Computing Services

Strengthening Authentication

October 2016
ID and password pair is the sole means of authenticating access

- Email
- File storage
- Enterprise applications (including human resource, financial, and student data)
- Sponsored project information (including conflict of interest information)
- Library subscriptions
- Licensed software downloads
IDs and passwords are vulnerable to attack and disclosure

- Attacker use of compromised accounts includes attempts to change employment direct deposit instructions, launch of additional phishing attacks and reconnaissance and exploitation of the university network and computers.
- Identification of root cause for credential loss is often costly. For this reason, root cause is not always determined and metrics are incomplete and under-represented.

The trend in phishing attacks and their success is undeniable.
Significant growth in Phishing attacks and users who fall victim to these attacks requires a substantial increase in work effort.
Current Mitigations

- User awareness via email
- Web content
- Simulated phishing tests
- Published guidelines for securing passwords and computers
- Inbound email filtering
- System and application monitoring
- Timely incident response including:
  - Network and response blocking (where we can)
  - Victim notification
  - Forensic analysis
  - Forced password resets when account compromise is known or suspected

...but it is not enough!
Potential Proactive Tactics

ADDITIONAL AUTHENTICATION FACTOR
Add a factor beyond something that is known and can be easily disclosed.

REQUIRE REGULAR PASSWORD CHANGE
May be less secure overall if users write down or create guessable passwords to remember them.
People are easily tricked into disclosing what they know and they often don’t even remember disclosing the information.

An additional factor, such as something they are (a biometric) or something they have (a smartphone or token) addresses this weakness.
What is Two-Factor Authentication

Requires use of two of the three authentication factors.

Something only the user:
1. Knows (e.g. password, PIN, secret answer)
2. Has (e.g. ATM card, mobile phone, hard token)
3. Is (e.g. biometric – iris, fingerprint)

Most Common Example – Automated Teller Machine

Insert bank card (Something you have)
Provide PIN (Something you know)
Receive money (Access)
TRENDING
Two-Factor Authentication in Industry

Security risks associated with reliance on passwords alone is well known and widely discussed. Based on this risk, a shift to multi-factor authentication is under way in the federal government, across industry and in higher education.

• Consumers are increasingly provided option for multi-factor authentication. Examples: Google 2-step Verification, Facebook login approvals, and Bank of America’s SafePass

• Many colleges and universities have implemented 2-factor authentication.

• There is an opportunity to address gaps in published research on usability and other factors.
DUO Adopters

- Currently 110 organizations have subscribed to the Duo + InCommon partnership.
- Carnegie Mellon is a DUO adopter for certain use cases since March 2016.
DUO EXPERIENCE

1. Log into application that is configured for Duo
2. Sign in with Andrew credentials at login.cmu.edu
3. Prompted for either Duo Push or Duo Token
4. Send Push to phone OR enter passcode
5. Start using application(s)
CURRENT STATUS

1. **IN PRODUCTION** since March 2016
   - Risk Based Roles (~600 users)
   - Mostly System & Application Administrators

2. **IN TEST**
   - Various weblogin-supported applications like Box

3. **IN DEVELOPMENT**
   - Various applications and campus organizations
   - Contact [it-help@cmu.edu](mailto:it-help@cmu.edu) if you would like more information about implementing DUO for your application and organization.
QUESTIONS

Contact it-help@cmu.edu.