Multi-Factor Authentication

Pilot Project Update

SWITCH

Etienne Dysli-Metref
etienne.dysli-metref@switch.ch

Project members

- University of Geneva
- Swiss edu-ID
- developer: me :)

University of Geneva

Goal

Stronger authentication for a HR web application handling personal data of university staff

Second factors

- Google Authenticator (OATH-TOTP)
- SMS OTP

Authentication server with RADIUS interface to verify OTPs

Swiss edu-ID

Goal

Offer stronger authentication methods on the edu-ID IdP

Second factors

- First demo with Google Authenticator
- Add more as required

Project links

- SWITCH toolbox (https://toolbox.switch.ch/en/combos/idpv3-mfa)
  - wiki (meeting notes)
  - mailing list (announcements)
  - Discourse (forum)
- SWITCH Forge (https://forge.switch.ch/projects/idpv3-mfa)
  - issue tracking, roadmap
  - source code (git://git.switch.ch/idpv3-mfa.git) (public read access)

Project links

- Public demo IdP & SP in AAI Test federation
  https://mfa-dev.ed.switch.ch/index.html (https://mfa-dev.ed.switch.ch/index.html)

IdP 3.3 enhancements for MFA

IDP-962 (https://issues.shibboleth.net/jira/browse/IDP-962)

- Orchestrator flow to combine login flows
- Execute several authentication methods and aggregate results
- Attribute resolution during authentication
- Transition logic

The SAML & MFA horror scenario

1. SP wants “MFA”
2. SP requests a particular AuthnContext
3. IdP does not support this AuthnContext
4. Failure!

How can SPs request MFA and IdPs indicate that MFA was used, without getting too precise about the actual authentication method?

⇒ The InCommon MFA interoperability profile working group (https://spaces.internet2.edu/display/MIPWG) tackled this problem and published two profiles to help solve it

MFA interoperability profiles

InCommon MFA profile

- AuthnContext
  `http://id.incommon.org/assurance/mfa` says "MFA was used"
- Factors must be independent
- Combination of factors mitigates single-factor-only risks related to non-real-time attacks: phishing, offline cracking, online guessing, theft
- Limited to authentication: nothing about registration or identity proofing
- Not technology-specific