

Security Awareness



Module 6: Authentication and Strong Passwords

Notes:

Note:

This PowerPoint presentation can be licensed as part of Inspired eLearning's Enterprise Security Awareness Program or as a stand alone product. It can be fully customized once purchased.

Authentication

(Your Logo Here)
Inspired eLearning
education for your enterprise

```
graph LR; Client[Client] -- "Username/Password" --> Switch[Switch]; Switch -- "Username/Password Verified" --> Server[Server];
```

- **Authentication**
This is the process of proving you are who you say you are. This is usually done with a user name and password.
 - Your username and password are verified against a user account database that resides on a server.
 - Once verified you are allowed access to system resources.

Notes:

As discussed previously, Authentication is a way of proving you are who you say you are. Without authentication, any user could have access to any resource on a computer or network. This could include files, emails, databases and any other network services not protected by authentication. The most common form of authentication is done with usernames and passwords. You identify yourself as 'Joe Smith', then prove you are Joe Smith by entering a password that only Joe Smith should know. That passwords are verified against a user account database and you are authenticated. Pop3 email, Windows 2000 domains, Online banking and ATM account numbers and PIN numbers are examples of systems that use authentication.

Passwords Fundamentals



- **What is a password?**

A password is a string of usually no more than 14 characters. Passwords are stored in a user account database and associated with a particular username.

- **With your username and password a hacker can access anything you can on the network.**

- **Any damage done by the hacker using your username and password will appear to have been done by you!**

Notes:

A password is a string of usually no more than 14 characters. Passwords are stored in a user account database and associated with a particular username. If a hacker knows your username and password, then he or she can access whatever you can on the network, such as your files, emails, resources, etc. Also, the hacker can pretend to be you on the network. With this level of access the hacker can then attempt to break into critical information resources. **If successful, whatever damage was done will appear to have been done by you!**

How Passwords Are Attacked



- Passwords may or may not be protected by encryption.

Pop3 email, IMAP4 email, telnet and ftp are examples of computer systems that do not have encrypted passwords.

- Most critical passwords are encrypted.

- But the encryption can be broken and the weaker the password, the faster it will be broken.

Remember that passwords can be pulled right off the network by eavesdropping on the packets.

- Password cracking programs can be downloaded from the Internet.

Notes:

Passwords may or may not be protected by encryption. Pop3 email, IMAP4 email, telnet and ftp are examples of computer systems that do not have encrypted passwords. However, most critical passwords, such as a Windows 2000 logon password or your online banking account number and PIN (Personal Identification Number) are encrypted. But the encryption can be broken and the weaker the password, the faster it will be broken. Password cracking programs can be downloaded from the Internet by anyone.

Password Cracking Methods



- Password cracking programs use mathematical algorithms to decrypt passwords.
- There are 3 kinds of attacks:
 - Dictionary Attack:
“Mercedes” would be cracked quickly.
 - Hybrid Attack:
“Mercedes123” would not take long to decrypt.
 - Brute Force Attack:
“!eLmgc!” would take very long to crack. Depending on the strength of the encryption – it could take up to 200 years! Powerful computers can test millions of combinations per second.

Notes:

Password cracking programs understand the mathematical algorithms used to encrypt your password and attempt to reverse engineer your password in order to find it.

There are 3 primary kinds of attacks they use:

1. **Dictionary Attack:** If your password is a word in a dictionary in any language the program will decrypt it within minutes.
“Mercedes” would be cracked quickly.
2. **Hybrid Attack:** If your password is a word or combination of words in a dictionary in any language with a number or special character attached to it, it would also be decrypted within hours.
“Mercedes123” would not take long to decrypt.
3. **Brute Force Attack:** If your password is not a word or combination of words and characters, the password cracking program will have to revert to a brute force attack, in which it attempts to break the encryption key by randomly guessing using all possible combinations. Any encrypted password can be broken this way and the faster the computer the faster it can break them. Depending on the strength of the encryption, this could take anywhere from 24 hours to 200 years.
“!eLmgc!” would take very long to crack. Depending on the strength of the encryption – it could take up to 200 years!

Creating Strong Passwords



- Any encrypted password can be captured and decrypted or “cracked.”
- A strong password will be a long alpha-numeric sequence including:
 - Numbers
 - Upper and lower case characters
 - Special characters (!, ;, &, etc.).
- These cannot easily be guessed by a hacker or a password cracking program.
- However these kinds of passwords are not easy to remember so you will need a special technique.

Notes:

Any encrypted password can be captured and decrypted or “cracked.” Once captured, it is only matter of time before your password is cracked and a hacker can therefore steal your digital identity. To prevent this create strong passwords for your user account.

Ideally, a strong password will be a long alpha-numeric sequence of characters, including numbers, upper and lower case characters and special characters (!, ;, &, etc.). These kinds of strong passwords cannot be easily guessed by a hacker or a password cracking program. However, they can be hard to remember. Let’s look at a way to make them more easy to remember.

Using Phrases for Passwords



- To easily remember a complicated password use a phrase and follow these rules:
 1. Only use the first character in each word.
 2. Use upper or lower case as in the phrase.
 3. Use actual numbers, meaning use “2” for “two”.
 4. Include punctuation.
- The Phrase
“Inspired eLearning makes great
courseware for me!”
= “lemgc4m!”
- Exercise: Create your own password.

Notes:

A great way of creating strong passwords that are easy to remember is by basing your password on a phrase. Follow these rules: (1) Only use the first character in each word. (2) User upper or lower case as in the phrase. (3) Use actual numbers, meaning use “2” for “two”. (4) Include punctuation.

Sample Phrase: “Inspired eLearning makes great courseware for me” = “lemgc4m!”

This is a strong, complicated alpha-numeric password that can easily be remembered, but would be very difficult to crack.

Exercise: Come up with your own password based on the phrase method. This method can be used at work and anywhere else you use a password, such as online banking. Once you are done we will discuss your passwords as a group.

Password Best Practices



- Best Practices

- Use the phrase method to create strong, complicated passwords that cannot easily be guessed.
- Change your password often.
- Do not use familiar names (family, friends, pets, etc.) because they can be guessed by an attacker.
- Do not use familiar dates such as your birthday because this is information about you that can easily be attained.
- Do not use other personal information, such as the name of a favorite sports team. These are also easy guesses.
- Do not use a word that can be found in a dictionary in any language or a combination of numbers.

Notes:

There are a few simple guidelines that can be followed to dramatically increase the strength of your password.

(See Slide)

(Your Logo Here)
Inspired eLearning
education for your enterprise

Other Authentication Methods

- Smart Cards
- Biometrics
 - Thumbprint scanners
 - Retinal Scanners
 - Voice Scanners
 - Face Scanners

Notes:

Username and passwords are the most common form of authentication. However, because there are so many ways to capture and crack passwords, newer and more secure authentication methods are being developed.

Smart Card: These are credit card sized cards with your authentication method on them. To logon, you must physically have the card, place it into the computer and enter a PIN number to gain access to the card, which then logs you on to the network. This method is more secure because you must have 2 things in order to logon: the card and the PIN for the card.

Biometrics: This is a way of authenticating a person by verifying certain physical traits that are unique to that individual, such as a retina pattern, a finger print, a voice or even a face! As these products become more reliable and prices fall, they will eventually replace standard usernames and passwords because they will provide such a greater degree of security.