Authentication Track

What this is: The OSIdM4HE work has identified "Authentication" as a significant element of an IAM system. Unlike the other areas, a team to look at authentication-related requirements and gaps is still to be convened. This page collects some initial items in this area to invite further discussion and participation, and eventual formation of a subteam and workstream.

Introduction

Higher Education environments are rarely able to rely on a single authentication service or technology to meet all needs. Different business processes often have differing requirements for the overall strength of authentication. For example, campus authentication processes for user access to highly sensitive data are typically quite different from those applied when the same user authenticates to read email and access files stored in personal folders. Likewise, a single technical solution is rarely viable due to the differing strength requirements and, more importantly, the differing authentication assumptions made by application designers. It is still too often the case that the choice of authentication technology is effectively made by the application provider. A likely focus for the CIFER authentication effort will be a design that provides a single back-end support infrastructure that manages the user authentication credential lifecycle and provides, or integrates with, a variety of front-end user and application facing authentication services.

The key work for this effort will be to gain consensus on a a set of feature requirements for authentication services. Once this feature list is complete, we can move forward in a parallel process to:

- Identify existing commonly-deployed open-source tools that provide all or some of the features needed
- Analyze the available tools and determine the gaps between what is available and what CIFER needs
- Specify core services that the authentication subsystem will need from other parts of CIFER.

Levels of Assurance

A fundamental underpinning for user authentication its reliance on the mapping between the physical individual and the identifier used to represent that individual in the electronic world, e.g., the user's login-id. The Identity Proofing process used to perform this mapping and the documentation checked during the proofing process are some of the key factors that determine the Level of Assurance (LoA), i.e., the overall strength of the authentication process. Other important factors include the credential issuing process and credential maintenance services (e.g., password changes and reset).

An early part of the CIFER authentication work should focus on campus use cases to understand what set or sets of LoAs meet the needs of most campuses. This effort will likely be guided by the work done by InCommon on the Bronze and Silver LoAs. These LoAs were, in turn, initially guided by NIST 800-63. A High Assurance LoA, similar to what is anticipated for InCommon "Gold", might also be needed to meet the business needs of the various campus business processes.

A likely first step for the CIFER authentication effort may be to map campus requirements to InCommon LoAs to determine, for example, if the Bronze LoA will meet the needs of the vast majority of campus applications and become the standard assurance level. The use case mapping process will also determine the extent of campus requirements for higher LoAs such as InCommon Silver and the potential need for a strong "Gold" Level of Assurance.

Authentication Technical Components: Back-end Support Infrastructure

The CIFER campus use case process should also be designed to inventory the set of authentication technologies presently in use by campus applications. This list will be used to ensure that the back-end infrastructure is able to support the needed forms authentication services. The use case process will most likely determine that the back-end infrastructure will at least need to support the following types of services:

- Password-based Authentication
  Support of the use of passwords, typically for standard assurance processes including authentication to end systems and the campus SSO environments. These passwords might be held internally in the CIFER system and may need to be provisioned out to other CIFER components or, in some cases, to end systems.

- PKI-based Authentication
  Support for standard assurance authentication where ease of use (e.g., wireless (eduroam) and VPN authentication) and/or anti-phishing (local authentication to campus web SSO environment) are desired.

- 2-Factor Authentication
  USB or stand-alone tokens with a display have been the traditional 2-factor authentication solutions used in campus environments. These devices typically leverage one-time passwords or digital certificates. Newer solutions based on software modules for smart phones (and even SMS messaging) are also available. Depending on technology choices and deployment practices, 2-factor authentication devices are able to achieve Silver and higher Levels of Assurance.

Authentication Technical Components: Application Services

- Support for SAML-based assertions and Federation
- Support for campus Web SSO
- Support for Kerberos/AD
- Support for certificates (e.g., cert revocation, etc)
- Strong 2-factor solutions (e.g., PKI, OTP, SMS, etc)
- Radius support
  - Certificate use cases (wireless, e.g., eduroam)
  - Potentially password-based usage
- Mobile Authentication
  - WebSSO that is mobile friendly
  - Use of digital certificates
- Support for authentication delegation (i.e., portal-style delegation)
  - e.g., SAML-ECP and Shibboleth plugin or CAS

Authentication Technical Components: Identity Proofing, Credential Issuance, and Maintenance

- The binding between the Identity Proofing and credential Issuance
  - One-time secret issued
  - On-site credentialing
- Password Policy Management Enforcement
  - Password strength (entropy) including dictionary, constructor rules
  - Local and remote password reset rule enforcement
  - End user web site for password change (and provisioning selection to remote systems?)
  - Use of CAPTCHAs to help defeat automated attacks on web password change site
- Provisioning to remote systems (and prevention of provisioning certain passwords)
- User notifications of creation/changes to passwords
- Enforcement of any requirement(s) for time or use based password changes
- Provisioning and life-cycle management of digital certificates

Authentication Technical Components: Real-time and Process Auditing

- End user notification of all password changes
- Real time monitoring of AuthN for password guessing attacks
- Logging of all password changes and presumed password guessing attacks
- Temporary delays and semi-permanent password locking on presumed password guessing attacks

Authentication Technical Components: Provisioning to Other Systems

- Ability to securely provision passwords to designated systems
- Ability to enforce policy of password synchronization
  - Explicitly enable synchronization of passwords
  - Explicitly prevent user from using same password

Authentication Policy Components: Mapping Use Cases to LoA Needs

The campus authentication use case effort should yield common sets of application requirements and (hopefully) common expectations for tolerance of risk for these application types. This information could be used to tune the default CIFER settings and inform InCommon Assurance Levels (if any need for update is detected).

Authentication Policy Components: LoA Enforcement Requirements

One likely focus for this area is to create a set of default and vetted policies but help influence the software design such that it is relatively easy for

- Identity Proofing Requirements for differnt LoAs
  - In-person proofing
  - Remote ID proofing

- Password Management (per supported LoA)
  - Password provisioning policy (remote system, etc)
  - Password reset from forgotten password
  - Password strength requirements (e.g., entropy)
  - Time-based password reset requirements

Authentication Service Components Commonly used by the Higher Education Community

- Shibboleth
- MIT Kerberos, Heimdal, and Microsoft Kerberos
- InCommon Certificate Service
- CAS / PubCookie
- FreeRADIUS
- LDAP (e.g., OpenLDAP)
- Microsoft Active Directory

Authentication Functional Model Concepts

account, subscriber

credentials, credential assignment, credential store

authentication service

authentication protocols, federated authentication

password-based authentication

strong authentication, PKI, two-factor, hard/soft tokens

web-redirect-based authentication

password management, key management

monitoring and risk-based authentication

assurance

Authentication System Requirements / Gaps / Opportunities

password management: A collection of utilities dealing with password changing.

- Initial account/password setup
- Web-based user password change: strength meter, dictionary checking, etc
- Web-based user forgotten-password reset: question&answer, SMS, knowledge-based, etc
- Helpdesk-based user password reset: logging, mail trail, etc
- Password policy management: notifications, service shutoff, role-based strength enforcement, etc
- Propagation of changed passwords to multiple credential stores (maybe via standard provisioning)

strong authentication:

- 2- (or multi-) factor: integration of token/SMS/etc schemes into web signon, other authn services (eg Kerberos, AD)
- PKI: cert issuance and management, client tools, policy management, integration, etc etc

risk-based authentication: methods used by large-scale consumer and commercial sites to reduce password theft and abuse.

- Real-time monitoring of authentication service logs looking for guessing, logins from unusual locations, etc
- Use of long-term cookies, net addresses, etc to better identify clients
- CAPTCHAs, email callbacks, etc to respond to monitor-based threats

mobile authentication: Authentication methods tailored to the needs of mobile devices

- Small display size, low bandwidth, non-browser mobile apps all make traditional web signon systems not work well with mobile devices.
- OAuth, other?

process authentication: Authentication methods tailored to the needs of processes and software clients.

- PKI, OAuth, other?
- methods to manage accountability of processes similarly to persons (linkage to registries, orgs)

social identity: social2SAML web authentication gateway

account linking: Tools and patterns for applications to deal with users with many accounts/logins.

eduroam: eduroam is a world-wide federation supporting wireless network access using RADIUS, EAP, and 802.1x technology. eduroam-US is the US participant.

- FreeRADIUS deployment for eduroam-US
- EAP methods and authn infrastructure

non-web federated authentication: Moonshot, SAML-ECP, etc

Commonly-used OS/HE Authentication Service Component Products

MIT Kerberos, Heimdal

CAS, Shibboleth, simpleSAMLphp

LDAP directory (OpenLDAP, etc etc)

FreeRADIUS

(Active Directory)

(anything in PKI? InCommon cert service?)

Other Potential Products

CAS-PM for password management