Multi-factor Authentication

Richard Biever
Security Officer & Director of IdM, Duke University

Shilen Patel
Senior IT Analyst, Duke University
What is multi-factor authentication?

• Requires the usage of 2 or more authentication methods.

• Usually including something you know and something you have. For instance a password and a phone.

• Necessary because simply using a password isn’t good enough.
Drivers

• Security (password issues/compromised accounts)

• One size fits all approach (technology OR population) would not work

• Opt-in (consumer-style) OR Role/Data-driven
Technical Approach

• Framework designed to allow multiple authentication methods.
• Each authentication method is given a strength value.
  – A password may have a strength value of one.
  – A phone based factor may have a strength value of two.
• Users and applications may choose requirements.
  – An application may require that all users have to meet a specific strength requirement. An application may also have user specific requirements.
  – A user may require that he meet a higher strength requirement when accessing an application.
• The required strength value for a user to access an application is the maximum of the two requirements.
• The user can use a password along with one or more additional factors.
“Low-hanging fruit” strategy

• Start with the Shibboleth
  – 1100+ on-campus SPs (Service Providers) and growing
  – If we’re careful, most SPs won’t need to do anything and their users won’t notice anything
  – Infrastructure behind the IDP can be reused
  – New apps are largely web-based; older apps continue to grow better web interfaces
New IDP external authmech

- Pluggable interface for custom credential verifiers
- Recognizes different strength values for different credential types
- Computes required strength based on claimed identity and SP making request.
New IDP external authmech

• IDP Login Extensions
  – ajaxy and context sensitive
  – authN options depend on user capabilities and preferences
  – constrained feedback to defeat incremental attacks
New IDP external authmech

- Data repositories for rules and preferences
  - IDP stores mech strength rules locally
  - User data stored in LDAP
  - SP data stored in Grouper. This allows SP owners to easily manage requirements for their users.
Multifactor Progress

- Proof of Concept complete – 2012
- Selection of Duo for 1st “2nd” factor – 2012/13
- Initial pilot Spring 2013 – Summer 2013
  - Opt-in
  - IT Administrators
  - Researchers (protected data)
- Updates to self-service interface and support interface
  – Summer 2013
- 2nd pilot – late Summer 2013
- Production service – Fall 2013 (Shibboleth, VPN, SSH, RDP)
- Future – Databases and ERP Services (PeopleSoft and SAP)
Duo Security

Options for authentication include:

- Duo Push via mobile app
- Passcodes via mobile app
- Passcodes via SMS
- Temporary passcodes
- Phone calls
- Hardware tokens (e.g. YubiKeys®)
Duo Security (continued)

• Integration options:
  – Various APIs
  – SSH
  – RDP
  – VPN
User interfaces

• Self service interface allows users to:
  – Self enroll into Duo.
  – Modify enrollment information.
  – Register hardware tokens.
  – Modify site specific preferences.
  – Retrieve backup codes valid for 72 hours after challenge response verification.
User interfaces (continued)

• SP owners can use Grouper to modify user specific requirements.
• Admin interface allows service desk to impersonate users and modify their information.
• Functionality also allows users to enroll their service accounts.
Demo