Network threats

1. Network security threats

The data stored on networks and personal computers often has great value to criminals and they try many ways to get their hands on it.

Over the next few pages we will look in detail at the types of threats that can compromise both individual PCs and larger computer networks.

Network threats

2. Malware

Malware is short for 'malicious software'.

Malware is a general term for any hostile or intrusive software. For example it may disrupt computer operations (virus), or it may seek to secretly monitor what the user is doing (spyware).

Malware types include:

- Computer Virus
- Trojan
- Spyware
- Adware
- Pharming
- Click fraud
- Ransomware
- Rootkits
- Scareware

We cover malware in much greater detail in the next section: Malware Theory.

Network threats

3. Social engineering

A well-designed network can make it almost impossible to directly attack the hardware of a system. But even the most secure network is made vulnerable when it is used by real live humans. People can make mistakes; they can be tricked, fooled, bribed, or threatened.

All of these threats to a network are labeled together as 'social attacks'.

It is difficult to generalise social attacks because there are so many ways an attacker can convince a user to compromise security either willingly or unwillingly.

What social attacks all have in common, though, is that they target people rather than hardware or software.

Examples of social attacks include:

- Bribing a user into allowing an attacker access to a system
- Putting a thumb-drive full of malware somewhere a user might pick it up, and labelling it so that they would want to open it on their system. Something like "Salary Records" or "Staff redundancies".
- Phoning up a user at work and convincing them to break policy and give them the information they want directly, like patient information records.

There are hundreds of other ways social engineering could be used to threaten a network, and criminals are constantly coming up with new ones.

Read this news story: Malware-infected USB sticks posted to Australian homes

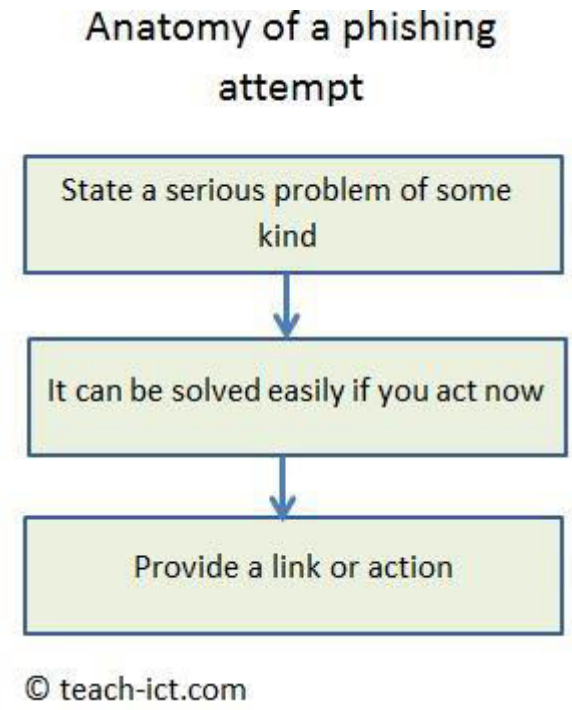
Network threats

4. Phishing

One type of social attack important enough to be given its own name is "phishing".

Phishing involves sending out e-mails, instant messages, or phone calls pretending to be someone in authority, like a bank manager or Windows technician. The attacker then uses that fake authority to convince users to voluntarily give up sensitive information such as passwords, bank account details, etc., or to download harmful software.

A typical phishing attempt is shown in the diagram below:



First of all you are made aware that there is an urgent problem of some kind. For example 'Your bank account is suspended', or 'Your internet connection is to be terminated'.

Then they suggest a simple way to resolve the problem. For example, 'click on this link' or 'phone this support number'.

Then you are taken to a fake web site or 'support line' where you are required to provide your login details to the service or bank account.

A common phishing method is by email. The message looks like it comes from a trusted bank or service provider and it includes a link for you to click on. It takes you to a fake site that looks just like the real one.

Network threats

5. Brute force guesswork

The most basic way to guess a password is called the 'brute force' approach.

This means a computer program is written to go through every possible combination of letters (and / or symbols) until the right one comes up.

For example, there are 26 letters in the english alphabet, so if your password is just a single letter long, it would only take, at most, 26 guesses to find it.

The more characters there are within a password, the stronger it is. This isn't the only factor, though. Setting your password as "password", for example, is not very secure.

Brute force attacks rely on being able to automatically try many different combinations of characters. They can be stopped by limiting the number of attempts a user can have at logging in within a certain time period, or by including an additional authenticaiton step that is more difficult for computers to solve. An example of one such system is CAPTCHA.

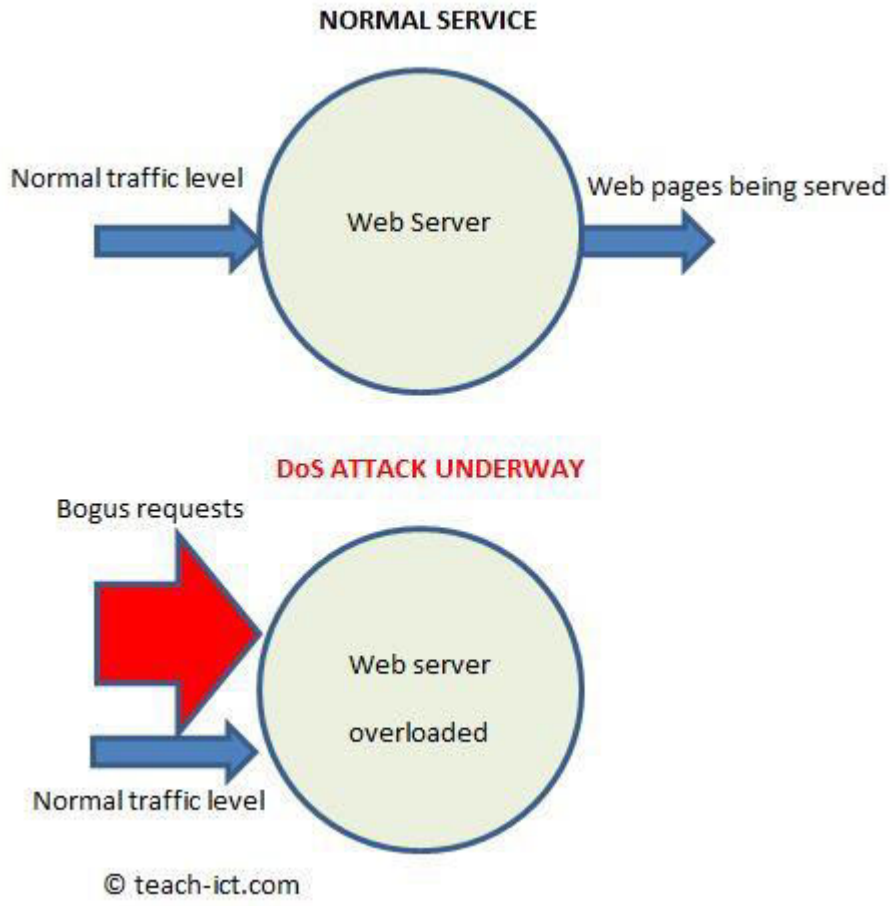
Dictionary method

The problem with '*password*' as a password is that it is very easily guessed by a "dictionary attack", where all the words of the most popular languages are used before brute force is tried. The entire dictionary only amounts to a few hundred thousand words and so can be applied very quickly.

Network threats

6. Denial of Service

This is a method of preventing legitimate users from connecting to a server. Web sites can be blocked with this method.



It works by flooding the targeted server with millions of bogus requests. There are so many requests that all the server memory and CPU cycles are used up and the server then crashes.

A DoS attack often involves hundreds or thousands of computers which have been infected with botnet malware. It is then called a 'Distributed Denial of Service' attack (DDoS). Each machine sends a stream of bogus requests. The legitimate owner of the infected computers are unaware that their machine is being used in this way.

If an ISP or data centre detects a DoS attack they will try and block these requests, but it is not easy if they come from random computers.

Criminals may demand money from the web site owner to stop the attack. The DoS attack may also have been carried out as a punishment for 'unethical' behaviour in the view of the attackers.

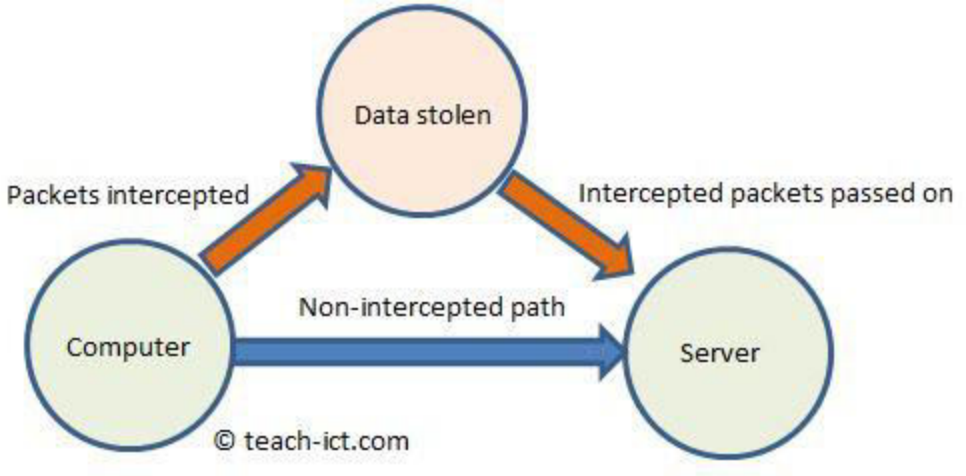
Network threats

7. Data interception and theft

Sometimes called the "man-in-the-middle" attack or "passive attack", as it doesn't damage data.

It is a form of eavesdropping as users are unaware that their data is being extracted.

All data moving across the internet or IP network does so in the form of data packets. So those packets may be intercepted as shown below.



In normal operation, data packets passing back and forth between server and computer get passed along in the normal way, from router to router.

But with a man-in-the-middle attack, an extra server or router has been placed in the network so that packets coming from the target computer are re-directed, copied, and sent on.

The data within each packet, such as passwords or confidential information, is then extracted from the copied packets.

An effective defence against this to encrypt each data packet. The eavesdropper would then have the extra task of decrypting the information.

Network threats

8. SQL injection

This is a form of database attack with the aim of getting access to confidential information such as other peoples' login details.

SQL injection is the deliberate addition of malicious sql code into a web form in order to view, modify, delete database records or to gain unauthorised access.

Behind most username and password dialogue boxes will be a database to handle the information.

When the user inputs their name and password, the system sends an "SQL request" to the database. Something like this:

SELECT * WHERE username = 'binny' AND password = 'mypassword'

This is a command to look for a record matching the username / password combination.

With SQL injection, the attacker tries to insert extra SQL commands into the input boxes, hoping that these commands will be carried out by the server.

The first step to protect against this is for the server to **validate** the information properly before the SQL request is formed. For example, the user name and password may only be a certain length and to not allow invalid characters.
The next line of defense is to add an **escape character** to non-alphanumeric characters for example & becomes "\&". This forces the input to be treated as characters only rather than commands.
The next step is to write the database code in such a way that the raw input is not allowed direct access to the queries being run - '**prepared statements**' and '**stored procedures**' separate the input information from the actual queries.

Network threats

9. Summary

- There are many forms of threat to compromise network security
- Malware is a general term for any hostile or intrusive software
- Malware includes virus, spyware, phishing, pharming, ransomware

- Social engineering takes advantage of the fact people are the weakest link
- Brute force and dictionary attack try and guess passwords
- Denial of Service (DoS) flood a server with requests to crash it
- Man-in-the-middle is a form of data interception
- SQL injection tries to attack a database to gain access to confidential information
- A good network policy needs to be in place to reduce security risk