Listening Session
Guidelines for Authentication

Passwords, Passphrases and Multi-Factor Authentication

Authentication Design Considerations

- What is the data?
- Accessing one's own information
- Accessing the information of others
- Accessing research data
- Legal or regulatory considerations
- Affiliation with campus
  - Status of employment
  - Status of student
  - Other affiliations
- Integrity of administrative processes
  - Submitting grades
  - Approving payments
  - Enrolling students
  - Submitting coursework
  - Creating new employees
  - Managing research grants
- Usability by end-users (claiments)

UW-Madison Data Classifications

Restricted:

Data should be classified as Restricted when the unauthorized disclosure, alteration, loss or destruction of that data could cause a significant level of risk to the University, affiliates or research projects.

Sensitive:

Data should be classified as Sensitive if the loss of confidentiality, integrity or availability of the data could have a serious adverse effect on university operations, assets or individuals.

Internal:

By default, all Institutional Data that is not explicitly classified as Restricted, Sensitive or Public data should be treated as Internal data.

Public:

Data should be classified as Public prior to display on web-sites or once published without access restrictions; and when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates.

https://data.wisc.edu/data-governance/

Terminology

Authentication: The process of verifying that someone who holds an account on an IT system is who they purport to be.

Claimant: A subject (e.g. person, process, or thing) whose identity is to be verified using one or more authentication protocols.

Entropy: A measure of the amount of uncertainty an attacker faces to determine the value of a secret. Entropy is usually stated in bits. A value having n bits of entropy has the same degree of uncertainty as a uniformly distributed n-bit random value.

Credential: An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber (e.g. NetID).

Authenticator: Something the claimant possesses and controls that is used to authenticate the claimant's identity (e.g. Password).

Assertion: A statement from a verifier to an RP that contains information about a subscriber. Assertions may also contain verified attributes (e.g. Alumni).

Terminology Expanded: Authenticators

Password: A character string intended to be memorized or memorable by the user (claimant), permitting the user to demonstrate something they know as part of an authentication process.

a52X79*1Z

Passphrase: A passphrase is sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is similar to a password in usage, but is generally longer for added security.

TheLong&WindingRoad

One-Time-Password: A character string provided to be used once during a short period of time.

https://howsecureismypassword.net/

Single-Factor and Two-Factor Authentication

Single-Factor

Username plus select from one of the following:

- Password
- Passphrase
- One-Time-Password

Two-Factor

Username Plus:

- Password or Passphrase

 - AND -

- One-Time-Password

Discussion Topics

For Users (Claimants)

1. How many systems do you sign into each day?
2. How do you manage passwords for your university accounts and personal accounts?
3. What are the problems with passwords?
4. Do you use an account that is shared by others?

For Technical Administrators

1. How are password controls implemented?
2. How are accounts created and removed when there is a change in user status?
3. What controls can you implement to address Man-In-The-Middle attacks?

Send thoughts and questions to:

grc-cybersecurity@cio.wisc.edu