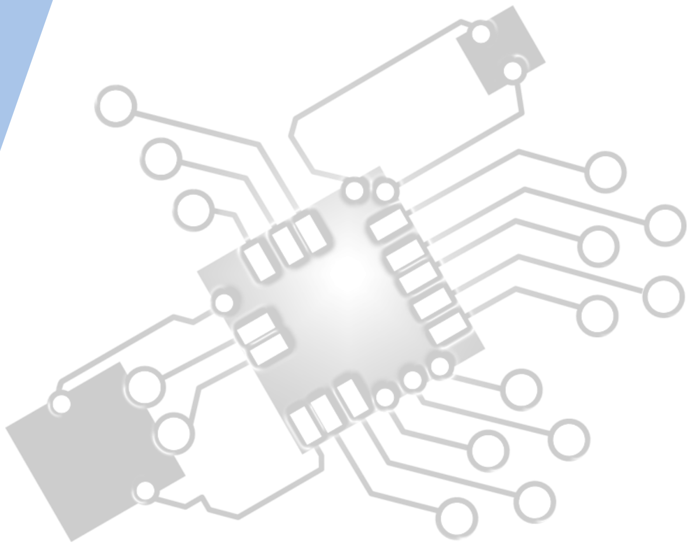
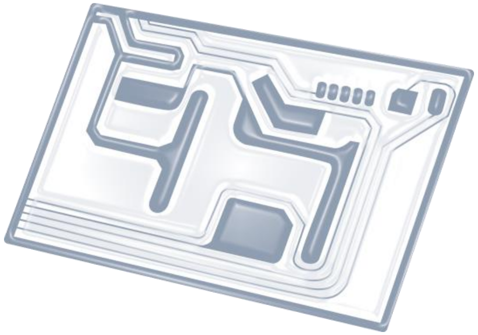
Wireless networking

IB Computer Science



Content developed by
Dartford Grammar School
Computer Science Department

HL Topics 1-7, D1-4



1: System design

2: Computer Organisation

3: Networks

4: Computational thinking

5: Abstract data structures

6: Resource management

7: Control

D: OOP

Content developed by Dartford Grammar School Computer Science Department

HL & SL 3 Overview

Network fundamentals

3.1.1 Identify different types of networks

3.1.2 Outline the importance of standards in the construction of networks

3.1.3 Describe how communication over networks is broken down into different layers

3.1.4 Identify the technologies required to provide a VPN

3.1.5 Evaluate the use of a VPN

Data transmission

3.1.6 Define the terms: protocol, data packet

3.1.7 Explain why protocols are necessary

3.1.8 Explain why the speed of data transmission across a network can vary

3.1.9 Explain why compression of data is often necessary when transmitting across a network

3.1.10 Outline the characteristics of different transmission media

3.1.11 Explain how data is transmitted by packet switching

Wireless networking

3.1.12 Outline the advantages and disadvantages of wireless networks

3.1.13 Describe the hardware and software components of a wireless network

3.1.14 Describe the characteristics of wireless networks

3.1.15 Describe the different methods of network security

3.1.16 Evaluate the advantages and disadvantages of each method of network security

1: System design

2: Computer Organisation

3: Networks

4: Computational thinking

5: Abstract data structures

6: Resource management

7: Control

D: OOP

Content developed by Dartford Grammar School Computer Science Department

Topic 3.1.15

Describe the **different methods** of **network security**

Content developed by Dartford Grammar School Computer Science Department

What is security?

Making sure systems don’t get hacked?

Security breaches can happen without being hacked…

Making sure data is not stolen or leaked?

But what about systems where data is public?

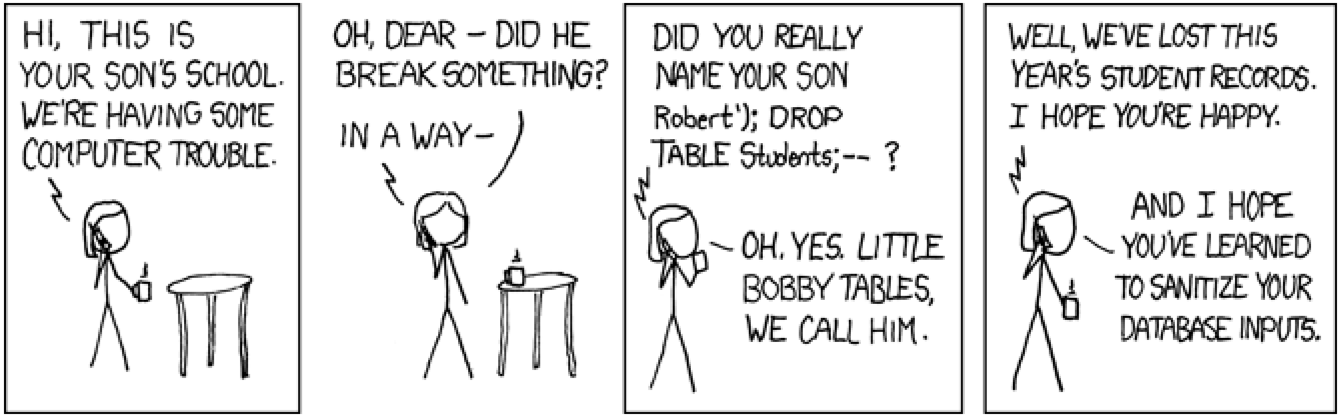
Security properties

Its much easier to think of these three factors when talking about security.

1. **Confidentiality**
2. **Integrity**
   - Maintaining accuracy of data
3. **Availability**
   - DoS attacks

Why is securing systems so hard?

- Cannot plan for every eventuality
- The “arms race”
- Systems can unravel from a weak point
- Users!


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Authentication

Is someone who they claim to be?

- One factor authentication
- Two factor authentication
- Three factor authentication

One factor

Something you **know**.

Two factor

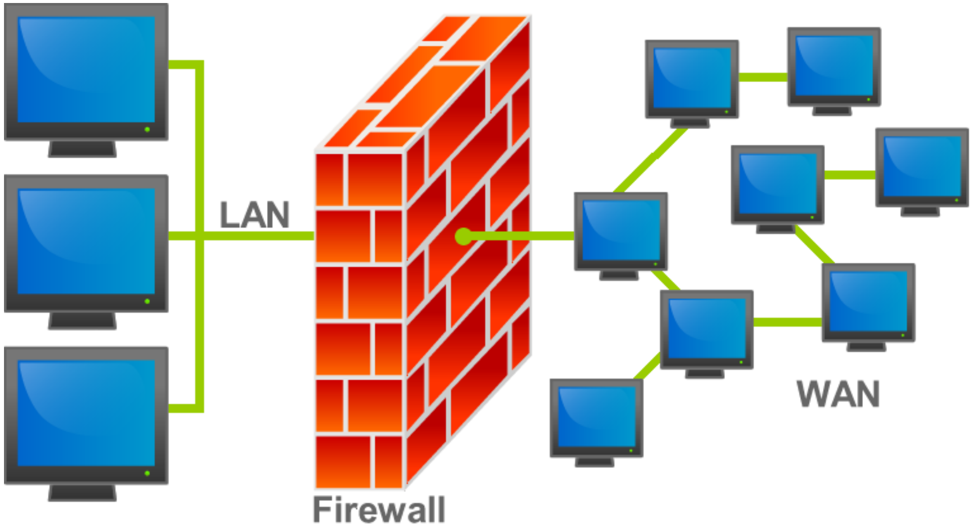
Something you **have**.

Three factor

Something you **are**.

Firewalls

- Hardware or Software (or hybrid of both).
- Controls incoming and outgoing network traffic.
- Analyse data packets based on pre-determined set of rules.



MAC Address

- **Media Access Control** address.
- Hard-coded into devices by manufacturers
- Managed by the IEEE (institute of Electrical and Electronics Engineers).

- Are used to identify specific pieces of hardware.

Physical security

- Locked doors?
- Security personnel?
- Cages / sealed units?
- Reinforced/secure rooms?
- Walls with barbed wire?
- Ravenous guard dogs?

People? Natural Disasters?

Encryption

Only focusing on encryption over wireless networks

- **UserID (and passwords)**
- **PSK (pre-shared key)**
- **WEP (dead)**
- **WPA / WPA2**

WEP

Wireless Equivalent Privacy

Very simple algorithm…

… that was very quickly broken!

- Superseded by WPA in 2003
- Deprecated in 2004.

WPA / WPA2

- Wi-Fi Protected Access (I or II)

WPA	WPA2
2004 - 2006	2006 onwards
Intrusion can be made from outside the network.	Intrusion can only come from since who already has access to the network.