Problem

Password compromise and identity impersonation continues to be one of the top information security threats on campus. It is well known in the industry that simple password authentication is not effective anymore for verifying identity and enforcing access control. However this type of security control is often the only protection for university high-value assets.

Solution

Implementing Duo multi-factor authentication virtually eliminates the risk of password compromise and identity impersonation by requiring the user to also enter a one-time passcode generated from a device only in their possession (either smartphone app or hardware token) when authenticating to a system. This combination of "something you know" (password) with "something you have" (Duo token) would then require an attacker to steal not only their password but also a physical device in their possession, which is much less likely than password compromise.

How?

- Identify the high-risk systems or high-risk roles within those systems for which multi-factor authentication should be enforced
  - Priority given to roles with access to sensitive "restricted" data or system administrator type roles
- Identify the users in those high-risk roles
  - If using KSAMS for role-based access management, we can produce a report of current role membership
- Provision users with Duo tokens
  - OIT covers user license cost including software token, if user doesn't have smartphone or wants a hardware token for whatever reason, they will need to purchase them via Duo Hardware Token Order Form.
- Configure applications/systems to enforce Duo multi-factor authentication
  - Programmer or system administrator responsibility, currently support native WebAuth (not Shibboleth yet), SSH, RDP, VPN/Radius, LDAP or ActiveDirectory proxy authentication.
  - Protecting Your System Using Duo Multi-Factor Authentication
  - Protecting Your Web Application Using WebAuth And Duo Multi-Factor Authentication