Identity Assurance Program

Purpose

Introduce identity assurance concepts, motivate the need for identity assurance support in UW IAM services, describe existing services and planned work.

Identity Assurance

Some information resources and applications are public: anyone with network access can see the resources and interact with the applications. Other resources are protected: access to read, update, or other operations is restricted by policy to authorized users or processes. Traditionally access to resources has been administered via accounts local to the resource or application. The resource administrator engaged the users, created the accounts, assigned the passwords, set up permissions, removed accounts when no longer needed, etc. Each resource or application administrator could decide how much effort to put into these activities to meet the security needs of their system within their security budget.

Today, in response to the common needs of thousands of institutional applications, account management has become an institution-wide service called identity management. The term "identity", rather than "account", expresses the importance of individuals rather than systems, and the emphasis on managing multiple relationships and characteristics useful in access control. Resource and application administrators rely on institutional identity management services as a key part of controlling access, and generally appreciate the benefits of doing so. But administrators still have their own requirements for how accounts are managed to access their systems, perhaps based on local policies or external compliance regimes. They need to have confidence that the identity management services on which they rely (which may be many different services, in the case of federated applications) are meeting those requirements.

"Identity assurance" is the component of an identity management service that clarifies the processes and controls, both business and technical, that are used to guarantee the accuracy and security of identities used for resource access. An identity assurance program provides a framework for the alignment of organizational identity management practices and the needs of resource and application owners and users. Institutions of all kinds are developing formal identity assurance programs to meet the needs of external service providers relying on federated access, where considerations of liability between organizations are significant. As intra-institutional applications increasingly are obliged to meet external compliance rules, identity assurance is useful internal to the institution as well.

There are many factors related to identity assurance that might be of concern to policy-makers relying on identity management services. They fall generally into these categories:

- The maturity and effectiveness of the organization operating the identity management services.
- The business processes used to ensure that user entries in the service are accurate, that user identifiers and credentials (such as passwords) are assigned securely, and that users know their rights and responsibilities.
- The technical elements that support secure operation of authentication and other services and protect the system from technical attacks.

One principle of an institutional identity management program is that one size does not fit all. Some resources are very sensitive and require high-quality, expensive identity management processes and methods (for example, hardware token-based authentication). Other resources and applications must provide access to hundreds of thousands of users and cope with remote users and those with only a casual contact with the institution. Identity management services must scale in strength and breadth to meet these varying requirements; identity assurance concepts provide the necessary framework for this to happen coherently. See NIST Special Publication 800-63, "Electronic Authentication Guideline", for a widely-used identity assurance framework.

Identity Assurance Program Vision

The UW IAM identity assurance program must support these broad identity management goals:

- meet identity assurance needs of most systems with practices based on industry and peer-institution standards;
- meet detailed requirements of some systems, such as higher assurance to protect sensitive resources, or efficient outreach to large populations;
- be cost-effective, in particular using expensive higher-assurance practices only in those cases that need them.

Supporting these goals implies these elements in the assurance program:

- a limited menu of assurance choices, based on well-defined "assurance profiles"
- technical implementation of assurance procedures and profiles in the identity management system
- documentation to support assessment, decision-making and integration by customer organizations
- collaboration with partners in the assurance process, in particular business systems that are sources of identity information (primarily HR and student) to ensure conformance
- formal certification of compliance with relevant assurance standards (e.g. the InCommon Identity Assurance Framework)

Program Status

Formal identity assurance in the UW IAM service set is in an early stage. A range of assurance-related services is available today:

- Mainstream UW IAM services and UW NetID practices are meeting the needs of thousands of UW academic and business applications and organizations every day.
- A token (aka two-factor) authentication service provides higher-assurance authentication for applications that choose to use it.
- Low-assurance UW NetID management is available to support uses such as wireless network authentication and conferences.
- The Sponsored UW NetID Service supports both high- and low-assurance identity proofing procedures for users outside of the usual populations (faculty, staff, students, alumni, medical).
- Applications have the ability to check the age of a UW NetID password and make access decisions using this information (e.g. requiring the user to change their password if it is too old).

Specific work supporting defined identity assurance and compliance includes:

- In 2005, the UW NetID service underwent a trial assurance assessment by the US Government General Services Administration, using the US E-Authentication Program Credential Assessment Framework (CAF). The UW was one of only three universities to participate.
- In 2008, UW IAM conducted an in-house assessment of the UW NetID service using the InCommon Assurance Profile framework, to meet the assurance requirements of the Fred Hutchison Cancer Research Center.

Work is in progress in these areas:

- An assessment of assurance regarding the undergraduate student identity lifecycle, reflecting recent changes in UW NetID setup procedures for this population.

Work is needed to address these issues (this list is representative but incomplete):

- Documentation of identity management system procedures (e.g. change management in server operations) in support of audit and customer needs.
- Technical methods for tracking assurance status of individuals and making status accessible to applications.
- Analysis of alignment of UW business needs and support capabilities with the InCommon Identity Assurance Framework and any other applicable regimes.
- Reconciliation of identity proofing practices in HR and student areas to applicable standards.
- Differentiation in password policy to support lower-assurance populations such as alumni.
- Formal assessment and audit for certification via the InCommon Identity Assurance Framework and any other applicable regimes.
- Remediation of any technical gaps in identity management procedures, e.g. password lifetime.