Password Management Guidance

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of UAEX's resources. All users, including contractors and vendors with access to UAEX systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this guidance is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this guidance includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any UAEX facility, has access to the UAEX network, or stores any non-public UAEX information.

General Guidance

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least every 6 months.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

Passwords must not contain the user's entire samAccountName (Username) value or entire displayName (Full Name) value. Both checks are not case sensitive:

- The samAccountName is checked in its entirety only to determine whether it is part of the password. If the samAccountName is less than three characters long, this check is skipped.

- The displayName is parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, the displayName is split and all parsed sections (tokens) are confirmed not to be included in the password. Tokens that are less than three characters in length are ignored,

and substrings of the tokens are not checked. For example, the name "Erin M. Hagens" is split into three tokens: "Erin," "M," and "Hagens." Because the second token is only one character long, it is ignored. Therefore, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password.

Our Minimum Requirements:

- Minimum Password Length 8
- Maximum Password Length 30
- Must not contain the user's account name or parts of the user's full name
- Contain characters from each of the following categories:
  - Uppercase letters (A - Z)
  - Lowercase letters (a - z)
  - Numbers (0 - 9)
- No special characters allowed
- Password not used the past 6 times
- Maximum Password Age 90 days
- Account Lockout Threshold 10 invalid attempts
- Account Lockout Time 20 minutes *(except for HR)*

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R" or "Tmb1W2r" or some other variation.

(NOTE: Do not use either of these examples as passwords)

Password Protection Standards

- Always use different passwords for UAEX accounts from other non-UAEX access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various UAEX access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for email authentication access.
- Do not share UAEX passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential UAEX information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the Information Technology Security Group.

- Always decline the use of the "Remember Password" feature of applications (e.g., Eudora, OutLook, Internet Explorer).

If an account or password compromise is suspected, report the incident to the Information Technology Security Group or the Call Center immediately.

Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Shall support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval wherever possible.

Use of Passwords and Passphrases for Remote Access Users

Access to the UAEX Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.