Macs Factor: The Risks and Rewards of Single Sign On

Sean Rabbitt

Session Info: https://sched.co/1dFq7
Feedback: https://bit.ly/psumac-2024-34

Security, Intermediate • Deans Hall 2
Thursday, July 11, 2024 • 09:00AM - 10:15AM

Three factor types we've been using:

- Knowledge (something you know) pin, password, secret
- Possession (something you have) PIV/SmartCard, FIDO2 key, CAC, etc.
- Biometric (something you are) Touch ID, Face ID, fingerprint and retinal scanners, etc.

"macOS is UNIX"
"Passcodes and passwords are essential to the security of Apple devices" ~ Apple Platform Guide

"If the cloud is just somebody else's server, passwordless is just somebody else's hash" ~sean rabbit
Knowledge is a phishable method. Combining phishable and non into multifactor makes the end result non-phishable. But procedures to recover the phishable method may be used in conjunction with other methods to take access.

Apple Extensible Single Sign On, makes your mac into a possession-based factor.

Definitions:
Kerberos Single Sign-On: replacement for enterprise connect (RIP), ask for AD certificate to act as tok
Extensible Single Sign-On (SSOe): same as above but for accessing cloud-based server.

- authenticationServices API - "credential"
- URL intercept method - "redirect": local device creates proxy to reroute

Enrollment SSO: iPhone and iPad
Platform SSOe:

Extensible SSO

Single Sign on - A possession factor

- Needs a managed device
- Only active via MDM profile
- Once it's active, it's active
- Works in Private Browsing mode
- Currently not working with Firefox and Chrome,

[ed: no more notes, tendonitis acting up]

Platform SSO

- Entra (uses redirect)
- Okta, need two profiles (redirect and okta desktop password sync?)
- Can require authentication to IdP on filevault screen
    - This can also require being connected to a KNOWN network to log on or ethernet, (which could run into a USB device restriction)
    - AD binding problems are back

Hardening

- Turn on filevault
- Cloud IdP (jamf connect, xcreds)
- Offline MFA
    - Jamf connect
    - Okta desktop MFA
    - Entra ID/Company Portal as a passkey (might be available in the future)
- Cloud security
    - Entra
        - FIDO2 key
        - Authenticator
        - OAUTH token
        - Conditional access
            - Set requirement for multifactor or non phishable multifactor
    - Okta Identity engine
        - User must authenticate with:
            - Any 1 factor, excluding password
            - Any 2 factors
            - Can’t keep up
- Network security
    - If a device is compromised can get refresh tokens
    - If malicious site is detected, can tell idp to not send out more tokens (ssf sender ->CAEP signal receiver)
- SSO is a possession factor, (single factor)
- PSSOe also possession factor
- If you accessing a resource and the device is the factor, protect the device
- Can combine PSSOe with something like jamf connect to separate possession factor from authentication factor

Filevault feedback to apple:

- Filevault uses a single method to encrypt data. Should be MFA
- Basic authentication is no longer acceptable to decrypt data at rest

Q&A

Q: Is Platform SSO something that can be used in lab environments?
A: every device would have to be touched so probably not

Q: Is there a good way to test the Single Sign on Extension
A: non production test equipment Companion app on device (company portal/authenticator//microsoft, Okta app)
Some info available to see if an account has been “adopted” by sso

`app-sso` will show main help page
Re-pair (if initial auth doesn't work) or reauthenticate button (revoke session to re-log in)

I missed a question and didn't quite manage to keep up.