BCNET

Shared IT Services for Higher Education & Research

Conference 2017

Applying Multifactor Authentication to Banner

An update on YubiKey and MFA @ UVic

Presentation Overview

- Introduce the team
- Motivating factors to use MFA
- Recap of YubiKey and MFA at UVIC
- Integration of YubiKey Service
- Systems Architecture
- Industry Best Practices
- Banner INB and MFA
- Working through the Non-technical steps
- Lessons Learned and Next Steps

The team

- Corey Scholefield, Senior Systems Analyst
- Jeff Albert, Senior Systems Administrator
- Mike Cave, Senior Systems Administrator
- Tracey MacNeil, Client Account Manager
- Vugar Mehraliyev, Programmer Analyst

Motivating factors to use MFA

- External Auditors
- Increase in phishing attacks
- Manage risk, protect sensitive data

Recap of YubiKey and MFA at UVIC

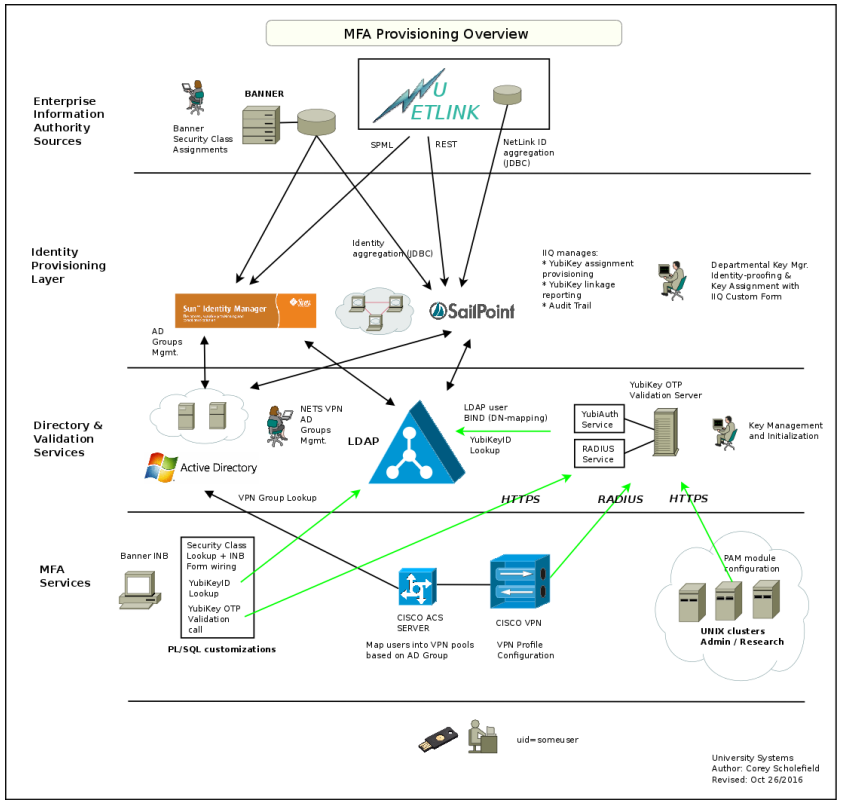
- How we started with MFA
  - UNIX
  - VPN
- Where we are now
  - Banner

Integration of YubiKey Service

- Integration of YubiKey to UVic Systems and Infrastructure

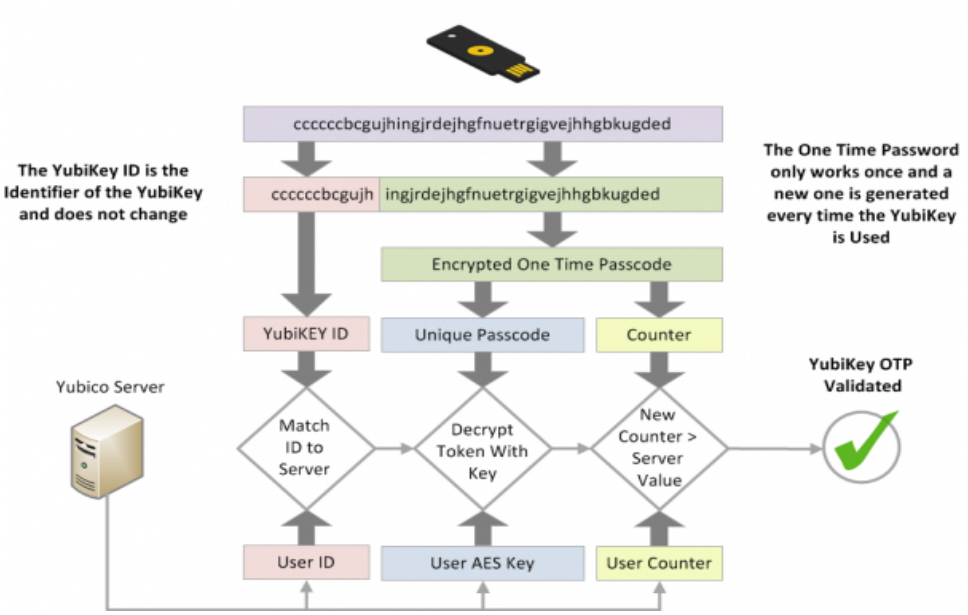
Systems Architecture

- Design a solution to fit with UVic existing systems



Systems Architecture cont'd

- YubiKey and OTP (one-time password)



Systems Architecture cont'd

- Banner INB design
  - an INB form (GUAINIT) MFA proof-of-concept was completed earlier in the project, to accept an OTP, and send it to the YubiKey Validation server for checking
- We needed this process has to work for:
  - Primary NetLink ID holders coming in on the banner.uvic.ca form
  - Primary NetLink ID holders coming in via SSO
  - BANSECR account holders that can only access these INB forms from the banner.uvic.ca site

Industry Best Practices

- Review Gartner professional advice
  - Evaluation Criteria for User Authentication
  - Applying Identity Proofing to Reduce Fraud and Improve Customer Experience
  - *Implementing Strong Authentication Using OTP Tokens and OOB Methods*
- Implementation
  - link to existing directory system – LDAP / AD
- Distribution
  - Cookie Jars and Birthday cakes…
- Application migration
  - Evaluate application readiness

Banner and MFA

- What we did to make it work
  - GUANIT mod
  - Custom database package
- Capitalizing on Banner security – pre-work
  - Banner Objects
  - Banner Security Classes
  - Banner Security Groups
- Audit logging

Working through the non-technical steps

- Buy-in
  - From leadership
  - From IT
  - From clients
- Consider the driving forces to foster adoption
  - Audit compliance – reactive
  - Information Security – risk reduction
  - Fear of compromised data – risk to reputation
- Developing new business processes
  - mapping work to people, procedures and technology
  - Identify who is responsible for what

Lessons learned

- What worked and what we would do differently

Next steps

- Where to go from here?

Questions?

- Corey Scholefield – coreys@uvic.ca
- Jeff Albert – jralbert@uvic.ca
- Mike Cave – mcave@uvic.ca
- Tracey MacNeil – tmacneil@uvic.ca
- Vugar Mehraliyev – vugarm@uvic.ca