1. We have discussed certificates as a primary in the management of a security strategy.  Describe what certificates are, how they are used, and how they are secured.

Certificates, or digital certificates, are electronic encryption files that allow for secure exchange of data over the internet. They determine the authenticity of servers using through cryptography and public keys, so that only trusted devices can connect to a specific network. Certificates also authenticate websites in the web browser through which they are accessed. In that regard, we can say that certificates work like some form of online passwords.

According to this [SOURCE](https://learn.microsoft.com/en-us/exchange/architecture/client-access/certificates?view=exchserver-2019), there are three primary types of digital certificates:

* Self-signed certificate, which is signed by the application that created it. It is free but isn't automatically trusted by client devices. It needs to be manually added to the trusted root certificate stores on all client devices. Not all services work with these types of certificates.
* Certificates issued by an internal certification authority (CA). These are issued by a public key infrastructure within an organization, which also proves as a disadvantage, in that PKIs are complex to deploy and maintain. This certificate also isn't automatically trusted by client devices, similar to self-signed.
* Certificates issued by a commercial CA, these are automatically trusted by all client devices and servers, but they are costly and need to be planned for ahead to minimize the number required.

Certificates have key pairs, public and private, which they are associated with, and contain the following information:

* User's name.
* User's company or department.
* IP address and serial numbers of user's devices.
* Copy of public key from a certificate holder.
* Duration of certificate validity.
* Domain that is represented by the certificate.

Certificates are beneficial in that they provide security, authentication, scalability (can be used across a wide range of platforms), reliability, and ensure that the organization maintains public trust. [SOURCE](https://www.okta.com/identity-101/digital-certificate/)

1. A direct memory access (DMA) device can improve the concurrency of a computer and operating system in general. What are the ways that it does so? How can a DMA cause the hardware design to be more complex?

DMA can allow the CPU to perform other tasks while it transfers data through the system and memory buses, which is one way it can improve concurrency of a computer and operating system.

It can cause hardware design to be more complex because not only does a DMA controller need to be integrated into the system, the system also needs to allow the DMA controller the ability to initiate transactions that require direct memory access (bus mastering). The CPU and DMA controller may use the memory bus at the same time where cycle stealing is applied. In this case, the CPU is not interfered with while the memory or memory bus is accessed by the DMA controller.

1. Explain the advantages and disadvantages of HDD and NVM devices. In what ways are HDD devices better than NVM devices and vice versa? What applications are optimal for each of these kinds of devices?

Hard Disk Drives (HDD) and Non-Volatile Memory (NVM or NVMe) are both forms of storage.

Advantages of HDD and NVMe devices:

|  |  |
| --- | --- |
| **HDD** | **NVM** |
| Less expensive compared to most other forms of storage, cheaper to produce. | Impressive performance characterized by fast r/w speeds with lower power consumption, achieved by multiple parallel command queues. |
| Large storage capacities, you may find as large as 6TBs in the modern market. | Portability is better, because it use smaller form factors such as PCIe bus, smaller size advantage. |
| Easily available due to a relatively low demand and the rise of SSDs. | Uses solid state storage and multi-core CPUs, therefore hundreds of times faster, especially compared to HDDs. |
| Do not use flash memory, therefore has more read/write cycles and a longer lifespan. | Developed on flash technology, which can handle a lot of commands per queue, reducing CPU cycles. Data is stored in flash memory, thereby reducing risk of data loss. |

Disadvantages of HDD and NVMe devices:

|  |  |
| --- | --- |
| **HDD** | **NVM** |
| Much slower speeds compared to SSDs. They reach r/w speeds of 150mbps, whereas SSDs can reach r/w speeds of 3.5GBps. | Expensive than most other types of SSDs due to the ability to provide quicker rates and the fact that it is designed for developing data transit/storage technologies. |
| Is designed and developed from mechanical components, making it relatively difficult to build. | Not compatible with older systems. |
| As we work with larger files, HDDs may be noticeably louder due to vibrations from the mechanical elements. |  |

[SOURCE 1](https://www.gbcloud.net/blog/gb-cloud-hdd-vs-nvme-drives-what-are-the-advantages-and-disadvantages-of-the-drives/)

[SOURCE 2](https://www.promax.com/blog/explaining-difference-between-the-hdd-and-nvme-drive#:~:text=Speed%3A%20The%20speed%20difference%20between,4%20GB%2Fsecond%20peak%20speeds.)

According to the sources above, NVMe is already used in eCommerce, banking, AI, machine learning, big data and DevOps. HDD would be suited for applications that do not require large memory to process read and write commands.

1. Explain the concept of copy-on-write used in operating systems. Why and when is it useful or helpful? What hardware may be necessary to support this capability?

Copy-On-Write is a method of managing resources within an operating system to efficiently implement duplicate or copy operations on resources that can be modified.

According to this [SOURCE](https://en.wikipedia.org/wiki/Copy-on-write#:~:text=The%20copy%2Don%2Dwrite%20technique%20can%20be%20extended%20to%20support,marked%20copy%2Don%2Dwrite.), Copy-on-write can be implemented efficiently using the page table by marking certain pages of memory as read-only and keeping a count of the number of references to the page. When data is written to these pages, the operating-system kernel intercepts the write attempt and allocates a new physical page, initialized with the copy-on-write data, although the allocation can be skipped if there is only one reference.

In the case of forking, where a system call creates a child process from a parent process, both the processes share the same pages in memory, which will be marked as copy-on-write. If any of those processes try to modify the shared pages, then only a copy of the pages is created and the modifications are completed on that copy, therefore not affecting other processes. [SOURCE](https://www.geeksforgeeks.org/copy-on-write/)

For necessary hardware, the page table needs to verify if every memory access is write-protected.

1. Explain what demand paging is. What would have to be implemented in either hardware or software to enable this type of paging?

Demand paging is a technique of managing virtual memory. The OS copies a disk page into physical memory if an attempt is made to access it while that page is not already in memory, also referred to as page fault. The idea behind demand paging is pages should only be brought into memory if necessitated by the executing process.

Page tables are implemented by mapping logical memory to physical memory, the the table uses bitwise operator to make valid (page in main memory) and invalid (page in secondary memory) pages.

Thrashing occurs where there is a high number of page faults such that the CPU remains occupied for a lengthy period of time just reading invalid pages, or if the number of page faults is equal to the amount of referred pages.

[SOURCE 1](https://en.wikipedia.org/wiki/Demand_paging)

[SOURCE 2](https://www.javatpoint.com/os-demand-paging)

Demand paging requires hardware support, including: [SOURCE 3](https://cseweb.ucsd.edu/classes/sp16/cse120-a/applications/ln/lecture13.html)

* Page tables entries with disk addresses.
* The capabilities needed to detect page faults.
* Address translation mechanisms.
* Restartable instructions.

1. How are operating systems relevant to cybersecurity? This is a fairly open-ended question. Please explain in detail.

Cybersecurity involves ensuring the security and maintaining the integrity of a system's organizational structure or any other capacities within which the systems serves a purpose.

It is a field that operates within the halls of developing, testing, and maintaining secure software systems, and protecting them against external attacks. Operating systems are a big part of that, because in order to achieve the standards required to preserve a secure system, a Cybersecurity Engineer would need to understand how to employ the resources that are pre-defined within the various OS systems available in today's market.

OS systems like Windows and Linux offer tools needed to set up encryption and authentication checkpoints that can help keep a system secure. Part of setting up secure systems also involves other factors, a solid understanding of memory allocation, or CPU process management, the various functionalities of each OS, Virtual Memory management, etc. System vulnerabilities can be investigated and solutions developed to seal those loopholes, all within the confines of cybersecurity.

