MFA Technologies, Threats, and Usage

Introduction

The two tables on this page are used to explain our selection of acceptable multi-factor authentication technology for use in assurance 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.

Table 1 - Authentication Factors and Threat Resistance

AuthN Type Number	**Authentication Factor**	**Resistance to Threat**				
		Theft (Phishing, etc.)	**Theft via Dynamic MITM Phishing**	**Guessing / Offline Cracking**	**MFA Device Compromise**	**User Workstation Compromise**
1	Password	Low	Low	Depends	n/a	Low
2	Phone call *see Voice Restrictions, note 1*	Low	Low	High	Low	High
3	Phone call (VoIP) *see Additional VoIP Restrictions, note 2*	Low	Low	Medium	Low	High
4	SMS	Low	Low	High	Low	High
5	SMS (VoIP) *see Additional VoIP restrictions, note 2*	Low	Low	Medium	Low	High
6	HOTP cell phone software *see notes 1 and 3*	Medium	Low	High	Medium	High
7	TOTP cell phone software *see notes 1 and 3*	Medium	Low	High	Medium	High
8	HOTP token	Medium	Low	High	High	High
9	TOTP token	Medium	Low	High	High	High
10	HOTP written (back up codes)	Low	Low	High	High	Low
11	DUO Push *see note 3*	High	Low	High	Medium	High
12	FIDO U2F token with password	High	High	High	High	High
13	PKI device certificate with device password	High	High	High	High	Medium
14	PKI token certificate with token password	High	High	High	High	High

Notes:

1. *Voice Restrictions: Institutions deploying a phone call based solution for one of their authentication factors must incorporate multi-factor authentication concepts into their security awareness training. Specifically, a prohibition on configuring voicemail greetings to respond to MFA prompts must be in-place and discussed in training. Training should also include the prohibition against using Enterprise passwords on personal devices.*

2. *Additional VoIP Restrictions: The use of VoIP systems (or traditional PBX solutions) that use the Enterprise password for call control or call redirection may not be used. The creators of this document note that accessibility needs can often be addressed using a hardware token instead of a voice-based solution.*

3. *Campus deployers should pay careful attention to cell phone security. Some data sources report that the majority of Android devices are not updated and are thus highly vulnerable. Some vendors have the ability to restrict MFA use to fully patched cell phones. This table assumes that cell phones used for MFA are receiving software updates.*

Table 2 - Authentication Types and Combinations of Authentication Types that meet profile requirements.

The Standard MFA Profile that we are developing now focuses on simple passwords no longer being sufficient in a modern world full of phishing threats. The Stronger MFA profile column would be for some future work to support an overall higher LoA, likely coupled with corresponding Identity Proofing requirements. It's helpful to see how the two might differ in their technology requirements.

Item	MFA Type Number(s) from Table 1	Standard MFA Profile (anti-phish - replace passwords)	Stronger MFA Profile (could support a stronger LoA)
1	1 plus any one of 2-14	Yes	n/a - see below
2	12	Yes	Yes
3	13	Yes	No
4	14	Yes	Yes
5	1 plus any one of 12-14	Yes	Yes