Top Ten Applications for MFA in Higher Education

A List initially provided/seeded by Joe St. Sauver, of Internet2 and the University of Oregon

"Top Ten" Applications for MFA in Higher Education

1. Privileged Access ("root", "Admin," "System," or similar privileged access) to large or critical system: examples of such systems include campus ERP systems with financial data or student records; identity management systems; centralized backup systems; DNS servers; DHCP servers; campus web cache boxes, etc.

- Typical job titles of MFA user: system administrator, database administrator, DNS administrator

2. Core Network Devices: "Enable" access to core routers and similar privileged access to other key network devices (including firewalls and other network security appliances with traffic visibility)

- Typical job titles of MFA user: network engineer, network security engineer

3. Physical access to critical facilities [e.g., machine rooms, telecom switch rooms, colo facilities, other high value assets]

- Typical job titles of MFA user: facilities engineer, computer operator, etc.

4. Access to institutional financial accounts (commercial bank accounts, institutional brokerage access, etc.); note that this will typically use a credential specified by the bank, brokerage, etc., not by campus

- Typical job titles of MFA user: campus business officer, portfolio administrator, financial manager

5. Access to HIPAA covered health data (teaching hospital patient records, on campus health center records, testing center records, etc.)

- Typical job titles of MFA user: doctor, hospital/health center administrator, insurance billing specialist, etc.

6. Financial Aid data: because of the Department of Education special push in this area, Financial Aid administrators get a special call out (e.g., Department of Education is pushing 2FA hard tokens to all financial aid admins)

7. High Performance Computing Resources: many so-called supercomputer centers require 2FA after the unfortunate Stakato attacks.

8. VPN access from off campus (punching through a campus perimeter firewall, or accessing a specially sensitive internal network)

9. Campus Messaging (e.g., in an effort to preventing phishing and subsequent spam runs, resulting in widespread phishing)

10. Google (pushed by Google, rather than the campus)

Plus one more (not strictly two factor, think more "alternative factor to traditional passwords"):

11. Automated (machine-to-machine) connections (e.g., for things like scheduled bulk data transfers) [think ssh pre-shared key access]