TWO-FACTOR AUTHENTICATION PROJECT

A QUICK INTRODUCTION TO 2FA AND ITS USE AT GEORGIA TECH
What is Two-Factor Authentication (2FA)?
Why Two-Factor?
Two-Factor Project Goals
Cas + Duo Project Scope
Project Progress
Project Ahead
Project Considerations
Demo
TWO-FACTOR IS....

SOMETHING YOU KNOW + SOMETHING YOU HAVE
WHAT IS TWO-FACTOR AUTHENTICATION (2FA)?

Computer access control requiring two or more types of authentication factors

1. Knowledge Factor
   • Something you know *(Password/hints)*
   • Typical single factor method

2. Possession Factor
   • Something you own/possess
     – Tokens

3. Inherence Factors
   • Something you are *(Fingerprint(biometric))*

4. Location Factors

5. Time Factors
WHY TWO-FACTOR?

• Because hackers are gonna hack!
• Passwords are not secure
• Successful phishing attacks escalate need for more secure system access
• Administrative Access
  • Data Access Risk
WHY TWO-FACTOR AUTHENTICATION?

• Currently, many critical applications are secured with a single authentication method using CAS
• Early phases of Two-factor Authentication with Duo for specific applications have been successful in limited release
• Institute directive to implement a multi-factor integrated solution on a more comprehensive scale
TWO-FACTOR PROJECT GOALS
TWO-FACTOR PROJECT GOAL

- Maintain the integrity of Institute data and computing resources
- Build a framework for OIT and campus unit resources
- Provide two-factor authentication to faculty, staff, and students
- Leverage familiar access method with added multifactor capability to ease change impact
CAS + TWO-FACTOR PROJECT SCOPE

Slow and Steady!

• First: Experienced Duo users
  • Leverage existing tools for support used today
    – Cas
    – Passport
    – Technology Support Center (TSC)
    – Duo administrators

Identify opportunities for improved deployment in next phase

• President’s Office and Cabinet
• Development Office

Campus Deployment for Administrative Departments in Phases
Deployment has been multi-phased to date:

- **Phase 0**: Campus Multi-Factor Infrastructure and VPN
- **Phase 1**: IT Systems
  - Users Impacted: IT Personnel
- **Phase 2**: Banner Grades
  - Users Impacted: Grade submitters (Limited faculty)
- **Phase 3**: Two-factor VPN for Campus Unit Firewalls
  - Users Impacted: Faculty and Staff
- **Phase 4**: Enforcement of all existing users of two-factor authentication
  - All of OIT
  - Primarily IT personnel on campus
PROJECT AHEAD – NEXT STEPS

Phase 5
• Development Office
• Presidents Office and Cabinet

Phase 6 – forward
• Reflect and improve process
• For 2016
  • Administration and Finance
  • Academic Departments
  • Faculty
  • Students
  • Retirees?

Current Use:
• Approximately over 3800 registered users
In progress

• Self-service enablement methods
• Onboarding process
• Change management
• Out-reach to off campus users
SINGLE SIGN-ON WITH DUO - DEMO

Enter your GT Account and Password
Login requested by: mail.gatech.edu

GT Account: 

Password: 

☐ Warn me before logging me into other sites.

LOGIN  clear

Device: iOS (XXX-XXX-5611)

☐ Duo Push RECOMMENDED

☐ Phone call

☐ Passcode 
Next SMS passcode starts with 1 (send more)

☐ Automatically send a push to XXX-XXX-5611 from now on.

Manage devices  Log in  >
RESOURCES

FAQ’s

https://faq.oit.gatech.edu/security

https://faq.oit.gatech.edu/duo-2fa

https://faq.oit.gatech.edu/content/using-2-factor-authentication-vpn-windows

https://faq.oit.gatech.edu/content/vpn-2-factor-authentication-osx

Related References

http://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821

