device, that supports interaction or biometric unlock, to the computer. As mentioned, then requesting the user performs an action using their FIDO2 device; a unique public-private key pair will be generated, with the private key remaining on the device and the public key being sent to the server / service. Registering this public key against the user’s profile, the server will now be able to generate challenges for future authentication. Following the successful registration with FIDO2, the system automatically generates a TOTP, encrypting and embedding it into a URL to be sent to the user's registered email address as a Magic Link. The user is required to access their email and click on this link, verifying they are the rightful owner of the account. This method also acts as an account confirmation feature which is prevalent in numerous systems today, acting as an additional factor in authentication.

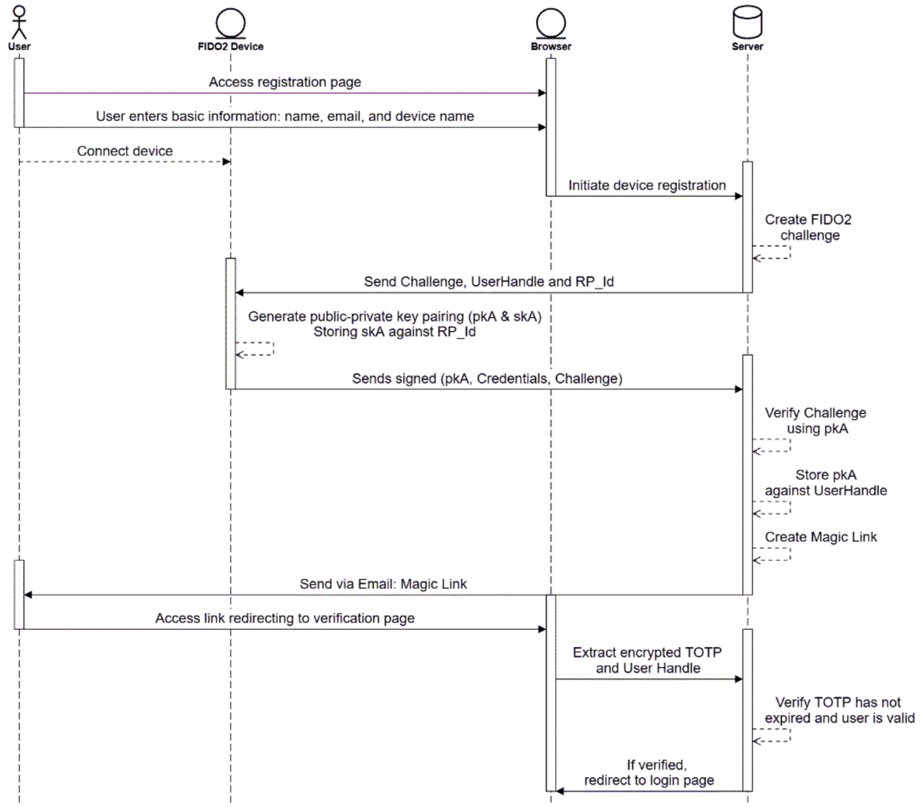

User
FIDO2 Device
Browser
Server
Access registration page
User enters basic information: name, email, and device name
Connect device
Initiate device registration
Create FIDO2 challenge
Send Challenge, UserHandle and RP_Id
Generate public-private key pairing (pkA & skA)
Storing skA against RP_Id
Sends signed (pkA, Credentials, Challenge)
Verify Challenge using pkA
Store pkA against UserHandle
Create Magic Link
Send via Email: Magic Link
Access link redirecting to verification page
Extract encrypted TOTP and User Handle
Verify TOTP has not expired and user is valid
If verified, redirect to login page

Figure 2: Registration Process

Authentication Process: To authenticate a pre-registered user within the system, they must first navigate to the login page of the site; entering their email address as means of identifying the account to authenticate. Upon doing so, the system will prompt the user to authenticate using their registered FIDO2-enabled device. Involving the server generating a challenge based on the user handle (email) to be sent to the FIDO2 device, with the relaying party ID (RP) and credentials and a nonce protecting against replay attacks. [12] From which the FIDO2 device will identify the corresponding credentials for the given RP, signing the challenge and credentials to be sent back to the server. The server then checks this signature against the stored public key of the user, verifying its integrity and authenticity before proceeding onto the distribution of magic links. Where, the generation of a TOTP is encrypted along with the user handle and embedded into a URL to redirect the user to a verification page from a trusted email service for final authentication steps. If all successful, the user is authenticated and granted access to all services.

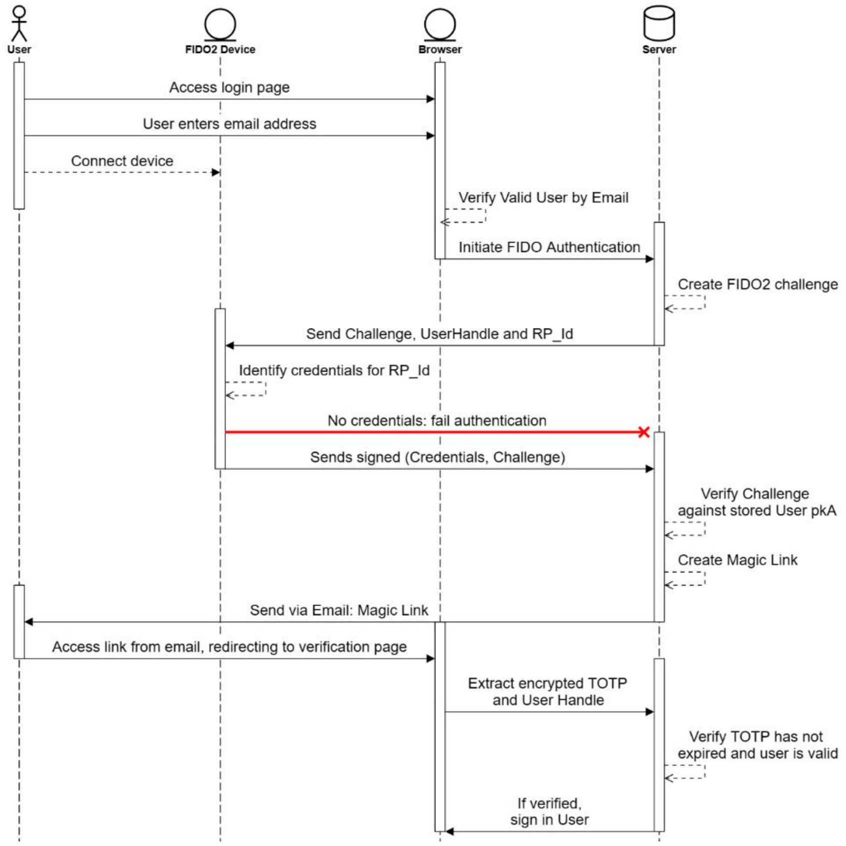

User
FIDO2 Device
Browser
Server
Access login page
User enters email address
Connect device
Verify Valid User by Email
Initiate FIDO Authentication
Create FIDO2 challenge
Send Challenge, UserHandle and RP_Id
Identify credentials for RP_Id
No credentials: fail authentication
Sends signed (Credentials, Challenge)
Verify Challenge against stored User pkA
Create Magic Link
Send via Email: Magic Link
Access link from email, redirecting to verification page
Extract encrypted TOTP and User Handle
Verify TOTP has not expired and user is valid
If verified, sign in User

Figure 3: Authentication Process

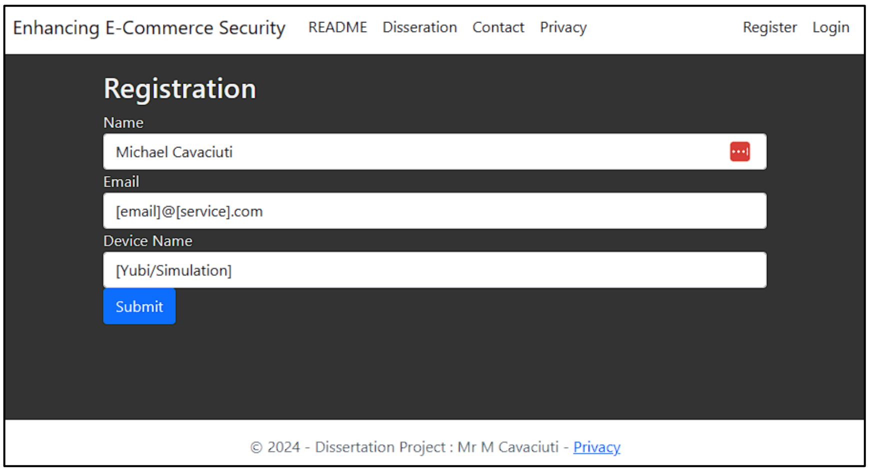
4.3 Implementation

With the implementation of this ASP.NET MVC project, we aim to establish a robust and secure authentication system: requiring focus on integrating both FIDO2 and Magic Link schemes efficiently and independently for maintainability. This implementation will involve configuring essential services, setting up middleware and crafting endpoints that handle the registration and authentication processes mentioned prior.

4.3.1 FIDO2 Integration

Through extensive research into the FIDO2 market, the selection of the RSK-FIDO2 library from IdentityServer [17] for our project was driven by its robust support for web authentication, making it an ideal choice for implementing passwordless authentication mechanisms. With the additional support for current password-based systems as multi-factor authentication. This library seamlessly integrates with the ASP.NET Core and Identity frameworks, simplifying the development of security features by leveraging built-in functionality: user management and role-based access control to name a few.

Registration: Within the registration the users are required to populated fields for their name, email address and device name, as seen in Figure 4. The system utilises the ASP.NET Identity framework to verify that the user does not already exist by ensuring that each email address is unique. For instance, registration attempts by two users sharing the same email address will be denied, although it is permissible for multiple users with the same name to register using differing email addresses.



Registration

Name: Michael Cavaciuti

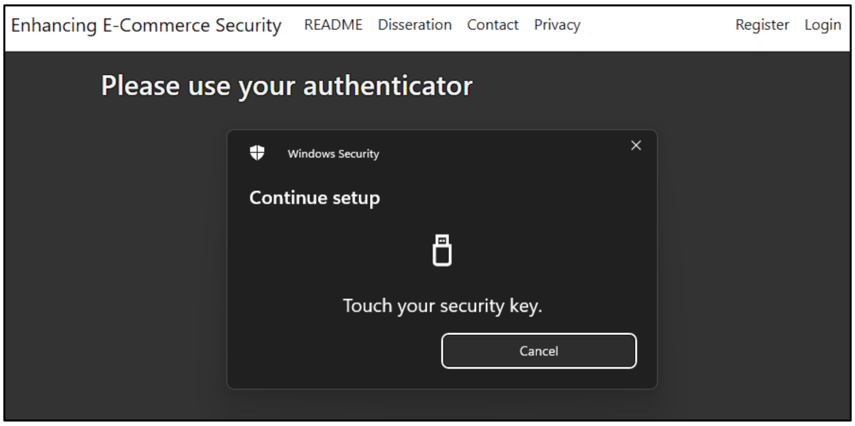
Email: [email]@[service].com

Device Name: [Yubi/Simulation]

© 2024 - Dissertation Project : Mr M Cavaciuti - Privacy

Figure 4: Registration Page

Upon submission of valid entries, the system leverages the '*IFidoAuthentication*' interface provided by the RSK-FIDO2 library to generate a challenge. This challenge is uniquely associated with the user's handle (email) and is used to prompt a FIDO2-compliant device to create credentials for the relying party (service) against the user. Following this, the user is directed to a verification page, instructing them to authenticate using the security device. A request is made, attempting to interact with the connected device using generated encoded credentials (containing challenge; service id; user; public key credential parameters – selection of supported algorithms). As illustrated in Figure 5, this request utilises the Windows Security feature to detect a security key, subsequently initiating the creation of a public-private key pair that will be used for future authentication.



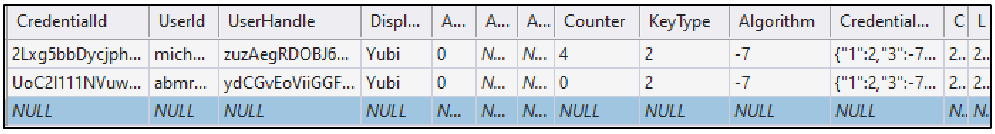
Please use your authenticator

Continue setup

Touch your security key.

Figure 5: FIDO2 Device Interaction

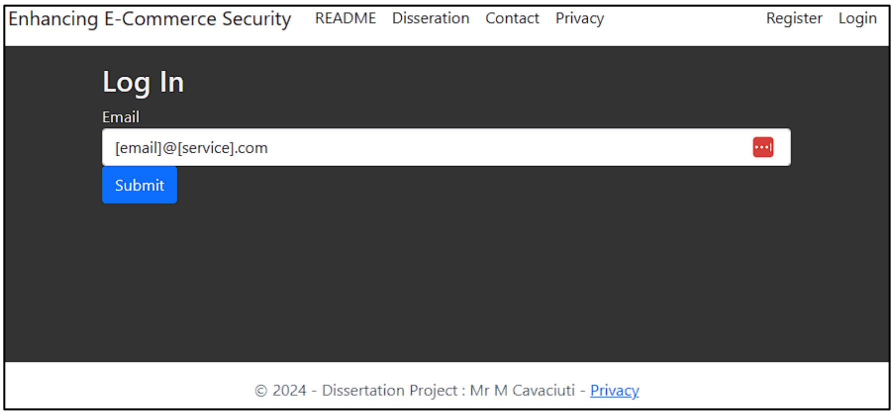
Once a valid security key is registered for the user, the corresponding public key is securely stored in a SQL Server database within the FIDO_keys table, as shown in Figure 6. Access to this table is strictly controlled and only permissible during registration and authentication processes.



CredentialId	UserId	UserHandle	Displ...	A...	A...	A...	Counter	KeyType	Algorithm	Credential...	C	L
2Lxg5bbDycjph...	mich...	zuzAegRDOBJ6...	Yubi	0	N...	N...	4	2	-7	{"1":2,"3":-7...	2..	2..
UoC2I111NVuw...	abmr...	ydCGvEoViiGGF...	Yubi	0	N...	N...	0	2	-7	{"1":2,"3":-7...	2..	2..
NULL	NULL	NULL	NULL	N...	N...	N...	NULL	NULL	NULL	NULL	N..	N..

Figure 6: FIDO_Keys Table

Authentication: When attempting to access the services offered by the site, the user must begin by navigating to the login page where they are required to enter the email address registered with their account. This step is crucial in identifying the account for authentication, as the email is a unique identifier for retrieving the corresponding user details. If the email does not match any registered accounts, an error will persist, informing the user of the invalid entry. This ensures that authentication processes are only initiated for existing users, as depicted in Figure 7.



Log In

Email

[email]@[service].com

© 2024 - Dissertation Project : Mr M Cavaciuti - Privacy

Figure 7: Login Page

After the submission of a valid email address, the system will proceed to generate a cryptographic challenge using the '*IFidoAuthentication*' entity, constructing the challenge based on the user's handle (email). The challenge is crucial for verifying the user's identity in a secure manner without transmitting sensitive information. Retrieving the necessary details from the '*FIDO_keys*' SQL table, such as the public-key algorithm, the system will encode the credentials to be requested of the FIDO2-compliant device. Using the stored private key corresponding to the credentials on the server, the device signs the challenge, generating a response back that includes the signed challenge and other cryptographic assertions needed for verification.

Upon receiving the cryptographic credentials from the device, the server verifies the signed challenge using the public key from the database. If successful, the user is authenticated for the first stage of authentication. This process is visualised using the same design as Figure 5, facilitated using a FIDO.js file, ensuring all cryptographic operations adhere to the security standards required.

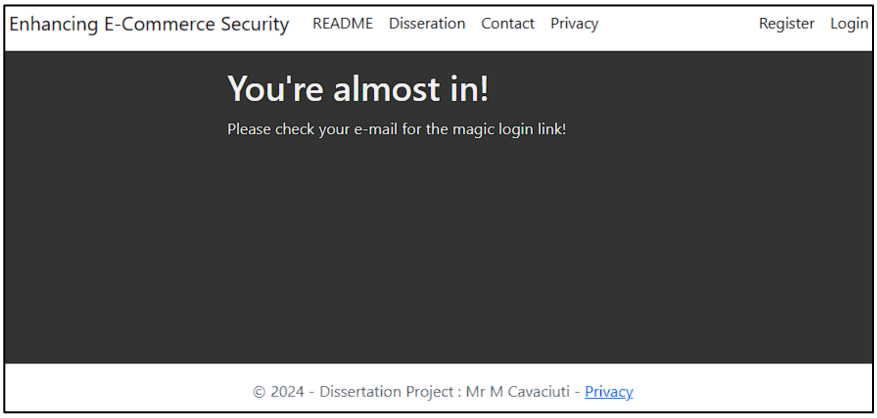
Following each process, they must successfully authenticate using the magic link scheme of TOTP via Email, before account creation or authentication.

4.3.2 Magic Link Integration

Adopting the ‘Security-First’ approach, our system employs a two-step authentication process: initially authenticating using a FIDO2-compliant device, followed by Magic Link authentication. The second step involves the user receiving a URL link embedded with an encrypted TOTP for secure verification.

To facilitate this authentication, a trusted and robust Email Service Provider (ESP) is integral to our system. Within the ASP.NET artifact, this capability is implemented through an SMTP client [] that establishes a connection to an ESP such as Gmail or Outlook. This setup not only enables the dispatch of Magic Links via email but also ensures that these communications are reliable and secure. Each email is UTF-8 encoded to support a wide range of characters and symbols.

Using the ASP.NET Identity framework, a unique TOTP token is generated based on user details, ensuring that each token is unique and bound to a specific user account. The token is then securely encrypted using AES-GCM [18] along with the user’s identification details, and subsequently embedded into a URL to the verification page using an HTML encoder. The final URL is then sent to the user’s email address for authentication using the SMTP client, as depicted in Figure 8.



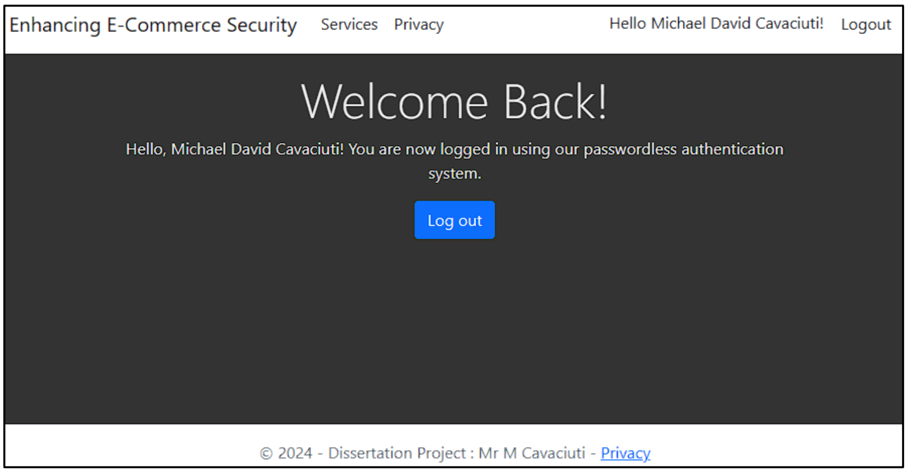
You're almost in!

Please check your e-mail for the magic login link!

© 2024 - Dissertation Project : Mr M Cavaciuti - Privacy

Figure 8: URL TOTP via Email Sent

Within the user's inbox, in the received email they will click 'magic link' and be redirected to the TOTP verification. On this page, the encrypted token and user identification is extracted from the URL and decrypted. Once we have the original token and user identification, using the Identity framework we can verify the generated user token using the same token provider for generation. If successful, the user account will either be registered for the registration process or authenticated and granted access to the services provided by our site: transactions, communications etc. An authenticated user is shown in Figure 9.



Enhancing E-Commerce Security
Services
Privacy
Hello Michael David Cavaciuti!
Logout

Welcome Back!

Hello, Michael David Cavaciuti! You are now logged in using our passwordless authentication system.

Log out
© 2024 - Dissertation Project : Mr M Cavaciuti - Privacy

Figure 9: Authenticated User

4.4 Artifact Testing

To evaluate the robustness and functionality of our authentication schemes, we utilised a simulated FIDO2 security key. This approach allowed for systematically testing the authentication process under controlled conditions, mimicking real-world user interaction without the need for a physical security device. The simulation was conducted using online resources and tooling published on GitHub [19], where I had discussions with the developer to understand the programming and achievements of such a tooling. The tool was configured to interact with our system just as an actual hardware security key would, providing consistent, reproducible inputs for testing purposes.

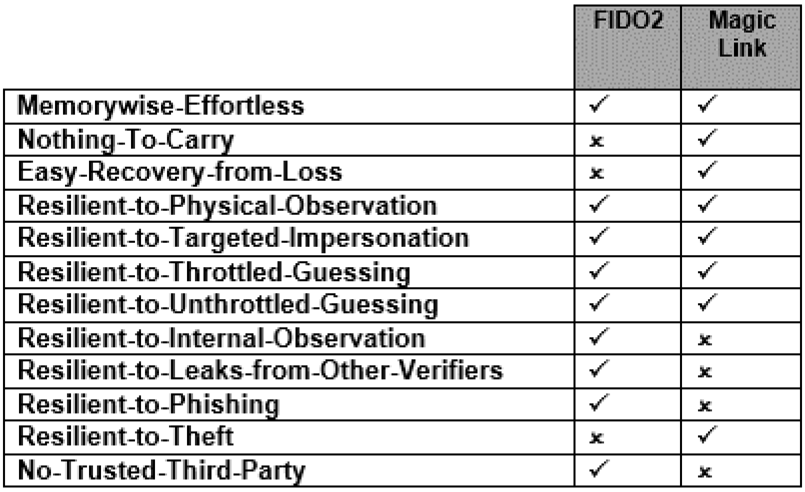
The primary objectives of this testing were to: verify the system integration, ensuring that the system correctly communicates with FIDO2 devices and ESP's; test the system's ability to handle errors or unusual responses, such as failed authentications or corrupted data transmissions; lastly confirm that all cryptographic operations, such as challenge generation and verification, are executed securely and in accordance with specification.

In the following section, I shall evaluate the system based on the tests, discussing how well the system safeguards against potential security threats and considering the usability despite using a simulated device for testing.

5 Evaluation

In the pursuit of enhancing the security framework of e-commerce platforms, this study integrated two primary passwordless authentication technologies: FIDO2 and Magic Link. This evaluation of these technologies focuses on their ability to mitigate the inherent vulnerabilities of traditional password-based systems and their efficacy in preventing new or adapted types of cyber threats.

In accordance with the framework for evaluating passwordless authentication mechanisms presented by Bonneau et al. [11], below is a table detailing the capabilities of our chosen authentication solution:



	FIDO2	Magic Link
Memorywise-Effortless	✓	✓
Nothing-To-Carry	×	✓
Easy-Recovery-from-Loss	×	✓
Resilient-to-Physical-Observation	✓	✓
Resilient-to-Targeted-Impersonation	✓	✓
Resilient-to-Throttled-Guessing	✓	✓
Resilient-to-Unthrottled-Guessing	✓	✓
Resilient-to-Internal-Observation	✓	×
Resilient-to-Leaks-from-Other-Verifiers	✓	×
Resilient-to-Phishing	✓	×
Resilient-to-Theft	×	✓
No-Trusted-Third-Party	✓	×

Figure 10: Bonneau et al. Framework

5.1 Authentication Ordering

The sequencing of authentication methods plays a pivotal role in ensuring the robustness of the security framework, as it is known that the combination of two schemes in cryptography does not always improve security. For this reason, we explored two sequencing strategies:

Security-First Approach: Beginning with the strong cryptographic verification of FIDO2, the system establishes a secure session before generating a Magic Link and sending it to the user’s registered email. This sequence prioritises high security, making it suitable for highly confidential operations requiring stringent security measures. Though this method does have its potential flaws, where an adversary could compromise the user’s registered email address and lie dormant, awaiting the user to begin the authentication process and steal the magic link to authenticate themselves: granting unauthorised access to the user’s account and services. Despite this, the approach with FIDO2 at the forefront of authentication creates a strong first barrier to potential attackers, and with its higher security assurance protects against brute-force, credential reuse and phishing attacks.

User-Convenience Approach: As the name suggests, starting with the Magic Link authentication, involving a time-sensitive OTP to the user’s registered email, can enhance the user experience. Reducing the upfront authentication barriers and bolstering subsequent security with FIDO2 authentication. By integrating the stronger authentication scheme second, this approach deals with the issue of a potentially compromised email address with the physical security key still required to access the account and services. However, this approach is still susceptible to phishing or man-in-the-middle attacks due to the reliance on the security of the 3rd party service: Email Service.

Despite the potential flaws of each, the ‘User-Convenience’ approach is more likely to be adopted with less resistance, with the necessity of rigorous security measures around email services, including advanced spam filters and phishing detection techniques. However, this presents an opportunity for an adaptive security strategy in future to dynamically select the type of approach depending on the sensitivity of the interaction, or role of the user.

5.2 Encryption and Data Security

Our implementation utilises NIST recognised encryption standards through the form of AES-GCM to encrypt the transmission of authentication tokens and user credentials over any network to prevent against interception. As well as, making any user information leaving the server/site unidentifiable when viewing data records within our SQLServer. Due to constraints with time regarding this project, we were unable to use the encryption techniques on stored data within our database, failing to adhere to GDPR at current. However, this would be the first step before deploying this solution. With current cyber hygiene it is our assumption that all services and e-commerce platforms already adhere to the data security standards issued by institutions such as NIST and the GDPR.

5.3 Usability Evaluation

While the primary focus, as detailed in the methodology, was to enhance security using passwordless authentication, understanding the impact on user experience is crucial. However, due to the time constraints of this project, we were unable to include comprehensive usability testing to validate and refine the proposed authentication methods. Future work should include this, thereby enhancing both security and user engagement in real-world applications. The proposed methodology of this usability testing would the aim to assess ease of use, focusing on understanding user interaction; identify user pain-points, understanding where users may experience confusion and frustration; evaluate user satisfaction; finally testing accessibility.

All of which would aid in the support and deployability of passwordless schemes.

To test usability, we suggest using surveys to collect quantitative data on users' experiences, as well as: task completion tests, interviews and focus groups. Where in each method users are presented with the two variants of the authentication sequence to determine which provides a better user experience. See Appendix A for a draft of a survey and task completion test.

5.4 Methodology & Research Questions

Here it is our aim to evaluate the methodology and reflect on the research questions laid out in the introduction.

Methodology Assessment: Through theoretical analysis, this dissertation reviewed extensive literature on passwordless authentication, establishing a theoretical base and highlighting development areas and challenges. Most of which were taken forth in the system design and implementation to allow for a practical exploration of the subject and understand its real-world applications. The goal of our methodology was to implement a functioning registration and authentication site for demonstrating the combined security of FIDO2 and Magic Link technologies; detailing the benefits of a passwordless system for e-commerce sites that are at the heart of cyber attacks in our digital age. We believe through simulated scenarios and theoretical assessments within this evaluation, this was achieved; however, usability is a major factor in authentication acting as the balance against security for the 'perfect' scheme.

Research Questions Revisited: Reflecting on the questions proposed in the introduction, the successful integration of FIDO2 and Magic Link authentication does significantly bolster security when addressing vulnerabilities associated with traditional password-based systems, due to the incorporation of two-factor/multi-factor authentication. A solution with a layered defence mechanism, where the user must own the physical device, have knowledge and access to a valid email address, and in some cases the FIDO2 device is locked by biometric data – inherent of the user. As discussed, we are unable to address the compromise/balance of the security with user experience until further research has been conducted, a valuable key aspect that is missing from this dissertation. The evaluation framework presented by Bonneau et al [11] is a key framework for measuring security and usability of passwordless practices, with new models and frameworks being developed each year, as passwordless schemes become more common. Linking this to the discussions of new threats and potential risks, it is imperative that communication channel security is strongly considered when developing such schemes.

6 Conclusion

This dissertation embarked on the exploration into passwordless mechanisms within the context of e-commerce security, driven by the increasing vulnerability of traditional password-based systems against the growing risk of cyber threats. Through a comprehensive study integrating theoretical research, system design and security evaluation, we critically analysed the potential for combining passwordless schemes, such as FIDO2 and Magic Link, to provide a more secure authentication framework. With the opportunity to take this research further to assess the usability of the proposed solution.

6.1 Key Findings

Enhanced Security: The integration of the two authentication schemes has demonstrated significant potential for enhancing security within e-commerce platforms, through eliminating the reliance on traditional passwords. Combatting risks such as phishing, brute force, and other forms of cyberattacks. Passwordless authentication mechanisms offer a more robust defence against unauthorised access, increasing the difficulty and resistance to an adversary with the goal of stealing information or control.

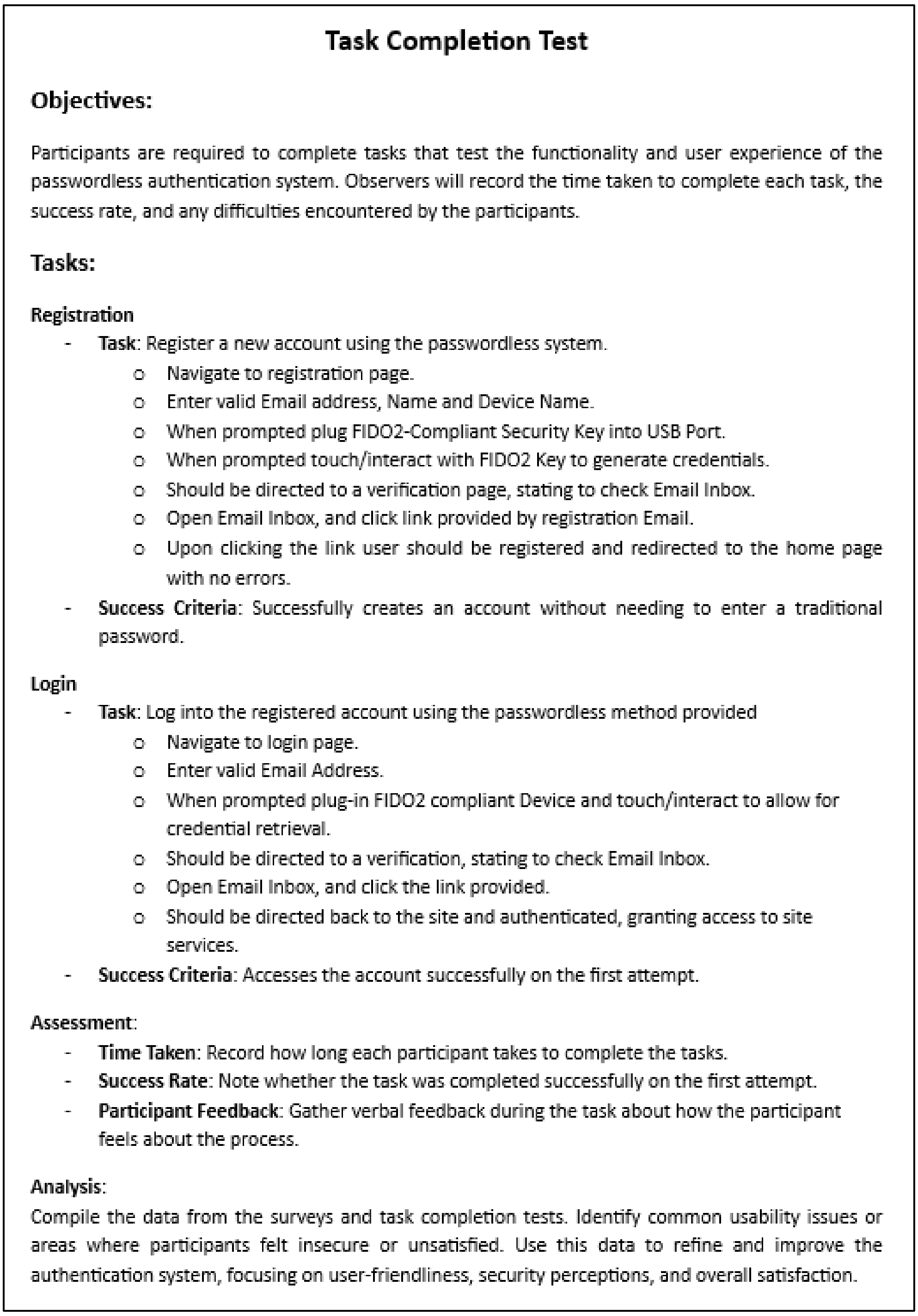
Usability Considerations: Although the full scope of usability testing could not be realised within the timeframe of this study, initial theoretical analysis suggests that the path to a ‘perfect’ authentication scheme cannot be created due to the balance between security and usability. A system cannot yet be 100% user-friendly and incorporate the highest level of security; for example, with FIDO2 devices, the recovery mechanism is troublesome and difficult [20], while being prone to theft and loss.

New Challenges: The shift towards passwordless authentication does not come without introduction of new challenges, particularly in terms of device security (from theft) and the integrity of email services, relying on 3rd party security for technologies such as Magic Links. Though the potential of passwordless schemes, the transition should be managed carefully to address new vulnerabilities and may take some time to convince the password-reliant world that it is time for change.

In conclusion, this dissertation supports the growing consensus that passwordless authentication represents the future of secure digital interactions in e-commerce and beyond. By advancing our understanding of how such systems can be implemented effectively, this research contributes to the broader field of cybersecurity, advocating for a shift towards more secure, efficient, and user-centred authentication methods.

Appendix A

Task Completion Assessment for Usability



Task Completion Test

Objectives:

Participants are required to complete tasks that test the functionality and user experience of the passwordless authentication system. Observers will record the time taken to complete each task, the success rate, and any difficulties encountered by the participants.

Tasks:

Registration

- **Task**: Register a new account using the passwordless system.
  - Navigate to registration page.
  - Enter valid Email address, Name and Device Name.
  - When prompted plug FIDO2-Compliant Security Key into USB Port.
  - When prompted touch/interact with FIDO2 Key to generate credentials.
  - Should be directed to a verification page, stating to check Email Inbox.
  - Open Email Inbox, and click link provided by registration Email.
  - Upon clicking the link user should be registered and redirected to the home page with no errors.
- **Success Criteria**: Successfully creates an account without needing to enter a traditional password.

Login

- **Task**: Log into the registered account using the passwordless method provided
  - Navigate to login page.
  - Enter valid Email Address.
  - When prompted plug-in FIDO2 compliant Device and touch/interact to allow for credential retrieval.
  - Should be directed to a verification, stating to check Email Inbox.
  - Open Email Inbox, and click the link provided.
  - Should be directed back to the site and authenticated, granting access to site services.
- **Success Criteria**: Accesses the account successfully on the first attempt.

Assessment:

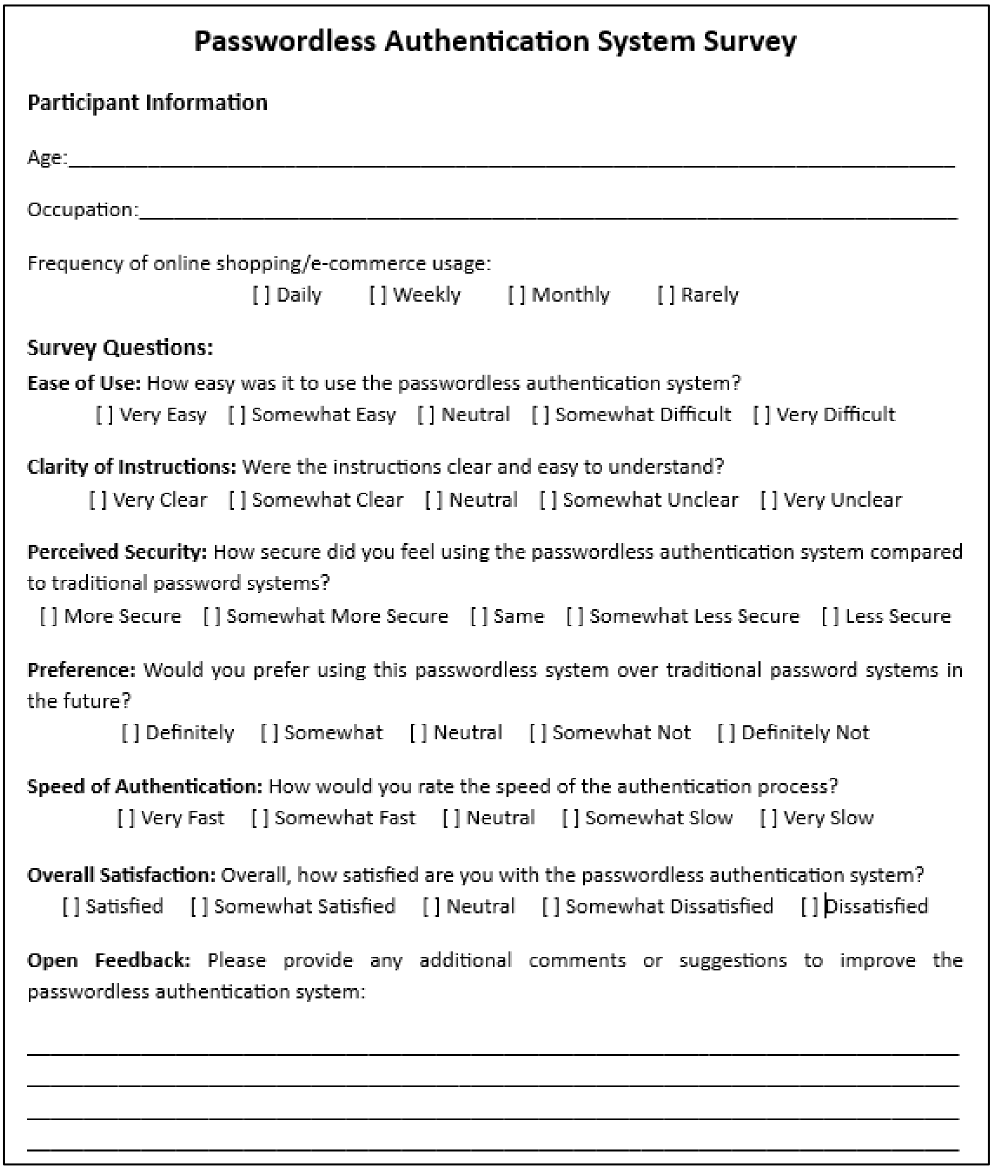
- **Time Taken**: Record how long each participant takes to complete the tasks.
- **Success Rate**: Note whether the task was completed successfully on the first attempt.
- **Participant Feedback**: Gather verbal feedback during the task about how the participant feels about the process.

Analysis:

Compile the data from the surveys and task completion tests. Identify common usability issues or areas where participants felt insecure or unsatisfied. Use this data to refine and improve the authentication system, focusing on user-friendliness, security perceptions, and overall satisfaction.

Appendix A

Survey Following the Task Completion Assessment



Passwordless Authentication System Survey

Participant Information

Age:____

Occupation:____

Frequency of online shopping/e-commerce usage:
[ ] Daily [ ] Weekly [ ] Monthly [ ] Rarely

Survey Questions:

Ease of Use: How easy was it to use the passwordless authentication system?
[ ] Very Easy [ ] Somewhat Easy [ ] Neutral [ ] Somewhat Difficult [ ] Very Difficult

Clarity of Instructions: Were the instructions clear and easy to understand?
[ ] Very Clear [ ] Somewhat Clear [ ] Neutral [ ] Somewhat Unclear [ ] Very Unclear

Perceived Security: How secure did you feel using the passwordless authentication system compared to traditional password systems?
[ ] More Secure [ ] Somewhat More Secure [ ] Same [ ] Somewhat Less Secure [ ] Less Secure

Preference: Would you prefer using this passwordless system over traditional password systems in the future?
[ ] Definitely [ ] Somewhat [ ] Neutral [ ] Somewhat Not [ ] Definitely Not

Speed of Authentication: How would you rate the speed of the authentication process?
[ ] Very Fast [ ] Somewhat Fast [ ] Neutral [ ] Somewhat Slow [ ] Very Slow

Overall Satisfaction: Overall, how satisfied are you with the passwordless authentication system?
[ ] Satisfied [ ] Somewhat Satisfied [ ] Neutral [ ] Somewhat Dissatisfied [ ] Dissatisfied

Open Feedback: Please provide any additional comments or suggestions to improve the passwordless authentication system:

____
____
____
____

Bibliography

[1] Morris, R., & Thompson, K. (1979). Password Security: A Case History. *Commun. ACM*, 594-597. doi:10.1145/359168.359172

[2] Corbato, F. J., Merwin-Daggett, M., & Daley, R. C. (1992). CTSS: The Compatile Time-Sharing System (1962). *IEEE Annals of the History of Computing, 14*, 31-54. doi:10.1109/85.145324

[3] Biddle, R., Chiasson, S., & Oorschot, P. C. (2012). Graphical Passwords: Learning from the first twelve years. doi:10.1145/2333112.2333114

[4] Ometov, A., Bezzateev, S., Makitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. doi:10.3390/CRYPTOGRAPHY2010001

[5] Parmer, V., Sanghvi, H., Patel, R., & Pandya, A. (2022). A Comprehensive Study on Passwordless Authentication. *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 1266-1275.

[6] Clercq, J. D. (2002). Single Sign-On Architetcure. *Infrastructure Security, International Conference, InfraSec 2002*, (pp. 40-58). doi:10.1007/3-540-45831-X_4

[7] Hsieh, W., & Leu, J. (2011). Design of a time and location based One-Time Password authentication scheme. *2011 7th International Wireless Communications and Mobile Computing Conference*, 201-206. doi:10.1109/IWCMC.2011.5982418

[8] Chowhan, R., & Tanwar, R. (2019). Password-Less Authentication: Methods for User Verification and Identification to Login Securely Over Remote Sites. In *Machine Learning and Cognitive Science Applications in Cyber Security* (pp. 190-212). doi:10.4018/978-1-5225-8100-0.ch008

[9] Matiushin, I., & Korkhov, V. (2021). Passwordless Authentication using Magic Link Technology. *9th International Conference "Distributed Computing and Grid Technologies in Science and Education"*, (pp. 434-438). doi:10.54546/MLIT.2021.89.13.001

[10] Al Kabir, M., & Elmedany, W. (2022). An Overview of the Present and Future of User Authentication. *2022 4th IEEE Middle East and North Africa COMMunications Conference*, (pp. 10-17). doi:10.1109/MENACOMM57252.2022.9998304

[11] Bonneau, J., Herley, C., Oorschot, P., & Stajano, F. (n.d.). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *2012 IEEE Symposium on Security and Privacy*, (pp. 553-567). doi:10.1109/SP.2012.44

[12] Guan, J., Li, H., Ye, H., & Zhao, Z. (2022). A Formal Analysis of the FIDO2 Protocols. *European Symposium on Research in Computer Security.* doi:10.1007/978-3-031-17143-7_1

[13] Ghorbani Lyastani, S., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020). Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. *2020 IEEE Symposium on Security and Privacy (SP)*, 268-285. doi:10.1109/SP40000.2020.00047

[14] Johns, E., & Ell, M. (2023). *Cyber Security breaches survey 2023.* Retrieved from GOV.UK: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

[15] Ell, M., & Rizvi, S. (2024). *Cyber Security breaches survey 2024.* Retrieved from GOV.UK: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024

[16] GeeksForGeeks.Org. (2024). *.NET MVC Framework*. Retrieved from https://www.geeksforgeeks.org/mvc-framework-introduction/

[17] IdentityServer.Com. (2023). *FIDO2 for ASP.NET - RSK Documentation*. Retrieved from https://www.identityserver.com/documentation/fido2/quickstarts/installation/

[18] Microsoft. (n.d.). *AES-GCM Class - .NET API*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.aesgcm?view=net-8.0

[19] Lglesia, C. d. (2024). *Virtual Fido*. Retrieved from GitHub: https://github.com/bulwarkid/virtual-fido

[20] Kunke, J., Wiefling, S., Ullmann, M., & Lo Iacono, L. (2021). Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication. *Open Identity Summit 2021.*