The Computer Security class covered 8 big topics: the Introduction, Steganography, Cryptography, Access Control, Network Security, Kerberos, Web Security and Social Engineering.

The Introduction describes the context in which Computer Security became a major concern and that was when legal systems throughout the world recognized the common threats in information systems (hackers, spies etc.) and identified the various motivation behind them, notably money, revenge and bragging. Laws like "The Computer Misuse Act (1990)", the amendments in the "Serious Crime Act (2015)" and the recent"GDPR" were introduced to penalize entities that attempt to break the Confidentiality, the Integrity or the Availability (CIA triad) of information and resources. One important lesson I learned from the Introduction is about the existence of the Risk Matrix which tells how dangerous a cyber attack is according to the impact it produces on a system and the likelihood of it happening. It also became clear to me that the next 7 topics arose from the need of ensuring the CIA triad of digital data.

Steganography is the process of hiding information (usually referred to as payload) inside other pieces of data called cover objects, the most common ones being media files. The payload is hidden in a cover object which turns it in a stego-object, hence achieving confidentiality of data. The stego-object is supposed to be hard to differentiate from the original cover object.

There are a handful of methods for building stego-objects, the ones I came across being the Least Significant Bit (LSB) and the Bitplane Complexity (BPCS) algorithms, the latter doing better against Steganalysis. What I learned is that LSB stores the payload in the right most bit of say an RGB pixel and hence requires the cover object to be big enough to store the entire payload. BPCS stores the payload inside bitplanes according to their complexity. Steganalysis is the process of identifying (passive) information being hidden using Steganography and extracting it (active) from the stego-object. Multiple techniques were developed to perform steganalysis; a popular one is studying the first order statistics of colour distribution of a stego-picture. Personally, I find it very interesting that Steganography was born from really old ideas like Acrostics.

Cryptography is all about secure communication between parties. Turning data into a an unreadable format that wants to be as hard as possible to decipher by actors not involved in the communication. The first thing I learned is that while Cryptography also aims to achieve Confidentiality of data, it is very different from Steganography in the sense that it does not hide it from the attacker, but make it impossible for him to grab hold of it. A good analogy is hiding money under the mattress versus putting it in a multi-layer security vault. In fact, for better security, the 2 techniques can be combined; that is putting the money in a vault and then hiding the vault in a very difficult to find location. Modern day Cryptography was born from traditional ciphers like the Caesar (substitution), Vigenere (permutation), Playfair (block) and Rail Fence (stream) ciphers which led to complex encryption algorithms like the Data/Advanced Encryption standards. They have different operation modes: CBC and ECB, the latter being less secure because it is vulnerable to pattern detection. Encryption can be symmetric (requires the key to be known by both parties before the process starts) or asymmetric. In the case of asymmetric encryption, the key is agreed on by the parties using the RSA public/private (one-way functions like modulo arithmetic) key encryption and Diffie-Hellman key exchange algorithms. This innovation secures the communication over the internet today, powering the HTTPS protocol. However, the perfect theoretical Cryptography can only be realized with randomly generated one-time pad locks. Cryptanalyis can be done through Frequency or even Brute-Force attacks. Looking back, it's important to note that hash functions and Cryptography can also be used to achieve Integrity and Authenticity of data — Message Digests and Digital Signatures.

Access Control deals with the steps users need to take to gain access to a system. The first step is identification — make a claim, provide a username. Next, you need to be authenticated — provide a proof that you are who you claim to be and then you may or may not be authorized. There are 3 types of authentication factors — knowledge (something you know, a password for example), token (something you have, a number received in an email) or biometrics (something you are, like fingerprint or iris — it is highly important for these factors to not give false positives). In general, there is a trend to choose 2 different factors to achieve multi- factor authentication which is more secure. The problem with passwords is that humans are bad at remembering them — so they reuse them, choose easily guessable ones, share them or even write them down in unsafe ways. A good password should have a minimum length, combine lower-case and upper-case letters and include both numbers and special characters. The class also made an emphasis on how passwords should be stored. In fact, hashes of passwords plus random strings of characters (called salts) should be stored in databases to avoid rainbow table attacks. Web applications should also limit the numbers of attempts to prevent dictionary or brute-force attacks. It's important for the authorisation process the work correctly to avoid vertical or horizontal escalation — gain access to resources owned by more privileged accounts.

Network security is concerned with the potential vulnerabilities that can take place at different OSI layers of a network. There are Port and Router threats like port scanning that listens on a host open port for incoming and leaving data. It can be very simple (vanilla), attempting to connect to all I/O ports or Strobe — looking for specific services. For better results, an attacker can use Stealth Scan with fragmented packets that can get to filters and firewalls. Web Servers can be threatened by Denial of Service attacks caused by service request/SYN/bandwidth floods or pings of death. These attacks can be performed by bots, zombies or botnets. Firewalls can be used to restrict access to certain websites in a network. TLS/SSL uses Digital Certificates provided by CAs to prove authenticity of certain servers on the internet so they communicate safely with their users using RSA public key encryption.