Great webinar session yesterday and appreciate all your efforts in this much needed area, Zero Trust Identity Assurance (ZTIA).

I have a concept called 'Identity Air-Gap' that I believe could be a good fit for xAL3, specially defines a standard in IAL3 and FAL3. Here are the thoughts & purpose of Identity Air-Gap,

- Minimize the security impact when an identity is compromised.
- Treating 'authorization' information relates to person's primary identity as private & confidential information.
- Having a separation to general login and privileged access.

The concept of Identity Air-Gap,

- The first login method used in xAL1 & xAL2 cannot be used to gain privileged access in xAL3.
  - For example, whatever the SSO method for first login cannot be used to login to xAL3 service. This will prevent if xAL1/2 services got compromised, the result of the user info cannot be used to gain access to xAL3 services.
  - Example, a user login to gov service using xAL2 using username/Password + OTP (soft token) for read-only activities. When the user is ready for update privileges in downstream service, the RP will request for a short-timed user certificate as authentication method to xAL3 service for privileged access (update access). SSO of user's token from up-stream service cannot be accepted.
- Separate IdP and authorization (authZ) services using federation.
  - IdP is mainly focus on identity lifecycle management, while 'authZ service' functions as IdP (being trusted by apps & services) but mainly focus on authorizations. Therefore, when Identity is compromised, only general service is impacted.
  - 'authZ service' typically don't house identities (therefore, not much for phishing target) but have a trusted method to federate w/ IdP's.
  - 'authZ service' will issue ID-token and/or access token, on behalf of the user from IdP, to xAL3 services & apps; thus, the identity air-gap.

There are more to build out the technical details, but I want to run by you all to see if this is off scope or maybe it is addressed somewhere else already.

Also, comments on NIST.SP.800-63B-4 document, section 2.5, line 678 Figure 1, AAL3 permitted authenticator type, SF cryptographic plus password,

- Assuming the certificate based authentication we are dealing with is a long-term certificate (TTL is more than 24 hours).
- What if we have some of the following attributes in the user cert, can we use it as 'SF Cryptographic' for AAL3?

- The cert is short-lived user cert for authentication, minutes to less than 8 hours, for example.
- The cert is issued from trusted ‘authZ service’ and the issue time is within few minutes of the login attempt. (so we know the intent)
- The cert has authorization in the payload.
- The verifier checks against revocation list and other means.

My concept is to avoid using password, so there is way less value to phish username/Password. Thanks.

Please let me know what you think. Thanks.

Jamie Lin