Multifactor Fusion in a Verifiable Credential

Francisco Corella
fcorella@pomcor.com

Presentation at IIW 38 on April 18, 2024

pomcor
pomcor.com

Cryptographic authentication

- Definition: authentication by proof of possession of a secret, such as a private key
- Provides protection against man-in-the-middle attacks
  - … If done right
- But it is only one-factor authentication
  - No protection against capture of the secret
- **Strong security requires authentication with 2 or 3 of the following factors: knowledge, possession, inherence**

Three methods of providing multifactor cryptographic authentication

1. Use the factors independently of each other in separate authentication procedures
   - Possession factor provided by presenting a cryptographic credential
   - Knowledge and/or inherence factors provided by authenticating with a password and/or a biometric
2. Use a knowledge factor and/or an inherence factor to unlock the use of a cryptographic credential (as in FIDO)
3. Combine knowledge and/or inherence factors with a possession factor into a fusion credential and use them together in a single authentication procedure with the credential

Method 1 is weaker than method 2 because the knowledge and/or inherence factors can be attacked separately from the possession factor

Security strength of the methods

- Method 1 inherits the drawbacks of the knowledge and/or inherence factors
  - If a password is used, it is vulnerable to phishing, reuse, brute force guessing and dictionary attacks after a backend breach
- Method 2 removes some of these drawbacks by not submitting the knowledge and/or inherence factors to the backend, but some drawbacks remain
  - If a password is used, it is not vulnerable to a backend reach, but it is still vulnerable to ~~phishing~~, reuse and guessing
- A fusion credential provides the strongest security

Examples of fusion credentials

- Camenisch et al., 2013. Fusion of a biometric factor with a zero-knowledge cryptographic factor
- Gunasinghe and Bertino, 2015. Another fusion of biometrics with zero-knowledge technology
- Pomcor, 2016. Fusion of a selective disclosure certificate with a password and/or a biometric
- Pomcor, 2023. Cross-browser authentication with a fusion a selective disclosure certificate with a password and/or a biometric.

Question

- Can a verifiable credential be fused with knowledge and/or inherence factors?
- Yes, by combining **any existing VC** with a two-party fusion credential
  - A two-party credential is a credential used by a relying party for returning user authentication, without relying on claims asserted by a third party

Recipe

- Ingredients:
  1. VC with claims, metadata, and issuer's signature
  2. Two-party credential with public and secret portions
  3. Knowledge and/or inherence factors provided by the user
- Prep:
  1. Run a simulation of the registration procedure of the two-party credential. Obtain the registrand that the two-party relying party would store in its backend.
  2. Use your favorite encoding algorithm to format the registrand as a DID method-specific identifier and put aside.
  3. Put aside the entire two-party credential

Recipe, continued

- Cooking:
  1. Create a fusion DID, consisting of the "did" scheme, followed by a method name specific to the type of two-party credential being used, followed by the registrand
  2. Replace the DID of the subject in the verifiable credential with the fusion DID
  3. Bake a signature in a credential issuing oven at medium heat and let it cool down
  4. Replace the original signature in the VC with the newly baked signature
- Serving:
  - Serve the fusion credential in a wallet, putting the entire two-party credential in the secure enclave of the wallet

Example

- The kind of two-party credential specified in Pomcor 2023 consists of a key pair and a secret salt.
- The knowledge and/or inherence factors consist of a password
- The simulated registration computes a hash of the password and the secret salt, and a hash of the salted password and the public key, which it outputs as the registrand

Example, continued --- authentication protocol

- The wallet:
  - receives a challenge from the relying party which it signs with the private key;
  - obtains the password from the user which it hashes with the secret salt; and
  - sends the signature, the salted password, the public key, and the credential to the relying party
- The relying party:
  - verifies the signature on the challenge;
  - computes the hash of the salted password and the public key, encodes the result, and verifies that the encoded result agrees with the method-specific identifier of the DID of the subject of the credential;
  - discards the public key and the salted password;
  - verifies the issuer's signature in the credential

Fusion with a biometric

- Challenge: biometric samples vary
- Naïve solution: put a biometric template in the credential as a claim
- Better solution: use revocable biometrics and use a biometric key to construct the did:fusion decentralized identifier

- DETAILS TO BE WORKED OUT