

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

Click or tap here to enter text.

Statement of Ethics

Click or tap here to enter text.

Table of Contents

[Executive summary 8](#_Toc164791721)

[1 Introduction 1](#_Toc164791722)

[1.1 Motivation 1](#_Toc164791723)

[1.2 Problem Scenario 2](#_Toc164791724)

[1.3 Research Questions 2](#_Toc164791725)

[2 Literature Review 3](#_Toc164791726)

[2.1 Evolution of Authentication Methods 3](#_Toc164791727)

[**2.1.1** **Traditional Passwords** 3](#_Toc164791728)

[**2.1.2** **Two-Factor and Multi-Factor Authentication** 4](#_Toc164791729)

[**2.1.3** **Notable Authentication** 5](#_Toc164791730)

[**2.1.4** **Biometric Authentication** 6](#_Toc164791731)

[**2.1.5** **Passwordless Authentication** 7](#_Toc164791732)

[2.2 Evaluation Method of Passwordless Authentication 10](#_Toc164791733)

[2.3 Security Threats within Authentication 11](#_Toc164791734)

[2.4 Mitigation Strategies and Effective Technologies 12](#_Toc164791735)

[3 Methodology 15](#_Toc164791736)

[3.1 Research Approach 15](#_Toc164791737)

[3.2 Analysis of Existing Solutions 15](#_Toc164791738)

[3.3 Functional Requirements 16](#_Toc164791739)

[3.4 Non-Functional Requirements 16](#_Toc164791740)

[3.5 Hardware Specification 17](#_Toc164791741)

[3.6 Software Specification 17](#_Toc164791742)

[4 This is a new chapter 18](#_Toc164791743)

[5 This is a new chapter 19](#_Toc164791744)

[6 This is a new chapter 20](#_Toc164791745)

[Appendix A 21](#_Toc164791746)

[Appendix B 22](#_Toc164791747)

[Bibliography 23](#_Toc164791748)

Table of Figures

[**Figure 1.1**: A figure containing UoY logo and its caption. 2](file:///C:\Users\lilia\Google%20Drive\UoY%20Admin\CBoE\Assessment%20Paper%20Templates\FinalYearReportTemplate.docx#_Toc525300866)

Table of Tables

[**Table 1.1**: A table with its caption. 2](#_Toc525300873)

# Executive summary

# 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.

## 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.

## 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.

## 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?

# 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.

## 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 (1979) [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.

In exploring advancements beyond traditional password protocols, there were attempts 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 aimed not only to bring enhancement of memorability and usability but also to bring increase in security by diversifying the password domain. This approach was, however, vulnerable to the same weaknesses as that of conventional passwords: making it a user's burden to accurately remember the exact context or pattern 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.

## 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.

## 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 “” (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 “” 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.

## 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; furthermore, MFA will safeguard against deceptive tactics like phishing, as even with one factor obtained, additional credentials are still required separate to the compromised solution. Partnering this approach 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.

# Methodology

This methodology aims to provide a description of the expected achievements of this dissertation. As outlined in the introduction, the need for passwordless authentication is promising; this dissertation will define an implementation for multi-factor authentication using passwordless schemes. Included in this chapter will be the requirements and specifications for a successful implementation of the prototype utilising both FIDO2 and Magic Link (TOTCs) technology.

## Research Approach

As discussed in the literature review, passwordless authentication mechanisms are sophisticated with inherent complexity building their security benefits. Given this, a qualitative research approach was adopted incorporating an in-depth analysis of existing literature, to aid in contextualising the challenges faced by the online world: particularly within e-commerce and its vulnerabilities of currents solutions.

## 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 impetus 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].

## 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.

## 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.

## Hardware Specification

In terms of hardware, there are no necessary specifications for the hosting server for the project to operate. A standard system configuration consisting of:

* Dual-core CPU or better for processing
* 4GB+ of RAM
* Ethernet connection or a Wi-Fi adapter
* 20GB of storage
* FIDO2 standard security key for USB-A

## Software Specification

[Visual Studio 2022, ASP.NET Core etc]

# Design

# Evaluation

# Conclusion

# Appendix A

# Appendix B

# Bibliography

|  |  |
| --- | --- |
| [1] | J. Zobel, Writing for computer science, Springer, 2015. |