**Secure Boot Authentication: Implementing a QR-Based Access Control System for Computer Startup**

Mac Hideyoshi P. Asoi ¹, Ceejay C. Imperial ², Jamier Ivan Madrid ³, Paul Gerald T. Sebastian ⁴

¹Information Technology

²College of Computer Studies

³Research Development and Innovation Center

⁴Our Lady of Fatima University

⁵Research Adviser

September 2024

1. Introduction

In a time when cyberattacks are becoming more common, safeguarding computer networks against illegal access is essential. Conventional security methods concentrate on protecting the system's functions and data after it has been initiated. To guarantee that unauthorized users cannot even turn on the computer without the appropriate authentication, a new strategy is required.

This thesis introduces a novel approach to limiting computer access—the use of a QR-based authentication system that needs to be finished before the machine turns on. Under this technique, the computer doesn't do anything until a legitimate QR code—which is associated with specific authorized users—is scanned and confirmed. The PC won't finish starting up unless authentication is successful. By guaranteeing that only authorized users can even start the computer's power-on procedure, this technique addresses the growing requirement for reliable pre-boot authentication procedures and provides a crucial layer of security.

2.0 Background of the Study

Before the operating system loads, conventional computer startup procedures lack safeguards against unwanted physical access. Because of this gap, there is a security risk that unauthorized individuals could access or tamper with the system before it powers up. To solve this problem, pre-boot authentication requires user verification prior to the system booting up completely. The efficient encoding and transmission of data provided by QR codes makes this kind of authentication workable. Using QR code-based access control, the computer is turned off until a legitimate QR code is shown and validated. By guaranteeing that the power-on sequence can only be started by authorized users, this technique improves security right away when the computer is turned on. This study looks on how well QR codes are implemented when preventing unauthorized access to computer devices.

3.0 Statement of the problem

It is essential to always protect computer systems from unwanted access in the modern digital environment. Conventional security methods, such as Secure Boot, do not address the risk of unauthorised access prior to the operating system loading; instead, they concentrate on safeguarding the system once it has started. Because of this, there is a chance that someone not authorised might access or alter the system before it ever boots up. A way that keeps the computer from turning on until it has been verified by an authorised user is required. By investigating a QR code-based pre-boot authentication system that makes sure only authorised users can start the computer's power-on procedure, this thesis seeks to close this gap and improve system security in general.

3.1 Main Problem

The absence of pre-boot authentication techniques, which stop unwanted access to a computer before it fully boots up, is the key issue this study attempts to address. Conventional startup procedures provide a serious security risk by enabling the machine to turn on and possibly being accessed or altered by unauthorised users. The problem is coming up with a way to mitigate the hazards of unauthorised physical access by requiring user authentication before the computer will even start up.

3.2 Specific Problem

Authentication Mechanism: To guarantee that only authorised users are able to turn on the computer, how can a QR code-based authentication system be incorporated and developed effectively?

System Integration: To prevent unauthorised power-ons, what are the technological concerns and problems involved in integrating QR code-based authentication with the hardware and startup procedure of the computer?

User Experience: What is the expected impact on convenience and efficiency of implementing a pre-boot authentication system based on QR codes, and how may these elements be optimised?

4.0 Objective of the Study

The objective of this study is to design, develop, and evaluate a QR code-based pre-boot authentication system that prevents unauthorized access by ensuring that only users with valid QR codes can power on the computer. The study aims to enhance computer security by integrating an additional layer of user-specific authentication into the startup process, thereby addressing vulnerabilities associated with traditional pre-boot security measures.

4.1 General Objective

The general objective of this study is to enhance computer security by implementing a QR code-based pre-boot authentication system that requires users to authenticate via a QR code before the computer will power on. This approach aims to prevent unauthorized access and ensure that only authenticated individuals can initiate the computer's startup process.

4.2 Specific Objective

Design and Implementation: To design and implement a QR code-based authentication system that integrates with the computer’s hardware and startup process, ensuring that only authorized users can power on the system.

Security Evaluation: To evaluate the effectiveness of the QR code-based authentication system in preventing unauthorized access and assess its impact on overall system security compared to traditional pre-boot security measures.

User Experience Assessment: To analyze the impact of the QR code-based authentication system on user experience, including ease of use and convenience, and identify any potential challenges or areas for improvement.

5.0 Scope and Limitation

This study focuses on developing and evaluating a QR code-based pre-boot authentication system designed to prevent unauthorized users from powering on a computer. The scope includes the design and integration of the QR code authentication system with the computer's hardware and firmware, ensuring that only authorized individuals with valid QR codes can initiate the power-on sequence. The study will cover the technical implementation, security assessment, and user experience aspects of the QR code-based system within a controlled environment.

Limitation:

Hardware Compatibility: The implementation and effectiveness of the QR code-based authentication system may be limited by the compatibility of the system with various computer hardware configurations and firmware setups. The study may not cover all possible hardware variations.

Security Testing Scope: The security evaluation will be conducted in a controlled environment, which may not fully replicate real-world scenarios. The study may not address all potential attack vectors or advanced persistent threats.

User Experience Variability: The user experience assessment will be based on a limited sample of users and may not account for all possible user scenarios or preferences. Variations in user interaction and hardware setup could impact the findings.

6.0 Significance of the study

The significance of this study lies in its potential to advance computer security by introducing a novel approach to pre-boot authentication. By requiring users to authenticate via a QR code before the computer will power on, the proposed system aims to significantly enhance security measures against unauthorized physical access. This approach addresses a critical gap in traditional security protocols, offering a more robust solution for protecting sensitive systems from being tampered with or accessed by unauthorized individuals.

The study's findings could have broad implications for both individual users and organizations, particularly those with high-security requirements. Improved pre-boot authentication can contribute to overall system integrity and data protection, reducing the risk of unauthorized access and potential security breaches. Additionally, the research provides insights into the practical integration of QR code technology into security systems, which may inform future innovations and developments in the field of cybersecurity.