**EMERGING TECH CONFERENCE – Edge Intelligence**

Volume 02, 2023, Page 125 – 130

**Proceedings of Emerging Tech Conference:**
**Edge Intelligence 2023**

# Analysis of SQRL: A Comparative Study with Traditional Authentication Mechanisms

Department of Informatics-University of Economics - Varna,9002 Varna, 77
Kniaz Boris I, Blvd. Bulgaria

## Abstract

This paper presents a comprehensive analysis of the Secure Quick Reliable Login (SQRL) authentication system, comparing its strengths and weaknesses with traditional authentication methods. SQRL is a modern approach designed to address the inherent security and usability issues associated with traditional username/password-based authentication. We delve into SQRL's security features, usability, and its potential to replace conventional authentication methods. The analysis highlights the challenges and advantages SQRL brings to the authentication landscape, emphasizing its suitability for various scenarios.

## 1 Introduction

Authentication is a fundamental element of digital security, serving as the primary method for individuals to access online services. Historically, traditional username/password authentication has been the default approach for this purpose. However, this conventional method comes with inherent vulnerabilities that have increasingly made it a target for cyberattacks.

One of the most pressing issues with traditional authentication is the widespread problem of password reuse. Users tend to employ the same passwords across multiple services, creating a significant security risk. In the event of a data breach on one platform, malicious actors can potentially gain access to a user's accounts on various other services, compounding the damage.

Additionally, traditional password-based systems are plagued by weak password choices. Many users opt for easily guessable passwords or fail to update them regularly, leaving their accounts vulnerable to brute-force attacks. Furthermore, the rise of sophisticated phishing attacks has made it even more challenging to protect login credentials.

**Secure** Quick Reliable Login (SQRL) represents a promising alternative to traditional authentication methods. It aims to address the weaknesses of conventional systems while prioritizing both security and user-friendliness. SQRL offers several notable advantages:

**Security**: SQRL employs advanced cryptographic techniques, making it highly resistant to interception and unauthorized access. By eliminating the need for passwords, it mitigates the risks associated with password reuse and weak passwords.

**Reliability**: SQRL is designed to be highly reliable, with mechanisms in place for account recovery and protection in case of device theft or loss.

**Ease of Use**: SQRL provides a user-friendly experience by enabling login through a simple QR code scan. This eliminates the need for users to remember and type complex passwords.

**Integration**: While SQRL represents a departure from traditional authentication, it has the potential for seamless integration into various online services, offering a more secure authentication method.

However, SQRL is not without its own set of challenges and limitations. It relies on additional applications for secure key storage and lacks inherent protection against DNS spoofing. Compatibility issues may arise on devices with limited resources, and its widespread adoption depends on service providers incorporating SQRL into their platforms.

In conclusion, SQRL presents a compelling alternative to traditional username/password authentication. By addressing the vulnerabilities of traditional methods while prioritizing security and user-friendliness, SQRL has the potential to enhance the overall landscape of digital authentication. However, its successful integration and adoption will require collaboration between technology providers, service operators, and end-users to ensure a more secure and reliable online experience.

## 2 SQRL vs. Passwords

Traditional passwords present numerous challenges, including the need for users to remember multiple complex passwords and the risk of password reuse. SQRL offers several advantages in this context:

### Strengths

**Security**: SQRL adopts Trust No One (TNO) principles and proven cryptographic techniques, making it resilient against interception.

**Phishing Prevention**: SQRL's unique identity creation for each web domain makes it challenging for phishing attacks to succeed.

**Usability**: SQRL simplifies account creation, eliminating the need for email addresses and complex passwords.

## 3 SQRL vs. Password Managers

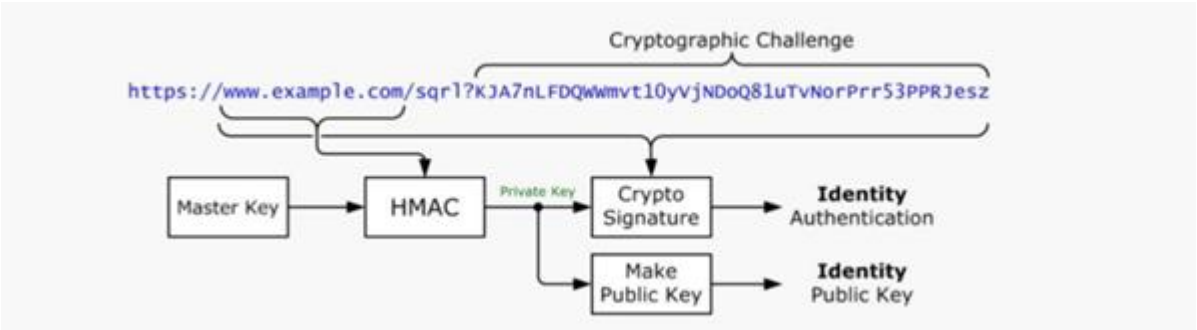
Password managers provide a centralized repository for passwords and offer some similarities to SQRL:

### Strengths:

**Security**: Both SQRL and password managers prioritize security and encryption.

**Reliability**: Password managers offer reliable access to stored credentials. SQRL is exactly where every user needs it. If stopped working or damaged, rescue can be usedcode to restore the SQRL ID.

- ✓ in case of theft of the device, the SQRL ID of the user, it is protected cryptographically, making it almost impossible to used by third parties.
- ✓ It is possible to replace SQRL ID in order to the potential attacker is excluded from the various accounts of the user.
- ✓ There is the possibility to transfer SQRL ID when changing the user's device to ensure its continuity interoperability.




### Weaknesses:

**Usability on Untrusted Devices**: Password managers may expose passwords when used on untrusted devices, unlike SQRL's QR code scanning.

**Phishing Vulnerability**: Like traditional passwords, password managers are susceptible to phishing attacks.

**Dependency on Passwords**: Password managers rely on passwords to function, hindering the goal of password-free authentication.

## 4 SQRL vs. Client Certificates

Client certificates offer an alternative to passwords but come with their own set of challenges:

### Strengths:

Security: Client certificates can provide strong security when properly implemented.

### Weaknesses:

**Usability**: Client certificates can be complex to set up and transfer between devices.

**Dependency on Certification Authorities**: Trust in third-party Certification Authorities (CAs) is required for client certificates.

**Phishing Vulnerability:** Similar to passwords, client certificates can be vulnerable to phishing on untrusted devices.

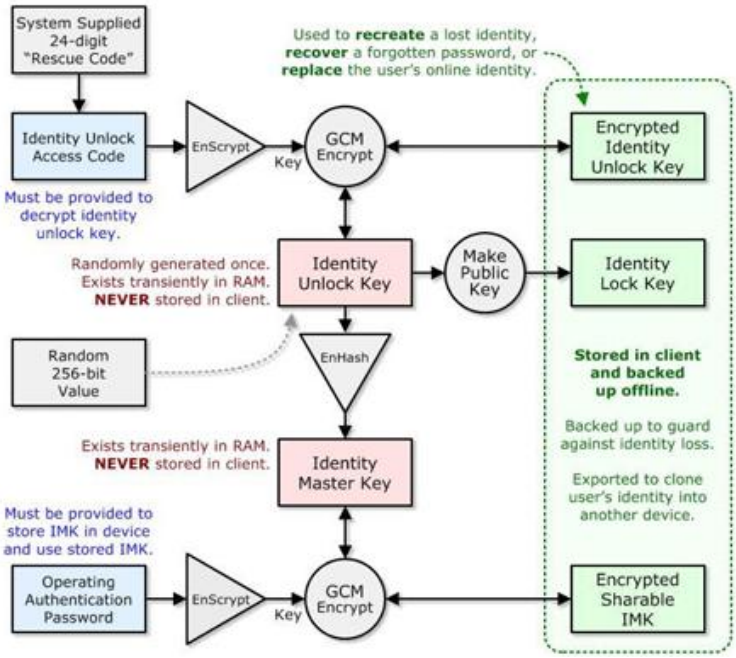
**No Email Addresses:** SQRL's anonymity feature eliminates the need for email addresses, enhancing privacy.

**Phishing Prevention:** SQRL's identity creation based on domain names helps prevent phishing attacks. Although the SQRL identity connection system is not promoted as a solution against phishing but as it turns out, the control architecture SQRL identity presents significant opportunities to prevent such kind of attacks.

When using SQRL, users do not recognize and authenticate themselves with a username and password. On the other hand, their unique identity comes from the Secret Master Key and the site's full domain name. Given that SQRL creates a unique user identity for each web domain, the identity of the user for a phishing site such as ebbay.com or ebay.cn or anything other than the original site

that the user he thinks visiting would be useless to any intruder.

This means that the SQRL connection link provided by a website that is malicious, must be correct and authentic. In our example it should be. "ebay.com" is why this string domain name is used in the creation of the identity by which ebay.com knows the user. This means that the SQRL application of the user will connect directly to the original website and not to the fake phishing website.




**Effectiveness:** SQRL's time-consuming account creation deters attackers.

**Ease of Learning:** SQRL simplifies the authentication process, enhancing usability.

**Reliability and Recovery:** SQRL offers reliable authentication and the ability to recover from identity theft.

**Integration Potential:** SQRL's potential to replace passwords entirely benefits websites and users.

## 5 Limitations and Challenges of SQRL Authentication

Secure Quick Reliable Login (SQRL) is a robust authentication method, but it has its share of limitations and challenges that must be considered for a complete evaluation.

### Dependency on Additional Applications

One notable limitation of SQRL is its reliance on additional applications, especially for securely storing the Master Key. Although SQRL emphasizes security, it necessitates users to store their Master Key on a device, typically a smartphone. However, this dependency can be problematic on devices with limited RAM or storage capacity. Storing cryptographic keys demands memory resources, and older or budget smartphones may not meet these requirements. Consequently, SQRL's effectiveness may be constrained by the user's choice of hardware, potentially excluding those with less advanced devices from adopting this authentication method.

### Vulnerability to DNS Spoofing

SQRL faces a critical challenge related to its susceptibility to DNS spoofing. DNS spoofing involves manipulating the Domain Name System (DNS) to redirect users to fraudulent websites. SQRL, in its basic form, lacks inherent mechanisms to detect DNS spoofing, making it susceptible to such attacks. If a user unknowingly accesses a spoofed website, their SQRL authentication could be compromised, leading to unauthorized access to their accounts. This vulnerability underscores the importance of implementing additional security measures, such as secure DNS protocols, alongside SQRL to mitigate the risks associated with DNS spoofing.

### Device Compatibility and Resource Limitations

SQRL's effectiveness is contingent on the user's choice of devices. While modern smartphones are well-equipped to handle the cryptographic demands of SQRL, older or less powerful devices may struggle due to limited RAM and storage. This can create a barrier to entry for users who do not possess the latest hardware, potentially limiting the widespread adoption of SQRL.

### Lack of Built-in DNS Protection

SQRL, as a standalone authentication method, does not offer built-in protection against DNS spoofing. Users and service providers must take additional steps, such as implementing secure DNS protocols, to safeguard against this type of attack. This places the onus on both parties to ensure the security of the authentication process.

In conclusion, SQRL presents a compelling alternative to traditional authentication methods, prioritizing security and user privacy. However, its limitations, including dependence on additional applications, vulnerability to DNS spoofing, and compatibility issues with resource constrained devices, should be carefully considered. To maximize its effectiveness, users and service providers must implement additional security measures and address these challenges proactively. As technology evolves, addressing these limitations will be crucial for SQRL's continued success in the authentication landscape.

## 6 Conclusion

During this work, SQRL technology was analyzed in order to see whether it can replace traditional SFA and 2FA Identity Methods.

It was found that SQRL technology is a technology for secure authentication over the internet, using modern devices such as Smartphones. It provides several advantages over traditional means of authentication. The analysis shows that the main vulnerability is mainly caused by the way of Use and the errors of the user, commonly the human factor.

Currently there is not a plethora of SQRL implementations and its integration in several applications. Due to this, the impact of application errors cannot be determined. However, history shows that many points of vulnerability come from the field of authentication. Security checks must be performed on both applications and server applications. Devices infected with malware used for authentication enable identity theft. Practice shows that malware is persistent. This justifies the need for as safe an environment as possible. The proposed solutions are a never-ending process. SQRL supports identity recovery with Rescue Code in case the user's identity has been exposed or stolen. Current technology does not have an automated "lock" and "change of identity" process, and the processes must be performed by users

themselves on all websites they visit.

## 7 References

[1] SQRL Translations. CrowdIn.com. [Accessed: September 30, 2023] [URL: https://www.crowdin.com/project/sqrl]

[2] Gibson, Steve. "Secure Quick Reliable Login: A highly secure, comprehensive, easy-to use replacement for usernames, passwords, reminders, one-time-code authenticators... and everything else." GRC.com. Gibson Research Corporation. [Accessed: March 7, 2021] [URL: https://www.grc.com/sqrl/sqrl.htm]

[3] Gibson, Steve. "SQRL Q&A #176 (Transcript)." Security Now!. Gibson Research Corporation. [Accessed: October 16, 2013] [URL: https://www.grc.com/sn/sn-176.htm]

[4] Babioch, Karol. "Security Analysis and Implementation of the SQRL Authentication Scheme (BSc)." IT Security, Department of Informatics, Technical University of Munich. [Accessed: March 18, 2015]

[5] Gibson, Steve. "How SQRL Can Thwart Phishing Attacks." GRC.com. Gibson Research Corporation. [Accessed: March 7, 2021] [URL: https://www.grc.com/sqrl/phishing.htm]

[6] "Secure QR Login." Drupal.org. https://www.drupal.org/project/sqrl] [Accessed: December 2022] [URL:

[7] Persson, Daniël. "SQRL Login – WordPress plugin." WordPress.org. [Accessed: November 2019] [URL: https://www.bestpractices.dev/pt-BR/projects/3269]

[8] Sylvester, Paul. "SQRL implementations on Android and it works!" Paul's Tech Talk. [Accessed: December 2014] [URL: "SQRL implementations on Android and it works!"]

[9] Lambert, Patrick. "SQRL: A new method of authentication with QR codes." Tech Republic. [Accessed: 2013] [URL: "SQRL: A new method of authentication with QR codes"]

[10] Holmlund, Daniel. "Authentication Without Passwords Implementing SQRL." 2014 HTML5 Developer Developer Conference. Silicon Valley International Game Developers Association. [Accessed: January 3, 2014] [URL: Authentication Without Passwords Implementing SQRL]