CSE487

**Date**: 09 - 06

**Topics**: What is network security and why do we need it? The CIA Triad. Levels of impact of security breach.

**Learn today**: Digital security is for local files and forensic is more like for online based tools. Need for network security is to protect data’s integrity, confidentiality, availability. **Ensuring confidentiality is keeping the data secret from the rest of the internet. Ensuring integrity in the network is that the content won’t be changed in the network.** **Ensuring availability is it will only be available for authorized users or groups.** These are the CIA Triad. But in addition, there are two more called **Authenticity**, which makes the user authentic and **Accountability**, which makes the user responsible for cyber activity. Security breach has 3 level of impact and these are low, medium and high. Also, there are **RFC** (Request for Comments) where **threat and attack** have been discussed. For example, I haven’t make sure the security of my door locked and then my house has been compromised. Here didn’t door locked is threat and house compromised is attack.

**Date**: 14 - 06

**Topics**: Top Ten Vulnerability of Network, CVE (Common Vulnerabilities and Exposures), 0-day vulnerability, Active presentive threat, ExploitDB, Traffic Analysis, Passive Attack, Hash, Computational Security, Unconditional Security, Symmetric and Asymmetric Encryption

**Learn today**: Top ten vulnerability of network some of them are injection some falsified data, deconfiguration and so on. Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. NVD is a vulnerability database built upon and fully synchronized with the CVE List so that any updates to CVE appear immediately in NVD. An exploit that attacks a zero-day vulnerability is called a zero-day exploit. Because they were discovered before security researchers and software developers became aware of them and before they can issue a patch. **Active presentive threat** is done by **following the user regularly with details data**. ExploitDB is a database where ever vulnerable things and how to attack them are given. Also, **there are passive attacks** where **hackers can only know the data and the sender and receiver won’t know that.** **Hash** is one way function for encoding and decoding which is used for **integrity**. We can ensure our file integrity by a tool called File Checksum Integrity Verifier (FCIV). There are two types of encryption, Symmetric and Asymmetric. For example, sender has a key called K1 and receiver has a key called K2. If both keys match with each other then it is called Symmetric and if not then Asymmetric.

**Date**: 16-06

**Topics**: Distance increasing attack, spoofing, Modification of Messages, How to bypass Hash, DOS, DDOS, How to protect from DDOS

**Learn today**: Distance increasing attack is done by some delaying some response. Hackers can delay this response time by three-way handshake. If we want to bypass the Hash, we can do it by changing the hashing key. DOS attack is done by frequently sending the response to fully allocate the resources and we can stop it by blocking the response we are getting for some IP. It can be a temporary block and can only be done by one person. DDOS attack is done by in some distribution of some zombie pc and some hackers are can give us services like that though it is illegal. For protection we can implement some software to our website, like Cloudflare, Captcha and so on.

**Date**: 21-06

**Topics**: What is Steganography? How meta data of images can be overwritten? About OSINT, Security Service and mechanism, Attack surface and tree.

**Learn today**: Steganography is the practice of hiding the presence of data. Information can be buried in the meta information of a picture, the image's EXIF data, the image's color value, and so on. Open-source intelligence, or OSINT, refers to acquiring information on someone from publicly available sources. Authentication, access control, data confidentiality, data integrity, non-repudiation, route control, notarization, and traffic padding are examples of security services. **Detect, prevent, and recover are the three security mechanisms**. **We also learned about the assault tree and attack surface.**

**Date**: 23-06

**Topics**: Encryptions types and their work. What is PGP? 3DES, AES, What is birthday attack? Symmetric Requirements, Cryptography Categorization, Unconditional and Conditional Security.

**Learn today**: Symmetric encryption can be called ROT-13 or private encryption. PGP means pretty good privacy. There are two types of encryption and these are asymmetric and symmetric encryption. Symmetric encryption uses same key for both encryption and decryption and on the other hand asymmetric encryption uses private and public key pair. There are some terminologies in symmetric encryption like plain text, cipher text and so on. DES is another encryption technique which can be more powerful by 3DES. Cryptology is the field of both cryptography and cryptanalysis. We have also learned about birthday attack and rainbow table. Birthday attack exploits hash collision. Cryptography has two category called block and stream. Unconditional is perfect security and Conditional is making the target area small.

**Date**: 28-06

**Topics**: Pseudo Random Generator, AES, Modular Arithmetic, Tor Network (The Onion Routing), The Prime Factorization Theorem, Discreet Logarithmic Problem, Euler Totient Function, And Others. Stream Cipher, Block Cipher, Pseudorandom Number, GCD, One-time-pad, Linear Feedback Shift Register, Trivium, RC4, DES(Data Encryption Standard) And 3DES.

**Learn today**: Pseudo Random Generator is a stream cypher. We don’t know how much we will when stream cypher. There are some sifting algorithms which controls this. Block cypher works like block by block and we know how much data we will get. Block cypher has two types of primitives. One is Confusion and another one is Diffusion. NIST is a USA base cryptography organizations whom are responsible for tracing data. gcd, onetime pad, linear feedback shift Register, RC4, DES and 3DES, NIST, confusion, defusing, AES, Modular Arithmetic, Tor network (The onion Routing), The prime factorization theorem, Discreet logarithmic problem, Euler totient function etc.

**Date**: 30-06

**Topics**: Security mechanism of Public key, Digital Signature, Asymmetric encryption, Discreet logarithmic and Elliptic curves cryptography, Diffie-Hellman algorithm, MITM, Triangulation, Wardriving, OSTIN

**Learn today**: Security mechanism of Public key can be work like this e.g., of all I have to send my symmetric key by asymmetric encryption and then receiver will decrypt the secret key by his private key. Then the sender and receiver can communicate with symmetric secret key through clear channel. "Digital Signature" means that you can guarantee the origin of the document or the id of the user; this is AUTHENTICATION. "Non-Repudiation" means that the document is approved, this is content commitment also called ELECTRONIC SIGNATURE (not digital signature). Asymmetric key encryption techniques include discrete logarithm, elliptic curve, and Diffie-Hellman. Three encryptions were taught to us: discrete logarithm, elliptic curve, and Diffie-Hellman. We also discovered that MITM can be used to crack the Diffie-Hellman algorithm (Man In The Middle). We also learnt about Triangulation, in which attackers masquerade as a middleman in online buying, and Wardriving, in which attackers look for wireless networks with vulnerabilities.

**MID- 2**

**Date**: 19-07

**Topics**: What exactly is Digital Signature Algorithm (DSA)? What are the three stages of RSA algorithm ensures? How does RSA work?

**Learn today**: The Digital Signature Algorithm provides the following: i) confidentiality, ii) integrity, and iii) availability. DSA supports key distribution and digital signatures. RSA has three steps: i) key setup, ii) encryption and decryption, and iii) digital signature. Digital signature is how to verify a message comes intact from the claimed sender. Cryptography has some hard problems which are prime factorization, discrete logarithm problem and ECC(Electric curved cryptology). The message(m) must be smaller than n.

RSA algorithm working steps are:

1. encryption, m^k mod n = c

2. decryption, c^k mod n = m

3. cert Alice = hash( Public key Alice)

4. cert Bob = hash (Public Key Bob)

5. sign (encrypt ( m, Private key CA))

6. ver ( decrypt ( m, Public Key CA))

**Date**: 26-07

**Topics**: Today we discussed about digital signature, DSA signature, Hash function requirements, message authentication, also discussed about Kerberos.

**Learn today**: Today I learned about digital signature, signed certificate, after that this topic related some math. Verification, DSA signature, Hash function requirements. Also learned about hash collusion. After that, MAC which is Message Authentication Code, also learned about OAuth2, SAML, Shibboleth, Kerberos.

**Date**:

**Topics**:

**Learn today**:

**Date**:

**Topics**:

**Learn today**:

**Date**:

**Topics**:

**Learn today**:

**Date**:

**Topics**:

**Learn today**:

Research questions have cleared out what should be our objective for this study. At first, need to specify the user requirements in a structured way. The more we can structure these requirements, the more it will be effective for our study. Our second objective is to save time for both the user and developer end. If users can give instant feedback on an instant diagram, it will shorten the iteration cycles of requirements collecting. Our last objective is to draw a diagram using Business Process Modeling and Notation with a possible feature tree. Why have we chosen BPMN as a diagram? Our study has shown that some% of people understand better when a diagram is drawn with BPMN rather than UML, Flowchart, etc.