Friday 13th May 2022

Last Minute Revision

Embedded Systems

Key Features:

* Single Purpose – Designed for a **specific task**
* Limited memory and processing power
* Low power consumption
* Small physical size and little/no user interface **(UI/GUI)**
* Low maintenance
* Wireless connectivity
* Customized Hardware + Software

Hardware Components:

* Long Life Battery – Powers the system
* On Chip Sensors – Supplies information from the outside world.
* Microcontroller – Low power microcontroller that contains **RAM, flash memory, input/output.**

On-chip and Off-chip inputs

When drawing diagrams of embedded systems, on-chip inputs are physically on the board (such as a built-in light sensor). Off-chip inputs are normally attached to the system through a cable. On-chip sensors must be drawn **within the embedded system box,** whereas off-chip sensors are in a separate box attached with an arrow. The arrow points in the **direction of data transfer** (both ways in some cases).

Diagram, schematic

Description automatically generated

Interpreters and Compilers

Similarities:

Both translate high-level code into machine code, as CPUs cannot execute high-level code.

Differences:

* Compilers show errors after the compilation process, whereas interpreters stop and pinpoint the error.
* Interpreters are needed each time the program in run, whereas compilers are only needed to **recompile** the code if changes were made.
* Interpreted code is not platform specific, whereas compiled code only works on the platform it was compiled for.
* Interpreted code is easy to edit, as it is always stored as source code, whereas compiled code cannot be edited without changing the original source code (you can’t edit a .exe file, you would need to change the original code and recompile).

High-Level and Low-Level Code

|  |  |
| --- | --- |
| High-Level Languages | Low-Level Languages |
| * Easy for programmers to use. * Have tools for maintenance and debugging. * Not machine specific – will run on computers with different types of CPU. * Generally, less memory efficient when compared to low-level languages. * Example – Device drivers/embedded system firmware. | * *Difficult and time-consuming to use.* * *Little/no tools for maintenance and debugging.* * *Machine Specific – will not run-on devices with a different type of CPU.* * *Interacts directly with the hardware, making it more efficient.* * *Example – Most modern software is developed using a high-level language.* |

POP vs IMAP3

POP3 (Post Office Protocol 3) – Downloads emails from the remote mailbox and deletes the version on the server. **The only copy of the email is now on the device.** Good if you only access mail on one device.

IMAP (Internet Message Access Protocol) – Downloads emails from the remote mailbox **but leaves a copy on the server.** Good for accessing mail from multiple devices.

Wired vs Wireless

Wired:

|  |  |  |
| --- | --- | --- |
|  | Copper Wire | Fibre-Optic Cable |
| Range | Up to 100m | Up to 80 Km |
| Bandwidth | Up to 10 Gbps | Up to 100 Gbps |
| Latency | Can be affected by electrical interference. | Not affected by electrical interference. |
| Common Usage | Connecting devices in a LAN | Long-distance data traffic |
| Cost | Cheap | Expensive |

Wireless:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Range | Power Consumption | Uses |
| Wi-Fi | Up to 100, physical objects can obstruct the signal. | High | Networking devices in a LAN, connecting devices to the internet. |
| Bluetooth | Up to 10m | Low | Pairing devices over a short distance. |
| Zigbee | Up to 100m | Low | Home Automation and IOT (Internet of Things) devices, such as smart devices. |
| RFID | Up to 1m | Low | Security tags, passports. |
| NFC | Close Proximity (around 10cm) | Very Low/None | Contactless payment systems. |

Security (Networks)

The need for Network Security:

* Only authorised users can access the network and its resources.
* Users can only access data relevant to them.
* Prevents misuse such as deleting information or installing software.
* Prevents damage to hardware.

Network Vulnerabilities:

* Hackers – People who exploit security vulnerabilities to gain unauthorised access to a network.
* Insiders – People have **authorised access** to the network. Not all insider threats are malicious, they are mostly caused by human error.
* Malicious Software (Malware) – Viruses, Spyware, Ransomware… Designed to cause damage and destruction.

Penetration Testing – Testing a computer system/network to find and fix vulnerabilities that an attacker could exploit. Testers try to gain unauthorised access and test the awareness and effectiveness of users and security policies.

**Black Box-Testing** – Testers are given no information about the network and approach the problem exactly like an outside attacker would.

**White-Box Testing** – Testers are given access to network/system information. They use the information to find potential loopholes that could be exploited by both insiders and outsiders.

Protecting Networks

Access Control – Limiting who can log into a network and what they are permitted to do:

* Authentication – Determining whether someone is who they claim to be.
* Multi-Factor Authentication (MfA) – Using multiple methods of authentication, for example password **and** fingerprint.
* Permissions – Controlling access to files. For example:
  + Some users are unable to view certain folders/files
  + Read Only – Users can see the file but cannot make any changes.
  + Read and Write – Users can see **and edit** files.

Physical Security – Preventing unauthorised people from entering areas where network equipment is located:

* Access doors should be kept locked and be fitted with keypads or fingerprint scanners.
* Swipe Cards containing workers’ details allow them to access certain areas.
* CCTV systems can be used to monitor the interior and exterior of the building.
* RFID chips fitted to equipment will notify people when equipment is removed from the premises.

Firewalls – Protects devices connected to a WAN (such as the internet)

* They can either be a software firewall, or hardware. Most businesses use hardware firewalls as they have more control over configuration.
* Firewalls allow control over communications in and out of the network.

Algorithmic Bias

Algorithmic Bias – When an algorithm is biased (makes decisions that discriminate against certain individuals. This can happen for because:

1. The dataset that was used to train the algorithm was biased.
2. There is a design flaw in the algorithm that causes it to exaggerate bias instead of ignoring it.
3. The developers of the algorithm accidentally incorporated their own bias into the algorithm.

Data Protection Act

The Data Protection Act of 2018 (DPA) is a set of rules defining how companies should handle personal details from their users:

* Lawfulness, Fairness, and Transparency – There must be a valid reason for holding this data, and the user **must** be aware of this andgive their consent.
* Purpose Limitation – The data must only be used for the purpose it was collected for.
* Data Minimalization – Only collect as much data as is needed.
* Accuracy – The data must be accurate and current. When notified that data is incorrect, the data must be updated promptly.
* Storage Limitation – The data may only be kept for as long as it is necessary.
* Security – Data must be secure and protected from loss or damage.
* Accountability – Companies must show that their data protection methods are adequate.

The DPA gives **data subjects** (anyone who has data stored about them) to:

* Be informed about the collection and use of their data.
* Access their data.
* Have inaccurate data corrected.
* Have data erased.
* Object to how their data is processed.
* Withdraw consent at any time.
* Obtain and reuse their data for their own purposes.
* Complain to the Information Commissioner about their data.