Bradley W. Goldstein
CSG256 – Security, Privacy, and Usability
Professor Simson L. Garfinkel
Northeastern University
May 25, 2004

Assignment 4 – Password Catalog

PASSWORD CATEGORIZATION

The following report discusses the various passwords personally used either to gain access to various resources or to authenticate identity for the purpose of some transaction. My passwords can be divided into the following categories:

Category	Approximate Number of Passwords
Computer / Hardware / Network Access	10
Email Account	5
Personal Finance	10
Website Administration	5
Miscellaneous Website / Application	90

Computer, Hardware, and Network Access passwords consist of Windows logon passwords and Linux / UNIX account passwords for standalone personal computers and for domains at various companies for which I have worked. This category also includes passwords for administering hardware devices such as gateways and routers.

Email Account passwords include all free online email accounts, as well as the Post Office Protocol (POP) account passwords for my personally owned email address and passwords for Northeastern University email accounts.

Personal Finance passwords are all the account passwords for accessing services through the websites of financial institutions at which I have accounts, such as various banks and credit card companies. Personal Finance would also include Automated Teller Machine (ATM) pins and in some cases personal information like "Mother's Maiden Name" that is often used to verify identity over the phone or online.

Website Administration passwords consist of File Transfer Protocol (FTP) accounts that can be used to access the file directories on various web servers. Also, this category includes passwords used to access website administration features through a third party host's website.

The **Miscellaneous** category is reserved for the many passwords that I possess for shopping-websites, free electronic communication services like Instant Messaging, and other administrative sites.

Individual Password Characteristics and Restrictions

Since there are too many passwords to consider them all, I have selected several important examples and diagramed each password's characteristics in the following table:

Account	Password Type	Method of Submission	Restriction(s)
Windows Logon Account (Standalone PC)	Alphanumeric String	I/O device (keyboard) directly attached to local PC	• Windows XP: 1 – 127 characters • Windows 95/98: 1 – 14 characters • Case sensitive
Red Hat Linux Root Account (Standalone PC)	Alphanumeric String	I/O device directly attached to local PC	• At least 6 characters • Case sensitive • `passwd` program prevents easily guessable passwords
Northeastern University myNEU Account (used for @neu.edu email access)	Alphanumeric String	I/O device attached to computer user is working on at the time, then transmitted over the Internet	• 6 – 14 characters • Case sensitive
An Online Bank Account	Alphanumeric String	I/O device attached to computer user is working on at the time, then transmitted over the Internet	• 6 – 32 characters • Must have at least 1 letter and 1 number • No special characters (e.g. # or %)
A Standard Bank Account (Password is ATM Pin)	Numeric String	I/O device (keypad or touch screen keypad) directly attached to ATM machine	• 4 digits • Must accompany verifiable token (ATM card)

Recommendations for Password Authentication System Development

Users always seem to choose passwords that are easy to remember and easy to type, and often sacrifice security for usability. Therefore, developers must restrict the characteristics of a user's password to the highest degree possible, so that users are unable to select easily breakable passwords. This would include requiring some combined use of uppercase, lowercase, numbers, and punctuation. It would also involve checking password strings with various algorithms to determine how easily it is to decrypt and/or guess using brute force.