From: Nick Borgers
Sent: Saturday, August 22, 2020 2:11 PM
To: dig-comments-RFC <dig-comments-rfc@nist.gov>
Subject: Definition of multi-factor authenticator is problematic

A single factor of authentication presented to a verifier can only provide a single factor of authentication.

A flawed approach to multifactor authentication has been elevated to a standard, and we need to correct it.
The problematic approach is allowing a single authentication factor to qualify as multi-factor authentication.

For all these terms I look to NIST's SP 800-63-3 Appendix A.

Unfortunately, the same standard goes on to define a "multi-factor authenticator" in Appendix A:

> Multi-Factor Authenticator
>
> An authenticator that provides more than one distinct authentication factor, such as a cryptographic authentication device with an integrated biometric sensor that is required to activate the device.

SP 800-63B further clarifies the distinction between a single factor authenticator and a multi-factor authenticator. I restate the distinction made in the 800-63 suite as:

- A single-factor authenticator is one that does not, itself, require authentication to generate a valid OTP
- A multi-factor authenticator is one that, itself, requires authentication to generate a valid OTP

This is, at best, prone to misunderstanding. At worst, a standard has been defined which allows authentication schemes requiring compromise of a single factor **to be understood** as a multi-factor authentication system.

What is the problem?

The verifier of a one-time password (OTP) is only ever provided with that OTP. This is the single factor of authentication provided to the verifier. 800-63B §5.1.5.2 recognizes this fact (emphasis mine):

> Multi-factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator, but **without the requirement that a second factor be provided**.

§5.1.5.2 includes a requirement for the verifier to, "when a multi-factor OTP authenticator is being associated with a subscriber account":

> The verifier or CSP SHALL also establish, via the authenticator source, that the authenticator is a multi-factor device.

It does not matter what the device is; this requirement enables misunderstanding.

The only factor of authentication available to the verifier at the time of authentication is an OTP demonstrating possession of the authenticator token's secret key.

The authenticator is a single point of compromise; it must only ever be a single factor of authentication. An authentication requirement on an authenticator device does protect that authentication factor, but does not change the nature of the authenticator it protects. Placing the key to a vehicle in a combination safe does not provide the vehicle with "multi-factor authentication". The adversary still only requires the key to drive the vehicle.

Application to Modern OTP Tokens

Software OTP Authenticators

Let's apply this to software tokens in-use today:

- Unauthenticated software authentication token
- Authenticated software authentication token

A single factor OTP authenticator implemented as software is generally compromised in both of these scenarios:

- Adversary has physical access to the device hosting the token when the device is unlocked
- Adversary compromises the device hosting the token, including any TPM / Secure Enclave

A multi factor OTP authenticator implemented as software is able to withstand compromise if:

- Adversary has physical access to device when the device hosting the token is unlocked

However, the token still fails if:

- Adversary compromises the device hosting the token, including TPM / Secure Enclave

There are two options for protecting the authenticator token's secret key with encryption laid out in 800-63B:

- Derive an encryption key from a memorized secret, and encrypt the authenticator token's secret key
    - NIST specifies that the memorized secret be "at least 6 decimal digits in length"; trivially cracked if the ciphertext is available to a modestly capable adversary.
- Protect an encryption key in a device which requires physical biometric authentication, and encrypt the authenticator token's secret key

  - The protection is contingent on the device resisting compromise; this protection is tautological.

Neither ensures that the adversary must possess either second factor; only the OTP key is required and the adversary can directly compromise it in a single attack. This is not multifactor authentication.

Hardware OTP Authenticators

For comparison, let's consider a hardware token scheme in which the user provides the verifier with both:

1. An OTP generated by hard token
2. A memorized secret

This scheme provides the verifier with two distinct factors of authentication:

- An OTP demonstrating the subscriber **has** the OTP authenticator token
- A memorized secret the subscriber **knows**

Placing the hard token in a biometric safe would not make this three-factor authentication, because the act of authentication is performed by the verifier. Whatever protections exist for the factors cannot be relied upon by the verifier: the authentication decision must be made only with what is known.

It is possible to perform MFA with a single value provided to the verifier

Software OTP authenticators which can generate OTPs may only be able to generate valid OTPs when additionally provided with a memorized secret. This is not encryption of the OTP key with the memorized secret, but instead using both the memorized secret and the time or sequence number to generate a valid OTP. An invalid memorized secret, or a null/empty memorized secret, still allows the generation of an OTP value; just not a valid one.

The verifier is only presented with a single OTP, but must combine both the authenticator's OTP key and the memorized secret to verify the validity of the presented OTP. The difference is that the authenticator OTP key alone is not sufficient to produce a valid OTP: the single factor of authentication cannot be used to authenticate.

Notably, memorized secrets used in such schemes are likely to be short and numeric, e.g. a PIN. This results in a relatively weak memorized secret. Where a high assurance authentication is required, such as at time of a session establishment, a separate memorized secret informed by SP 800-63B Appendix A may be required as part of authentication in addition to the OTP which is technically MFA alone.

On Biometrics

This is in notable contrast to 800-63B §5.2.3.

Physical biometric information can only be used as an authentication factor to a device, it cannot be used by a remote verifier. A sensor is used to collect information about a physical object submitted for biometric authentication. This information is then used to perform a biometric comparison which may, or may not, result in a match.

If the device collecting biometric information is separate from the verifier, the verifier of the biometric information is receiving a data object. This data object can be copied, saved, replayed, etc. The verifier is not performing a biometric authentication, it is acting as a credential store to provide a verification result to the device collecting the information.

If the device is locally authenticating the biometrics, a verifier on the remote system is not authenticating the user's biometrics. The remote system may choose to trust the device which has performed biometric authentication of the user, but authentication of the device and determination that it is trusted must not imply that the user has biometrically authenticated to the remote system. The identity of the user is merely **asserted** by the device to the remote system, and the remote system must trust that assertion.

Biometric authentication cannot be used for remote authentication of users, it can only be used to authenticate a user to a device.

Summary

NIST Term	NIST Claim	My Claim
Multi-Factor OTP Device	2FA	1FA
Multi-Factor Cryptographic Software	2FA	1FA
Multi-Factor Cryptographic Device	2FA	1FA

To provide multi-factor authentication a verifier must use multiple, different, and discrete information to perform authentication. This requires either multiple values to be conveyed to the verifier, or the conveyance of a value whose verification and creation requires multiple factors of authentication. Examples include:

- An OTP that must be created or verified by combining a memorized secret and an OTP authenticator key (2FA)
- An OTP and a memorized secret (2FA)
- A valid biometric physically presented to the verifier, a memorized secret, and proof-of-possession of a private key (3FA)

Depending on requirements, biometric or password protection of OTP authenticators may be appropriate, but it cannot transform the single-factor authenticator into a “multi-factor authenticator”.

Regards,
Nick Borgers