



**Inclusive Threat Modelling: Identifying and
Mitigating Cybersecurity Risks Faced by People
with Multiple Sclerosis**

Snow White

BSc (Hons) Ethical Hacking

School of Design and Informatics

Abertay University

2025/26

Note that Information contained in this document is for educational purposes.

Contents

Table of Figures	5
Table of Tables	6
Acknowledgements.....	7
Abstract.....	8
Abbreviations, Symbols and Notation	10
1 Introduction	11
1.1 Background.....	11
1.2 Aim.....	12
1.3 Objectives	12
1.4 Structure of the Dissertation	13
2 Literature Review	14
2.1 Introduction.....	14
2.2 Usable Security, Privacy, and Authentication Systems	16
2.2.1 Password-Based Authentication	16
2.2.2 Multi-Factor Authentication (MFA).....	18
2.2.3 Account Recovery Mechanisms	18
2.2.4 Usable Security and Human Behaviour.....	19
2.2.5 Privacy Risks in Authentication and Recovery	20
2.2.6 Standards and Current Best Practices.....	20
2.2.7 Summary	21
2.3 Accessibility and Inclusive Authentication	22
2.3.1 Accessibility, Disability, and Interaction Barriers	22
2.3.2 Cognitive Accessibility and Authentication	22

2.3.3	Motor Accessibility and Interaction Cost	23
2.3.4	Inclusive Authentication Principles	24
2.3.5	Accessibility as a Security and Privacy Concern	24
2.3.6	Summary	25
2.4	Challenges for Users with Multiple Sclerosis in Authentication.....	26
2.4.1	Cognitive Challenges and Authentication	26
2.4.2	Motor and Sensory Challenges in Authentication	26
2.4.3	Fatigue, Variability, and Interaction Consistency.....	27
2.4.4	Implications for Security and Privacy Risk.....	27
2.4.5	Summary	28
2.5	Gaps in Existing Research	29
3	Methodology.....	31
3.1	Research Approach.....	31
3.2	System Scope and Modelling Strategy	32
3.3	Threat Modelling Frameworks	34
3.3.1	STRIDE	34
3.3.2	LINDDUN	35
3.4	Inclusive Adaptation for Multiple Sclerosis	36
3.5	Prototype Design Methodology	37
3.5.1	Purpose and Scope of the Prototype	37
3.5.2	Prototype Overview	37
3.5.3	Authentication and Recovery Flow Design	40
3.5.4	Prototype Limitations.....	48
3.6	Tools and Artefacts.....	49
3.7	Ethical Considerations and participants	49
3.8	Evaluation Strategy.....	50

3.9	Summary.....	51
4	Results.....	52
4.1	Introduction.....	52
4.2	System Usability Scale (SUS) Results	52
4.3	Heuristic Evaluation Results	54
4.4	Qualitative Feedback results	55
4.4.1	Positive Themes Identified.....	55
4.4.2	Suggested Improvements	56
4.5	Summary of Results	57
5	Discussion.....	58
5.1	Introduction.....	58
5.2	Objective 1: Analysis of Authentication and Account Recovery Using Threat Modelling.....	58
5.3	Objective 2: Adapting STRIDE and LINDDUN to Incorporate Accessibility.....	60
5.4	Objective 3: Identification of Accessibility-Driven Security and Privacy Risks	61
	Phishing Susceptibility	62
	Privacy Risks	62
5.5	Objective 4: Development of Inclusive Security Guidelines.....	62
5.6	Objective 5: Prototype Implementation and Evaluation.....	63
5.7	Significance of Findings	65
5.8	Limitations	66
5.9	Summary.....	67
6	Conclusion and Future Work	68
6.1	Conclusion	68
6.2	Future Work.....	69
	References	71
	Appendices.....	76

Appendix A – System Context Diagram 76

Appendix B– DFD Diagram 79

Appendix C – STRIDE Table 82

Appendix D – LINDDUN Table 85

Appendix E – Registration Flow Diagram..... 88

Appendix F – Authentication (Login) Flow Diagram 89

Appendix G – Account Recovery Flow Diagram..... 90

appendix H – Prototype Code 92

Appendix I – Data Management Sign Off Sheet 92

TABLE OF FIGURES

Figure 2.1 The Scope of this research	15
Figure 3.1 System Context Diagram.....	32
Figure 3.2 Small section of the DFD Diagram	33
Figure 3.3 Registration Interface	39
Figure 3.4 Login interface with passkey option	40
Figure 3.5 Account recovery interface.....	40
Figure 3.6 Registration Flow Diagram.....	43
Figure 3.7 Login Flow Diagram.....	45
Figure 3.8 Account Recovery Flow Diagram	47
Figure 4.1 Responses to the System Usability Scale (SUS) Questions	53
Figure 4.2 Heuristic evaluation responses.....	54

TABLE OF TABLES

Table 1 Extract of STRIDE Threat Analysis (Login Process)	34
Table 2 Extract of LINDDUN Privacy Threat Analysis (Login Process).....	35

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor, **Dr Lynsay Shepherd**, for her guidance, feedback, and support throughout the development of this project. Her expertise and encouragement were invaluable in shaping both the direction and completion of this research.

I would like to thank my lecturers and the staff within the programme for their guidance, support, and encouragement throughout my studies. In particular I would like to thank **Jamie O'Hare** for his continued support and leadership as Programme Lead, and for being consistently encouraging throughout my academic journey.

I am grateful to all participants who contributed their time to this study by evaluating the prototype and providing valuable feedback. Their input was essential to the completion of this project.

A special thank you goes to **my mum**, for always supporting me, believing in me, and encouraging me throughout my academic journey.

I would also like to acknowledge my mentor, **Wanda**, whose guidance, and support have been invaluable since I began university.

I am also grateful to my friends and classmates for their encouragement, support, and shared experiences throughout my time at university.

Finally, I would like to thank my friend **Elisa**, who has been a constant source of support and encouragement since we met while I was finishing college. Thank you for always being there through every challenge, conversation, and everything shared in our little corner of “the ether.”

Finally, I would like to acknowledge **my uncle**, whose experience living with Multiple Sclerosis inspired this project. Seeing the challenges and daily barriers associated with MS over the past ten years inspired me to explore how technology and security systems can be designed more inclusively.

ABSTRACT

Authentication and account recovery are crucial parts of cybersecurity systems. Nevertheless, they often do not consider users with cognitive, motor or sensory impairments. Inaccessible design of the authentication process can lead to the indirect creation of security vulnerabilities, such as higher error rates, the encouragement of risky behaviours due to such errors, and reduced control over the process for the user. Such issues are particularly relevant for Multiple Sclerosis (MS) patients due to their problems related to cognitive and physical disabilities.

This project explores how existing methods for performing threat modelling have been adapted to incorporate accessibility issues into authentication and account recovery procedures. This study utilized a qualitative approach that involved integrating STRIDE security threat modelling with LINDDUN privacy threat modelling using accessibility issues based on Multiple Sclerosis (MS) symptoms.

System context diagrams, data flow diagrams, and workflow analysis were utilized to capture critical authentication processes, such as user registration, authentication, and account recovery. Threats revealed using this approach were mapped to an extensive set of security design guidelines, which informed the creation of a practical prototype for web authentication that incorporates passphrase and passkey authentication as well as several account recovery mechanisms.

Evaluation of the prototype and other design outputs was done by means of expert review involving the use of the System Usability Scale (SUS) and heuristic evaluation. Based on the evaluation process, positive feedback was provided regarding the usability, interface, and balance between security and accessibility, but room for improvement is seen in onboarding and interactive design.

In summary, this study provides an adaptation of the existing threat modelling technique that accounts for accessibility issues, which have been shown to represent potential risks regarding

security and privacy. This research supports the hypothesis that accessibility must be an inseparable part of system security.

ABBREVIATIONS, SYMBOLS AND NOTATION

MS – Multiple Sclerosis

HTML – Hypertext Markup Language

CSS – Cascading Style Sheets

DFD – Data Flow Diagram

STRIDE – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

LINDDUN – Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, Non-compliance

FIDO – Fast Identity Online

SUS – System Usability Scale

WCAG – Web Content Accessibility Guidelines

UX – User Experience

UI – User Interface

MFA – Multi-Factor Authentication

PII – Personally Identifiable Information

DoS – Denial of Service

HCI – Human-Computer Interaction

NIST – National Institute of Standards and Technology

CAPTCHA – Completely Automated Public Turing test to tell Computers and Humans Apart

OWASP – Open Worldwide Application Security Project

SMS – Short Message Service

ACM – Association for Computing Machinery

1 INTRODUCTION

1.1 BACKGROUND

Cybersecurity authentication systems play a critical role in safeguarding user accounts and protecting sensitive personal information. As digital services increasingly underpin communication, healthcare, finance, and social interaction, secure authentication has become essential to ensuring trust and safety in online environments. However, conventional authentication approaches, such as passwords and account recovery mechanisms, often prioritise security requirements while overlooking usability and accessibility considerations. This imbalance can disproportionately disadvantage certain groups of users, particularly those with impairments, introducing not only usability challenges but also unintended security and privacy risks.

The field of usable security recognises that the effectiveness of security mechanisms depends not only on their technical robustness but also on how well they align with human capabilities and behaviours. As highlighted by (Cranor, 2008), systems that fail to account for user needs may lead individuals to adopt insecure coping strategies, such as reusing passwords or simplifying authentication steps. In this sense, usability is not a secondary concern but a fundamental component of security design.

Multiple Sclerosis or MS is a nervous system disorder that may influence the brain functions of the patient by affecting their cognitive processing, memory, motor skills, and fatigue level (MS Society, no date). These symptoms can significantly influence how individuals interact with authentication systems, particularly those that require sustained attention, rapid responses, or precise physical input. As a result, users with MS may experience increased difficulty completing authentication and account recovery processes, leading to higher error rates, repeated failures, and potential exclusion from digital services. Despite this, many existing

authentication systems implicitly assume a uniform level of user capability and do not adequately consider the diverse needs associated with disability.

At the same time, established threat modelling methodologies, such as STRIDE and LINDDUN, are widely used to identify security and privacy risks during system design. While effective in analysing technical vulnerabilities and attacker behaviours, these approaches typically do not account for risks arising from usability or accessibility barriers. This creates a critical gap, as any difficulties in user interaction can indirectly introduce security vulnerabilities, for example through predictable coping behaviours, increased susceptibility to phishing, or reliance on external assistance.

This highlights a broader issue within cybersecurity design, where authentication mechanisms may unintentionally act as barriers rather than enablers of secure access. As noted by Dr Lynsay Shepherd (White, 2026), *“Authentication should never act as a barrier to accessing digital services. Designing inclusive and accessible security mechanisms for those living with conditions such as multiple sclerosis is essential to making cybersecurity truly human-centred.”* This perspective reinforces the need to rethink authentication not only as a technical control, but as a human-centred process that must accommodate diverse user capabilities.

1.2 AIM

The aim of this project is to investigate how cybersecurity threat modelling can be adapted to support inclusive design, specifically for users living with Multiple Sclerosis, in the context of authentication and account recovery systems.

1.3 OBJECTIVES

The objectives of this project are as follows:

- To analyse authentication and account recovery processes using threat modelling techniques

- To apply and adapt STRIDE and LINDDUN frameworks to incorporate accessibility considerations.
- To identify security and privacy risks introduced by accessibility barriers
- To develop inclusive security design guidelines
- To implement a prototype authentication system demonstrating these guidelines
- To evaluate the effectiveness of the proposed approach through expert feedback

1.4 STRUCTURE OF THE DISSERTATION

This dissertation is structured as follows:

- Chapter 2 reviews existing literature on usable security, authentication systems, and accessibility considerations
- Chapter 3 outlines the methodology, including threat modelling approaches and prototype development.
- Chapter 4 presents the results of the evaluation.
- Chapter 5 discusses the findings in relation to the research objectives.
- Chapter 6 concludes the project and outlines future work.

2 LITERATURE REVIEW

2.1 INTRODUCTION

Authentication and account recovery are integral parts of contemporary digital systems that allow users to access their digital accounts securely. In contemporary society, digital systems play an integral role in facilitating communication, trade, health services, and social interactions. Therefore, authentication and account recovery are critical in providing digital systems with robust security systems. In response to changing security challenges, digital systems are increasingly adopting robust security systems to ensure user authentication and account recovery. These robust security systems include multi-factor authentication systems, phishing-resistant authentication systems, and automated bot detection systems(Grassi *et al.*, 2020). Although these systems provide robust security systems to digital users, they are also becoming increasingly more complex.

When evaluating digital systems, it is imperative to differentiate security and privacy concepts. Security relates to protecting digital systems and data from unauthorised access and misuse. In contrast, privacy relates to data collection, data processing, data disclosure, and user control. Although security and privacy are integral concepts in digital systems, they are not synonymous. Inadequate security systems can inadvertently create privacy challenges in digital systems, particularly due to user behaviours and data disclosure.

Recent studies on usable security have shown that security systems need to be designed according to human capabilities. When there are too many requirements for human cognition or physical capabilities, users may have difficulties performing tasks successfully. These problems are more critical for people with disabilities, as their interactions with security systems may be influenced by various factors such as cognitive, motor, or sensory disabilities.

One of the groups that may experience such problems more critically is people with Multiple Sclerosis (MS), which is a neurological disorder that causes cognitive fatigue, decreased

processing speeds, memory problems, and motor problems. These problems may have critical effects on the success of authentication or account recovery processes. Therefore, accessibility problems may not only cause usability problems but may also lead to security and privacy problems.

Although considerable research efforts have been devoted to authentication technologies, accessibility, and security, these three concepts are treated as different domains. Not enough attention has been paid to exploring the potential role that accessibility barriers play in security and privacy threats, particularly with reference to users with neurological disorders like MS. In addition, existing threat modelling methods do not consider accessibility-related factors, which is an important dimension in threat modelling that has not been fully explored.

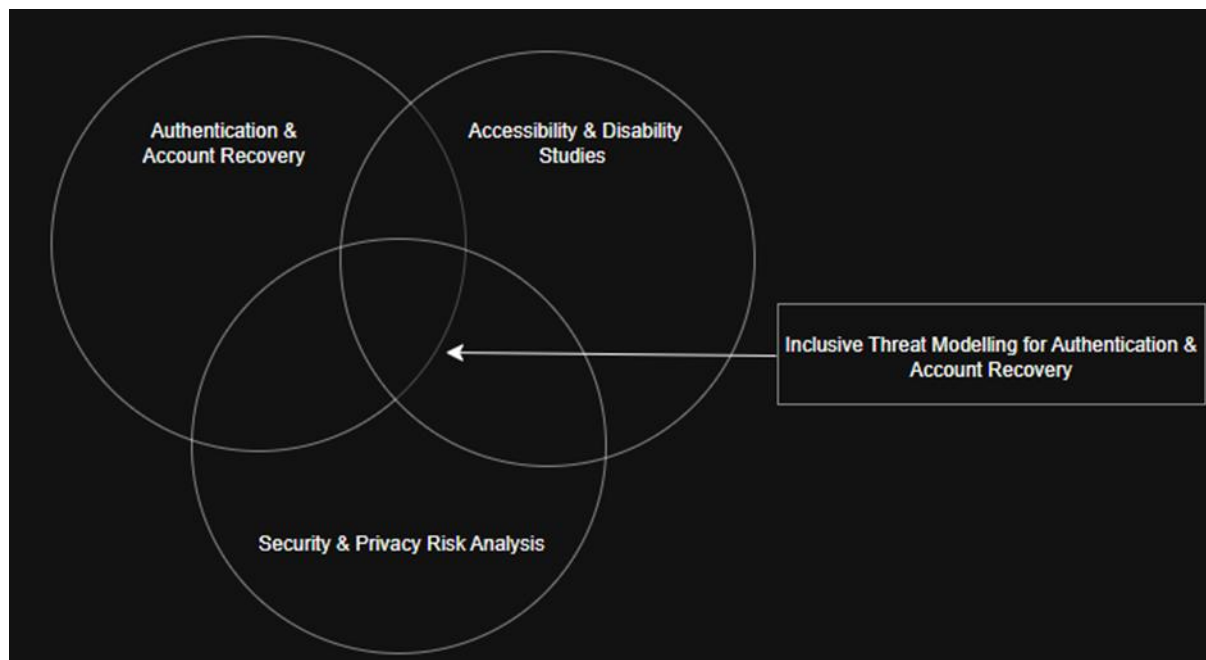


Figure 2.1 The Scope of this research

As illustrated in Figure 2.1, the current research lies at the intersection of three domains: Authentication and Account Recovery, Accessibility and Disability Studies, and Security and Privacy Risk Analysis. While prior work typically addresses these areas independently, this study focuses on their overlap, where accessibility barriers directly influence security and privacy. The central focus of this research is the development of an inclusive threat modelling methodology

that integrates these three areas, accounting for usability, accessibility, and risk in authentication and account recovery systems.

This chapter reviews the relevant literature across these areas, examines how usability and accessibility influence security and privacy outcomes, and identifies key gaps that motivate the methodology presented in Chapter 3.

2.2 USABLE SECURITY, PRIVACY, AND AUTHENTICATION SYSTEMS

User authentication and account recovery are integral to user access, security, and autonomy in online systems. They are essentially security mechanisms that ensure users are not accessing online systems without authority while allowing users to recover access to online systems when they lose their account details.

However, user authentication and account recovery are cognitively and physically demanding tasks for users. They require users to perform tasks that involve attention and memory. In essence, user authentication and account recovery can create challenges for users that can limit access to online systems. In this regard, user authentication and account recovery can create barriers to security.

Studies in usable security emphasize that security systems must be aligned with user capabilities. Adams and Sasse (1999) assert that security systems are not compromised by users who are careless but by systems that are not user-centered in terms of cognitive and behavioural demands. In essence, when user authentication systems are difficult to use, users tend to behave in ways that compromise security. Therefore, usability can be understood as an integral part of security rather than an auxiliary function. This perspective is further supported by frameworks that explicitly model the human as part of the security system, highlighting how user behaviour interacts with system design to produce security outcomes (Cranor, 2008).

2.2.1 Password-Based Authentication

Password-based authentication is the most dominant form of authentication currently used in digital systems. Although it has been the most dominant form of authentication, it has always

been a major contributor to usability and security problems. Users must remember passwords that are composed of several characters, including upper- and lower-case letters, numbers, and symbols. This has been a major contributor to usability problems, as the complexity of the passwords has been a major issue to security problems.

Empirical studies have revealed that several users have been using coping strategies as a way of dealing with the usability problems of passwords. Gaw and Felten (2006) revealed that several users have been using several coping strategies, including reusing passwords, writing them down, or simplifying them. Although this has reduced usability problems, it has increased security problems significantly. Newer studies have also shown that such practices continue even when there are improvements in authentication guidelines and systems (Florêncio, Herley and van Oorschot, 2014; Alodhyani, Theodorakopoulos and Reinecke, 2020). Although these minimize cognitive effort, these practices substantially raise the risk of credential theft.

More recent recommendations have seen a move towards usability-conscious design. The NIST Digital Identity Guidelines (SP 800-63B) propose the use of more memorable passphrases, as well as the avoidance of complex composition, as excessive complexity can create insecure usage patterns (Grassi *et al.*, 2020). Nevertheless, even passphrases will require memory and consistent usage patterns, which may create difficulties for some users with cognitive impairments.

There are usability difficulties with password systems that have direct security and privacy implications. The practice of reusing passwords increases the likelihood of many accounts being compromised, as does writing down or sharing passwords, which increases the likelihood of unauthorized access and information disclosure. For people with disabilities, including MS, these difficulties may be compounded by cognitive fatigue, memory, and processing speed. This means that password systems have the potential to create a cycle of failure, as well as insecure coping strategies, including the sharing of credentials.

This is further supported by accessibility-focused authentication research, which shows that cognitive differences significantly influence how users create and manage passwords. Studies on users with dyslexia demonstrates that authentication design often fails to accommodate

diverse cognitive processing styles, leading to increased errors and reliance on coping strategies (Ophoff, Johnson and Renaud, 2021; Ophoff and Renaud, 2023).

2.2.2 Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) enhances the security of user accounts by requiring that users undergo additional verification steps to gain access to their accounts. MFA has been proven to greatly reduce the chances of users' accounts being compromised, especially when considering cases of phishing (Bonneau *et al.*, 2012; Grassi *et al.*, 2020).

The usability of MFA has been proven to differ based on the approach that is used. According to Reese *et al.* (2019), MFA mechanisms that require users to reproduce short-term numeric codes have higher rates of user error as well as decreased rates of completion when compared to approval-based MFA methods, which require users to approve a login on a trusted device. This shows that not all MFA methods have equal usability.

For users with MS, MFA has been proven to bring along some challenges. These challenges are mainly because cognitive fatigue as well as decreased processing speeds make it hard for users to recall MFA codes. Additionally, motor difficulties make it hard for users to input MFA codes. This makes MFA a challenge for users with MS, as they might be forced to seek external help. This would bring along additional security as well as privacy challenges.

New approaches have been developed to resolve these challenges. The FIDO Alliance (2022, 2023) supports phishing-resistant authentication on devices through passkeys. This reduces the need to memorise anything and makes interactions simpler. This proves that security measures can be enhanced without conflicting with usability and accessibility.

2.2.3 Account Recovery Mechanisms

Account recovery is an essential yet understudied aspect of authentication. Where users lose access to their credentials and authentication factors, account recovery processes such as password reset emails, security questions, CAPTCHAs, and customer support services are employed to facilitate access. Such processes must strike a fine balance between security and ease of use, especially in situations of high user stress.

Account recovery processes often involve considerable usability and accessibility challenges. Completing tasks such as answering CAPTCHAs, answering security questions, and so on can be cognitively demanding. Gaggi (2022) points out that one of the most employed anti-bot services, reCAPTCHA, is also inaccessible to users. This is since it involves activities like image recognition, quick response time, or dealing with ambiguous visual and cognitive problems, which may pose challenges for those with visual, cognitive, or motor disabilities. This creates significant abandonment and frustration.

In addition to usability concerns, account recovery processes introduce notable security and privacy risks. Poorly designed recovery flows may enable account enumeration, where attackers can determine whether an account exists based on system responses (OWASP, no date). They may also increase susceptibility to phishing attacks, particularly when users are already under stress or attempting to regain access (Wash, 2010). Furthermore, recovery processes often involve the disclosure of sensitive information or interaction with external communication channels, increasing the risk of information leakage.

These challenges are particularly significant for users with MS, who may require multiple attempts due to cognitive fatigue or processing difficulties. Repeated failures can lead to lockouts, effectively creating a denial-of-service scenario, or may push users towards insecure practices such as seeking assistance from others.

2.2.4 Usable Security and Human Behaviour

Usable security studies have highlighted that user behaviour is influenced by the security system. This means that instead of seeing users as inherently insecure, the concept of usable security sees users as rational actors who act within the boundaries of the system. This means that if the authentication process requires significant effort, memory, or accuracy, users are more likely to exhibit behaviours that minimize these requirements, even if it means compromising security.

The relationship between security and usability can be clearly seen during authentication or recovery processes. When processes are complicated or difficult to use, predictable results are

likely to occur. This does not mean that the user has failed, but that the system fails to consider human capabilities.

The concept of authentication under the context of usable security highlights the significance of developing mechanisms that minimize user burden. This not only enhances the user experience, but it also helps to minimize the risks of security and privacy threats arising from user behaviour.

2.2.5 Privacy Risks in Authentication and Recovery

There is several privacy risks related to authentication and account recovery systems. This is mainly due to the design of the system that ends up revealing certain information to the attacker. The most common privacy risk is that of account enumeration. This is mainly due to the difference in the system's response to certain inputs.

The use of recovery mechanisms is also likely to increase the privacy risks. This is mainly due to the use of external communication channels such as email or SMS. There is a possibility that these channels may reveal certain information that may result in risks of Linkability and Information Disclosure. There is also the possibility of generating certain patterns that may be used to profile the user.

User unawareness represents another significant privacy concern. Authentication interfaces often fail to clearly communicate what data is being processed or how recovery actions affect account security. This lack of transparency can lead to unintended information disclosure or misuse of recovery features. These issues disproportionately affect users with cognitive impairments, who may struggle to interpret complex or ambiguous system feedback.

2.2.6 Standards and Current Best Practices

Industry standards and guidelines are now acknowledging the need to consider usability as well as security. The NIST Digital Identity Guidelines, part of SP 800-63B, suggest that there is a need to limit reliance on "knowledge" authentication, to discourage the use of security questions, and to limit unnecessary complexity in authentication or recovery processes (Grassi *et al.*, 2020) With recent updates to these guidelines which further emphasise phishing-resistant

authentication and improved usability considerations in modern authentication systems (Temoshok *et al.*, 2025).

The Web Content Accessibility Guidelines 2.2 have introduced specific criteria for accessible authentication. These guidelines discourage methods that rely on memory recall, complex puzzles, or time-sensitive challenges. This is because such methods are known to disadvantage people with cognitive or motor impairments. This is a step in the right direction as they have accepted that such methods are not accessible or inclusive (W3C, 2023).

The FIDO Alliance (2023) has been at the forefront of developing secure methods such as passkeys that are not only secure but also easy to use. This is because they reduce not only security issues but also usability issues. These are steps in the right direction as they have accepted that security needs to be inclusive. However, they have not offered any tools to assess how accessibility issues could be translated into security issues.

2.2.7 Summary

This section has explored authentication and account recovery systems using the dual perspectives of usability, security, and privacy. It has been shown that popular methods, such as passwords, multi-factor authentication, and recovery mechanisms, often require users to make substantial cognitive and physical demands. These demands often result in users exhibiting predictable coping mechanisms that compromise security and amplify privacy threats.

The field of usable security has proven that these challenges are not due to limitations within users themselves but are instead caused by system design that does not take into consideration human capabilities. Although modern standards are moving in a positive direction to emphasize accessible and user-centered authentication, they still do not go far enough to consider how accessibility limitations translate to security and privacy threats. This has created a need to discuss methods that explicitly consider usability and accessibility within security, which will be done in the next sections.

2.3 ACCESSIBILITY AND INCLUSIVE AUTHENTICATION

2.3.1 Accessibility, Disability, and Interaction Barriers

Authentication systems are often created with an implicit assumption that there is an “average” user, without considering that users have diverse cognitive, physical, and sensory capabilities. Accessibility research has challenged this assumption by showing that users are using these systems under various conditions, including temporary or permanent disabilities, fatigue, or environmental limitations.

Thus, disability is not only an individual characteristic; rather, it is created by the interaction between individual abilities and system design. When authentication systems are created with high memory, attentional, or speed requirements, they may not allow users who cannot cope with these demands to access them. Therefore, accessibility limitations are not only usability issues; they may directly influence a person’s ability to independently access a system securely.

Continuing with the ideas presented in Section 2.2, inaccessible authentication systems may force users to make mistakes repeatedly, to stop using a system, or to use risky compensatory strategies. Therefore, accessibility is not only an optional feature that may be added to secure systems; rather, it is an essential part of secure system design.

2.3.2 Cognitive Accessibility and Authentication

Cognitive accessibility refers to the degree to which a system caters to different levels of memory, attention, processing speed, and comprehension. The process of authentication and account recovery usually heavily depends on these cognitive abilities, as the user must remember their credentials, understand the system’s feedback, and complete a series of tasks.

The Web Content Accessibility Guidelines (WCAG) 2.2 have recognized the difficulties faced by users with cognitive impairments through their Accessible Authentication guidelines. The guidelines advise against systems that heavily rely on memory recall, transcription, or solving complex puzzles, as these systems might have a greater disadvantage for people with cognitive impairments (W3C, 2023). The guidelines have also advised systems to use methods that have a low cognitive load, especially those that do not require short-term memory.

From a security point of view, systems with a high cognitive load might result in authentication failure, which might further result in insecure practices, as discussed earlier in Section 2.2. This shows that cognitive accessibility not only affects the usability of a system but also has an impact on security and privacy.

2.3.3 Motor Accessibility and Interaction Cost

In addition to cognitive factors, authentication processes also involve specific physical interactions. This includes processes such as entering one-time passcodes, selecting specific elements on the interface, and CAPTCHAs. These processes may become difficult for users with limited fine motor skills, tremors, and fatigue.

Studies on human-computer interaction have provided frameworks to understand the complexities in authentication processes. One such framework is Fitts' Law. This law attempts to explain the relationship between movement time, target size, and distance.

$$T = a + b \log_2(1 + WD)$$

Fitts' Law states that the time it takes to move to a target increases when the distance to the target increases or when the size of the target decreases. This suggests that small targets close to each other and targets that are poorly positioned on the interface may cause interaction difficulties, resulting in potential errors (Fitts, 1954; MacKenzie, 1992).

This has important implications in authentication scenarios, where interfaces with limited input boxes, constrained layout, and/or high interactivity may place users with motor disabilities at a disadvantage. The higher cost of interaction may cause users to make repeated errors, take longer to complete interactions, or even fail to authenticate.

As discussed in Section 2.2, repeated failure may result in lockouts, which equate to denial-of-service attacks on the users. This is another example where accessibility issues map to security issues.

2.3.4 Inclusive Authentication Principles

Inclusive authentication builds upon the principles of usable security by explicitly considering user diversity in ability in designing authentication systems. In other words, rather than treating accessibility as an afterthought in system design, inclusive authentication recognizes that systems must be designed to accommodate a wide range of human abilities.

The key principles of inclusive authentication are:

- Minimize reliance on memory and recall
- Minimize pressure and interaction complexity
- Support multiple authentication methods
- Provide clear and accessible feedback

These principles are very similar to existing standards like WCAG 2.2 and recommendations from organizations like the FIDO Alliance. As discussed in Section 2.2, device authentication and passkeys are examples of security and accessibility objectives being aligned.

However, in practice, many systems are built around authentication systems that place considerable demands on users' cognitive and motor abilities. Examples include CAPTCHAs, codes with a limited time to input, and multi-step recovery flows. This disparity between recommended best practices and actual system design suggests a gap in current systems.

2.3.5 Accessibility as a Security and Privacy Concern

Recent research is increasingly acknowledging that there is a possibility for accessibility barriers to act as indirect sources of security and privacy risks. For instance, when users experience difficulties in authentication processes, they may resort to certain practices that may undermine security and privacy risks. For example, they may share their credentials with others, use the same passwords for different applications, or even seek assistance from third parties (Erinola *et al.*, 2023).

Empirical work on accessible authentication further reinforces this relationship, demonstrating that users with cognitive differences experience disproportionately higher authentication

failure rates and usability barriers, which can translate into security vulnerabilities (Ophoff, Johnson and Renaud, 2021; Ophoff and Renaud, 2023).

Such practices may undermine security and privacy risks because they may increase the chances of unauthorized access to certain information. Inaccessibility may also make certain processes more difficult for legitimate users than for malicious users.

It is evident that these risks are not considered in the conventional threat modelling techniques that usually focus on attacker practices and technical vulnerabilities. The risks related to inaccessibility arise from the interaction between system design and human limitations.

The above discussion supports the idea that inaccessibility is a critical component of security and privacy risk assessment.

2.3.6 Summary

In this section, accessibility and inclusive authentication concepts have been discussed from both theoretical and practical points of view. It was demonstrated that authentication systems can put considerable demands on users' cognition and motor skills, which can create obstacles for users with different abilities. Moreover, human-computer interaction theories, like Fitts' law, also confirm that interface design can affect interaction difficulties and error rates.

However, it is noteworthy that accessibility obstacles are not only related to usability issues but can also directly impact security and privacy risks because they can influence users' behaviour and authentication failure rates. Although standards like WCAG 2.2 provide recommendations for more inclusive authentication design, in practice, there is a gap between recommendations and implementations.

The theories and findings form a basis for the next section, which discusses authentication challenges for users with MS in authentication and account recovery contexts.

2.4 CHALLENGES FOR USERS WITH MULTIPLE SCLEROSIS IN AUTHENTICATION

2.4.1 Cognitive Challenges and Authentication

MS, which is a chronic neurological disorder, is one such condition that usually affects cognitive processes such as memory, attention, and speed. Such cognitive processes tend to vary and may also vary over time. This makes it difficult to interact with complex systems in a consistent manner.

Authentication and account recovery usually involve cognitive processes that are affected by MS. Such processes may include remembering passwords, interpreting system messages, shifting one's attention between different devices, and so on. Cognitive fatigue is also a phenomenon that has been reported to affect users. Such cognitive fatigue is also referred to as 'cognitive fog.'

As previously explained in Sections 2.2 and 2.3, high cognitive demands in MS can lead to increased error rates and failure in the authentication process. For users with MS, it can be even more difficult, which can lead to further problems, including repeated attempts, failure in the recovery process, and even account lockouts. These can not only affect the usability of the system but also lead to potential security threats, including increased susceptibility to phishing or the use of coping strategies.

2.4.2 Motor and Sensory Challenges in Authentication

Besides these cognitive challenges, individuals with MS can also face motor and sensory challenges in the form of tremors, motor skill difficulties, weakness in muscle function, and other sensory challenges. Such challenges can impact an individual's ability to interact with authentication systems.

For instance, basic authentication tasks such as entering one-time passwords, selecting small interface elements, or completing CAPTCHA challenges can be difficult for individuals with motor skill challenges. Moreover, individuals with MS can face challenges in completing tasks in a timely manner due to the need to take more time to perform tasks.

As discussed in Section 2.3, this increased interaction difficulty can also lead to increased error rates and longer time to complete tasks. This can particularly lead to a situation in which users may experience repeated failures in authentication attempts. This may also lead to a denial-of-service situation in which users with MS cannot access their accounts.

These difficulties may also encourage users to devise different strategies to overcome these challenges. This may include reducing the complexity of authentication processes and/or relying on others to perform these tasks. Both these factors also raise security and privacy concerns.

2.4.3 Fatigue, Variability, and Interaction Consistency

Another characteristic of MS is that the symptoms are variable, both between people and over time. This means that the user may experience fluctuations in their cognitive or motor skills during the day, depending on factors such as fatigue, stress, or the environment. This variability makes it difficult to base an authentication system on any given assumption of user capabilities.

Fatigue, for example, affects the user significantly. This means that some tasks may be relatively easy at one time of the day and much more difficult at another. This could result in a situation where the user may not complete the process, especially if it involves an authentication process.

From a security point of view, this could result in the user being locked out of the system after several attempts. This could be a barrier to the user. From a privacy point of view, several interactions may result in the user being exposed to various system messages, external communications, or even activity patterns.

All these factors emphasize the need to design authentication schemes that are flexible enough to accommodate variability, thus allowing users to perform their tasks at their own pace without any emphasis on time factors or specific interaction patterns.

2.4.4 Implications for Security and Privacy Risk

The challenges presented by MS illustrate how accessibility barriers can have a direct impact on security and privacy. Cognitive, motor skill, and fatigue-related limitations do not simply make

authentication processes more difficult; they also alter how users interact with security features in a way that creates new security challenges.

MS users may face a greater risk of:

- Repeated authentication failures and lockouts
- Simplification and use of similar credentials
- Requiring others to assist in authentication processes
- Avoiding security features that are difficult to use

These patterns can make users more susceptible to common security attacks such as phishing, unauthorized access, and information disclosure. What is significant is that these security challenges are not caused by the inherent characteristics of users with MS; rather, they are caused by the interactions between users and system features.

As discussed in the previous sections, traditional approaches to threat modelling do not consider these types of interaction-related security challenges. They only consider technical vulnerabilities and the behaviour of attackers. They do not consider how accessibility and usability barriers can create indirect paths to security and privacy challenges.

2.4.5 Summary

In this section, the specific issues associated with users who have MS have been examined. These issues are related to the context of authentication and account recovery. The cognitive, motor, and fatigue-related factors associated with this illness have significant implications for the overall success of authentication processes, which may result in an increased number of errors.

The issues associated with users who have MS are not limited to the context of usability. They have significant implications for security and privacy risks. This is because they have a direct impact on user behaviour. This relationship between system factors and user capabilities is an important, yet under-explored, factor that influences security risks.

The issues associated with users who have MS have significant implications for the overall understanding of security risks. This is because it highlights the importance of considering

accessibility factors within the context of security risks. This has resulted in the identification of gaps within the existing research, which will be highlighted in the following section.

2.5 GAPS IN EXISTING RESEARCH

The reviewed literature clearly indicates that there is substantial progress in the areas of usable security, authentication design, accessibility, and privacy-aware systems. Past research has focused on the usability problems that users face in using authentication technologies (Reese *et al.*, 2019; Gaggi, 2022), coping strategies that users develop to deal with the complexity of security requirements (Adams and Sasse, 1999; Gaw, Felten and Fernandez-Kelly, 2006) , and the accessibility problems that users with disabilities face when using digital technologies (Erinola *et al.*, 2023) . While recent studies have begun to explore accessibility in authentication contexts, including work on cognitive accessibility and password use (Ophoff, Johnson and Renaud, 2021; Ophoff and Renaud, 2023) these efforts remain largely focused on usability outcomes rather than explicitly framing accessibility barriers as security and privacy risk vectors.

At the same time, clinical research has clearly shown that MS impacts memory, attention, processing speed, and motor skills (Charvet, Serafin and Krupp, 2013; DeLuca *et al.*, 2015).

Despite these research efforts in the aforementioned areas, they are largely isolated from one another. While research in accessibility focuses on identifying the problems that users face when using digital technologies without exploring their relationship to security and privacy, research in cybersecurity typically considers users as a single entity without considering their cognitive and physical abilities that may affect their experience of security mechanisms.

As has been emphasized throughout Sections 2.2 to 2.4, authentication and account recovery mechanisms have cognitive and physical consequences that could result in user adaptation, especially for people suffering from MS. These adaptations could result in security and privacy threats. Despite this, little research has been done on how accessibility challenges act as risk vectors within authentication mechanisms.

Currently, various standards and guidelines, such as WCAG 2.2 and NIST SP 800-63B, recognize the need to consider accessibility and usability within authentication mechanisms. These are high-level guidelines that attempt to reduce cognitive load and prevent exclusionary mechanisms. However, these guidelines do not provide a means to analyse how accessibility challenges are translated into security or privacy threats. Moreover, they do not consider users suffering from neurological conditions such as MS.

Similarly, existing threat modelling methodologies, such as STRIDE and LINDDUN, have been widely adopted in the identification of security and privacy risks in the design phase. However, these methodologies have primarily concentrated on the technical aspects and the attacker's perspective, with little or no consideration given to the user's perspective, usability factors, or accessibility issues. Therefore, the risks related to the interaction between the design phase and the capabilities of users, especially users with disabilities, are either under-represented or entirely absent in the existing threat modelling methodologies.

This is where the importance of an inclusive threat modelling methodology, which takes into consideration the accessibility issues in the existing security and privacy risk analysis methodologies, comes into play. Such a methodology would be able to identify the risks not only related to the technical issues but also related to the interaction between the authentication factors, user capabilities, and real-world conditions.

Thus, the gap in the existing threat modelling methodologies is where the importance of the methodology discussed in Chapter 3 lies, which extends the existing threat modelling methodologies to include the accessibility analysis, with particular emphasis on users with MS.

3 METHODOLOGY

3.1 RESEARCH APPROACH

This project applies a qualitative, design-oriented research approach, investigating how cybersecurity threat modelling could be conducted in a way that inclusively supports people living with MS when they are interacting with authentication and account recovery systems (Merriam and Tisdell, 2016; Creswell and Poth, 2024; Mills, Birks and Mills, no date).

Instead of considering the measurement of attack likelihood or system performance quantitatively, this research aims to focus on understanding the introduction of security and privacy risks to a specific user group due to accessibility barriers (Blessing and Chakrabarti, 2009).

This project is exploratory in nature and focuses on the development and application of an inclusive threat modelling process, followed by translation of the identified risks into practical design guidelines and a working prototype. This approach is appropriate given the project's objective to bridge the gap between research in accessibility and cybersecurity practices, particularly in areas like authentication, recovery, and user-facing security mechanisms (Creswell, 2014).

A design led methodology was chosen because it enables the investigation of security risks not only as technical vulnerabilities but also as consequences of interaction design, usability constraints, and cognitive load (Norman, 2013).

This perspective is especially relevant for users with MS, whose experiences of fatigue, cognitive fog, and motor or sensory impairments may alter how security mechanisms are perceived and used (Rocca *et al.*, 2015).

3.2 SYSTEM SCOPE AND MODELLING STRATEGY

In determining the scope of the analysis, this project focused on a common set of users facing security processes typically found in online services. These Include:

- Registration of users and credentials
- Login and authentication
- Account recovery and password reset
- Session and Security State Management

A System Context Diagram was initially created to determine key actors, trust boundaries, and external dependencies for these processes (Shostack, 2014). A System Context Diagram helped determine a relationship between a user, the system authentication, third-party services (for example, email/SMS delivery), and possible malicious actors from the outside , as depicted in Figure 3.1 , full version available in Appendix A – System Context Diagram.

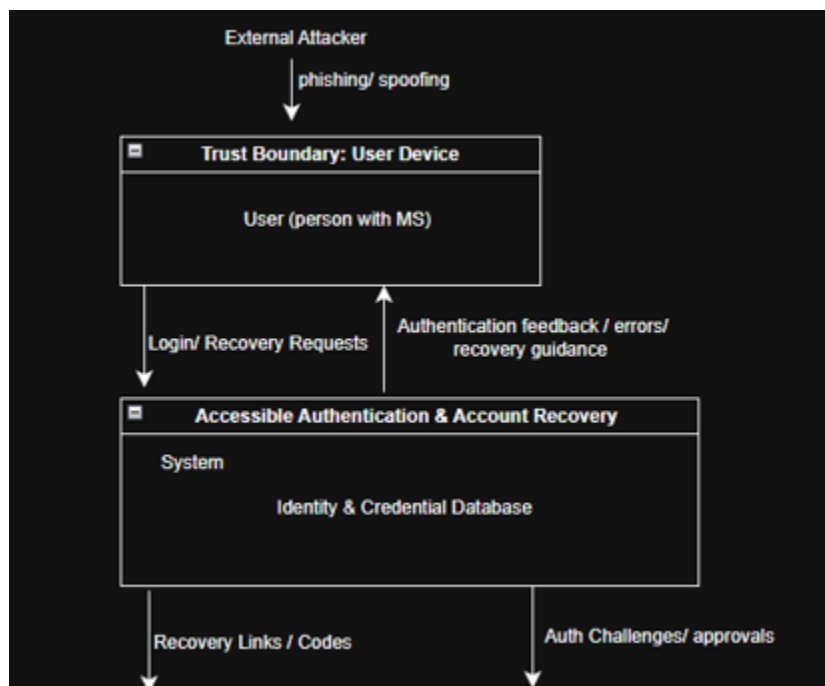


Figure 3.1 System Context Diagram

After this, a level 1 Data Flow Diagram was developed to represent the movement of data in the process for registration, login, recovery, and session management (Shostack, 2014;

Microsoft, no date). This DFD helps to conceptualise processes, data stores, and data flows in such a way that it can easily apply methods for performing threat modelling. As small section of the DFD is shown below in Figure 3.2 and full version is in Appendix B – DFD Diagram.

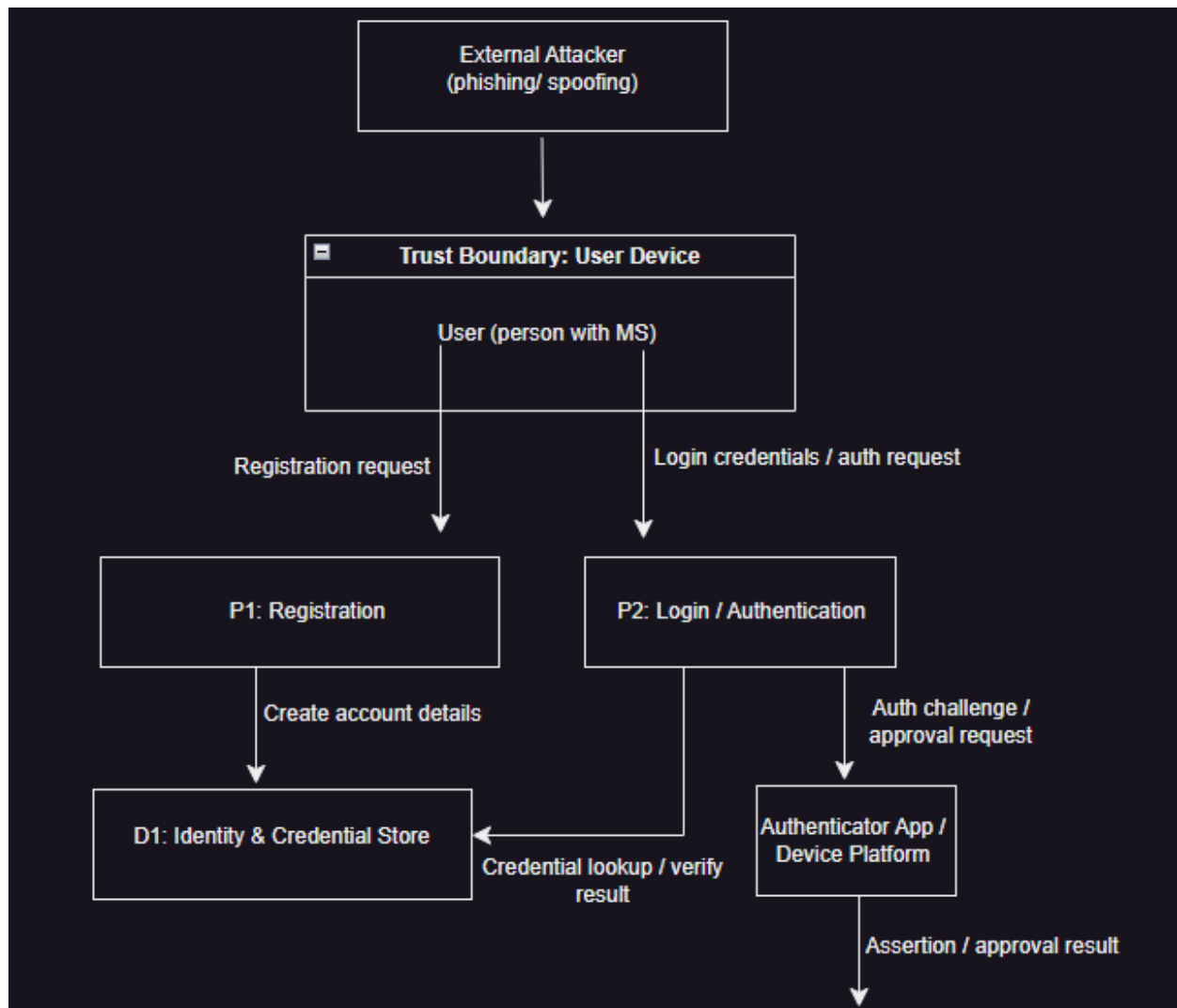


Figure 3.2 Small section of the DFD Diagram

The use of visual modelling artifacts enables tracing and clarity, by allowing the association of the threat with the specific processes and data flows. These diagrams provide a reference for the last two stages of the project, the development of the guidelines and the implementation of the prototype (Swiderski and Snyder, 2004).

3.3 THREAT MODELLING FRAMEWORKS

3.3.1 STRIDE

The STRIDE threat modelling methodology was employed to analyse the security threats within the scope of the system (Shostack, 2014; Microsoft, no date). STRIDE divides threats into six different categories, which are spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

STRIDE was chosen because of its popularity in the industry and the academic community, and because of its suitability for analysing authentication and account recovery processes (Swiderski and Snyder, 2004) , where threats like phishing, stealing authentication information, and account lockout are very frequent. STRIDE was used to analyse each process and the critical data flow in the level 1 DFD. An extract of the STRIDE analysis is shown in Table 1 to illustrate how threats were identified and mapped to system components.

STRIDE Category	Threat Description	MS-Specific Impact	Mitigation
S - Spoofing	Phishing steals login credentials or MFA approvals	Cognitive fatigue increases phishing susceptibility	Passkeys, phishing-resistant MFA, consistent login flows
I – Information Disclosure	Error messages leak account existence	May enable targeted scams	Generic error messages, no account enumeration
D – Denial Of Service	Lockouts from repeated failures	Motor or cognitive impairments increase error likelihood	Progressive lockout, alternative auth paths, recovery prompts

Table 1 Extract of STRIDE Threat Analysis (Login Process)

This extract demonstrates how traditional STRIDE threats can be amplified by accessibility-related challenges. For example, denial-of-service risks may arise not only from malicious activity but also from repeated user errors caused by cognitive fatigue or motor impairments. The full STRIDE analysis across all processes (P1–P4) is provided in [Appendix B – STRIDE Table](#).

3.3.2 LINDDUN

As a complement to STRIDE, the LINDDUN approach was used to evaluate privacy threats. The approach considers risks of linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, and non-compliance (Deng *et al.*, 2011).

LINDDUN provides a structured approach to identifying privacy risks by mapping data flows to specific privacy threat categories. In the context of authentication and account recovery processes, such risks are often evident, for example, where systems inadvertently reveal whether an account exists, expose personal data through system messages, or fail to communicate clearly how user data is processed.

To support the inclusive focus of this project, the LINDDUN framework was adapted to include an additional “MS-Specific Impact” consideration. This enabled the identification of how accessibility challenges associated with M, such as cognitive fatigue and reduced awareness, may amplify privacy risks, particularly in areas such as unawareness and detectability.

A representative extract of the LINDDUN analysis is presented in Table 3.2. The complete table is included in [Appendix C – LINDDUN Table](#).

Category	Privacy Threat	MS-Specific Impact	Mitigation
Linkability	Login metadata links sessions over time.	Predictable patterns increase profiling risk	Limit session correlation; rotate identifiers
Detectability	Error messages reveal valid usernames	Supports phishing and account enumeration	Generic login errors; no confirmation of account existence
Unawareness	User unaware of tracking or session persistence	Fatigue may limit understanding of session scope	Clear session indicators; explicit logout confirmation

Table 2 Extract of LINDDUN Privacy Threat Analysis (Login Process)

The analysis identified unawareness and detectability as particularly significant privacy risks for users with MS, as cognitive fatigue and reduced awareness may limit the ability to interpret

system feedback, increasing susceptibility to privacy risks such as unintended data disclosure or targeted attacks.

In combination with STRIDE, the use of LINDDUN supports a more holistic assessment of both security and privacy risks, aligning with the aim of this project to balance security, privacy, and accessibility in authentication system design.

3.4 INCLUSIVE ADAPTATION FOR MULTIPLE SCLEROSIS

Usually, threat modelling techniques assumes a generic user but, in this project, the inclusive security lens was used to incorporate the difficulties faced by people living with MS (Rocca *et al.*, 2015; Askari, Fanelli and Harvey, 2021). Both STRIDE and LINDDUN threat modelling techniques were adapted to incorporate this.

This adjustment included the following threats that may be escalated by MS-related deficits (Rocca *et al.*, 2015):

- Cognitive fatigue and decreased processing speed - May lead to error rates being elevated during complex authentication processes
- Memory issues, which could impede mechanisms that are recall-based/heavy on transcription
- Motor and sensory difficulties could potentially influence the processing of time-limited codes or precise input
- Error recovery barriers - where a series of errors or lockouts could preclude future access

Rather than treating these challenges solely as usability concerns, the project interprets them as potential security and privacy risks. For example, puzzling recovery paths could be seen as a possible reason for people to be more susceptible to attacks such as phishing scams, while lockouts could be a reason for people to engage in unsafe practices such as reusing passwords or sharing accounts.

This inclusive approach views accessibility barriers as essential components of threat modelling, ensuring that risks and mitigations are focused on reality rather than mere technical possibilities.

3.5 PROTOTYPE DESIGN METHODOLOGY

3.5.1 Purpose and Scope of the Prototype

A functional prototype has been designed to demonstrate how an inclusive security paradigm can be achieved from a threat modelling process (Lazar, Goldstein and Taylor, 2015; Glass *et al.*, 2016). This prototype is meant for research purposes and is not for production purposes and is intended to illustrate how inclusive design choices can be applied without weakening security.

The scope of the prototype is explicitly limited to:

- User Registration
- Login and Authentication
- Account Recovery

To support such workflows, the prototype uses baseline backend security measures that are relevant to a research demonstration, such as credential control and server-side validation (W3C, 2023). It is not, however, a purpose of the project to implement or assess production-standard security measures such as hardened key management, intrusion detection at scale, or authentication infrastructures that carry compliance certification.

This scope helps to ensure that the project remains focused on interaction design, accessibility, and user-facing security decisions while still maintaining a realistic level of security context sufficient to support threat modelling, the formation of guidelines, and the evaluation process.

3.5.2 Prototype Overview

The prototype was implemented as a web-based authentication systems to operationalise the inclusive security guidelines based on the adapted STRIDE and LINDUNN threat modelling process. This includes functionality such as user registration, login, and account recovery

workflows which are intended to show how accessibility-focused security measures can be incorporated into a realistic user-facing authentication process.

The registration workflow supports account creation which entails registering an account by creating a username and passphrase. To avoid multiple instances of authentication, users are allowed to select the option "Remember this device," which helps in maintaining authenticated sessions without placing much cognitive effort on the user.

The login workflow supports both passphrase-based authentication and passkey authentication; this allows users to select between traditional and device-based methods depending on their accessibility needs and preferences.

The account recovery workflow has 2 methods; one is recovery code validation and the second is device-based recovery using passkeys. These multiple options for recovery were implemented to reduce reliance on memory recall and to also mitigate account lockout.

A selection of the prototype interfaces is shown in Figure 3.3 to 3.5. These interfaces formed the basis of the expert evaluation discussed later in this chapter, with the results being presented in Chapter 4.

Registration

← Back

Create an account for the prototype. This is a research demonstrator and does not require personal information.

Account details

Prototype note: Please do not use your real password. No email address is required.

Username *

Use a non-identifying username (e.g., demo_user1).

Passphrase guidance

- At least 8 characters
- Avoid using a real password

Passphrase *

Show

Must be at least 12 characters.

Confirm Passphrase *

Show

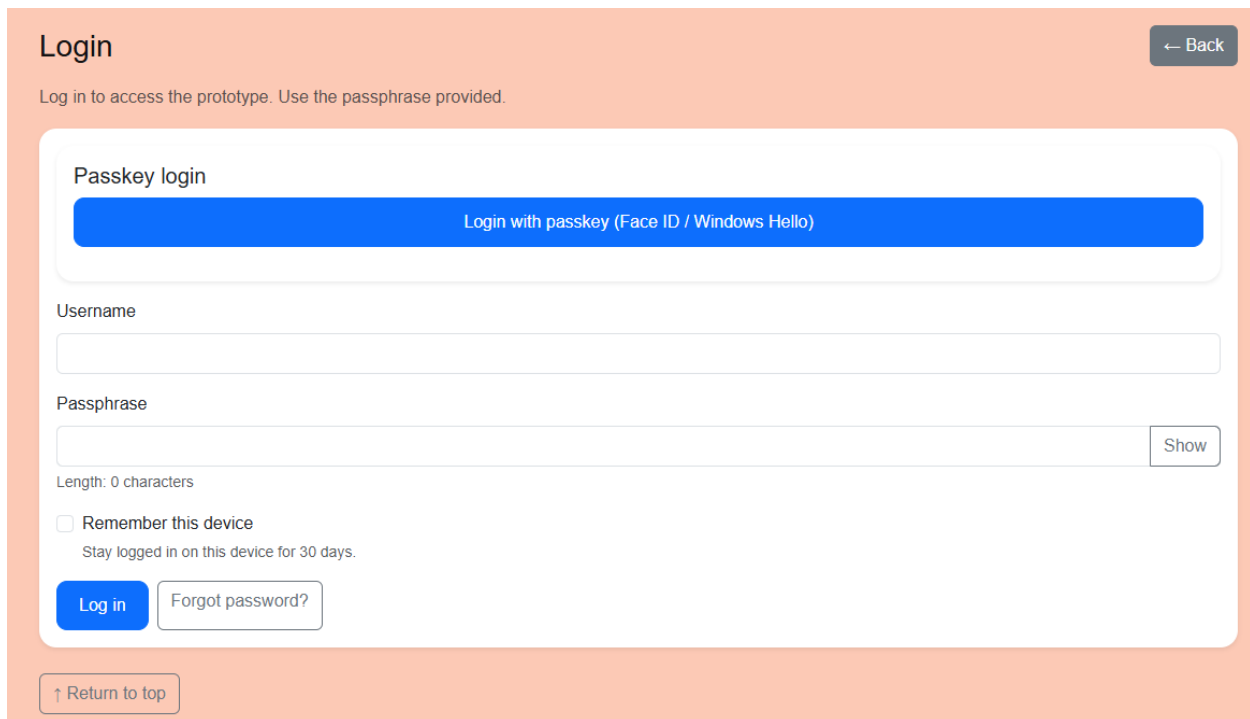
☐ Remember this device

Keeps you signed in on this device for 30 days (do not use on shared devices).

Create account

Go to login

Figure 3.3 Registration Interface



Login ← Back

Log in to access the prototype. Use the passphrase provided.

Passkey login

Login with passkey (Face ID / Windows Hello)

Username

Passphrase Show

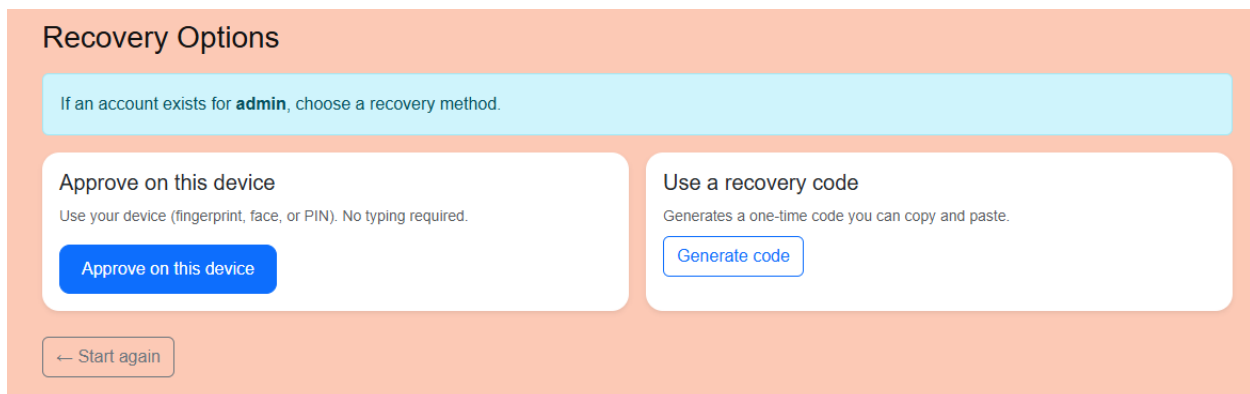
Length: 0 characters

☐ Remember this device
Stay logged in on this device for 30 days.

Log in Forgot password?

↑ Return to top

Figure 3.4 Login interface with passkey option



Recovery Options

If an account exists for **admin**, choose a recovery method.

Approve on this device
Use your device (fingerprint, face, or PIN). No typing required.

Approve on this device

Use a recovery code
Generates a one-time code you can copy and paste.

Generate code

← Start again

Figure 3.5 Account recovery interface

3.5.3 Authentication and Recovery Flow Design

The design of the registration, authentication and recovery flows were directly informed by the threats identified through the STRIDE and LINDDUN models, as well as the inclusive adaptations for MS. Emphasis was placed on reducing cognitive load, avoiding time pressure, and providing clear, and positive feedback during error conditions (Norman, 2013).

Account recovery was seen as a high-risk phase, as it poses a risk of phishing, account enumeration, or lockout spirals to users. Thus, this prototype highly favours ease of

understanding, simplicity, or redundancy in recovery mechanisms over rigid or punitive security mechanisms.

To support clarity and traceability between the threat modelling outputs and the implemented design, the authentication, registration, and account recovery processes are represented using flow diagrams. Simplified extracts are presented within this section, with full versions provided in Appendix D–F.

These design decisions directly reflect the inclusive security guidelines derived from the STRIDE and LINDDUN analysis, demonstrating how identified risks are translated into practical interface-level mitigations.

3.5.3.1 Registration Flow Design

The registration process was designed to minimise cognitive load and reduce the likelihood of user error during credential creation, in line with Guideline 1: Reduce Cognitive Load in Authentication and Recovery. The interface uses clear, plain language and avoids technical security terminology, ensuring that instructions are concise and easily understandable. Users are explicitly informed that the system is a research prototype and are advised not to use real credentials, reducing both cognitive burden and potential privacy risks.

The registration interface requires only a non-identifying username and a passphrase, avoiding the collection of personal data such as email addresses. This design decision supports data minimisation and aligns with Privacy by Design principles, while also addressing LINDDUN threats related to identifiability and linkability. Guidance is provided directly within the interface, including recommendations for username selection and passphrase length, helping users complete the process without relying on memory or prior knowledge.

To further support accessibility, the passphrase requirements are clearly stated (minimum length of 12 characters), and users are asked to confirm their passphrase to reduce the likelihood of input errors. The layout emphasises large, clearly separated input fields and interactive elements, reducing the precision required for user interaction and supporting users

with motor impairments. This reflects established human–computer interaction principles aimed at reducing both physical and cognitive effort.

A “Remember this device” option is also provided, allowing users to remain signed in on a trusted device for a limited period. This feature reduces the need for repeated authentication, thereby lowering cognitive load and the risk of repeated errors, while still requiring users to make an explicit, informed choice. Clear guidance is included advising against use on shared devices, supporting secure usage behaviour.

From a security perspective, the registration process mitigates STRIDE threats such as spoofing and denial of service by encouraging the use of strong passphrases and avoiding unnecessary complexity that may lead to repeated failed attempts. Additionally, the absence of detailed system feedback during registration helps reduce the risk of information disclosure. The simplified and privacy-preserving design ensures that users are not overwhelmed during account creation, which may otherwise increase susceptibility to insecure behaviours.

An extract of the registration flow is illustrated in Figure 3.3, with the full diagram provided in [Appendix D – Registration Flow Diagram](#)

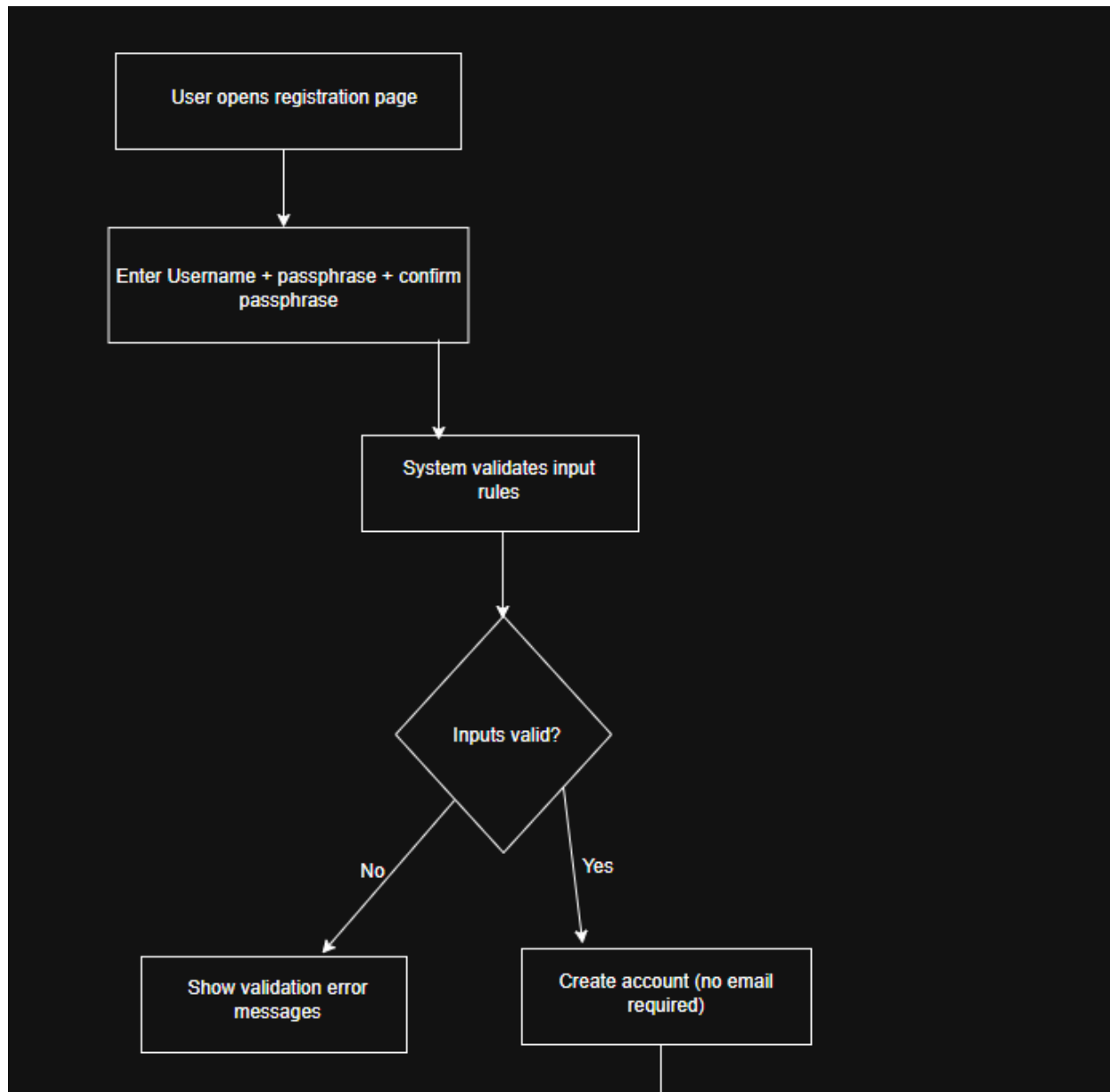


Figure 3.6 Registration Flow Diagram

3.5.3.2 Authentication Flow Design

The authentication (login) process was designed to minimise cognitive load, reduce error-prone interactions, and avoid time pressure, in line with Guideline 1: *Reduce Cognitive Load in Authentication and Recovery*. The interface presents a simple and consistent layout, requiring only a username and passphrase, with clear, concise instructions and technical security

terminology is avoided. This reduces the cognitive effort required to complete the task, which is particularly important for users experiencing fatigue or cognitive impairment.

To further support usability, the interface provides immediate, lightweight feedback through a passphrase length indicator, allowing users to recognise input issues without relying on memory or trial-and-error. Input fields and interactive elements are visually distinct and appropriately sized, reducing the level of precision required for interaction and supporting users with motor impairments. These design choices align with established human–computer interaction principles aimed at minimising both physical and cognitive effort.

The authentication process incorporates both passphrase-based login and passkey-based authentication, providing users with flexible and phishing-resistant authentication options. Passkeys enable device-bound authentication without requiring users to recall credentials, reducing cognitive load and supporting users who may experience memory difficulties. From a security perspective, this approach mitigates STRIDE threats such as spoofing and credential theft by eliminating reliance on shared secrets that can be phished or reused. This is particularly beneficial for users with MS, where cognitive fatigue may make traditional credential-based authentication more error-prone.

This design aligns with Guideline 2: *Provide Accessible Authentication Choices*, by supporting authentication methods that do not rely on memory or precise user input.

In line with both STRIDE and LINDDUN considerations, the system uses consistent, non-descriptive error messages regardless of the cause of authentication failure. This prevents the disclosure of sensitive information, such as whether an account exists, thereby mitigating risks related to information disclosure and detectability. By avoiding detailed system feedback, the design reduces opportunities for account enumeration and targeted attacks.

A “Remember this device” option is provided to reduce the need for repeated authentication on trusted devices. This supports accessibility by lowering cognitive load and minimising repeated interactions, while still requiring explicit user consent. Clear guidance is included to discourage use on shared devices, promoting secure behaviour without increasing complexity.

Overall, the authentication flow demonstrates how accessibility-focused design decisions can simultaneously reduce user burden and mitigate common security and privacy threats. An extract of the authentication flow is illustrated in Figure 3.4, with the full diagram provided in [Appendix E – Authentication \(Login\) Flow Diagram](#).

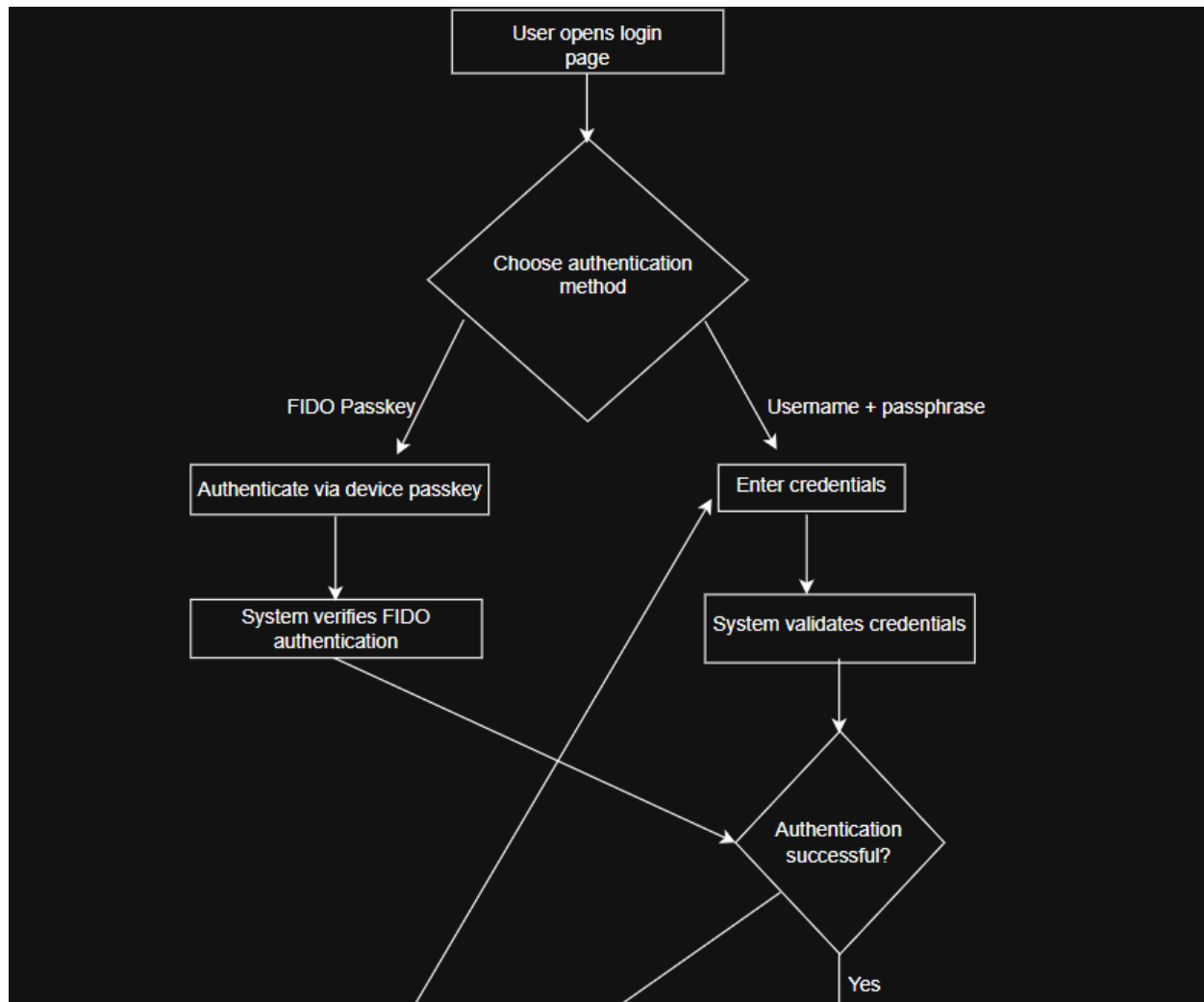


Figure 3.7 Login Flow Diagram

3.5.3.3 Account Recovery Flow Design

The account recovery process was identified as a critical and high-risk phase within the authentication lifecycle, where both security and privacy vulnerabilities are likely to emerge. This is particularly significant for users with MS, as cognitive fatigue, memory difficulties, and repeated interaction challenges may increase susceptibility to errors, phishing attacks, and lockout scenarios.

The recovery process begins with the user entering their username, after which the system presents recovery options. In line with privacy-by-design principles, the system behaves identically regardless of whether the entered username corresponds to a valid account. This prevents account enumeration and mitigates LINDDUN threats related to detectability and linkability, as well as STRIDE-related information disclosure risks.

Users are provided with multiple recovery options, such as device-based approval or the use of a recovery code. This reflects Guideline 3: *Design Account Recovery to Avoid Lockout Spirals*, by offering alternative pathways that reduce reliance on a single method and accommodate different user capabilities. These options are designed to minimise memory-dependent tasks and avoid unnecessary time pressure, supporting users who may experience cognitive or motor impairments.

Error handling within the recovery process is intentionally supportive and non-punitive. If recovery attempts fail, users are presented with consistent, generic error messages (e.g., indicating that a code is incorrect or expired) without revealing whether the account exists. This approach reduces confusion while maintaining privacy and security. Users are also provided with a clear option to restart the recovery process, preventing frustration and reducing the risk of repeated lockouts or abandonment.

To address ethical and privacy considerations, the recovery process avoids traditional email- or SMS-based mechanisms and instead implements secure, privacy-preserving recovery options, including device-based approval and recovery codes. These approaches reduce reliance on external communication channels while still enabling effective account recovery. By avoiding the use of personal identifiers such as email addresses, the system maintains strong data minimisation while still supporting functional recovery pathways. This demonstrates that secure and usable recovery mechanisms can be implemented without requiring the collection of personally identifiable information.

Device-based recovery leverages passkey authentication, allowing users to approve recovery requests through a trusted device. This provides a phishing-resistant mechanism that reduces reliance on memory-based credentials and mitigates spoofing risks. Recovery codes are also

supported as a fallback mechanism, providing an alternative pathway that does not depend on continuous device access while still maintaining security through one-time use and controlled validation.

Successful recovery leads to a passphrase reset process, followed by confirmation and redirection to the login page. This structured and predictable flow reduces cognitive burden and ensures that users can clearly understand the outcome of their actions.

Overall, the recovery flow prioritises clarity, flexibility, and privacy, demonstrating how inclusive design can mitigate both usability barriers and security risks. An extract of the account recovery process is illustrated in Figure 3.5, with the full diagram provided [in Appendix F – Account Recovery Flow Diagram](#).

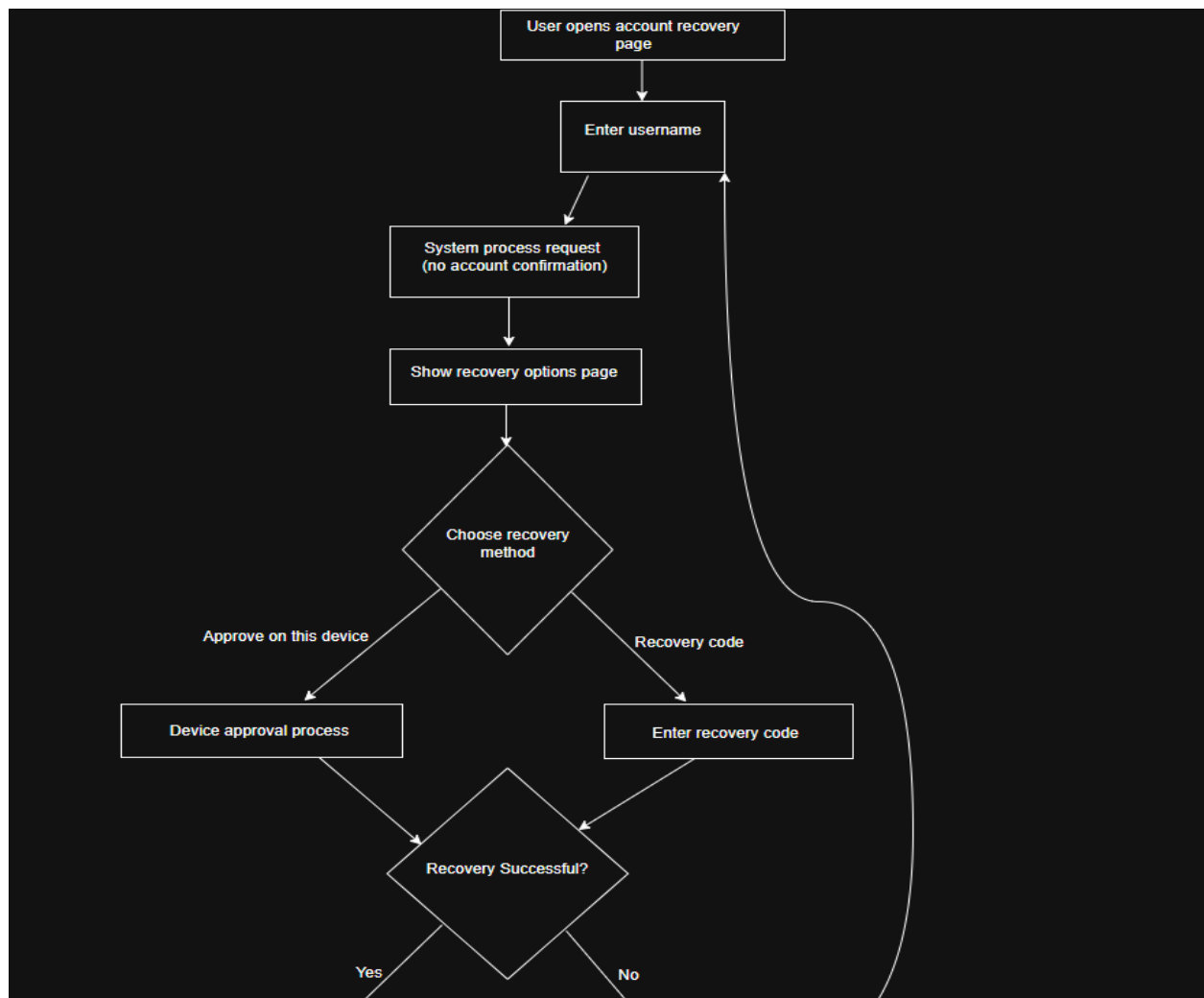


Figure 3.8 Account Recovery Flow Diagram

3.5.3.4 *Security-Accessibility Trade-offs*

Through the authentication and recovery processes, it is observed that design choices have been made with a focus on striking a balance between security, privacy, and accessibility. Instead of compromising on the security measures, the prototype has sought to address accessibility barriers as potential sources of security threats. For instance, reducing the cognitive load and complexity of interactions is not just beneficial to people with MS but also reduces the chances of authentication failures, repeated failures, and phishing attacks.

Through this prototype, it is observed that accessible design choices, like those discussed in the paper, have the potential to address STRIDE and LINDDUN attacks without compromising on security. The prototype has thus validated the initial premise of the project, which suggested that accessibility-aware threat modelling has the potential to result in accessible and secure designs.

3.5.4 *Prototype Limitations*

The prototype created for this project, while highly functional, is designed strictly as a research vehicle rather than a production-ready authentication system. Consequently, specific restrictions were implemented to adhere to ethical guidelines and prioritize participant data privacy. Perhaps the most significant of these is the intentional omission of email addresses or other communication methods for account recovery. This decision ensures that no Personally Identifiable Information (PII) is collected, aligning with the principles of data minimization and Privacy by Design. While functional recovery mechanisms are implemented, including passkey-based device approval and recovery codes, the system does not support identity verification through external communication channels (e.g., email or SMS). As a result, recovery remains dependent on the user's knowledge of their pseudonymous username, which represents a limitation compared to real-world systems.

3.6 TOOLS AND ARTEFACTS

A range of tools and artifacts were used to support this methodology:

- The system context diagram/DFD level 1 was designed using the tool draw.io (draw.io, no date)
- STRIDE and LINDUNN tables were designed to record identified threats and applicable mitigations (Shostack, 2014; Wuyts and Joosen, 2015)
- The WCAG 2.2 Accessible Authentication were taken into consideration in terms of the accessible design for authentication processes(W3C, 2023)
- HTML, CSS, and Bootstrap were used for the development of the prototype authentication and recovery system
- A project website was created with the goal of having a place to effectively represent artefacts, diagrams, and documentation in an accessible format.

These artefacts support the transparency process and traceability by linking the treat modelling stage, which are directly linked to the design guidelines and prototype implementation. The prototype implementation described in this section is supported by the full source code, provided separately and referenced in [Appendix G – Prototype Code](#).

3.7 ETHICAL CONSIDERATIONS AND PARTICIPANTS

This study received ethical approval from the Abertay University Ethics Committee (Reference: EMS11178). The research was conducted in accordance with the guidelines set out in Abertay University's Code of Ethics in Research as well as the ACM Code of Ethics and Professional Conduct (ACM, 2018). Informed consent had to be sought before the data was collected, and all participants were provided with a Participants Information Sheet in which the objectives of the research, the procedure of the research, and how the data would be used and the right to withdraw at any stage without penalty would be mentioned.

The participants recruited are those who have professional or academic interest, not those who experience or have MS themselves. None of the participants have MS, and there are no health

or clinical aspects focused on in the study. They are people from cybersecurity, accessibility, and healthcare who are asked to test the inclusive security guidelines and the authentication system.

Involvement in the study included the analysis of design artefacts (threat models and guidelines), engagement with the prototype for the login and recovery tasks, and the submission of completed questionnaire feedback, if applicable. No interviews were required, and the assessment was completed remotely at the participants' own convenience.

All the feedback data was collected in an anonymous fashion, was stored securely, and was used only for the purpose of this research. There was no gathering of personally identifiable information, nor was an attempt made to trace the information to individuals. Informed consent was obtained before the participants engaged in the research.

3.8 EVALUATION STRATEGY

This project adapts a qualitative, design-oriented evaluation strategy, focusing on how effectively the outputs of the inclusive threat modelling process translate into accessible and secure design decisions (Patton, 2014; Yin, 2018).

The evaluation is conducted through structured user testing involving expert participants, combining prototype interaction with questionnaire-based feedback.

The user testing procedure consisted of the following stages:

1. Participants were provided with a Participant Information Sheet outlining the purpose and procedure of the study
2. Informed consent was obtained prior to participation.
3. Participants interacted with the prototype, completing authentication and account recovery tasks
4. Participants evaluated the system through a structured feedback form

The evaluation instrument consisted of three components:

- System Usability Scale (SUS): A standardised set of Likert-scale questions used to assess perceived usability of the system
- Heuristic Evaluation: Participants assessed the interface against established usability principles, identifying potential usability issues
- Open-ended questions: Participants provided qualitative feedback on accessibility, usability, and perceived security

Evaluation focused on determining whether the prototype and associated guidelines:

- Reduce cognitive load in authentication and recovery processes
- Avoid exclusionary mechanisms such as unnecessary transcription or time constraints
- Provide clarity, transparency, and effective error handling
- Address security risks (STRIDE) and privacy risks (LINDDUN)

Feedback was collected via an online form and analysed qualitatively to identify recurring themes, strengths, and limitations in the proposed inclusive threat modelling methodology (Denzin and Lincoln, 2011).

3.9 SUMMARY

This chapter has discussed the methods which have been employed to develop and integrate the inclusive threat modelling process for authentication and account recovery. By using the combined STRIDE and LINDUNN threat models with an accessibility focused adaptation for MS, to develop a systematic yet dynamic model to identifying security and privacy risk that may otherwise be overlooked. The results of the methods described here have directly led to the development of the inclusive security guidelines and the prototype described in the following chapters.

4 RESULTS

4.1 INTRODUCTION

This chapter presents the findings from the evaluation of the inclusive authentication and account recovery prototype developed as part of this project. The prototype was evaluated using three complementary methods: the System Usability Scale (SUS), heuristic evaluation, and open-ended qualitative feedback.

The purpose of the evaluation was to assess the perceived usability, accessibility, and effectiveness of the prototype in supporting inclusive authentication and account recovery workflows. Results are presented factually in this chapter, with interpretation and discussion reserved for Chapter 5.

4.2 SYSTEM USABILITY SCALE (SUS) RESULTS

The participants completed the System Usability Scale (SUS) after interacting with the prototype authentication and account recovery system. The SUS is a standardised ten questions that are used to measure user satisfaction with system usability. Responses were collected using the five-point Likert Scale ranging from Strongly Disagree to Strongly Agree. Figure 4.1 presents the distribution of participant responses across all ten SUS questions.

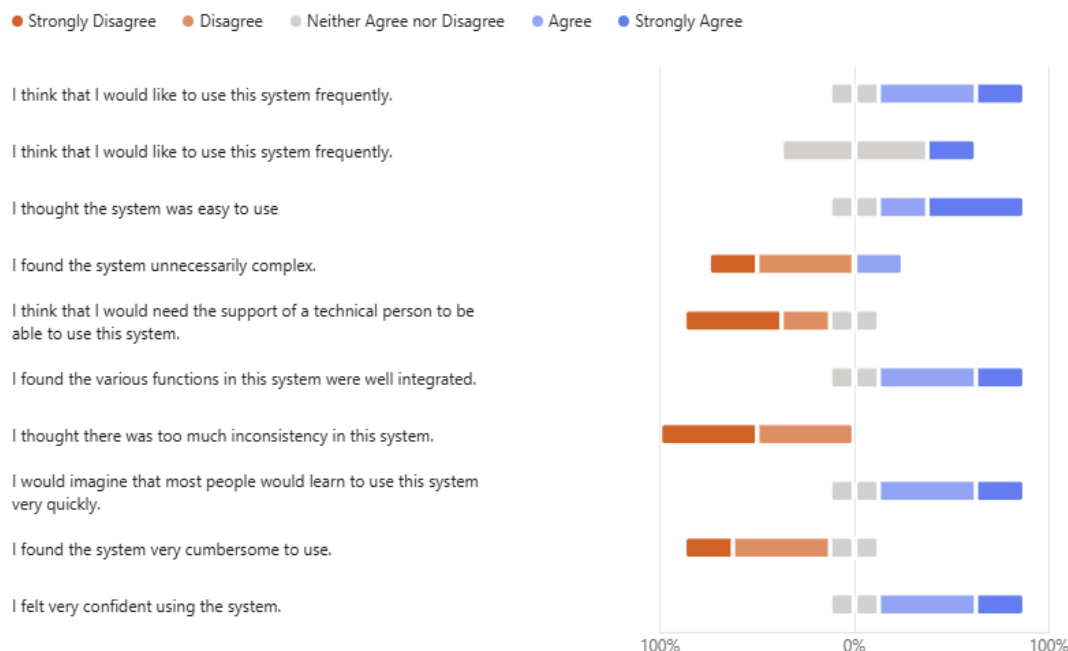


Figure 4.1 Responses to the System Usability Scale (SUS) Questions

Overall, participants provided a positive evaluation of the system's usability. Statements like "I found the system to be easy to use," "I found all the functions in this system to be well coordinated," and "I found myself to be very confident using the system" elicited Agree and Strongly Agree answers.

Negative statements on the other hand, such as "I found the system to be unnecessarily complicated," "I felt that there were too many inconsistencies in this system," and "I found the system to be very clumsy to use," received mainly Disagree and Strongly Disagree answers.

Responses showing neutrality were more common in statements concerning anticipated use frequency and the necessity of technical help in case of difficulties, revealing some uncertainty in their ability to interact with the prototype in the future.

Overall, the SUS results suggest that the participants found the prototype to be highly usable and comprehensible.

4.3 HEURISTIC EVALUATION RESULTS

Participants also completed a heuristic evaluation focusing on interface usability, accessibility, clarity, and interaction quality. The evaluation was carried out with an aim of establishing whether the interface adhered to the usability principles, which include visibility of feedback, consistency, navigability, and usability.

Figure 4.2 shows the participants' answers to the questions posed in the heuristic assessment.



Figure 4.2 Heuristic evaluation responses

The answers were largely positive, except in a few heuristics, where participants had mixed feelings on the following issues:

- visual hierarchy and emphasis in the interface elements
- instructions when errors occur and need to be handled
- flexibility for users with different levels of technical skills

Most of the heuristics got Agree or Strongly Agree responses. The participants were satisfied with the interface in terms of providing feedback, using understandable terminologies, making

key controls easily available, and ensuring ease of use. Navigation and clarity-related questions received high marks from the participants.

Despite some heuristics getting mixed answers, the evaluation shows that the interface is clear, accessible, and largely aligned with recognised usability principles.

4.4 QUALITATIVE FEEDBACK RESULTS

The participants were encouraged to give their comments regarding the usability, accessibility, security features, and general impression of the prototype.

From the analysis of the qualitative data, some common themes emerged positively, along with some recommended changes.

4.4.1 Positive Themes Identified

Clear and Intuitive Layout

One of the consistent themes was how simple and intuitive the interface design was. Many respondents described the software as being visually clear and easy to use.

The key processes, such as logging in, signing up, and recovering one's account, were all clearly displayed and arranged in a logical order.

Some other answers also mentioned how the homepage design and navigation through icons made it easy to find the available choices.

Authentication and Recovery Design

The participants responded positively to the design of the authentication process and the steps involved in recovering their accounts. The login process and the recovery process were described as intuitive, with users noting that there was clarity in what they could do and how to navigate through the process.

Perceived Balance Between Security and Usability

Several participants made explicit comments regarding the achievement of a good balance between security considerations and ease of use.

Comments such as:

"This seems to have a good balance."

and

"Seems like a balanced interaction."

These are clear indications that users perceive the prototype as having maintained security functionalities without increasing interaction burden.

4.4.2 Suggested Improvements

Although feedback was largely positive, participants also identified several areas for improvement.

Registration Clarity

One of the users expressed mild confusion when registering, implying that some parts of the registration process might require further clarification or explanation for easier understanding. This shows that even though the registration process is usable, there is still room for improvement to ensure that the instructions are clearer.

Motion and Animation Effects

A participant suggested that interface movement, like animations or motion, might be distracting or mentally taxing.

The implication is that while movement may be appealing visually, it may raise accessibility issues for some users, particularly in situations where mental exhaustion or distractibility is a factor.

Passkey Setup Clarity

One of the participants was unsure about some aspects of passkey setup. The comment was about the possibility of making things clearer regarding what is expected when enrolling or using a passkey. It seems, therefore, that even though passkeys are considered a valuable tool, the procedure needs to be clarified.

Overall, qualitative feedback was predominantly positive while also identifying a small number of interface and workflow refinements that may strengthen future iterations of the prototype.

4.5 SUMMARY OF RESULTS

Chapter four presents the results of the evaluation process conducted on the prototype of an inclusive authentication and account recovery feature.

The SUS score is indicative of positive perceptions of usability, whereby the system is described by participants as easy to use, integrated, and confidence-inducing.

Similarly, heuristic evaluation results reveal that the perceptions about interface clarity, navigability, feedback quality, and usability were high, apart from a few cases where perceptions on hierarchy, instructions, and adaptability were mixed.

From the qualitative feedback, the strengths noted in the evaluation include interface clarity, authentication and recovery design, and balance between usability and security. Suggestions for future improvements include registration experience, motion effects, and passkey onboarding.

The interpretation of results will be discussed in Chapter five.

5 DISCUSSION

5.1 INTRODUCTION

In this chapter, we discuss how the findings from Chapter 4 align with the project's goals, objectives, and existing literature as summarized in Chapter 2. The project's intention was to investigate how cybersecurity threat modelling could be used to accommodate people with MS within the scope of authentication and recovery services.

The findings suggest that if threat modelling takes accessibility into consideration that doesn't necessarily mean giving up on security. On the contrary, the findings prove that threat modelling of security and privacy measures take accessibility needs into account which provide useful design outputs while maintaining fundamental security properties.

5.2 OBJECTIVE 1: ANALYSIS OF AUTHENTICATION AND ACCOUNT RECOVERY USING THREAT MODELLING

The first objective of this project was to analyse authentication and account recovery processes using threat modelling techniques.

Threat modelling methods such as STRIDE and LINDDUN are commonly used approaches for detecting security and privacy threats within the system design process. The STRIDE model is used in addressing security threats such as spoofing, tampering, repudiation, information disclosure, denial of service, and escalation of privilege. On the other hand, the LINDDUN framework targets privacy threats such as linkability, identifiability, detectability, disclosure of information, unawareness, and non-compliance.

The findings demonstrate that these models can successfully be utilized to analyse workflows related to authentication and account recovery to uncover security and privacy threats. The context diagram and data flow diagrams prepared in Chapter 3 facilitated a systematic analysis of the relevant workflows.

Through this analysis multiple traditional risks were identified, including spoofing using phishing and credential theft, denial of service due to repeated authentication attempts, account lockouts, information disclosure due to feedback and recovery flows, as well as detectability due to account enumeration.

This result is consistent with past studies which have categorized authentication and recovery as critical components of security (Grassi *et al.*, 2020; OWASP, no date). Authentication and recovery flows represent attack surfaces which can easily be targeted since these two components play an important role in access control and usually involve sensitive user information. However, threat modelling can also highlight an apparent limitation in existing threat frameworks, especially with respect to their ability to capture risks associated with accessibility-related threat pathways. Although STRIDE and LINDDUN can effectively uncover technological and privacy risks, they fail to incorporate accessibility-based threat pathways which can increase the probability of attack execution.

Examples include the time pressure involved in the authentication process, reliance on memory recall, complex recovery flows, and complicated interactions between users and interfaces, among others (Reese *et al.*, 2019; Gaggi, 2022).

This is significant because a system can seem to be safe by looking at it using only technical threat modelling yet creating practical circumstances that gradually compromise the security results. In other words, although a particular authentication system is technically safe, it can still be unsafe in terms of practice if the actual users face challenges completing their security actions.

Thus, the presented results prove the idea proposed in Chapter 2, suggesting that threat modelling is still attacker-focused and technically oriented.

5.3 OBJECTIVE 2: ADAPTING STRIDE AND LINDDUN TO INCORPORATE ACCESSIBILITY

The second objective was the adaption of STRIDE and LINDDUN to consider accessibility issues. One of the key contributions of this research is the inclusion of an inclusive approach into existing threat modelling frameworks, specifically considering people who have MS.

Accessibility issues are not just seen as problems with usability, but rather as factors contributing to the risk of security and privacy breaches.

It was shown to be useful in uncovering the risks that would usually be missed by regular threat models.

Some of the risks discovered through the modified analysis process include:

- cognitive fatigue and memory difficulties increasing likelihood of authentication failure
- repeated failure creating denial-of-service-like lockout scenarios
- recovery complexity increasing phishing susceptibility
- memory dependence encouraging insecure coping behaviours such as credential reuse or credential sharing

These results are highly aligned with usable security research.

However, Adams and Sasse (1999) argue that users are not necessarily insecure but are merely adaptive, responding rationally to overly demanding security measures. Likewise, Cranor (2008) considers users as active agents of the security process, emphasizing the connection between user abilities and security consequences.

The research results further advance such views by proving that accessibility constraints may be viewed as threat multipliers.

This is of special importance since today's threat models lack systematic approaches to assessing how the constraints of users can influence the probability of threats.

The modified approach therefore provides an effective way of integrating accessibility with threat modelling.

It is important to note that the modification in question will not involve discarding the currently used approaches altogether but requires only some adjustments, for example, introducing accessibility issues in threat analysis tables and in workflow analysis.

Such conclusions indicate that accessibility threat modelling can be introduced into the security design process without any significant changes to the procedure itself.

5.4 OBJECTIVE 3: IDENTIFICATION OF ACCESSIBILITY-DRIVEN SECURITY AND PRIVACY RISKS

The third objective was to identify security and privacy risks introduced by accessibility barriers.

The findings support the hypothesis that accessibility barriers can directly contribute to both security and privacy risks. Several key risks emerged.

Authentication Failure and Lockout

Participant evidence and existent literature suggest that complex authentication processes have increased potential for human errors leading to authentication failures.

For people living with MS, factors such as fatigue, slowed cognitive function, memory issues, and fluctuating symptom severity can significantly compound this issue (DeLuca et al., 2015).

Consequently, frequent authentication failure may result in account lockout scenarios, creating denial-of-service situations for genuine users.

In doing so, the findings provide direct justification for the consideration of accessibility barriers as part of STRIDE denial-of-service analysis within the project.

The importance of the finding lies in the recasting of denial-of-service attacks from the perspective of intentional attack by an adversary to the unintentional denial of service caused by inaccessible interaction design.

Phishing Susceptibility

Complicated processes in authentication and recovery may enhance the level of user stress and limit the ability to critically evaluate interactions.

As noted by Wash (2010), users facing urgency or stress are more prone to becoming victims of phishing scams.

In turn, recovery processes appear especially at risk, considering that users frequently perform their tasks under uncertainty, urgency, or frustration.

Based on these findings, the decision was made to simplify recovery procedures, ensure workflow segregation, and avoid complexity.

Thus, the findings indicate that accessibility issues might affect usability negatively while altering the level of user threat exposure through decision-making during stressful situations.

Privacy Risks

The project also pointed out possible privacy issues relating to account enumeration, inconsistencies in error messages, and excessive information during recovery procedures. The above results align with the recommendations put forth by OWASP and the LINDDUN model of privacy categories. Thus, consistent system reaction and minimal information sharing were implemented in the prototype system design. It is essential to note that privacy threats in authentication systems do not necessarily come from data breaches but may be triggered by seemingly trivial interface issues that inadvertently leak sensitive information.

5.5 OBJECTIVE 4: DEVELOPMENT OF INCLUSIVE SECURITY GUIDELINES

Objective four involved the creation of the inclusive security design guidelines.

- There were four major guidelines produced from this project:
- Reduce cognitive load in authentication and recovery
- Provide accessible authentication choices
- Design account recovery to avoid lockout spirals

- Ensure privacy and transparency throughout security flows

These guidelines provided implementation of the threat modelling output into actionable design recommendations.

Evaluation results show that these guidelines can be easily applied in practice. High SUS scores and positive heuristic evaluation feedback indicate that the prototype was perceived as:

- easy to use
- clear and intuitive
- properly balanced in terms of security/usability trade-off

This suggests that the design guidelines successfully guided the design process, allowing to create secure and usable designs.

It is important to note that no guidelines involved lowering the security level at any point. On the contrary, they follow the current best practices in terms of authentication, including:

- WCAG 2.2 accessible authentication recommendations (W3C, 2023)
- NIST SP 800-63B (Grassi *et al.*, 2020)
- Passkeys (FIDO Alliance, 2022, 2023)

This demonstrates that following design principles related to accessibility and offering strong authentication are not mutually exclusive practices.

However, based on the feedback received from experts, certain issues require further attention, including onboarding and motion effect-related concerns. Therefore, design guidelines can be viewed as iterative principles rather than fixed prescriptions.

5.6 OBJECTIVE 5: PROTOTYPE IMPLEMENTATION AND EVALUATION

Objective five entailed development of a prototype authentication system based on the proposed guidelines.

Prototype achievements include the following implemented functionalities:

- registration
- login
- account recovery
- passkey enrolment
- passkey authentication
- code recovery
- device recovery

This accomplishment is important as it marks a shift from a theoretical to an empirical study in terms of demonstrating the applicability of the developed model.

Positive evaluation results point out that the prototype was able to effectively materialize the proposed guidelines.

Positive evaluation results are represented by the following:

- high usability ratings
- good heuristics assessments
- positive qualitative feedback related to clarity, recovery design, and security/usability trade-off

Among other things, users highly appreciated clarity of the workflow, simple recovery methods, and user-friendly navigation.

It means that a balance between accessibility and security can be struck in designing authentication systems without significantly undermining security.

Areas that need to be improved include:

- clarity of registration
- clarity of passkey onboarding
- animation effects

The findings are useful in the sense that it proves that an accessible system does not exist from inception; it needs iterations for improvements.

While the evaluation results are rather promising, they need to be cautiously interpreted because of the relatively small number of participants in the study and lack of evaluation with the targeted population, MS sufferers.

5.7 SIGNIFICANCE OF FINDINGS

This project contributes to the existing research and practice in three keyways.

First, it demonstrates a practical adaptation of established models of threat analysis such as STRIDE and LINDDUN with the inclusion of accessibility-based analysis. As described in Chapter 2, conventional methodologies for threat analysis generally focus on technical weaknesses and the actions of attackers, with little regard for how accessibility constraints could pose a security or privacy risk. By incorporating accessibility factors in relation to MS into these models, the proposed method attempts to extend conventional threat modelling than just technical analysis.

Secondly, the conclusions support the argument that accessibility is a matter of security and privacy, not merely usability. The evidence from the evaluation tests, design choices for the prototype, and threat modelling process as a whole demonstrates that the existence of accessibility barriers such as cognitive strain, reliance on memory, motor requirements, and lack of clarity regarding recovery procedures can create the conditions for potential threats such as susceptibility to phishing attacks, lockout, credential re-use, and data exposure. This supports and builds upon existing research in usable security by showing that accessibility barriers can serve as threat vectors in authentication and account recovery schemes.

Lastly, the study has practical implications beyond its theoretical contribution. In addition to the modified threat model approach, this project has delivered tangible outcomes in the form of

security design guidelines for accessibility, a practitioner-facing guide, and an authentic authentication and recovery prototype.

The outcomes obtained not only make the research applicable in practical settings but also demonstrate how potential risks can be made operational by being turned into design choices and incorporated into actual workflows.

This, in turn, makes the practitioner guide especially relevant since it helps make the research findings applicable to people with less technical knowledge such as medical staff, accessibility activists, and charity organizations. This increases the potential scope of applicability of the study results, beyond cybersecurity professionals.

To summarize, the results of the present research suggest that the approach to threat modelling incorporating accessibility considerations could become the basis for designing secure and usable authentication systems.

5.8 LIMITATIONS

There were several limitations that should be acknowledged. The study had several limitations due to the small sample size used. The number of participants was limited by the timeframe within which the project had to be completed and the difficulties in recruiting participants from relevant external agencies such as MS charities and other organizations dedicated to addressing MS issues. This meant that the research relied on a smaller number of experts than initially anticipated. While this did not affect data collection, it limits the generalization of the results obtained.

Firstly, the pool of participants was composed of experts and not people who suffer from MS, although this was seen as ethically and practically acceptable for the purposes of an undergraduate honours project. A direct validation using people with lived experiences of MS would be more appropriate in determining if the proposed design choices have effectively dealt with practical accessibility issues.

Secondly, the prototype is a research tool and is not a fully operational piece of software. While a degree of realism was brought about by the implementation of secure mechanisms such as authentication, password recovery, and even basic security measures, these did not include production-level criteria such as robust infrastructure, certification, mass roll-out, and enterprise identity management systems.

Thirdly, the project focused only on the condition of MS as an example of inclusive design of an authentication and password recovery mechanism. Many of the accessibility issues related to security and privacy risks might apply to users with other kinds of conditions. However, that was outwith the reach of this project at this time.

5.9 SUMMARY

This chapter provides an evaluation of the findings against the objectives of the project.

The findings suggest that modifying the existing threat modelling frameworks to include the aspect of accessibility is effective in revealing security and privacy threats associated with authentication and recovery of accounts which could easily be missed otherwise.

The developed guidelines and prototype demonstrate that designing for security with accessibility in mind is possible, resulting in solutions that do not sacrifice security and privacy principles.

Thus, the results confirm the main idea of the dissertation , accessibility threat modelling represents a useful starting point for developing inclusive authentication solutions.

The final chapter contains the conclusions drawn from the project as well as recommendations for further research.

6 CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

This project explores how traditional threat modelling approaches can be adapted to better account for accessibility-related security and privacy risks in authentication and account recovery systems, with particular focus on users living with MS.

There is a clear mismatch between threat modelling in cybersecurity and accessibility design. While threat modelling tools like STRIDE and LINDDUN provide a systematic approach towards the identification of security and privacy threats, there exists no framework that considers how accessibility constraints impact users' actions and increase the likelihood of failure, thereby exacerbating security and privacy threats.

To address this gap, an accessibility-based version of STRIDE and LINDDUN was created to consider the relevant characteristics associated with MS, such as cognitive fatigue, reduced processing speed, poor memory, and motor impairments. The approach used system context diagrams, data flow diagrams, and workflow analysis to investigate authentication workflows, including registration, login, and account recovery, to detect not only typical security threats but also risk paths linked with accessibility problems.

Based on the findings obtained during the analysis, inclusion-focused security design guidelines were formulated for mitigating cognitive overload and designing accessible authentication options, account recovery features, and privacy-transparent authentication interfaces. The practical realization of these guidelines was provided by developing an authentic web-based prototype featuring passphrase-based and passkey-based authentication as well as account recovery options.

The findings from the evaluation through the expert review, which comprised SUS evaluations, heuristic analysis, and qualitative feedback, were quite positive regarding usability,

understandability, and the trade-off between security and accessibility. The participants reported on user-friendly interfaces, navigable sites, and recovery options, among other strengths. However, there are areas for improvement, particularly regarding the understanding of the process and interaction design.

The results presented above support the main argument presented in this research: Accessibility barriers should not be addressed as usability barriers only, as they can potentially affect security and privacy outcomes. As a result, reframing accessibility barriers into threat amplifiers shows how inclusive design approaches can be incorporated into threat modelling to develop secure authentication systems.

Theoretical and practical contributions include an accessibility-conscious threat modelling framework, accessible security principles, and validation through a prototype implementation.

Ultimately, secure system architecture is meant to go beyond robustness and ensure that the various capabilities of end users engaging with security features are considered. This work provides the foundation for further development in accessible security practices, highlighting accessibility as an integral part of designing secure authentication and recovery systems.

6.2 FUTURE WORK

Several opportunities exist to extend this work.

Firstly, any future studies should involve an evaluation conducted among people who have been diagnosed with MS or related diseases. While a professional evaluation brought some interesting findings in relation to the usability, accessibility, and security of the system, an evaluation conducted by actual users would provide more credible information on how effective the proposed prototype is.

Second, another direction that can be explored in the context of this research is the use of the developed methodology in other diseases apart from MS. In fact, many accessibility issues highlighted in the present project, including those related to fatigue, slow reaction times, and poor motor coordination, can occur in people with such conditions as ADHD or dyslexia.

Another possible area of future research lies in the formalization of the extended threat modelling technique into a usable framework or toolkit. This framework can use templates or checklists for the use of the extended version of the STRIDE or LINDDUN techniques, facilitating the inclusion of considerations for accessibility in threat modelling practices.

The investigation of further threat modelling techniques along with STRIDE and LINDDUN techniques is another possibility for future research. Though STRIDE and LINDDUN offer methodologies to assess security and privacy risks in authentication and account recovery processes, there are other techniques that may prove useful due to their focus on the attacker and risk perspectives. One such methodology is the PASTA methodology.

By considering the PASTA framework, there is an ability to perform a much more detailed investigation on threat probability, motivation behind attackers, and impact on the business. Therefore, this will lead to a deeper investigation based on an accessibility-aware threat model that was created throughout the course of this project and extend its applicability from a threat assessment to risk management.

Moreover, another potential area for further investigation might involve the use of accessibility-aware threat modelling in the earlier stages of the software development lifecycle process, such as requirement generation, system architecture design, and threats assessment.

Finally, the prototype created by this project can be modified into a production system. This involves developing a stronger backend structure, deploying the prototype, handling key management securely, offering customizable access needs, and adopting other authentication mechanisms. A longitudinal analysis can then confirm if designing security from an accessibility perspective increases authentication efficiency, eliminates bad coping mechanisms, and boosts user confidence.

In conclusion, this paper presents an initial framework for incorporating accessibility requirements into threat models and secure authentication design. Future studies can then continue from this framework to reinforce the connection between accessibility, usability, security, and privacy in modern authentication systems.

REFERENCES

- ACM (2018) *The Code affirms an obligation of computing professionals to use their skills for the benefit of society*. Available at: <https://www.acm.org/code-of-ethics> (Accessed: 24 April 2026).
- Adams, A. and Sasse, M.A. (1999) 'Users are not the enemy', *Commun. ACM*, 42(12), pp. 40–46. Available at: <https://doi.org/10.1145/322796.322806>.
- Alodhyani, F., Theodorakopoulos, G. and Reinecke, P. (2020) 'Password Managers—It's All about Trust and Transparency', *Future Internet*, 12(11), p. 189. Available at: <https://doi.org/10.3390/fi12110189>.
- Askari, S., Fanelli, D. and Harvey, K. (2021) 'Cognitive fatigue interventions for people with multiple sclerosis: A scoping review', *Multiple Sclerosis and Related Disorders*, 55. Available at: <https://doi.org/10.1016/j.msard.2021.103213>.
- Blessing, L.T.M. and Chakrabarti, A. (2009) *DRM, a Design Research Methodology*. London: Springer. Available at: <https://doi.org/10.1007/978-1-84882-587-1>.
- Bonneau, J. et al. (2012) 'The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes', *2012 IEEE Symposium on Security and Privacy*. San Francisco, CA, USA: IEEE, pp. 553–567. Available at: <https://doi.org/10.1109/SP.2012.44>.
- Charvet, L., Serafin, D. and Krupp, L. (2013) 'Fatigue in multiple sclerosis', *Fatigue: Biomedicine, Health & Behavior*, 2, pp. 3–13. Available at: <https://doi.org/10.1080/21641846.2013.843812>.
- Cranor, L.F. (2008) 'A framework for reasoning about the human in the loop', *Proceedings of the 1st Conference on Usability, Psychology, and Security*. USA: USENIX Association (UPSEC'08), pp. 1–15.
- Creswell, J.W. (2014) *Research design : qualitative, quantitative, and mixed methods approaches*. SAGE Publications. Available at: <https://eduq.info/xmlui/handle/11515/19498> (Accessed: 24 April 2026).
- Creswell, J.W. and Poth, C.N. (2024) *Qualitative inquiry and research design : choosing among five approaches*. 5th edition. Thousand Oaks: SAGE Publications Limited. Available at: <https://login.eux.idm.oclc.org/login?url=https://resolver.vitalsource.com/9781544398426>.

DeLuca, G.C. *et al.* (2015) 'Cognitive impairment in multiple sclerosis: clinical, radiologic and pathologic insights', *Brain Pathology (Zurich, Switzerland)*, 25(1), pp. 79–98. Available at: <https://doi.org/10.1111/bpa.12220>.

Deng, M. *et al.* (2011) 'A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements', *Requir. Eng.*, 16, pp. 3–32. Available at: <https://doi.org/10.1007/s00766-010-0115-7>.

Denzin, N.K. and Lincoln, Y.S. (2011) *The Sage handbook of qualitative research*. 4th ed. Thousand Oaks: Sage.

draw.io (no date) *diagrams.net Online Diagramming Tool*. Available at: <https://app.diagrams.net/> (Accessed: 24 April 2026).

Erinola, A. *et al.* (2023) "As Usual, I Needed Assistance of a Seeing Person": *Experiences and Challenges of People with Disabilities and Authentication Methods*. Available at: <https://doi.org/10.1109/EuroSPW59978.2023.00070> (Accessed: 29 October 2025).

FIDO Alliance (2022) *Guidance for Making FIDO Deployments Accessible to Users with Disabilities*.

FIDO Alliance (2023) *UX Guidelines for Passkey Creation and Sign-ins*.

Fitts, P.M. (1954) 'The information capacity of the human motor system in controlling the amplitude of movement', *Journal of Experimental Psychology*, 47(6), pp. 381–391. Available at: <https://doi.org/10.1037/h0055392>.

Florêncio, D., Herley, C. and van Oorschot, P.C. (2014) 'Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts'.

Gaggi, O. (2022) 'A study on Accessibility of Google ReCAPTCHA Systems'. New York, NY, USA: Association for Computing Machinery (OASIS '22), pp. 25–30. Available at: <https://doi.org/10.1145/3524010.3539498>.

Gaw, S., Felten, E.W. and Fernandez-Kelly, P. (2006) 'Secrecy, flagging, and paranoia: adoption criteria in encrypted email', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New

York, NY, USA: Association for Computing Machinery (CHI '06), pp. 591–600. Available at:
<https://doi.org/10.1145/1124772.1124862>.

Glass, B. *et al.* (2016) 'The usability canary in the security coal mine: A cognitive framework for evaluation and design of usable authentication solutions', *Proceedings 1st European Workshop on Usable Security*. Available at: <https://doi.org/10.14722/eurosec.2016.23007>.

Grassi, P. *et al.* (2020) *Digital Identity Guidelines: Authentication and Lifecycle Management*. NIST Special Publication (SP) 800-63B (Withdrawn). National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-63b>.

Lazar, J., Goldstein, D. and Taylor, A. (2015) *Ensuring Digital Accessibility through Process and Policy*.

MacKenzie, I.S. (1992) 'Fitts' Law as a Research and Design Tool in Human-Computer Interaction', *Human-Computer Interaction*, 7(1), pp. 91–139. Available at:
https://doi.org/10.1207/s15327051hci0701_3.

Merriam, S.B. and Tisdell, E.J. (2016) *Qualitative research : a guide to design and implementation*. Fourth edition. San Francisco, CA: Jossey-Bass (The Jossey-Bass higher and adult education series).

Microsoft (no date) *Threats - Microsoft Threat Modeling Tool*. Microsoft Learn. Available at:
<https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats> (Accessed: 24 April 2026).

Mills, J., Birks, M. and Mills, J. (no date) 'Methodology and Methods', in pages 31-47, *Qualitative Methodology: A Practical Guide*.

MS Society (no date) *What is Multiple Sclerosis (MS)?* Available at:
<https://www.mssociety.org.uk/about-ms/what-is-ms> (Accessed: 18 April 2026).

Norman, D.A. (2013) 'The Design of Everyday Things: Revised and Expanded Edition'. Available at:
<https://api.semanticscholar.org/CorpusID:149414952>.

Ophoff, J., Johnson, G. and Renaud, K. (2021) 'Cognitive function vs. accessible authentication: insights from dyslexia research', *Proceedings of the 18th International Web for All Conference*. New York, NY,

USA: Association for Computing Machinery (W4A '21). Available at:
<https://doi.org/10.1145/3430263.3452427>.

Ophoff, J. and Renaud, K.V. (2023) 'Universal Design for Website Authentication: Views and Experiences of Senior Citizens', *2023 38th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)*, pp. 46–53. Available at: <https://doi.org/10.1109/ASEW60602.2023.00011>.

OWASP (no date) *Authentication - OWASP Cheat Sheet Series*. Available at:
https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html (Accessed: 24 April 2026).

Patton, M.Q. (2014) *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*. Fourth. SAGE Publications.

Reese, K. *et al.* (2019) 'A Usability Study of Five Two-Factor Authentication Methods', *Proceedings of the Fifteenth Symposium on Usable Privacy and Security* [Preprint]. Available at:
<https://par.nsf.gov/biblio/10110669-usability-study-five-two-factor-authentication-methods> (Accessed: 29 October 2025).

Rocca, M. *et al.* (2015) 'Clinical and imaging assessment of cognitive dysfunction in multiple sclerosis', *The Lancet. Neurology*, 14. Available at: [https://doi.org/10.1016/S1474-4422\(14\)70250-9](https://doi.org/10.1016/S1474-4422(14)70250-9).

Shostack, A. (2014) *Threat modeling : designing for security*. Indianapolis, IN : J. Wiley & Sons. Available at: <http://archive.org/details/threatmodelingde0000shos> (Accessed: 18 April 2026).

Swiderski, F. and Snyder, W. (2004) 'Threat Modeling'.

Temoshok, D. *et al.* (2025) *NIST SP 800-63-4: digital identity guidelines*. NIST SP 800-63-4. Gaithersburg, MD: National Institute of Standards and Technology (U.S.), p. NIST SP 800-63-4. Available at:
<https://doi.org/10.6028/NIST.SP.800-63-4>.

W3C (2023) *Web Content Accessibility Guidelines (WCAG) 2.2*. Available at:
<https://www.w3.org/TR/WCAG22/> (Accessed: 29 October 2025).

Wash, R. (2010) 'Folk models of home computer security', *Proceedings of the Sixth Symposium on Usable Privacy and Security*. New York, NY, USA: Association for Computing Machinery (SOUPS '10), pp. 1–16. Available at: <https://doi.org/10.1145/1837110.1837125>.

White, S. (2026) “‘My university project will improve digital access for MS patients’”, *MS-UK*, 27 April. Available at: <https://ms-uk.org/blog/my-university-project-will-improve-digital-access-for-ms-patients/> (Accessed: 28 April 2026).

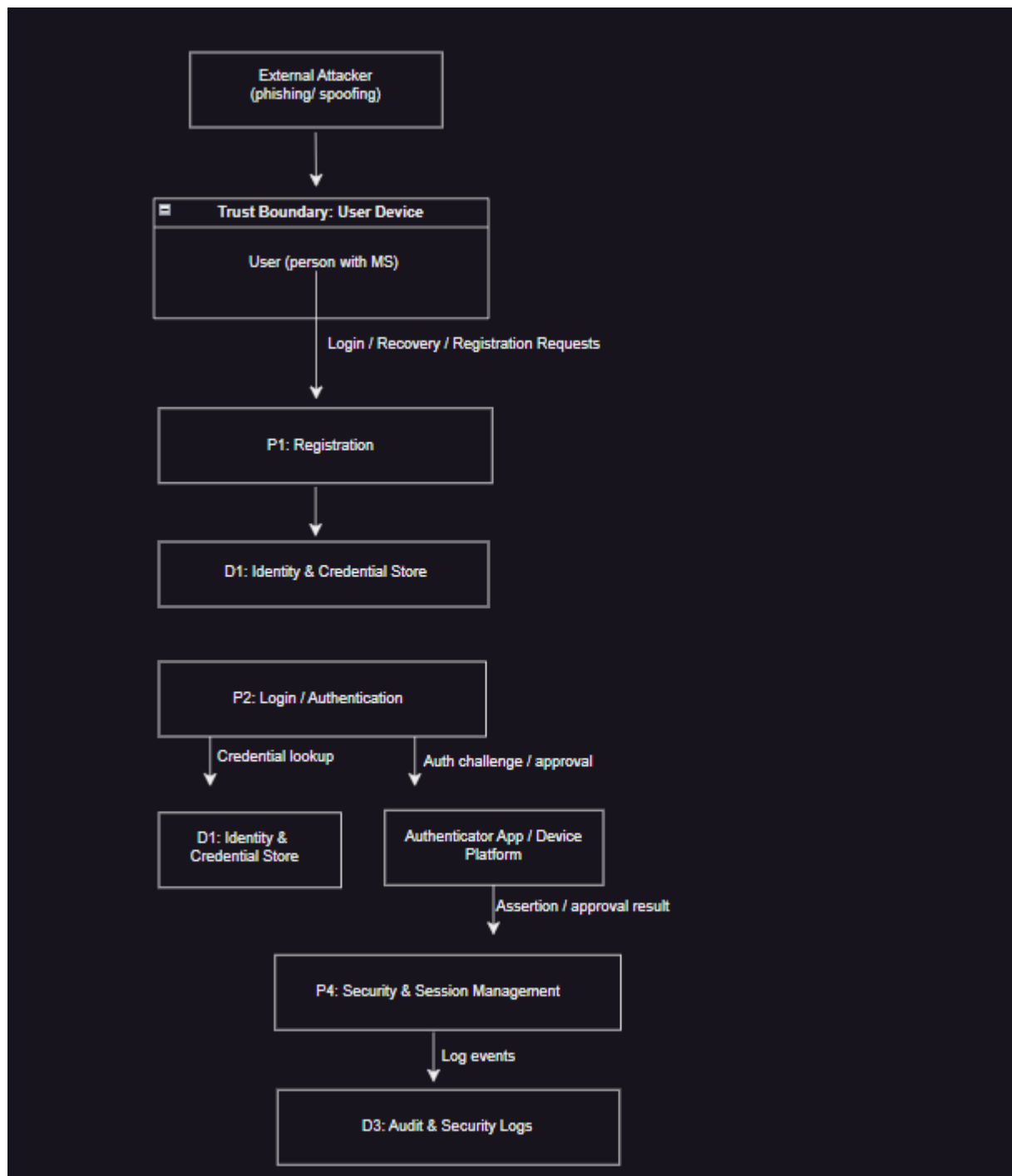
Wuyts, K. and Joosen, W. (2015) 'LINDDUN privacy threat modeling: a tutorial'. Available at: <https://api.semanticscholar.org/CorpusID:63402265>.

Yin, R.K. (2018) *Case study research and applications: design and methods*. Sixth edition. Los Angeles London New Delhi Singapore Washington DC Melbourne: SAGE.

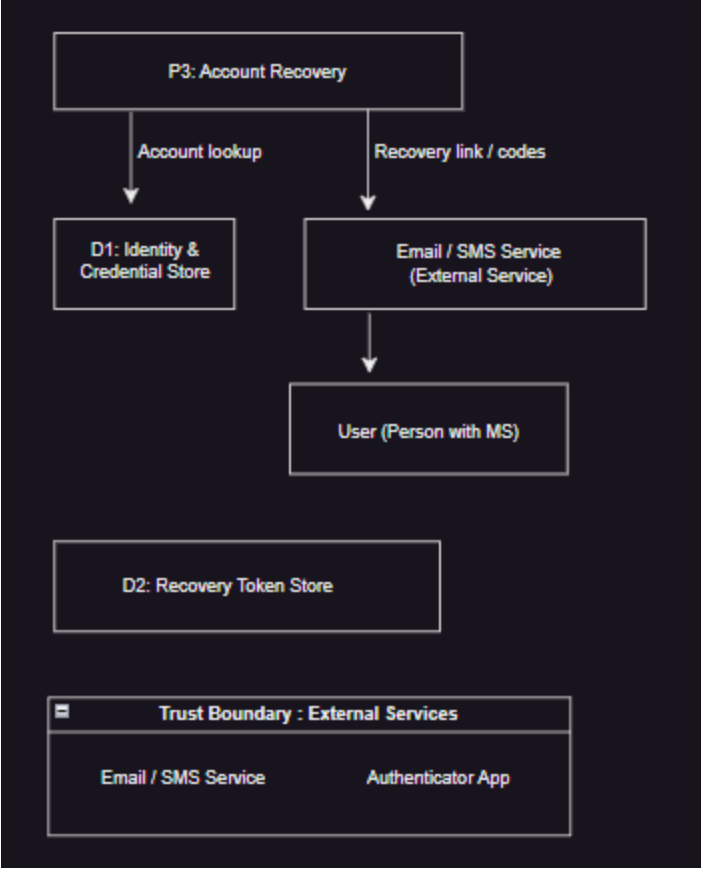
APPENDICES

APPENDIX A – SYSTEM CONTEXT DIAGRAM

Part 1



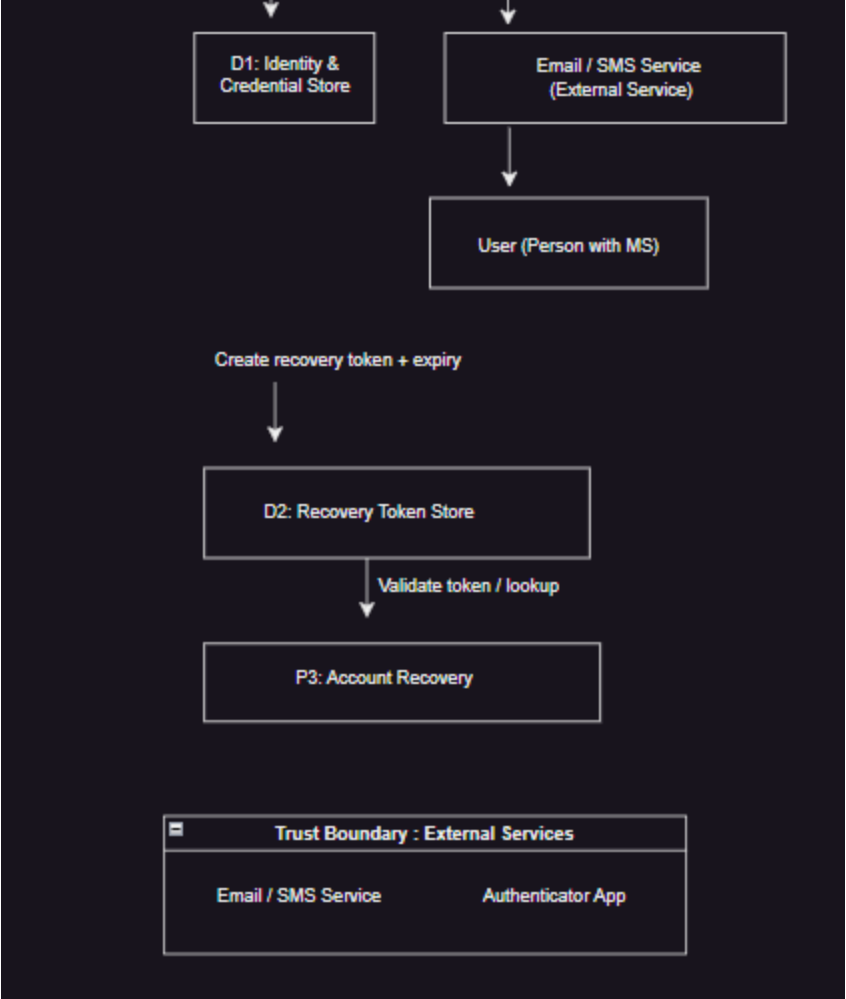
Part 2



APPENDIX B— DFD DIAGRAM

Part 1





APPENDIX C – STRIDE TABLE

STRIDE Threat Analysis Table

Using the Level 1 DFD, I applied STRIDE to each core process. A key finding is that denial-of-service and spoofing risks disproportionately affect users with MS due to fatigue, cognitive fog, and motor challenges. As a result, the threat model prioritizes adaptive lockout thresholds, phishing-resistant authentication, and accessible recovery flows that reduce cognitive load without weakening security.

Based on level 1 DFD: P1 - P4

P1 - Registration

Stride Category	Threat Description	MS-Specific Impact	Mitigation Strategy
S - Spoofing	Attacker impersonates user during registration (e.g. phishing site collects credentials)	Cognitive fog or fatigue may reduce ability to detect fake registration pages	Use domain-bound passkeys, clear domain indicators, no password reuse, and simple anti-phishing cues
T - Tampering	Registration data altered in transit	User may not notice subtle changes due to fatigue or attention issues.	Ensure TLS, input validation, server-side integrity checks
R - Repudiation	User denies having registered an account	Memory difficulties may make confirmation unclear	Clear confirmation messages, optional confirmation email with accessible wording
I – Information Disclosure	Personal data exposed during registration	Increased risk if user relies on assistance from others	Minimise data collected, mask inputs, WCAG-compliant forms
D – Denial Of Service	Excessive failed attempts lock out registration	Fatigue may cause repeated errors, triggering lockout	Gentle rate-limiting, adaptive lockout thresholds, accessible error guidance
E – Elevate of Privilege	Attacker gains higher access during registration	User unlikely to detect abnormal behaviour	Server-side role enforcement, no client-side trust

P2 - Login / Authentication

Stride Category	Threat Description	MS-Specific Impact	Mitigation Strategy
S - Spoofing	Phishing steals login credentials or MFA approvals	Cognitive fatigue increases phishing susceptibility	Passkeys, phishing-resistant MFA, consistent login flows
T - Tampering	Login requests or responses modified	Errors may be misinterpreted by user	TLS, message authentication, secure cookies
R - Repudiation	User disputes having logged in	Memory issues may affect recall	Audit logs (D3), session history visible to user
I – Information Disclosure	Error messages leak account existence	May enable targeted scams	Generic error messages, no account enumeration
D – Denial Of Service	Lockouts from repeated failures	Motor or cognitive impairments increase error likelihood	Progressive lockout, alternative auth paths, recovery prompts
E – Elevate of Privilege	Compromised session tokens reused	User may not detect session hijacking	Secure session management, device binding, re-auth on risk

P3 - Account Recovery

Stride Category	Threat Description	MS-Specific Impact	Mitigation Strategy
S - Spoofing	Attacker initiates recovery pretending to be user	Recovery is cognitively demanding	Rate-limit recovery, CAPTCHA-free but behaviour-based checks
T - Tampering	Recovery token modified or replayed	User may struggle with time-sensitive codes	One-time tokens, expiry, server-side validation (D2)
R - Repudiation	User denies requesting recovery	Memory issues may cause confusion	Clear recovery confirmations and summaries
I – Information Disclosure	Recovery reveals account existence	Enables targeted attacks	Uniform recovery responses regardless of account status
D – Denial Of Service	Repeated recovery attempts lock user out.	Fatigue increases failed attempts	Allow multiple accessible recovery methods
E – Elevate of Privilege	Attacker completes recovery and takes over account	User may not detect takeover quickly	Post-recovery alerts, step-up authentication

P4 - Security & Session Management

Stride Category	Threat Description	MS-Specific Impact	Mitigation Strategy
S - Spoofing	Attacker triggers false security alerts	Can confuse or overwhelm users with MS	Clear , concise alerts with consistent wording
T - Tampering	Audit logs altered	Undermines trust and investigation	Write-once logs, integrity protection
R - Repudiation	User disputes lockouts or alerts	Cognitive fog may impair recall	Transparent logs, user-accessible activity history
I – Information Disclosure	Security alerts expose sensitive info	May increase reliance on others for help	Minimal disclosure in alerts
D – Denial Of Service	Over-aggressive security controls lock user outs	Disproportionately affects users with MS	Adaptive risk scoring, human-centred thresholds
E – Elevate of Privilege	Misconfigured sessions grant excessive access	Hard for user to notice	Least-privilege sessions, continuous validation

APPENDIX D – LINDDUN TABLE

LINDDUN Privacy Threat Analysis Table

(Based on Level 1 DFD: Registration, Login, Recovery, Security Management)

Using LINDDUN, I identified privacy risks across registration, login, recovery, and session management. A key finding is that unawareness and detectability risks are amplified for users with MS due to cognitive fatigue, which informed my focus on clear privacy feedback, minimal data collection, and accessible recovery pathways.

P1 - Registration

LINDDUN Category	Privacy Threat	MS-Specific Impact	Mitigation Strategy
L - Linkability	Registration data can be linked across services (e.g. same email reused)	Users with MS may reuse identifiers to reduce cognitive load.	Support passkeys, minimise identifiers, avoid cross-service tracking.
I - Identifiability	Registration uniquely identifies user across systems	Increased risk if user relies on third-party assistance	Collect minimal personal data; pseudonymous identifiers where possible
N - Non-repudiation	Logs permanently tie user to actions they may not recall	Memory impairment may lead to disputes or distress	Allow user-visible activity history with clear timestamps and explanations
D - Detectability	Account existence detectable during registration	Enables targeted phishing campaigns	Uniform responses regardless of account existence
U - Unawareness	User unaware how data will be used or stored	Cognitive fog may reduce comprehension of privacy notices	Short, plain-language explanations; layered privacy notices
N - Non-compliance	Registration flow fails WCAG privacy requirements	Disproportionately affects MS users with cognitive impairments	Align with WCAG 2.2 accessible authentication criteria

P2 - Login / Authentication

LINDDUN Category	Privacy Threat	MS-Specific Impact	Mitigation Strategy
L - Linkability	Login metadata links sessions over time.	Predictable patterns increase profiling risk	Limit session correlation; rotate identifiers
I - Identifiability	Authentication data reveals user identity	Increases risk if devices are shared or assisted	Device-bound credentials; minimal visible identifiers
N - Non-repudiation	Login logs used to assert actions user may not recall	Cognitive fog may impair recall of sessions	Provide accessible session summaries and logout history
D - Detectability	Error messages reveal valid usernames	Supports phishing and account enumeration	Generic login errors; no confirmation of account existence
U - Unawareness	User unaware of tracking or session persistence	Fatigue may limit understanding of session scope	Clear session indicators; explicit logout confirmation
N - Non-compliance	Authentication requires memory or transcription	Violates WCAG 2.2 for cognitive disabilities	Avoid memory-based challenges; support passkeys

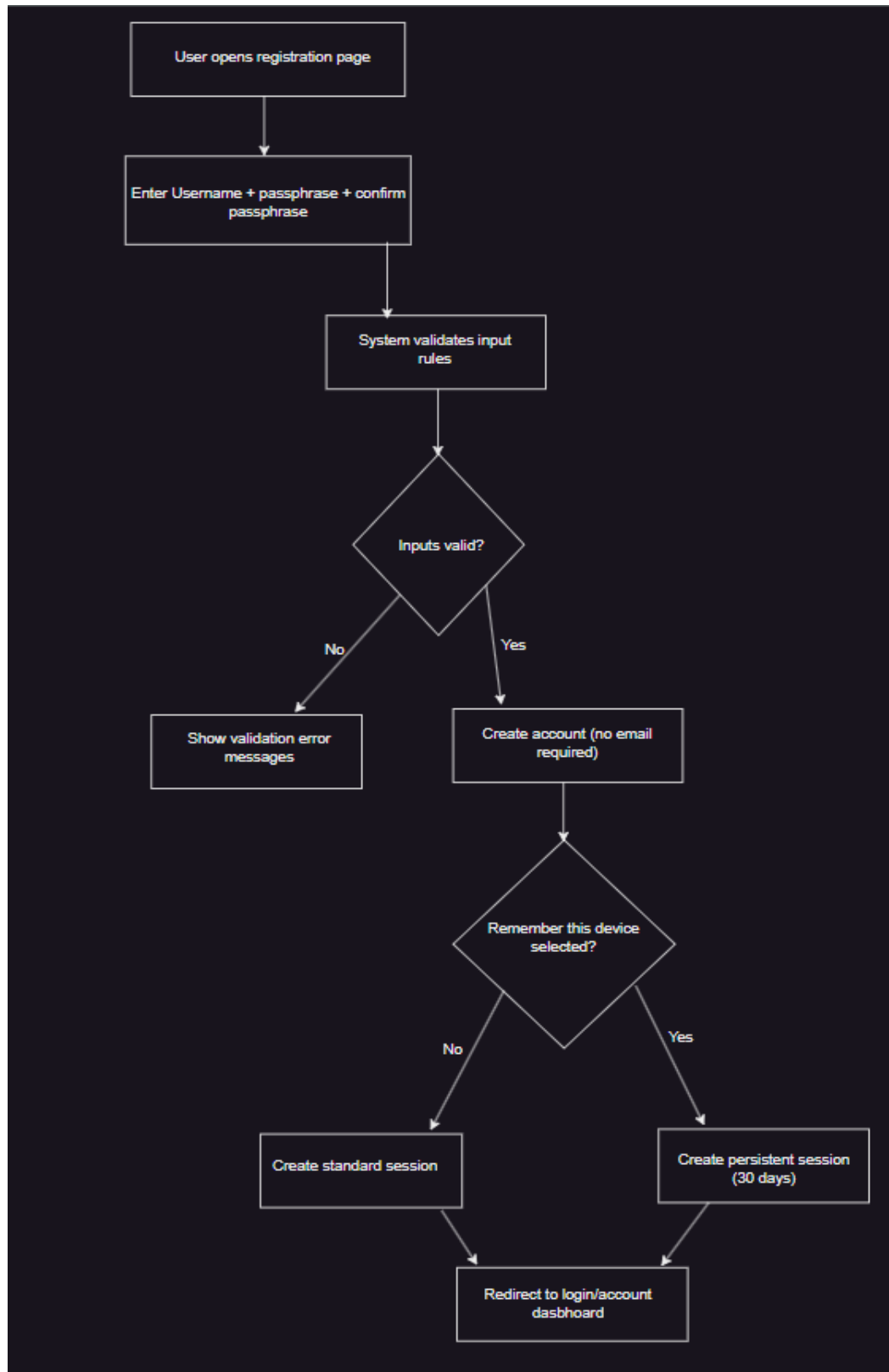
P3 - Account Recovery

LINDDUN Category	Privacy Threat	MS-Specific Impact	Mitigation Strategy
L - Linkability	Recovery requests link user across channels (email/SMS)	Increases exposure during recovery stress	Limit metadata sharing; avoid persistent recovery identifiers
I - Identifiability	Recovery process confirms identity externally	Heightened vulnerability during cognitive fatigue	Use generic recovery messaging; avoid explicit identity confirmation
N - Non-repudiation	Recovery actions permanently logged	User may not remember initiating recovery	Provide clear recovery summaries and confirmation steps
D - Detectability	Recovery flow reveals account existence	Enables targeted attacks	Uniform recovery responses regardless of account status
U - Unawareness	User unaware of how recovery data is stored or reused	Complex flows increase confusion	Step-by-step guidance; plain language explanations
N - Non-compliance	Recovery relies on timed codes or memory	Disproportionately excludes users with MS	Offer multiple accessible recovery pathways

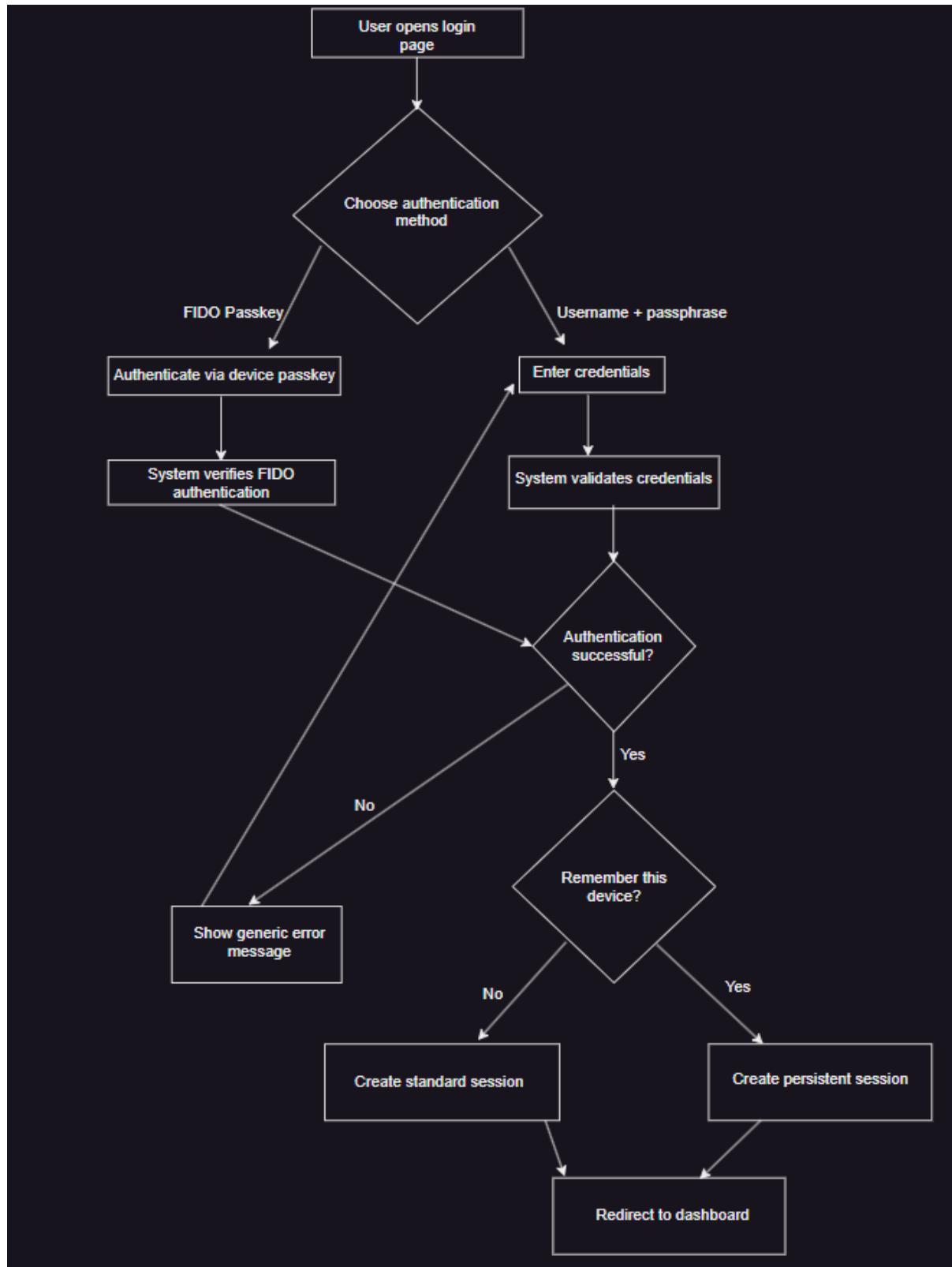
P4 - Security & Session Management

LINDDUN Category	Privacy Threat	MS-Specific Impact	Mitigation Strategy
L - Linkability	Audit logs correlate activity over long periods	Long-term profiling risk	Retention limits; aggregate where possible
I - Identifiability	Security alerts reveal sensitive activity details	May require external help to interpret alerts	Minimal, privacy-preserving alerts
N - Non-repudiation	Logs used to assert responsibility for actions	Memory impairment may cause distress	User-accessible explanations; dispute mechanisms
D - Detectability	Lockouts or alerts reveal user presence	Enables social engineering	Generic notifications without confirmation of identity
U - Unawareness	User unaware of ongoing monitoring	Cognitive load reduces awareness	Clear explanations of security monitoring
N - Non-compliance	Privacy controls inaccessible	Violates inclusive design principles	Ensure WCAG-compliant privacy interactions

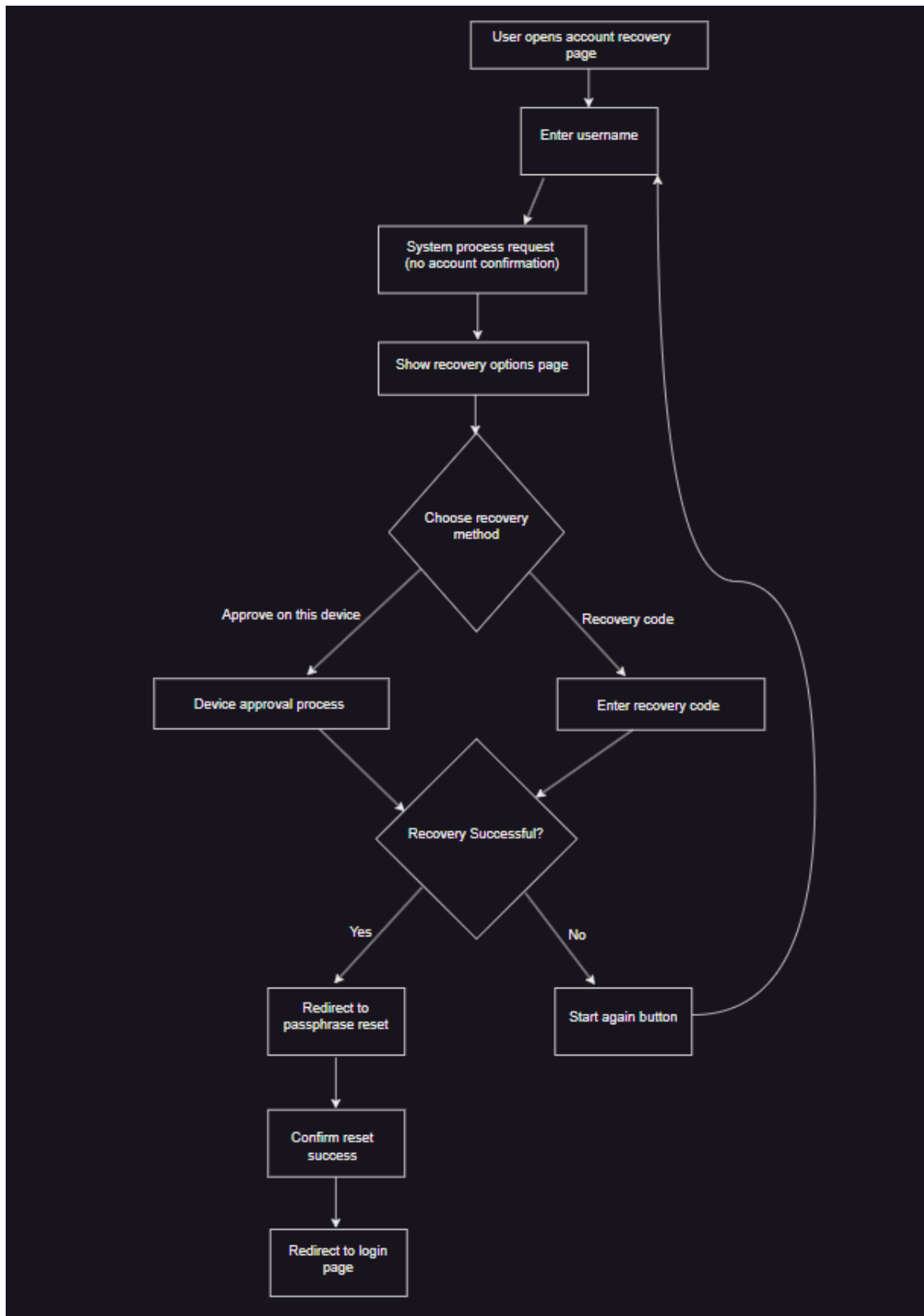
APPENDIX E – REGISTRATION FLOW DIAGRAM



APPENDIX F – AUTHENTICATION (LOGIN) FLOW DIAGRAM



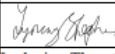
APPENDIX G – ACCOUNT RECOVERY FLOW DIAGRAM



APPENDIX H – PROTOTYPE CODE

All code for the prototype is at this link: <https://github.com/FairestRose/CMP400-Honours-Project-Proposal-and-Execution/tree/main/Inclusive%20Threat%20Modelling>

APPENDIX I – DATA MANAGEMENT SIGN OFF SHEET

 Abertay University		GDPR Data Management Data Sign Off Form	
GDPR Data Management Data Sign Off Form			
For undergraduate or postgraduate student projects supervised by an Abertay staff member.			
This form MUST be included in the student's thesis/dissertation. Note that failure to do this will mean that the student's project cannot be assessed/examined.			
Part 1: Supervisors to Complete			
By signing this form, you are confirming that you have checked and verified your student's data according to the criteria stated below (e.g., raw data, completed questionnaires, superlab/Eprime output, transcriptions etc.)			
Student Name:	Snow White		
Student Number:	2302444		
Lead Supervisor Name:	Dr Lynsay Shepherd		
Lead Supervisor Signature:			
Project title:	Inclusive Threat Modelling: Identifying and Mitigating Cybersecurity Risks Faced by People with Multiple Sclerosis		
Study route:	PhD ☐	MbR ☐	MPhil ☐
	Undergraduate ☒	Postgraduate taught ☐	PhD by Publication ☐
Part 2: Student to Complete			
		Initial here to confirm 'Yes'	
I confirm that I have handed over all manual records from my research project (e.g., consent forms, transcripts) to my supervisor for archiving/storage		SW	
I confirm that I have handed over all digital records from my research project (e.g., recordings, data files) to my supervisor for archiving/storage		SW	
I confirm that I no longer hold any digital records from my research project on any device other than the university network and the only data that I may retain is a copy of an anonymised data file(s) from my research		SW	
I understand that, for undergraduate projects, my supervisor may delete manual/digital records of data if there is no foreseeable use for that data (with the exception of consent forms, which should be retained for 10 years)		SW	
Student signature: Snow White Date:04/05/2026			

