LASS PASS, PASSKEYS, RAIDERS OF THE LOST ARK

JEFFREY I. SCHILLER

06/11/2024

INTRODUCTION

- I'm Jeff Schiller
  - Technically work for IS&T
  - Contribute to MIT App Inventor
  - Was the IETF Area Director for Security for 9 years 1994 – 2003

DISCLAIMER

- The opinions expressed here are my own and do not represent the opinion of IS&T or MIT
- I have no inside knowledge of what happened at LastPass
  - What I am going to say is based on published sources and my own knowledge of "how things work"

WHAT IS ZERO KNOWLEDGE?

- This is a buzzword we keep seeing.
- Passwords are **not** zero knowledge. When you enter your password to a site or application, you are giving that site a piece of information that it can turn around and use to impersonate you (if you use the same password in multiple places!).
- Zero Knowledge means that you do not turn over, or store, information that can be used to authenticate you.

ATTACKS ON PASSWORDS

- Threat Actors compromise sites and the passwords of the site's users.
- Many sites now "hash" stored passwords, but this provides only limited protection
  - Even with "salted" hashes, if **you** are targeted and your password is "leak" you can become a victim

USE A PASSWORD MANAGER!

- The only safe password is one that you likely cannot remember!
- Password managers make it easy to use a different, secure, password for each site.
- You only have to memorize a "master" password, which should be secure (sigh!).
  - But 2FA can help
- Many to choose from

PASSKEYS (OR FIDO/FIDO2)

- FIDO: Fast IDentity Online
- The FIDO Alliance publishes standards for FIDO/FIDO2
- These are cryptographic protocols for authenticating (zero knowledge!) without passwords
  - FIDO is an older standard which can be used for a second factor
  - FIDO2 is newer and can be used as an only factor
- Hardware tokens like newer Yubikeys support them.
- Passkeys already built into modern Android phones
- Some password managers are supporting them, soon all will

SO WHICH PASSWORD MANAGER SHOULD YOU USE?

- Many to choose from…
  - Some store your information in the Cloud, available on multiple devices
  - Some store your information in a local file, or the Apple Keychain
    - Some of these let you store the "file" in a dropbox or similar storage
- All of them encrypt your passwords based on a master key, which is never shared with the password manager
  - This is how "Zero Knowledge" is enforced

BUT NOT ALL ARE CREATED EQUAL

- Beware of security product companies that are purchased by a non-security company
  - Purchaser will cut staff to cut costs, often not cognizant of the special considerations that a security focused company should have…
  - Hint: LastPass was purchased to GoTo (LogMein) in 2015, spun off in 2024 (finally) with breaches in 2011 and 2022.

LAST PASS STORAGE

- Your data is stored on Last Pass's servers
- Only "sensitive" information is encrypted passwords, but not necessarily URL's or names of entries (this is bad, more in a bit)

"VAULT" PROTECTION

- There are two things protecting your password "Vault"
- The server will not hand it out without proof you are the legitimate user
- You have the "master" password to decrypt the vault contents
- You can prove yourself via knowledge of the master password and optionally with a second factor

TANGENT: PASSWORD DERIVATION FUNCTIONS

- Take a string and turn it into a key
  - Designed to be inefficient, you can tune the inefficiency
- Examples: PBKDF2 and Argon2
- These functions are used to turn a master password into an encryption key
- They need to be inefficient to prevent the use of "rainbow tables" to attack the password
  - As CPU power improves, need to tune the algorithms to be even less efficient

PBKDF2

- DK = PBKDF2(PRF, Password, Salt, c, dkLen) where:
  - **PRF** is a pseudorandom function of two parameters with output length hLen (e.g., a keyed HMAC)
  - **Password** is the master password from which a derived key is generated
  - **Salt** is a sequence of bits, known as a cryptographic salt
  - **c** is the number of iterations desired
  - **dkLen** is the desired bit-length of the derived key
  - **DK** is the generated derived key
- Source: Wikipedia

RAIDERS OF THE LOST ARK

- What does this have to do with anything…
- Well…
-

LAST PASS BREACH

- First their Source Code was stolen
- Then everyone's(?) Vault Contents were stolen (so authentication and 2FA didn't matter anymore!)
- I can forgive the first (maybe)
    - But not the later!

THREAT ACTORS COULD CHERRY PICK VAULTS

- Because URL's and other identifiable information was not encrypted…
- And the hash iteration count was also available for each vault (that has to be)
- Threat Actors could pick and choose which vaults to attack
- Millions of dollars in crypto currency likely stolen as a result

QUESTIONS?