SmallSEOTools

# PLAGIARISM SCAN REPORT

| | | | |
|---|---|---|---|
| Words | 715 | Date | April 26,2021 |
| Characters | 4727 | Excluded URL | |

| 0% | 100% | 0 | 33 |
|---|---|---|---|
| Plagiarism | Unique | Plagiarized Sentences | Unique Sentences |

## Content Checked For Plagiarism

Passwords have been used by humans since ancient times to ensure secrecy. With the introduction of the Internet, these passwords naturally transitioned to the web, and are used to authenticate users across applications. However, multiple accounts across various applications means maintaining these passwords is a tedious task. Many use the same password across applications, leaving them vulnerable to data breaches through attacks such as phishing, brute force attacks, or use of keyloggers. Thus, there is need for stronger, user-friendly authentication which accurately verifies the user's identity and eliminates the risk of compromised credentials. Certificate-based authentication is the solution.

Certificate Based Authentication

Security researchers Ron Rivest, Adi Shamir, and Leonard Adelman came up with the RSA cryptosystem in 1977, named after its developers. RSA is an asymmetric cryptography algorithm which calculates a key pair using some mathematical computation, and then splits it into two pieces: the private key and the public key. After generating a key pair, the private key holder shares the public key; the public key can then be used to encode secret messages that only the private key holder can decrypt. The reverse is also true, i.e., one can encrypt a message with the private key that can only be decrypted by the corresponding public key. Both keys encrypt to different hashes, but one key can decrypt the other's encryption. Even if a third party decrypts a message using the public key, they cannot change the content of the message because they don't have access to the private key. In other words, the message is digitally signed, as it would be in the real world.

In certificate-based authentication, digital certificates (an electronic document which is used to prove ownership of a public key) and signatures are used to confirm the identity of a user or device before being given access to a resource. This is the basis of Public Key Infrastructure (PKI), and this form of authentication is called certificate-based authentication. This is a password-less authentication method. Certificates are themselves encrypted and can only be decrypted with the private key pair (which is never shared), so even if the user accidentally authenticates a rogue network, the data that is sent is worthless to the attacker.

Moving to Authenticators using WebAuthn

The FIDO Alliance, a collection of companies supporting secure and usable authentication, and W3C, the World Wide Web Consortium, together make it possible to move from passwords to more secure modern authentication. W3C has published specifications for browsers as a formal W3C recommendation called the WebAuthn protocol. FIDO has published specifications for everything else as the Client to Authenticator Protocol (CTAP). These two protocols together enable the password-less user experience.

To use the WebAuthn protocol, a user must have a client and an authenticator. Clients are browsers or mobile applications. An authenticator is a device that performs the cryptographic operations necessary to implement the WebAuthn protocol. Two core actions performed with an authenticator are registration and authentication. The user experience can then be tailored to each person's unique preferences and constraints, while maintaining a level of security exceeding that which passwords can offer. Some users may prefer a PIN, while others may choose a biometric authenticator. Because users can re-use the same phone and same second factor across all relying parties, this technique is more scalable as compared to passwords.

However, each time a user upgrades a device, for each relying party where they have registered an old authenticator, the user will need to log in, delete the old authenticator and register a new one manually. Additionally, if they lose their registered device, then the WebAuthn scheme makes it difficult to recover account access. The solution to this is the

Pre-emptively Synced Keys (PSK) Protocol, which uses a backup device.

Conclusion

User certificates allow for the separation of roles unlike passwords, yet, they are still not very common due to lack of convenience. Use of certificate-based authentication is not exactly effortless, since it requires certain technical capability to configure and manage it. To overcome the pitfall of passwords, multi-factor authentication (MFA) is being deployed by many companies, requires two or more verification factors to grant access. As MFA does the job, companies don't feel the need to upgrade to certificate-based authentication, but only time will tell whether or not that remains the case.

| Sources | Similarity |
| --- | --- |