Multi-Factor Authentication:

One-Time Password

Overview

Presenter: John Kotolski
HRS Security Officer
Topics

- Why do we need Multi-Factor Authentication?
- Types of Multi-Factor Authentication
- One-Time Passwords (OTP)
- UW Implementation of OTP
Why do we need Multi-Factor Authentication?

Let us have a moment of silence...
Why are passwords failing us?

Attackers are better at collecting passwords.

Attackers are better at cracking passwords.
Remembering Passwords

Tr0ub4dor &3

2^28 = 3 days at 1000 guesses/sec

Difficulty to guess: EASY

Difficulty to remember: HARD

Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
How do we solve this problem?

Password Improvement:  
Make passwords longer and more complex.  

No more please...

Technology Improvement:  
Add additional technology to our current passwords.

Multi-Factor (Strong) Authentication
Types of Multi-Factor Authentication

1. Biometrics
2. One-Time Passwords
3. eToken Certificates
One-Time Passwords (OTP)

- A traditional, static password is usually only changed when necessary.
- Unlike a static password, a one-time password is valid for only one login session or transaction.
- Requires the user to carry a small hardware device (often on a key chain).
UW Implementation of OTP

- Symantec VIP Solution
- Maximized Usability
- Hardware FOB or Mobile Device Options
- Flexible Self-Service Contingency Access
- System to System Portable
Question & Answer