Multi-Factor Authentication (MFA) Interoperability Profile

Karen Herrington, Virginia Tech
David Walker, Internet2
September 26, 2016
Mission

- Working group formed at the request of the Assurance Advisory Committee
- Charge - To develop and document requirements for creating and implementing an interoperability profile to allow the community to leverage MFA provided by an InCommon Identity Provider by allowing SPs to rely on a standard syntax and semantics regarding MFA.
Status

- Weekly calls began February 2016 – building on the work begun by Jacob Farmer in 2015
- Community review mid-April - mid-May
- Approved by the Assurance Advisory Committee in August
- Awaiting approval of the InCommon Steering Committee
- REFEDS consultation ongoing - expected to complete soon
Work Products

https://spaces.internet2.edu

- Final Report
- MFA Baseline Profile
- Baseline Profile
- Usage Guidance document
- Technologies document describing Authentication Factors and Threat Resistance
- Use Cases
MFA Baseline Profile

• Maintained focus on the authentication event
• Defined in terms of risks mitigated
• Mitigated risks include non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor
• Asserted through authentication context
MFA Profile criteria

- The authentication of the user’s current session used a combination of at least two of the three distinct types of factors defined in NIST Special Publication 800-63-2: Electronic Authentication Guideline, section 3, Definitions and Abbreviations (something you know, something you have, something you are).
**MFA Profile criteria (cont’d)**

- The factors must be independent, in that access to one factor must not by itself grant access to other factors.

- The combination of the factors mitigates single-factor-only risks related to non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor.
Baseline Profile

• To establish a base over which other profiles could be defined
• To be used by SPs in conjunction with other profiles in SAML requests to indicate that a higher level profile is preferred, but base level is acceptable
• To provide a value for systems to affirmatively assert when authentication is done successfully but *without* MFA (necessarily) being used
Usage Guidance document

• Provides advice on the use of the profiles in practice
• More explanation about risks that must be mitigated
• Guidance about what constitutes an acceptable “second factor”
Mitigated Risk guidance

• Non--real-time phishing
  • Inducing a user to provide a credential (e.g., password) to a malicious agent through social engineering, forged websites or the like
  • Inducing a user to provide credentials using an insecure/observable protocol
  • Protection is provided against indefinitely reusable credentials, and not one--time user attacks
Mitigated Risk guidance (cont’d)

- Online guessing, offline cracking
  - Attacks that could obtain credentials without directly involving the user, through attacks on application login screens or (encrypted) password databases
Mitigated Risk guidance (cont’d)

• Theft of a (single) factor
  • Ability to (steal) each factor using a single theft mechanism. The intent is that the factors should require different theft mechanisms. For example, stealing a user’s phone or security FOB requires a different attack mechanism than phishing a user’s password.
  • Theft of a single OTP code is not protected against, but rather theft of the OTP device
Independence of Factors guidance

- Any factor that is directly accessible using the first factor is NOT considered a second factor
  - A software/virtual phone that is authenticated using the enterprise password is not an appropriate second factor
  - Users can take actions that reduce the ability to treat otherwise independent factors as “independent”; Ex: a user storing his software OTP generator on a network device accessible using just the “first factor” password
Independence of Factors guidance

• Implementers are expected to require greater scrutiny before allowing registration of replacement or additional second factors to prevent attackers with password access from simply registering and immediately using a new second factor.
  • Note that it is common practice to allow the initial registration of a second factor using only the existing factor, and the MFA profile does not restrict this initial MFA factor registration practice.
• Two tables intended to aid in the selection of acceptable multi-factor authentication technologies for use with the profiles
• Table 1 describes commonly used authentication factors and summarizes their resistance to common threats
• Table 2 summarizes Authentication Types or Groups of Types which meet the needs of authentication profiles
A Simple Use Case: An SP That Requires MFA

• An application managing human subjects data for a research project
  • Or an administrative tool for your IAM system
  • Or any application that needs strong verification of users
• The application’s authentication process must require the use of multifactor authentication
MFA-Requiring SP Authentication Process

Request authentication with the MFA profile only

Was authN MFA?

Fail! no

Success! yes
MFA for InCommon’s Certificate Manager

- Federated access to InCommon’s Certificate Manager
  - Registration Authority Officers (RAO) will be required to use multi-factor authentication
  - Department RAOs will not be required to use multi-factor authentication.

- The Certificate Manager’s authentication process must require MFA, or not, depending on the user’s role.
Certificate Manager Authentication Process

Request authentication with any profile (PPT, Basic, MFA)

Is role RAO?

no → Success!

Was authN MFA?

yes → Success!

Request authentication with the MFA profile only

Was authN MFA?

no → Fail!

yes → Success!
Certificate Manager Issues

• The IdP may not return control, so prior to the first authentication request prepare the user with:
  • A description of the overall process
  • MFA requirement for RAOs
  • How to recover if something goes wrong
  • Links and contact information for help
What Are Your Use Cases?

Let’s discuss...