MSS Lunch & Learn Series

YALE-MSS-9: Authentication and Authorization

Dan Tinari
James Tucciarone III

October 2024

What are the MSS?

Yale *Information Security*

- The Minimum Security Standards (MSS) are baseline requirements for securing Yale IT Systems based on risk.

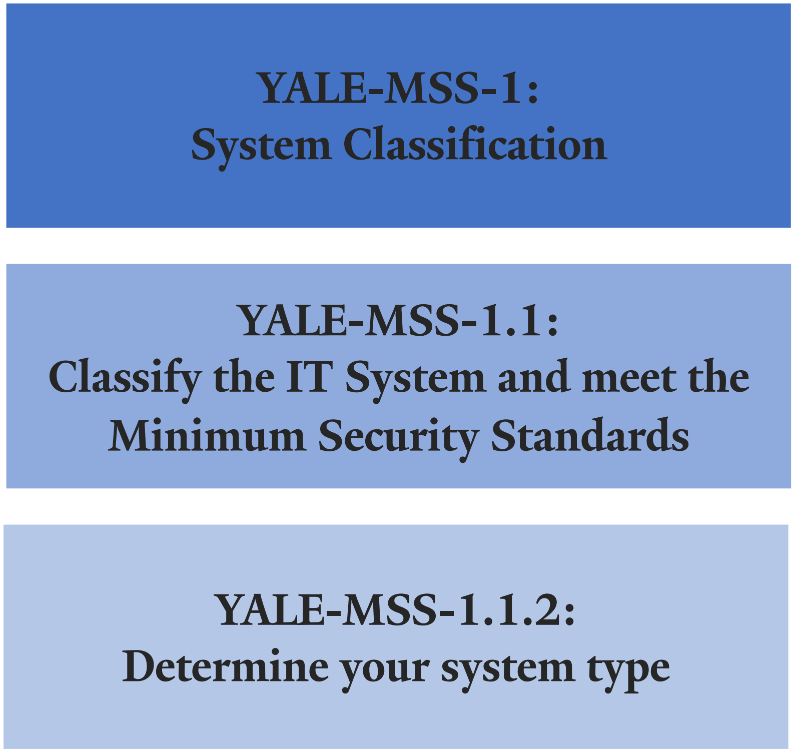
- The MSS apply to any Yale IT System that uses Yale data and/or operates in support of Yale's mission.

Understanding the MSS

Yale *Information Security*

The MSS are broken down into:

- Standard Groups (YALE-MSS-X): These group standards together based on cybersecurity requirements.
- Standards (YALE-MSS-X.Y): Standards tell us we must do to meet that cybersecurity requirement at Yale.
- Controls (YALE-MSS-X.Y.Z): Controls provide details on how you can meet the cybersecurity requirement.



YALE-MSS-1:
System Classification

YALE-MSS-1.1:
Classify the IT System and meet the Minimum Security Standards

YALE-MSS-1.1.2:
Determine your system type

YALE-MSS-9: Authentication and Authorization

Yale *Information Security*

- Authentication vs Authorization
  - **Authentication** – Verifies the identity of a user, process or device
    - Ex: When you go through airport security, you show your ID to authenticate your identity
  - **Authorization** – Determines a user's level of access and grants access based on that level
    - Ex: When at the airport and you arrive at the gate, you present your boarding pass to show which flight you are allowed to get on
- Both authentication and authorization are vital to secure enterprise systems, applications, and data. Authorization always comes after authentication.

Do not share account credentials (username/password)

- User accounts are defined as a username and password that grants an individual end-user access to Yale resources. For example, your Yale Net ID is your user account to access Yale resources that use CAS for authentication.

- Users are responsible for maintaining the security of their own accounts and passwords to Yale resources.

- Keep your passwords private. Do not share them with anyone including your supervisor, family, co-workers, or IT support provider.

- If your password is discovered or you determine that someone is using it to access your account, contact the Information Security Office (ISO) at information.security@yale.edu.

Utilize secure passwords for authentication

- Password complexity
  - Use a long password (8-127 characters)
  - Use diverse compositions including uppercase, lowercase, numeric and special characters
  - Use a passphrase. Example: myMottoIsLuxetVeritas!Yesitis!^3!
- Change all account passwords from defaults
- Align (or surpass) password security of the current requirements for Net ID credentials (Password Cleanup initiative)
- Lock mobile devices with a password, passcode or pin
- We prohibit Passwords from being reused during a password change
- Do not reuse passwords for different logins

Grant privileges to IT Systems and data according to the principle of least privilege

- The principle of least privilege
  - A concept used to minimize access to data and systems. This standard ensures that we grant access to Yale Data and IT Systems, only to those who need it to perform a function.
  - For example, a user account is only granted the access needed to perform their routine work. Access is not granted beyond their routine or daily responsibilities.
  - Storage shares – single file vs entire share

- To apply this standard, consider the following:
  - Identify a responsible individual for managing account access to resources
  - Maintain an inventory of all access to each resource
  - Periodically review all accounts with access to a system to ensure least privilege is applied

Deprovision accounts and access when roles & responsibilities change

Yale *Information Security*

- Ensure accounts are deprovisioned or altered to reflect necessary access when an individual’s role or responsibilities change, or a user leaves Yale
- Shared service account passwords should be renewed on a routine basis or when an individual who knew the credentials no longer needs access to the account
- Identify dormant accounts and remove them on a regular basis
- Create and utilize Onboarding and Offboarding checklists

Require Multi-Factor Authentication (MFA) for access to authenticated systems

Yale *Information Security*

- Multi-Factor Authentication (MFA) is a security method that requires users to provide more than just a password to log in to an account
- Web applications should use Yale's approved single sign on (SSO) methods that provide MFA -- CAS, Shibboleth, Entra AD.
- Yale uses Duo MFA and new NetIDs are automatically enrolled
- MFA helps prevent unauthorized access to accounts and data by making it more difficult for attackers to gain access. Even if a cybercriminal obtains a user's password, they still can't access the account without another form of verification.

Prevent brute force attacks

- Brute-force guessing at user credentials is an easy and common method of attackers

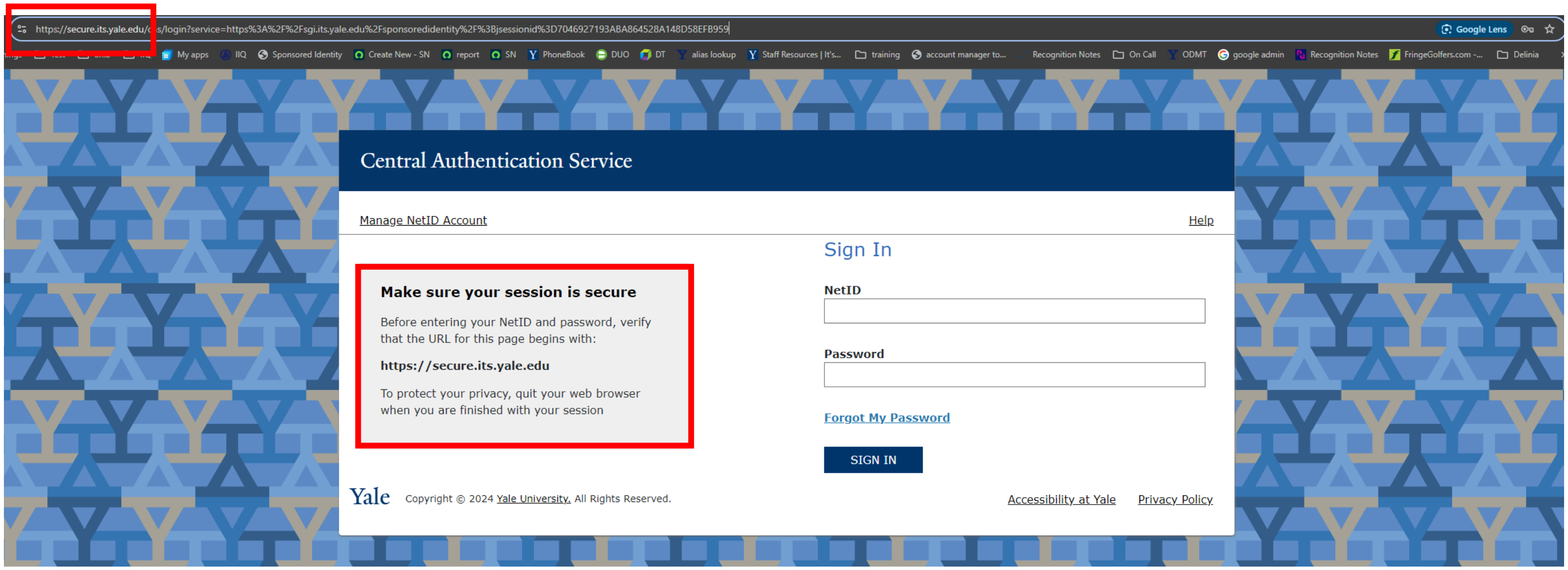
- How do we prevent this?
  - Rate limiting and temporary lockouts are effective ways to thwart automated, rapid-fire password guessing from an attacker.

    - Rate limiting – limits the number of invalid login attempts in a period of time
      - Yale allows 15 invalid attempts against Active Directory, CAS, Shibboleth and Entra
      - iPhone – 10 attempts
    - Temporary lockouts
      - Yale Logins – 10-minute lockout
      - iPhone – duration extends with additional incorrect login attempts
        - Settings can be changed including option to erase data

Allow only encrypted network protocols for authentication

Yale *Information Security*

- Https://
  - Hyper-Text Transfer Protocol Secure – Encrypts data sent between a web browser and web server



Central Authentication Service

Manage NetID Account

Help

Make sure your session is secure

Before entering your NetID and password, verify that the URL for this page begins with:

https://secure.its.yale.edu

To protect your privacy, quit your web browser when you are finished with your session

Sign In

NetID

Password

Forgot My Password

SIGN IN

Yale Copyright © 2024 Yale University. All Rights Reserved.

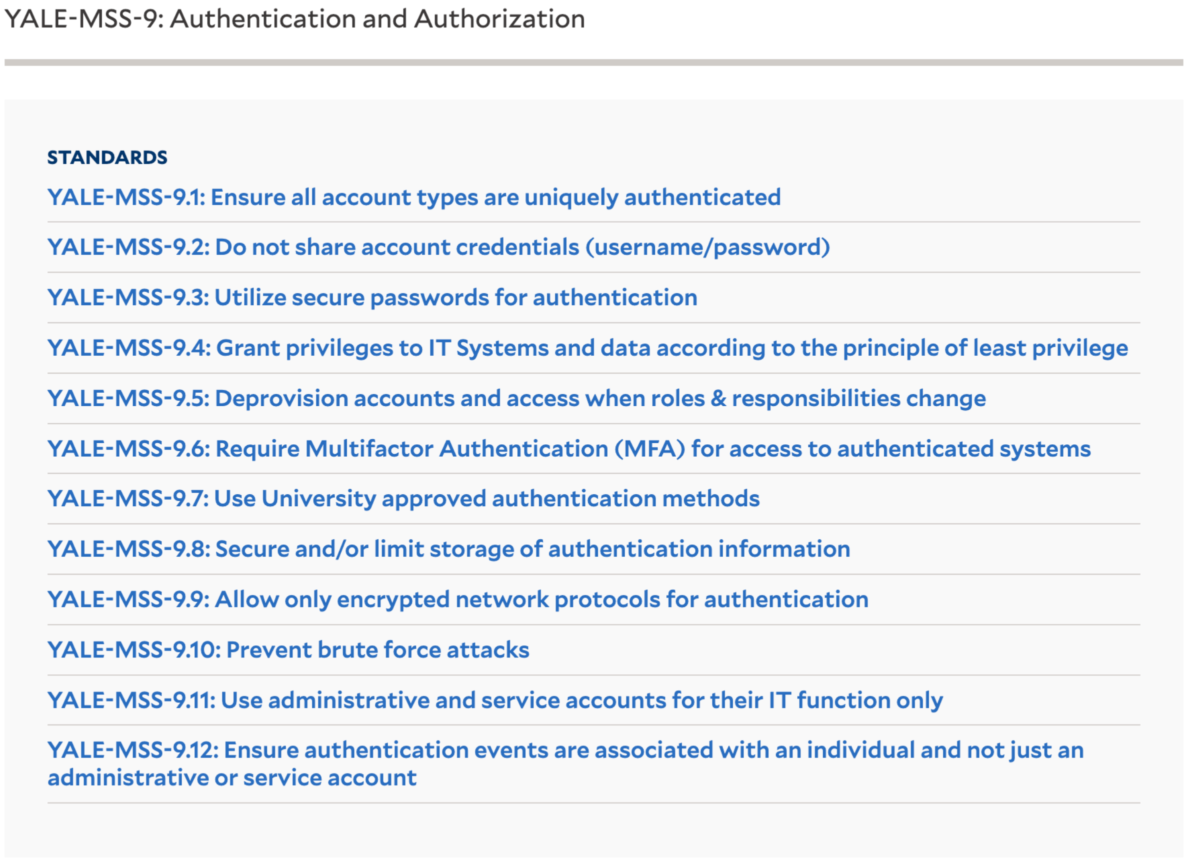
Accessibility at Yale Privacy Policy

Use administrative and service accounts for their IT function only

- Administrative accounts
  - A username and password that grants an individual privileged access to the IT System. Privileged access is access to make changes to the overall IT System.
- Service accounts
  - Special user accounts that an application, service or system uses to interact with the operating system. These types of accounts are typically used for automation between systems.
- Ensure authentication events are associated with an individual and not just an administrative or service account
  - These accounts should never be used to login to a personal workstation
  - Users should login to devices with their individual accounts (their own NetID) and only use Administrative / Service when elevate privileges are needed to perform a specific task.

Q&A

Yale Information Security



YALE-MSS-9: Authentication and Authorization

STANDARDS

- YALE-MSS-9.1: Ensure all account types are uniquely authenticated
- YALE-MSS-9.2: Do not share account credentials (username/password)
- YALE-MSS-9.3: Utilize secure passwords for authentication
- YALE-MSS-9.4: Grant privileges to IT Systems and data according to the principle of least privilege
- YALE-MSS-9.5: Deprovision accounts and access when roles & responsibilities change
- YALE-MSS-9.6: Require Multifactor Authentication (MFA) for access to authenticated systems
- YALE-MSS-9.7: Use University approved authentication methods
- YALE-MSS-9.8: Secure and/or limit storage of authentication information
- YALE-MSS-9.9: Allow only encrypted network protocols for authentication
- YALE-MSS-9.10: Prevent brute force attacks
- YALE-MSS-9.11: Use administrative and service accounts for their IT function only
- YALE-MSS-9.12: Ensure authentication events are associated with an individual and not just an administrative or service account