MULTI-FACTOR AUTHENTICATION

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism:

- **Knowledge:** Something the user and only the user knows
- **Possession:** Something the user and only the user has
- **Inherence:** Something the user and only the user is

TWO FACTOR AUTHENTICATION

Two-factor authentication (also known as 2FA) is a type, or subset, of multi-factor authentication. It is a method of confirming users' claimed identities by using a combination of two different factors:

1. Something they know
2. Something they have
3. something they are.

EXAMPLE: ATM

A good example of two-factor authentication is the withdrawing of money from an ATM, requiring a combination of:

1. **Bank card** (something the user possesses)
2. **PIN** (something the user knows)

FACTORS

KNOWLEDGE FACTORS

Knowledge factors are the most commonly used form of authentication. In this form, the user is required to prove knowledge of a secret in order to authenticate.

A password is a secret word or string of characters that is used for user authentication.

Many multi-factor authentication techniques rely on password as one factor of authentication.

Many secret questions such as "Where were you born?" are poor examples of a knowledge factor because they may be known to a wide group of people, or be able to be researched.

POSSESSION FACTORS

Possession factors ("something the user and only the user has") have been used for authentication for centuries, in the form of a key to a lock.

The basic principle is that the key embodies a secret which is shared between the lock and the key, and the same principle underlies possession factor authentication in computer systems.

A security token is an example of a possession factor. This can be disconnected (RSA SecurID token generator), Connected (device you need to connect), Software token (Google Authenticator on smartphone)

INHERENT FACTORS

These are factors associated with the user, and are usually biometric methods

- Fingerprint
- Face recognition
- Voice recognition
- Iris recognition.

Behavioral biometrics such as keystroke dynamics can also be used.

LOCATION BASED FACTORS

While hard wired to the corporate network, a user could be allowed to login utilizing only a pin code while off the network entering a code from a soft token as well could be required. This could be seen as an acceptable standard where access into the office is controlled.

QUESTIONS