R 20 Computer Security – Methods of Attack 2 - Reading

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

Data interception

Almost all computers connect to networks, along with many other devices such as mobile phones. This makes them vulnerable to **data interception**.

Data interception is the ability to view **traffic** (information) moving through a network. A computer or router on the network can be set up to view packets as they move past. They can read the packets without the original sender's knowledge and even change the contents of them. A program that performs this task is known as a **packet sniffer** or **packet analyser**.

Lots of information is sent through networks in **plaintext** (text that is not encrypted). For instance, any web pages that you view by using HTTP (Hypertext Transfer Protocol) are sent in plaintext, as will any information you send to them. This is why banks and many sites use the **encrypted** HTTPS protocol (Hypertext Transfer Protocol Secure).

Businesses also make use of **Virtual Private Networks** (**VPN**) to create a secure encrypted connection between an employee's computer at home and the company's network.

Intercepting data with **Wi-Fi** can be very easy if the network is not encrypted or makes use of poor-quality encryption such as **WEP**. The stronger encryption of **WPA2** should be used instead.

Data theft

By using packet sniffers on a network it is possible to make copies of the data. It is therefore vital to check that you are using secure encrypted connections when you use online banking, for example. Checking that HTTPS is used on a website is one way to do this.

Companies must be careful with any data they send as if it is stolen they may be liable under the **Data Protection Act**. Data can also be stolen by employees by using USB solid state media. It is important that a school or business takes precautions to make sure that people only have access to the data which they need to carry out their job. Many cases have occurred where very sensitive information has been stored on a **laptop** or **removable media** and then left on a train or stolen from a car. Companies must put in place policies and training to reduce the possibility of data being lost this way and to make sure that any data is stored encrypted.

Network forensics

Just as packet sniffers can be used to steal data, they can also be used to monitor and analyse computer network traffic. This is known as **network forensics**. Tools used in this way are often referred to as packet analysers or network monitoring tools.

Network forensics is used to find evidence of crimes or to detect attacks which are taking place on a computer system. There are two methods in which network forensics can occur:

1. All information which passes through the network is saved to be later analysed – this requires a lot of storage space.
2. Information is analysed as it passes through the network. Important information can then be saved. A school, for example, may save all inappropriate web addresses visited by students and staff so that they have evidence of any misconduct. This can require a fast processor.

Name: _____

Computer Security – Methods of Attack 2 - Questions

Q 20

1. Match the words on the left with their meaning on the right.

Traffic	Virtual Private Network
HTTP	Packets of information sent through a network
HTTPS	Hypertext Transfer Protocol
VPN	Secure (Encrypted) Hypertext Transfer Protocol

[4]

2. Which of the following protocols is encrypted? Fill in **one** circle.

❍ HTTP ❍ FTP ❍ HTTPS [1]

3. Arrange the following methods of securing Wi-Fi into order of which are the safest from data interception. **WPA2**, **WEP**, **No encryption**.

_____ ↑ Most secure
_____
_____ ↓ Least secure [3]

4. Which two of the following are insecure when dealing with sensitive or personal data? Tick **two** boxes.

❑ Using a laptop with an unencrypted hard disk
❑ Using servers with encrypted hard disks
❑ Using encrypted USB removable media
❑ Not having a company policy to deal with the use of the data [2]

___
10

5. If a company or organisation doesn't do enough to prevent personal data being stolen, which Act would they be in breach of?

_____ [1]

6. Looking at information as it travels through a network is known as what?

_____ [1]

7. Gathering evidence of crimes or attacks that occur on a computer network is known as what?

_____ [1]

8. Complete the text below using the words beneath.

If someone tries to intercept data as it moves through a network they can use a _____. This will view the contents of each individual network packet. When an organisation or the police do this, the tool is usually referred to as a _____. Packet sniffing or packet analysis can be very difficult if the data is _____. It is easy to "sniff" packets travelling through a _____ network if it is not encrypted. This is why care should be taken when using public Wi-Fi systems, especially if they are not encrypted. A company may use _____ to create an encrypted connection between an employee's laptop and the company's network. [5]

VPN **encrypted** **packet sniffer** **packet analyser** **wireless**

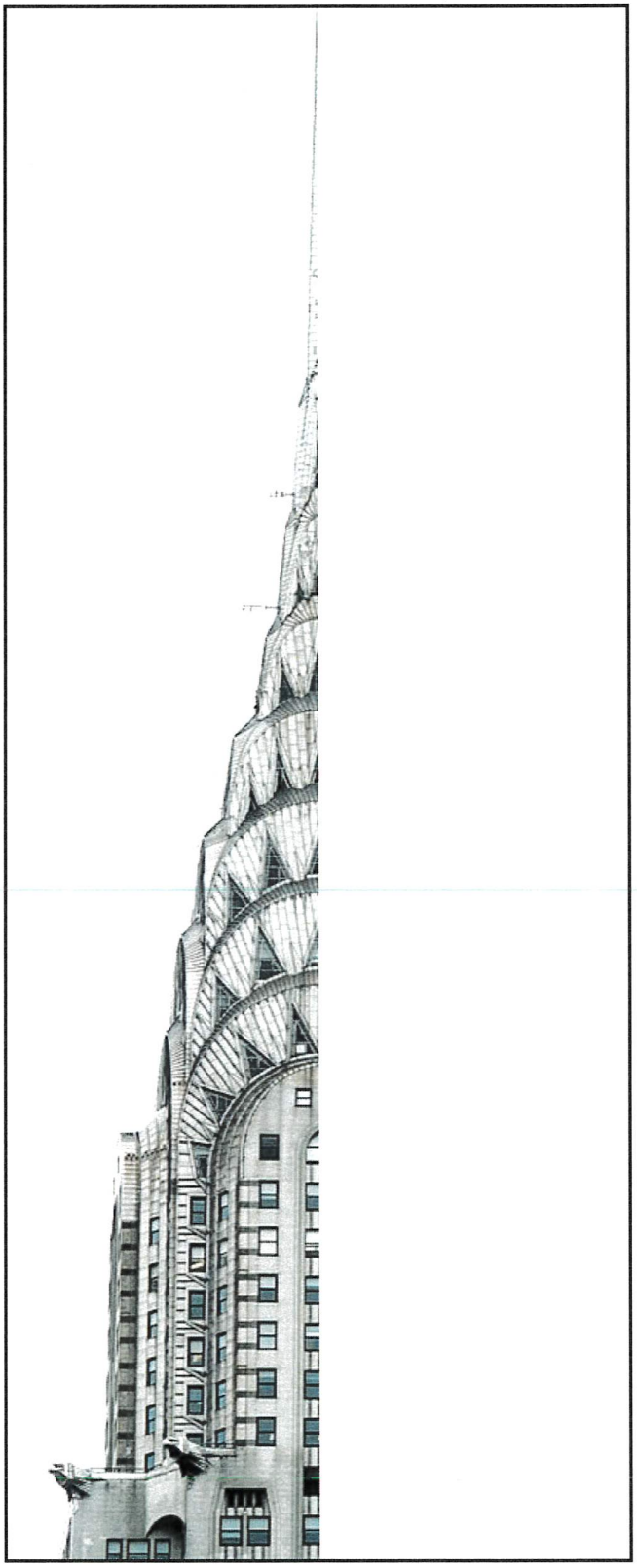
9. For each of the following methods of gathering evidence in network forensics, tick the factor which will be most important. Tick **once** per row.

Method	Storage space	Processing
Record all data which passes through the network		
Analyse data and record the most relevant		

[2]

___
10

Year 8 Art Homework 2: Draw my other half...



Complete the building by adding in the other half as accurately as you can. Focus on proportion and the tonal qualities you see.
Use a ruler to add guidelines if it will help you.

Can you name the item of architecture?

.....

Name: Class: