

Old Dominion University Computer Science Department Policies and Procedures

Title: Password Policy

ID: CSS005

Revision: 1.0

Purpose

This procedure provides guidance on how passwords are stored and updated for the Computer Science Department.

Scope

This procedure applies to all Windows and UNIX accounts for the Computer Science Department.

Windows Password Storage

Windows passwords are stored in two Active Directory (LDAP) databases on two Windows Server 2008 R2 servers. These two machines are completely inaccessible from outside CS domain and selectively accessible from inside CS. Only staff users are authorized to logon to these two servers. Passwords are one-way encrypted via NTLM.

UNIX Password Storage

UNIX passwords are stored on two Solaris 10 NIS servers. These servers are not accessible from outside CS domain to any user and are only accessible inside CS to staff users. Passwords are one-way encrypted via the UNIX crypt function which is based on the DES algorithm. Users should note that password hashes for all UNIX users are publicly available (to any authenticated user) via the ypcat command so weak passwords may be easily cracked. Users should exercise strong password complexity when setting their UNIX password. See <http://www.cs.umd.edu/faq/Passwords.shtml> for directions on creating secure passwords.

Resetting Passwords

If a user knows his or her current Windows password, he or she can change it to a new password themselves. After logging on to a computer lab machine or VCLab, press CTRL-ALT-DEL to change your password.

If a user knows his or her current UNIX password, it can be easily reset. Simply ssh to any of the fast aliases or fast.cs.odu.edu and run the `passwd` command.

If the user does not know or cannot remember their current Windows or UNIX password, the following link can be used to reset BOTH passwords to a default format:

<https://sysweb.cs.odu.edu/online/index.php?action=resetpw> If the user does not have a UIN, he or she must send an email to root@cs.odu.edu to have the password reset. The user will receive a response in less than 24 hours which contains the new password. THE USER SHOULD IMMEDIATELY CHANGE THE PASSWORD AFTER RESET. The default password is inherently insecure.

Definitions

VCLab: The "Virtual" Computing Lab which can be accessed through remote desktop at vclab.cs.odu.edu

SSH: The protocol most commonly used by users to connect to our UNIX machines and clusters. Use PuTTY or `ssh` to use SSH from Windows.

One-way encryption: A form of encryption that is computationally irreversible.

Password hash: The form a password takes after it is one-way encrypted. The only way a password can be obtained from any hashes at the CS department is through brute-force cracking and social engineering.

UNIX Crypt function: The one-way encryption our UNIX machines use to secure passwords. While this technique is not the most secure available, it is still considered sufficient by security professionals.

NTLM: The Windows encryption technique the CS Department uses to store Windows passwords. It is the successor to the weaker LanMan algorithm.

Revision History

02/07/2011 - Rev 1.0 Pending approval by Ajay Gupta