The Evolution of Internet Security

Authentication Technology Mechanics

St. Louis Linux Users Group

17 July 2025

Lee Lammert

Password vaults, authentication tools, and underlying tech

- Evolution and State of Password Vaults and Authentication Tools
- From early tools like KeePass to Bitwarden, authenticators, and hardware keys

---

Password reuse, phishing, and breaches

- Password reuse
- Phishing
- Breaches
- Human limitations on memorization
- Why a sticky note CAN be a good password vault!

Security 🔐 model

- Security 🔐 model

- Usability
- Sync & accessibility
- Open source vs closed source

Historical Timeline

Early Password Vaults (2003–2010)

- **KeePass** (2003): Open-source, local-only
- Plugin-based extensibility, portable DB format
- No cloud dependency, manual sync
- **KeePassX**, **KeePassXC**: Linux forks, Qt-based
- Limited UI/UX, but still actively used by privacy-focused

Cloud-Driven Vaults Emerge (2006–2012)

- **1Password** (2006): Mac-focused initially, later cross-platform
- Local vaults with sync via iCloud/Dropbox
- Later versions (1Password 8) became cloud-first
- **LastPass** (2008): Browser-based vaults
- First major cloud-based password manager
- 2015 & 2022 breaches exposed vault metadata/blobs

Password Manager Boom (2012–2018)

- **Dashlane** (2012): Cloud-first, business features
- Focused on autofill, cross-platform usability
- Subscription model, closed-source
- Business-focused UI, deprecated standalone apps

Modern Open Source Vaults (2016–present)

- **Bitwarden** (2016): Open source, cross-platform
- Self-host or cloud-hosted
- Zero-knowledge encryption, public audits
- Free usable tier, polished UI
- **Vaultwarden**: Lightweight Rust fork, self-hosting
- **Passbolt**, **Padloc**, **LessPass**: Alt models
  - Passbolt: GPG-based, team focus
  - LessPass: Stateless, no vaults
  - Padloc: Cloud sync + open source

Hardware Authentication

Rise of Hardware Authenticators (2008–present)

- **2008**: Yubico introduces the first **YubiKey**
- One-time password (OTP) generator via USB
- No drivers needed — emulates a keyboard

Evolving Protocols (2014–2018)

- **2014**: Launch of **U2F** (Universal 2nd Factor) — FIDO Alliance + Google
- **2018**: **FIDO2/WebAuthn** released: Passwordless standard
- Backed by Google, Microsoft, Apple, Yubico
- Challenge-response using asymmetric cryptography

Hardware Token Families

- **YubiKey**: Models like Nano, 5C, 5 NFC, Bio
  - USB-A, USB-C, NFC, fingerprint options
- **SoloKeys / Solo V2**: Open-source, WebAuthn-capable
- **Nitrokey**: Open-source hardware for OTP, FIDO2, PGP

Features and Tradeoffs

- Strong phishing resistance
- No shared secrets; resistant to man-in-the-middle
- **Offline-capable**, but physical access required
- Cost and loss risk (backup key important!)

Enterprise Integration

- **PIV (Personal Identity Verification)** smartcard support
- SSH login, GPG, VPN auth
- Used in enterprises, governments, and secure CI/CD

TOTP vs FIDO2 Hardware Tokens

- TOTP: Time-based codes (soft or hard tokens)
- FIDO2: Asymmetric key-based challenge-response
- TOTP more portable, FIDO2 more secure

TOTP-Based 2FA Tools

- Google Authenticator (mainstream, 2010s)
- Microsoft Authenticator: Azure/M365 focus
- Bitwarden Authenticator: May 2024

- Available in current Andriod/IOS
- Authy: Cloud sync, Twilio-owned
- Aegis, FreeOTP: FOSS alternatives
- Independent Authenticators - e.g. BitWarden

Bitwarden "Verification" ([TOTP] Authenticator)

Item	Details
Release Date	May 1, 2024
Available Platforms	Android and iOS
Standalone App	Yes — functions without Bitwarden vault
TOTP Sync	Optional (with Bitwarden Premium)
Desktop Version	Not available (as of July 2025)
Purpose	Lightweight mobile TOTP manager
Why Android/iOS Only?	Mobile-first rollout; desktop version

Other players

KeePass

- Original windows-based password manager
- First released 2003 by Dominik Reichl
- Feature/Price/Cloud/Source/Self-host

Launched: 2003

- Launched: 2003
- Open-source, local-only
- Plugin-based extensibility

No cloud dependency

- No cloud dependency
- Portable database format
- Extensive plugin ecosystem

Manual sync

- Manual sync
- Plugin management complexity
- Dated UI/UX

KeepassX, keepassXC: linux-focused forks

- KeePassX, KeePassXC: Linux-focused forks
- Cross-platform, Qt-based
- Still local-first

Simpler model than keepass

- Simpler model than KeePass
- More dated, less extensible

Local storage by default

- Local storage by default
- Cross-platform
- One-time purchase model
- Android/IOS: ownCloud, GDrive, nextCloud, et al

LastPass (Founded 2008)

- Cloud-first, browser-based vault
- Freemium model, proprietary
- 2015 and 2022 data breaches
- Vault blobs exposed (encrypted, but accessible)
- Now owned by GoTo (formerly LogMeIn)

1Password

Secret Key system (2016)

- Obfuscated encryption keys
- Cloud breach exposed vault blobs
- Limited user control

Strong brand reputation

- Strong brand reputation
- Proprietary, closed source
- Now cloud-first with (Electron based) 1Password 8

Business-focused features

- Business-focused features
- Subscription-only
- Recently deprecated standalone apps

Modern, Open-Source, User-friendly

Bitwarden, lessPass, padloc

- Bitwarden, LessPass, Padloc
- Modern architectures
- Open codebase, hosted/cloud sync

Fully open source

- Fully open source
- Offers self-hosting
- End-to-end encrypted vaults

Zero knowledge (Bitwarden, Padloc)

- Zero knowledge
- Vault data encrypted before leaving device
- Public audits
- Bitwarden: E2EE by default
- Padloc: Encrypted before sync
- LessPass - stateless

Free tier is usable

- Free tier is usable
- Transparent development
- 2FA, U2F, biometric support
- Bitwarden & Padloc

Modern and polished interface

- Modern and polished interface
- Streamlined browser extension
- Rapid evolution and UI improvements
- Bitwarden & Padloc

Open source, team-focused

- Open source, team-focused
- Based on GPG keys
- Self-hosting default
- Bitwarden, Passbolt

Bitwarden

- Multiple versions, from free to enterprise
- Multiple hosting options (including self for any version)
- Bitwarden-compatible Rust fork, lightweight, ideal for self-hosting

TOTP

Totp-based 2fa

- TOTP-based 2FA
- Time-based one-time passwords

Original mainstream totp app

- Original mainstream TOTP app
- Recently added sync (2023)
- Closed source

Focus on azure/m365

- Focus on Azure/M365
- Encrypted backup
- Push-based MFA for enterprise

Totp + backup/sync

- TOTP + backup/sync
- Twilio-owned
- Some concerns about cloud key storage

Freeotp: red hat, minimal

- FreeOTP: Red Hat, minimal
- Aegis: Open-source, Android-only, export/import support

Replay window

- Replay window

- Phone compromise risks
- Export key safety

Hardware-based 2fa

- Hardware-based 2FA
- Challenge-response using private keys
- Strong phishing resistance

Invented by yubico

- Invented by Yubico
- U2F, FIDO2, OTP, PIV, OpenPGP

2fa for web (u2f/fido2)

- 2FA for web (U2F/FIDO2)
- SSH via OpenPGP
- Static password for legacy

Nano, 5 nfc, 5c, bio

- Nano, 5 NFC, 5C, Bio
- USB-A, USB-C, NFC, Fingerprint

Strong phishing resistance

- Strong phishing resistance
- Offline capable

- Multi-protocol

Cost

- Cost
- Loss = access issues (unless backup key)

Open hardware alternatives

- Open hardware alternatives
- FOSS firmware
- Solo V2 supports WebAuthn

Piv = personal identity verification

- PIV = Personal Identity Verification
- Compatible with YubiKey, Nitrokey
- Used for SSH, VPN, login

Totp apps vs fido2 tokens

- TOTP apps vs FIDO2 tokens
- Security 🔐 vs convenience

Best practices

- Something you know (password)
- Something you have (token)
- Something you are (biometric)

Webauthn and passkeys

- WebAuthn and passkeys
- Apple/Google/Microsoft push

Synced fido credentials

- Synced FIDO credentials
- No passwords involved
- Bound to devices and accounts

Positives & Negatives

Vendor lock-in

- Vendor lock-in
- Syncing risks
- Lack of interoperability
- Ease if integration from same vendor

Azure ad, okta, duo

- Azure AD, Okta, Duo
- Role-based access control
- Central policy enforcement
- AD integration

Browser-based vaults

Chrome/firefox password managers

- Chrome/Firefox password managers
- Security 🔐 vs usability trade-offs

Export vault (encrypted!)

- Export vault (encrypted!)
- Store hardware token backups
- Paper recovery codes

Final points

Social engineering

- Social engineering
- Poor master passwords
- Misconfigured MFA

Bitwarden or vaultwarden for most users

- Bitwarden or Vaultwarden for most users
- YubiKey for critical accounts
- Avoid SMS-based 2FA

Secure enclave-based keys (tpm/iphone/android)

- Secure enclave-based keys (TPM/iPhone/Android)
- Hardware-bound passkeys
- Decentralized ID (DID) + verifiable credentials

No one-size-fits-all

- No one-size-fits-all
- Use layered security
- Evaluate threat model and pick tools accordingly

Thank you!

Lee Lammert

Omnitec