Device Recovery in WebAuthn

Pre-emptively Syncing Keys

Alex Takakuwa, University of Washington

Pre-emptively Syncing Keys

- Use Transfer Access style delegations
  - Chains of signatures from the original private key to the new private key
  - Chain of hardware attestations from the original device to the new device
- Pre-generate backup authentication keys (on the backup device) and send them to new authenticators.
  - Backup authenticators also create Transfer Access style delegations from **all** old keys and send them any newly activated authenticators (new authenticator also has to pre-generate keys)
- Registration:
  - Authenticators register a backup key and a standard authentication key.
- Recovery:
  - Newly restored authenticator delviers chain of delegations from the backup authenticator to its own generated key.
  - Relying party uses this chain to update authorized keys.

User Experience: Pre-emptively Syncing Keys

- Setup
  - User acquires and manages a backup device. (This can be pysical device(s) or a software service)
  - User “activates” each new authenticator once by syncing with the backup device
- Recovery
  - Same as setup: User buys a new device and “activates” it by syncing with the backup device
- Authentication
  - Same as normal
- Device Upgrade
  - Same as in Transfer Access

Caveats

- Requires a storage overhead on both the backup device as well as any primary authenticators
- Requires a computation overhead on both the backup device as well as any primary authenticators
- Revocation is a bit tricky.
  - Revoking any individual key from a site can occur in a straightforward manner, but the revocation must include replacing the backup key stored at the RP.
  - Revoking access from a previous device is difficult because the backup key does not know about all registrations from that device.
    - Can be done “on the fly” as a user visits each site
    - Could store information about registrations somewhere else, as in “Online Recovery Storage”

More Information on Recovery from Device Loss

https://docs.google.com/document/d/1tRLbXYLb9Z65QqhOX7v9D-aq_RUODyn5oALpCXj46K8/edit?usp=sharing