Hacker Highschool
SECURITY AWARENESS FOR TEENS

LESSON 11
PASSWORDS

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

Contributors

Kim Truett, ISECOM

Chuck Truett, ISECOM

J. Agustín Zaballos, La Salle URL Barcelona

Pete Herzog, ISECOM

Jaume Abella, La Salle URL Barcelona - ISECOM

Marta Barceló, ISECOM

11.0 Introduction

One of the principal characters in The Matrix Reloaded is the Keymaker. The Keymaker is critically important; he is protected by the Matrix and sought by Neo, because he makes and holds the keys to the various parts of the Matrix. The Matrix is a computer generated world; the keys he makes are passwords. Within the movie, he has general passwords, back door passwords and master keys – passwords to everywhere.

Passwords are keys that control access. They let you in and keep others out. They provide information control (passwords on documents); access control (passwords to web pages) and authentication (proving that you are who you say you are).

11.1 Types of Passwords

There are three main types of passwords.

11.1.1 Strings of Characters

At the most basic level, passwords are stings of characters, numbers and symbols. Access to a keyboard or keypad allows entry of these types of passwords. These passwords range from the simplest – such as the three digit codes used on some garage door openers – to the more complicated combinations of characters, numbers and symbols that are recommended for protecting highly confidential information.

11.1.2 Strings of Characters plus a token

The next level in passwords is to require a string of characters, numbers and symbols plus a token of some type. An example of this is the ATM, which requires a card - the token - plus a personal identification number or PIN. This is considered more secure, because if you lack either item, you are denied access.

11.1.3 Biometric Passwords

The third level in passwords is the biometric password. This is the use of non-reproducible biological features, such as fingerprints or facial features to allow access. An example of this is the retinal scan, in which the retina – which is the interior surface of the back of the eye – is photographed. The retina contains a unique pattern of blood vessels that are easily seen and this pattern is compared to a reference. Biometric passwords are the most sophisticated and are considered 'safer' but in reality a password that you 'carry' in your finger or eye is no safer than a strong password that you carry in your head, provided that the software that uses the password is correctly configured.

11.2 History of Passwords

Trivia in Password History:

In older versions of MS Excel and Word, passwords were stored as plain text in the document header information. View the header and you could read the password. This is valid for all versions older than Office 2000.

Windows once stored passwords as plain text in a hidden file. Forget your password? You could just delete the hidden file, and the password was erased.

Early on, Microsoft and Adobe both used passwords to mean that a file was password protected when opened with their applications. If you opened it with another application, such as Notepad, the password wasn't necessary.

Microsoft Access 2.0 databases could be opened as a text file easily by just renaming them with a ".txt" extension. Doing this allowed you to see the database data.

Adobe PDF files in versions 4.0 and older were printable and often viewable using Linux PDF readers or Ghostview for Windows.

Wireless networks have a problem with encryption as the key for the encryption can be guessed once you collect enough encrypted data out of the air to find the patterns and guess the keys. With todays computing power in the normal home, the key can be cracked almost immediately to find the password.

Bluetooth security is considered very secure, once it is setup. The problem is that bluetooth transmits a unique, freshly generated, password between the devices to establish the connection and the password is sent as plain text. If that password is intercepted, all future transmissions for that session can be easily decoded.

Exercise:

Download a PDF file off the Internet and try opening it with other programs. How is the data viewable?

11.3 Build a Strong Password

The best passwords:

- ✔ cannot be found in a dictionary
- ✔ contain numbers, letters and those odd swear symbols on top of the numbers
- ✔ contain upper and lower case letters
- ✔ the longer the "stronger"

With a 2 letter password, and 26 letters in the alphabet, plus 10 numbers (ignoring symbols), there are 236 possible combinations (687,000,000 possibilities). Increase the password length to 8 characters, and there are 836 combinations (324,000,000,000,000,000,000,000,000,000,000 possibilities).

There are many password generators available on the internet, but these will generate a nearly impossible to remember password.

Try instead to use a seemingly random string of letters or numbers that you can easily recall.

For example:

gandt3b! (goldilocks and the 3 bears!)

JJPL2c1d (john, jill, paul, lucy, 2 cats, 1 d – the members of your household)

Exercises:

1. Create a strong password, **that you could remember** that scores well at the following web page: http://www.securitystats.com/tools/password.php
2. Look at the Web pages for three different banks and find out what type of password is needed to allow an account holder to access restricted information. Do the banks also offer recommendations that would lead users to create strong passwords?

11.4 Password Encryption

People don't usually discuss password encryption, because there seems to be no options to discuss – passwords are, by definition, encrypted. While this is usually true, encryption is not a simple yes or no proposition. The effectiveness of encryption, usually described as its *strength*, ranges from very weak to extremely robust.

At its weakest, we have passwords that have been simply *encoded.* This produces a password that is not readable directly, but, given the key, we could easily translate it using a computer, pen and paper, or a plastic decoder ring from a cereal box. An example of this is the *ROT13* cypher. ROT13 replaces every letter in a text with the letter that is 13 places away from it in the alphabet. For example 'ABC' becomes 'NOP'.

Even when using algorithms that can more accurately be called encryption, the encryption is weak, if the key used to generate it is weak. Using ROT13 as an example, if you consider the 13 place differential to be the key, then ROT13 has an extremely weak key. ROT13 can be strengthened by using a different key. You could use ROT10, replacing each letter with the one ten places forward, or you could use ROT-2, replacing each letter with the one two places before it. You could strengthen it even more, by varying the differential, such as ROTpi, where the first letter is shifted 3 places; the second, 1 place; the third, 4 places; the fourth, 1 place; and so on, using pi (3.14159265...) to provide a constantly varying differential.

Because of these possible variations, when you are encrypting any type of information, you must be sure that you are using a reliable method of encryption and that the key – your contribution to the encryption – will provide you with a robust result.

You must also remember that a good system of encryption is useless without good passwords, just as good passwords are useless without good encryption.

Exercises:

1. Here is a list of fruits encoded using the ROT13 cypher. Try to decode them:
    a) nccyr
    b) benatr
    c) yrzba
    d) jngrezryba
    e) gbzngb

2. Find a web page that will allow you to decode the ROT13 encoded words automatically.

3. There are many different systems that are called encryption, but the truth is that many of these are simple encoding methods. A true encryption requires a password, called a *key*, in order to be encoded or decoded. Of the following systems, which ones are true methods of encryption and which ones are simple codes?
    a) Twofish
    b) MIME
    c) RSA

d) CAST
e) AES
f) BASE64
g) IDEA
h) TripleDES
i) ROT13
j) TLS

11.5 Password Cracking (Password Recovery)

Password cracking for illegal purposes is illegal. But if it is your password, then it's your information. Once you password protect something, and then forget your password, you are stuck. Hence password recovery.

Password cracking consists of a few basic techniques

"Looking around": passwords are often taped to the bottom of keyboards, under mousepads, posted on personal bulletin boards.

Brute force: just keep trying passwords until one works

Automated dictionary attacks: these programs run through a series of possible dictionary words until one works as a password.

There are many programs available on the web to assist with password recovery on documents. However, newer versions of programs are becoming more and more secure, and therefore, more and more difficult to obtain passwords using the techniques above, or using password recovery software.

Exercise:

Identify three different programs that are used for developing documents (text, spreadsheets, archives) and also allow the use of passwords to limit access to these documents. Next, using the Internet, find instructions on how to recover lost passwords for these files.

11.6 Protection from Password Cracking

Here are some suggestions on how to keep your passwords from being cracked:

1. Use strong passwords that cannot be determined by a dictionary attack.

2. Don't post your passwords near your computer.

3.Limit wrong attempts to three tries, then lock the account. The password must then be reset. (This does not apply to documents or password protected zip files – they do not have lock out options.)

4.Change passwords regularly.

5. Use a variety of passwords for different computers. Does this mean that you need to create a unique password for everything? Absolutely not. Maintain a master password for things that don't matter to you (perhaps the account you were required to create for TheSIMS.com or for your account on the local newspaper). But use good passwords for anything that actually needs to be secure.

Exercise:

Discuss with the class the recommendations found in

http://www.securitystats.com/tools/password.php

Further Reading

http://www.password-crackers.com/pwdcrackfaq.html

http://docs.rinet.ru/LomamVse/ch10/ch10.htm

http://www.ja.net/CERT/Belgers/UNIX-password - deadlink

http://www.crypticide.com/users/alecm/-security.html - deadlink

http://www.securitystats.com/tools/password.php

http://www.openwall.com/john/

http://www.atstake.com/products/lc/

http://geodsoft.com/howto/password/nt_password_hashes.htm