Cyber Security – Other Threats - Reading

WARNING: This sheet discusses ways in which computers and networks are misused. It is illegal to use these techniques yourself.

Passwords

Passwords are one of the most common ways to protect computers and user accounts to services.

It is possible to crack a password by using a **brute-force attack**. This tries every different password combination. If the password is short (say 3 lowercase characters) then the computer would need to try a maximum of 26*26*26=17576 different combinations. A computer could try these combinations very quickly. By using numbers, uppercase and other characters we could increase the number of characters to around 70 characters. This would give 70*70*70=343000 different combinations. This increase in the number of combinations is why many passwords have to include numbers or special characters. By making the password longer we significantly increase the number of combinations. An 8 character password would require 70^8 combinations. This is over 500,000 billion combinations.

Top 10 most popular passwords (2016)

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football

The table above shows the most popular passwords in 2016. Notice that all of them are weak passwords.

Passwords that use a single word are not secure. A **dictionary attack** tries every word in the dictionary. There are therefore only around 100,000 different possible words which a computer could try very quickly. A large number of programs and server software will have **default passwords** such as "password". If these are not changed then it is very easy for a user or computer to try the default password.

User Access Rights

Organisations have **network policies** which which control **user access rights**. This means that certain users are prevented from carrying out certain actions, e.g. accessing **removable media** or running **executable files**. Companies will also give different amounts of access to different groups of people, so a company director might have access to more sensitive files or a **network administrator** may have permission to install new programs. This is known as different **user access levels**. If these policies or rights are misconfigured then users may be able to do substantial damage to an organisation.

Removable media

Removable media today mainly covers **USB removable media**, but can also cover **SD cards**, **CDs** and **DVDs**. There are two security threats with removable media.

1. When the media is inserted, **executable code** may be run automatically. This may contain a **virus**. Even if the operating system does not automatically run files, a virus may still be on the media and introduced onto the computer
2. Many organisations need **confidential** or **personal data** to be held securely. Removable media allows users to take this data **off-site**. This will often be **unencrypted** and can be accidentally left in a place, such as a train or car, where it can then be stolen.

Outdated Software

It is likely that software will contain a number of **security vulnerabilities** which allow a computer to be **exploited**. When the software creator or company realises that there is a vulnerability, they will create a patch for it. It is important that users either allow the software to **automatically update** itself, or they **apply patches** and updates. **Unpatched** or **outdated** software is a major security threat.

Licensed to knole Academy, #10193259