Introduction to Passkeys

Irv Salzberg

June 2024

DEFINITIONS

AUTHENTICATION: (authentic: of undisputed origin **)** Refers to the process of proving that some fact or some document is genuine. In computer science, this term is typically associated with proving a user's identity.

PHISHING : Single most common form of cyber crime (90% of Cyber-Attacks Begin with Phishing?). A form of cyber attack where attackers impersonate legitimate entities, such as banks, companies, or government agencies, in order to deceive individuals into divulging sensitive information such as usernames, passwords, credit card details, or other personal information. This is typically done through email, messaging platforms, or fraudulent websites that mimic the appearance of trusted sources. The goal of phishing is to trick users into providing their confidential information, which can then be used for various malicious purposes, including identity theft, financial fraud, or unauthorized access to accounts.

SYMMETRIC ENCRYPTION: Uses a single secret key (name/password) to encrypt and decrypt data. Client & vendor have the same key

ASYMMETRIC ENCRYPTION: Uses a pair of keys – a public key and a private key – to encrypt and decrypt data.. Vendor only has the public key.

RSA: A public-key cryptosystem, one of the oldest widely used for secure data transmission. The phrase "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977.

FIDO (Fast Identity Online): A nonprofit alliance that seeks to standardize authentication at the client and protocol layers.

MFA (Multi-Factor Authentication): Something you know, Something you have, Something you are.

Password: A word, phrase, or string of characters intended to differentiate an authorized user or process from an unauthorized user, .A password is used for authentication, identification, authorization, access control and encryption.

PASSKEY: A new cross-platform FIDO standard for replacing both passwords, and 2FA/MFA authenticators with something more convenient and secure using a asymmetric encryption digital credential, tied to a user account and a website or application without having to enter a username or password.

PASSKEYS

Passkeys are kept on a user's devices (something the user "has") and — if the Relying Party requests User Verification — can only be exercised by the user with a biometric or PIN (something the user "is" or "knows"). Thus, authentication with passkeys embodies the core principle of multi-factor security.

SAMPLE PRIVATE RSA KEY & ASSOCIATED PUBLIC KEY

```
512-bit key-----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4WGeKLs1Pt8Qu
KUpRKfFLfRYC9AIKjbJTWit+CqvjWYzvQwECAwEAAQJAIJLixBy2qpFoS4DSmoEm
o3qGy0t6z09AIJtH+5OeRV1be+N4cDYJKffGzDa88vQENZiRm0GRq6a+HPGQMd2k
TQIhAKMSvzIBnni7ot/OSie2TmJLY4SwTQAevXysE2RbFDYdAiEBCUEaRQnMnbp7
9mxDXDf6AU0cN/RPBjb9qSHDcWZHGzUCIG2Es59z8ugGrDY+pxLQnwfotadxd+Uy
v/Ow5T0q5gIJAiEAyS4RaI9YG8EWx/2w0T67ZUVAw8eOMB6BIUg0Xcu+3okCIBOs
/5OiPgoTdSy7bcF9IGpSE8ZgGKzgYQVZeN97YE00
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN RSA PUBLIC KEY-----
MEgCQQCo9+BpMRYQ/dL3DS2CyJxRF+j6ctbT3/Qp84+KeFhnii7NT7fELilKUSnx
S30WAvQCCo2yU1orfgqr41mM70MBAgMBAAE=
-----END RSA PUBLIC KEY-----
```

VIDEO PRESENTATION

1.mp4 https://www.youtube.com/watch?v=FTweNDAc9Fs

2.mp4 https://youtu.be/6lBixL_qpro

PASSKEY SUPPORT

WEBSITES

Adobe
Amazon
Apple
Bitwarden
Coinbase
Discourse
GitHub
Google
Hancock.ink
Instacard
KAYAK
LinkedIn
Microsoft
Nintendo
Nvidia
PayPal
Playstation (Sony Account)
Robinhood
Roblox
Shopify
Stripe Checkout (Link)
Tailscale
TikTok (iOS)
Uber
Vercel
WhatsApp
X (Twitter)

APPS

KeePass XC
1Password
Bitwarden
Dashlane
Chrome (Google Password Mng)
Firefox
Brave
Windows “Hello” (TPM chip)

HARDWARE

Yubico Security Key

HMM – POSSIBLE ISSUES

- Vendor lock: a unique passkey is require for each web site,
- Passkey storage: Difficulty in direct access and control,
- Vendor implementation cost,
- Passkey compatibility is limited to modern devices with the latest operating systems: Trusted Platform Module (TPM),
- Most websites and apps do not support passkeys,
- Losing access to a device is a significant vulnerability, access security is the responsibility of the client and not the user.,
- Access private keys.

In Summary: Passkeys offer a significant improvement over passwords particularly in eliminating phishing attacks, but current problems exist with compatibility, storage and in the way they are being implemented today. The security responsibility for securely logging on to a site is now the user.