Summary for the Committee

Davide Caria

Transition to Passwordless Technologies
A Comprehensive Analysis and Real-World Implementation

1 Introduction

This thesis, titled ”Transition to Passwordless Technologies: A Comprehensive Analysis and Real-World Implementation”, explores the limitations of traditional password-based authentication systems and supports the move toward passwordless solutions. The topic has been a key area of focus for me over the past academic year, developed through a collaboration with Aruba S.p.A. and further enhanced during my internship at Microsoft. Password-based authentication has been the dominant method for securing digital identities since the early days of computing. Despite their widespread use, passwords have numerous security flaws that make them vulnerable to various cyberattacks, such as phishing, brute force attacks, and credential reuse. The human factor compounds these vulnerabilities; users often choose weak, easily guessable passwords or reuse the same password across multiple platforms, making accounts susceptible to breaches. Passwordless technologies appear to be a promising solution to the ongoing password problem. However, little attention has been paid to the integration of these technologies within existing architectures, which is essential for a successful transition from traditional password-based systems. This thesis examines how organizations can transition from password-based to passwordless authentication and provides a framework to support such a transition.

2 Background and Related Work

From the early days of computing, passwords have evolved from simple keystroke combinations to complex 32-character strings with special characters, numbers, and a mix of upper and lower case letters. Yet, despite these efforts, attackers always seem to find a way in proving that relying solely on usernames and passwords just isn’t enough. To tackle these issues, we’ve developed various technologies and protocols like password strength meters, password managers, and multi-factor authentication. These approaches represent our best shot at solving the problem, except when they don’t. Studies show that, while these technologies help mitigate the issue from a theoretical standpoint, they have little to no effect in the face of a targeted attack. To understand one of the key findings from those researches, consider the following example. Take the password **”DaV_01_IdEItA”**, which might score very high on a standard password strength meter. In a targeted attack, however, most components of this password could be quickly obtained through a simple OSINT (Open-Source Intelligence) exercise. Information like name, date of birth, and nationality, which are often readily accessible, makes this supposedly strong password much easier to guess. Similar findings can be found in the complete version of the thesis. We then move to the introduction of passwordless authentication, exploring modern technologies such as biometrics, cryptographic keys, security tokens, and session property evaluations. These methods are assessed from both a security and technological perspective to understand their strengths and limitations. Passwordless technologies eliminate the need to store or transmit passwords, significantly reducing the risk of exposure to attackers. By leveraging advanced cryptographic techniques and secure hardware, they provide an authentication mechanism that is not only more secure but also more seamless for the end-user, enhancing both usability and security. A straightforward example is biometric login on modern smartphones, where there’s no need to use passwords or PINs; instead, a simple scan of your face or fingerprint is enough to authenticate. However, each passwordless technology has its own set of drawbacks that must be carefully considered. For instance, biometric login aims to strike a balance between false positives (incorrectly granting access) and false negatives (failing to recognize a legitimate user).

3 Method

The first contribution of this work focuses on developing a structured approach for implementing passwordless authentication technologies within existing organizational infrastructures. The aim is to provide a clear, step-by-step framework that guides organizations from traditional password-based systems to the adoption of advanced, secure, and user-friendly passwordless authentication mechanisms. This transition framework is specifically designed to address the challenges of integrating these technologies into complex environments that often involve a mix of legacy infrastructure and modern cloud-based services. The lack of planning can be catastrophic and the following sections are thought to be a blueprint for architects. The framework can be ideally divided into three elements.

Service model for passwordless authentication
The first part of the framework outlines the core architectural requirements for deploying passwordless authentication systems, focusing on three key technologies: security keys combined with biometrics, one-time codes plus biometric authentication, and long-term code systems like magic links or token-based solutions. These categories include most of the technologies needed for implementing passwordless authentication, so by addressing all three, the reader gains a comprehensive understanding of the technologies required for deployment. Each of these architectures is broken down into its essential components that are viewed as LEGO bricks, meaning they can be interchanged to create different architectures to support the desired authentication methods. Two categories are presented:

- **Common Services** - Components that are used in every passwordless authentication design and must be implemented regardless of the chosen method.
- **Characteristic Services** - Bricks that are specific to the selected system and achieve a functionality of a passwordless design.

For example, an ”Authentication Service” is a common element across all designs, while the ”Onboarding Service” is required only for security keys. These ”bricks” are essentially software or hardware modules that can be combined into a unified solution or separated, as they have been described. This modular approach allows for flexibility in design and implementation, similar to how LEGO bricks can be assembled in different configurations to build a cohesive system. An ”Authentication Service” can be developed using a wide range of technologies, with the choice depending on the specific environment in which it is being deployed. Despite the variety of options available, the framework provides a set of recommendations to guide this selection process. One of the significant advantages of this modular approach is that it provides flexibility in deployment, enabling a phased implementation that aligns with an organization’s current capabilities. For instance, a company might initially deploy one-time codes, to then move to security key by selectively replacing the ”Characteristic Services” and leveraging the existing ”Common Services”.

Architecture assessment
Once the technology base is extensively discussed, the framework shifts to a broader perspective by introducing the concept of ”Passwordless Fit”. Transitioning to passwordless authentication requires identifying the appropriate target authentication method, as the wide variety of passwordless technologies demands a completely different design phase for each. Assessing how well the current architecture fits a particular authentication method can assist in selecting the right target. The first step in this assessment involves answering a set of questions specifically designed to evaluate passwordless technologies. After reviewing the current architecture, it becomes easier to choose a target and plan to achieve it. For example, an organization might choose token-based authentication over security keys due to lower costs after evaluating its current setup. Once the current state is accurately assessed, the decision becomes a matter of considering parameters such as costs, workforce overhead, compliance, and other factors. To guide this decision-making process, a set of flowcharts has been developed using these parameters as key discriminants.

Strategy for the transition
The final element of the framework offers a broader strategy for implementing the transition to passwordless authentication. It outlines four key steps: Deploy, Restrict, Shift, and Remove. Each step is discussed in detail, explaining how organizations should integrate passwordless technologies into their systems, starting from the initial deployment and progressing to the removal of the last password within the system.

4 Proof of Concept

The second contribution focuses on showcasing the practical application of the described framework in a real-life scenario. This PoC was requested by a Microsoft client, referred to as **”GripGotham”** for privacy reasons, and it demonstrates the theoretical analysis in action. The client’s initial goal was clear: to transition a manufacturing line in southern Spain to passwordless authentication.

Context and Target definition
It is important to highlight that the need for a new type of authentication stems from practical challenges. Workers are not primarily focused on security and often write down their long passwords on sticky notes that they leave around their devices. Moreover, they have no company phone and thus cannot configure MFA for their login. This setup is far from ideal, and in addition, once their tasks are completed, workers leave the devices with active sessions, compromising privacy. Furthermore, each login takes about three minutes, as users have to type the lengthy password multiple times. This led to the creation of a set of Functional and Non-Functional requirements, further divided into ”Security” and ”Business” requirements. With these requirements and the broader context in mind, the current state of the manufacturing line’s infrastructure has been analyzed. Security Keys, specifically the FIDO2-compliant YubiKey, have been chosen as a target. It is clear that the requirements go beyond the simple implementation of passwordless authentication, therefore, the final solution will include multiple components to achieve them. To facilitate testing and trials, a test environment has been set up to replicate GripGotham’s cloud infrastructure. It is worth mentioning that GripGotham had previously failed to integrate security keys. Specifically, deploying security keys in such a corporate environment requires more than just plug-and-play. The enrollment has to happen at the Active Directory level and the first login requires MFA to be verified. However, as mentioned before, MFA cannot be set up and the hybrid nature of the infrastructure makes it difficult to enroll the FIDO2 Keys.

Implementation phase
Moving into the implementation details, the proposed solution comprises four components designed to meet the established requirements: User Transition Manager (**UTM**), Device Transition Manager (**DTM**), SIEM Integration, Reporting Dashboard. The first two components form the core of the solution and are responsible for the passwordless deployment. These components allow to onboard the keys in the hybrid active directory and substitute the need of a phone for MFA. The last two components focus on the business requirements and manage the data lake needed to track each user’s transition, gathering metrics such as the time to onboard a security key and the duration of the first passwordless login. This data is crucial for creating dashboards and setting up alerts to detect misuse or attacks during the transition process. Finally, a set of tests were conducted to validate the Proof of Concept against the original requirements, ensuring that the solution meets the established goals.

Results
The Proof of Concept (PoC) was successfully implemented on GripGotham’s side and deployed into the production environment of their manufacturing line. This deployment led to the achievement of the initial requirements, particularly those focused on enhancing the login procedure with passwordless authentication. The transition to a passwordless system was accomplished with minimal changes to the existing architecture and keeping the cost within the current Azure tier plan. Finally, the login time has been cut by 90%, an impressive result considering the initial 50% stated in the requirements.

5 Conclusions

Passwordless authentication is an emerging topic with significant potential to transform the security landscape in the identity space. However, little effort has been made to describe the architectures necessary for a passwordless transition. This work aims to serve as both a theoretical and practical handbook for security professionals interested in exploring the details of this transition. This thesis illustrates that a lack of planning can lead to a complete compromise in integrating this technology. The objective has been to contribute with a theoretical framework for security professionals, along with its application to a real-life scenario that has enabled an organization to transition to passwordless technology. Furthermore, the content of this work is currently being further developed to enhance the framework and create additional use cases.