Multi-Factor Authentication

Eugene Davis

UAH Information Security Club

January 10, 2013

What is authentication?

- Authentication is the mechanism to verify the identify of a subject
  - A subject can be either a user, a process, another machine, etc.
  - For example, when you log onto a computer you enter your username (by which you identify yourself) followed by a password (by which you authenticate yourself

What is multi-factor authentication?

- Using two our more factors to authenticate a subject
- Also called Two-Factor authentication
- Increases the level of security by making it harder to spoof a subject
- The factors available are:
  - Knowledge Factors
  - Possession Factors
  - Inherence Factors

Knowledge Factors
"Something you know"

- Includes the most common approach to authentication, passwords
  - PINs are a variation of passwords
- Another approach is to ask questions that only the user would know (challenge-response)
  - An example of this approach is a security question
- Patterns that can be entered onto the device
  - For example, tracing a pattern to unlock an Android phone

Possession Factors

"Something you own"

- Utilizes an object to verify the identity of the subject
  - A simple example would be an ID card
- Better are devices that generate a one time string using strong cryptographic techniques
  - Examples are smart cards, yubikeys, and key chain code generators
  - Even a smart phone can serve this purpose, by receiving a text with a code or using a special application (e.g. Google Authenticator)

Inherence Factors (Biometrics)

"Something you are"

- Relies on a physical aspect of the individual to authenticate them
- Most common are fingerprint scanners
- Generally speaking the worst of the three factors
  - Often they are simple to spoof
  - Simple to obtain by force
  - Since most forms of biometrics work off of images, they are subject to false positives and negatives

Real World Systems Providing Multi-factor Authentication

- Google Authenticator works with your smart phone to improve security for Google accounts and other compatible accounts by providing a one time password
- SmartCards are used in many systems, even many desktop OSs include support for them
- Yubikeys are USB devices which emulate a keyboard to provide one time passwords. Much like Google Authenticator these work on various services configured to use them

Why should I use multi-factor authentication?

- Multiple factors of authentication make harder to compromise accounts
  - A leaked password alone is no longer enough to gain access to an account
- Makes it harder for a user to repudiate their actions
- Especially good for use on important accounts such as banking, email, etc.

Links of Interest

- http://www.whitehouse.gov/omb/e-gov/hspd12_reports
  - Homeland Security Directive 12, includes requirement for two-factor authentication
- https://code.google.com/p/google-authenticator/
  - Google Authenticator, runs on many mobile platforms
- https://www.yubico.com/
  - Yubikey emulates a USB keyboard and integrates with LastPass