UNT System Password Standards

Overview

Passwords are a critical control used to control access and protect the confidentiality, integrity, and availability of institutionally owned information and information resources. This standard establishes the minimal requirements for passwords, a heuristic for measuring the strength of a password authentication system, and best practices and procedures for the management of passwords.

Password Construction Guidelines

The minimum password construction standards are as follows:

Password Dimension	Standard
Minimum Length	8 characters
Maximum Length	30 characters
Complexity	Must contain uppercase letters, lowercase letters and digits.
Prohibited Characters	Space and Backslash
Password Reuse (History)	Users cannot use the last 8 passwords.
Prohibited Passwords	Common dictionary words are prohibited.
Character Set	93 ASCII printable character set excluding space and backslash.
Password Strength (NIST SP800-63-2)	20 bits

Passwords must meet or exceed these standards for all systems owned or managed by the UNT System and Institutions. The UNT System ISO may grant an exception if a system is unable to accommodate these standards.

Password Reuse

Credentials used for UNT System or Institution owned information resources must not be reused on other systems or services.

Password Expiration

Users must change passwords at least annually. The password expiration period may be shorter for some systems based on business or compliance needs. The UNT System ISO may grant an exception if a system is unable to accommodate these standards.

Special Considerations for Shared and Generic Privileged Accounts

The use of shared or generic privileged accounts, such as Administrator or root, should be avoided if possible. These accounts should only be used for maintenance, system repair, or recovery operations.

They should not be used for day to day operation. The credentials for any system or generic account should be changed from the default value supplied by the vendor before the system is placed in a production capacity or is put on a public network. Credentials for generic privileged accounts for system critical to business operations must be escrowed with the system administrator's supervisor and backup personnel. Passwords for shared or generic privileged accounts must be changed when any employee with access to the credentials leaves the organization or changes roles within the organization. This should be done before the employment change occurs if possible to ensure the confidentiality, integrity, and availability of the information resource tied to the credentials.

Measurement of Password Strength

NIST SP800-63-2 (Electronic Authentication Guideline) provides an entropy based heuristic for measuring the strength of a given password. Entropy is a measurement of the amount of information contained within a string of characters such as a password. The authors of the NIST document suggest that a user selected password will not have as much entropy as a randomly selected password from the same alphabet. The authors suggest the following heuristic to estimate the amount of entropy in an unknown user selected password (pp. 103-107).

- The entropy of the first character is taken to be 4 bits.
- The entropy of the next 7 characters are 2 bits per character.
- For the 9th through the 20th characters, the entropy is taken to be 1.5 bits per character.
- A "bonus" of 6 bits of entropy is assigned for a composition rule that requires both upper case and non-alphabetic characters. This forces the use of these characters, but in many cases these characters will occur only at the beginning or the end of the password, and it reduces the total search space somewhat, so the benefit is probably modest and nearly independent of the length of the password;
- A "bonus" of up to 6 bits of entropy is added for an extensive dictionary check. If the Attacker knows the dictionary, he can avoid testing those passwords, and will in any event, be able to guess much of the dictionary, which will, however, be the most likely selected passwords in the absence of a dictionary rule. The assumption is that most of the guessing entropy benefits for a dictionary test accrue to relatively short passwords, because any long password that can be remembered must necessarily be a "pass-phrase" composed of dictionary words, so the bonus declines to zero at 20 characters.

References

- *NIST Special Publication 800-63-2: Electronic Authentication Guideline*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

Version History

Version	Approved By	Date	Description
1		6/20/2013	Original Document
2	Rama Dhuwaraha	6/10/2016	Complete Revision Author: Richard Anderson