Three-factor Authentication (3FA)

Posted by: Margaret Rouse

Contributor(s): Matthew Haughn

Three-factor authentication (3FA) is the use of identity-confirming credentials from three separate categories of authentication factors – typically, the *knowledge*, *possession* and *inherence* categories.

Multifactor authentication dramatically improves security. It is unlikely that an attacker could fake or steal all three elements involved in 3FA, which makes for a more secure log in.

Authentication factors classically fall into three categories:

- Knowledge factors include things a user must know in order to log in: User names, IDs, passwords and personal identification numbers (PINs) all fall into this category.
- Possession factors include anything a user must have in his possession to log in. This category includes one-time password tokens (OTP tokens), key fobs, smartphones with OTP apps, employee ID cards and SIM cards.
- Inherence factors include any biological traits the user has that are confirmed for log in. This category includes the scope of biometrics such as retina scans, iris scans, fingerprint scans, finger vein scans, facial recognition, voice recognition, hand geometry and even earlobe geometry.

Three-factor authentication is mainly used in businesses and government agencies that require high degrees of security. The use of at least one element from each category is required for a system to be considered three-factor authentication -- selecting three authentication factors from two categories qualifies only as two-factor authentication (2FA). An additional factor, location, is sometimes employed for four-factor authentication (4FA).