DOMS Page No. 1
Date 22/05/2021

CSS ESE

Sanmit Sahu
1811038

Q1(A) 1) X.509

2) c) 2^{N-1}, $2^{N/2}$

3) RSA

4) c) Malware

5) 1) D
2) C
3) B
4) A

6) a)

7) 1- application, 2-SSL, 3-TCP, 4-IP

8) Transport mode or Tunnel Mode

9) Open Web Application Security Project (OWASP)

10) ~~X~~ ~~X~~ c) 3

Sanmit Salve
181038

DOMS Page No. 2
Date 22 / 05 / 2021

Q1B) 1) Cryptanalysis is the science of breaking cryptographic codes. Types of cryptanalysis attacks are:

i) Ciphertext only attack - Consider communication between Alice and Bob where Eve is trying to get unauthorised access to the data or supply false data. Here Eve knows encryption algorithm and can intercept ciphertext.

ii) Known Plaintext attack: Eve has access to some plaintext - ciphertext pairs in addition to some intercepted ciphertext that she wants to break.

iii) Chosen Plaintext attack: Eve chooses plaintext - ciphertext pairs. This is possible when she has access to Alice's computer.

iv) Chosen ciphertext attack: Eve chooses some ciphertext and decrypts it to form a plaintext - ciphertext pair. This is possible when eve has access to bob's system.

2) According to Kerckhoff's principle one should always assume that the adversary Eve, knows the encryption/decryption algorithm. The resistance of the cipher attack must be based only on the secrecy of key.

It is very relevant in cryptography as it makes people focus on strength of algorithm and key rather than depending upon the chance that Eve might be unaware of cryptographic algorithm used.

∴ The security lies in complexity of algorithm itself and secrecy lies in encryption key which is used for transmission and reception

3) In zero knowledge protocols the claimant does not reveal anything that might endanger the confidentiality of the secret. Thus keeping the secret secure all the time. The authentication is possible without revealing the secret. The claimant proves to the verifier that he knows a secret without revealing it. The interactions are so designed that secret can't be guessed or revealed.
Its essence is that it is trivial to prove that one possesses knowledge of certain information by revealing it, but this means that the verifier knows the secret too, the challenge is to prove the possession of information without revealing it

5) • Sniffing: It is a process of monitoring and capturing all data packets passing through a given network.
• Sniffers are used by network admins to monitor and troubleshoot network traffic. Attackers use sniffing tools to capture data packets containing sensitive data like passwords, account data etc. eg phone call tapping

• Spoofing: Spoofing is type of attack on computer device in which the attacker tries to steal the identity of legitimate user and act as another person. This is done to breach security and steal information of users. Hackers change their IP addresses before performing malicious tasks

Sanmit Sahu
1811038
Galaw

- ~~Sniffing Phissp~~
- Phishing : It is a type of attack on computer device where the attacker tries to find sensitive information of users in a fradulent manner through communication by intending to be from a trusted organisation.
  Attackers call any person, and pretend to be from any trusted banks and ask for sensitive bank details, OTP etc.

7) Denial of service or DOS attack occurs when a computer or network user is unable to access resources like internet, email etc. This type of attack can be directed at an operating system or network. In DOS attack the attacker makes machine/network unavailable to users temporarily or indefinitely thus disrupting services.

A Distributed Denial of service attack or DDOS attack is a subclass of DOS attack. It involves multiple connected online devices collectively known as botnet which are used to overwhelm a target network with unnecessary traffic. It makes servers and services unavailable to legitimate users.

Preventive measures
- Non global client addressing : Use path based addressing
- RPF checking of server addresses : Reverse path forwardings prevents a server to from spoofing address of a server

- Middlewalls : Gives upstream access control for a server under stress
- Seperate event and server address : clients can initiate connection to servers but not vice versa
- Use anti DDOS hardware and software modules
- Use more bandwidth
- Protect DNS server

Q2) a) Rabin cryptosystem is a public key cryptosystem. It uses asymmetric key encryption for communicating between 2 parties and encrypting messages.

b) The security is related to difficulty of factorization. It has the advantage of having very hard integer factorization.

c) It has a disadvantage that each output of rabin function can be generated by any of 4 possible inputs.

d) Working of Rabin cryptosystems

i) Key generation

- Generate two very large prime numbers p and q which satisfies the condition

$$p \neq q \rightarrow p \equiv q \equiv 3 \bmod 4$$

eg $p = 137$ $q = 191$ $(137 \equiv 3 \bmod 4 \equiv 191)$.

- Calculate value of n, $n = p \cdot q$

- Publish n as public key and save p and q as private key.

Sanmit Salve
1811038

ii) Encryption

- Get the public key n.
- Convert message to ASCII value. Then convert it to binary and extend the binary value with itself, and change the binary back to decimal m.
- Encrypt with formula, $C = m^2 \bmod n$
- Send C to recipient

iii) Decryption

- Accept C from sender.
- Specify a and b with extended euclidean GCD such that $a \cdot p + b \cdot q = 1$
- Compute r and s,
  $r = C^{(p+1)/4} \bmod p$
  $s = C^{(q+1)/4} \bmod q$
- Calculate X and Y using,
  $X = (a \cdot p \cdot r + b \cdot q \cdot s) \bmod p$
  $Y = (a \cdot p \cdot r - b \cdot q \cdot s) \bmod q$
- The four roots are, $m_1 = X$, $m_2 = -X$, $m_3 = Y$, $m_4 = -Y$. Convert them to binary and divide them in half.
- Determine in which part left and right half are same

Keep that binary one half and convert it to decimal no. Get the ASCII for the decimal no. The resultant character gives the correct message sent by sender.

e) Rabin is used to create and verify digital signatures. Digital sign are done using private key and verification using public key.
Data confidentiality is maintained using rabin cryptosystem as it is assymmetric ~~crypto~~ algorithm. only authorised user can view message.
To maintain data integrity we need to hash the encrypted message so that any unauthorised change can be detected using change in hash.
It implements authentication as users authenticate themselves using their public key (LA) and private key (for decryption)
~~Digital signature~~ Non repudiation is not implemented as everyone has access to public key, digital sign will be required to implement it

Q4) Network layer security controls have been used frequently for securing communications over shared network such as internet as they can provide protection for many applications without modifying them

Any scheme that is developed for providing network security needs to be implemented at some layer in protocol stack

Network layer $\xrightarrow[\text{protocol}]{\text{communication}}$ IP $\xrightarrow[\text{protocol}]{\text{security}}$ IPsec

Sanmit Sahu
1811038

Security issues

i) Fingerprint : It is a key that helps identify a public key. They are used in key auth and offers security and efficiency with smaller size.

ii) Information gathering : Gathering information against targeted victim.

iii) Interception : Unauthorised party has gained access to an asset.

iv) Routing Table Poisoning : Malicious change in routing tables. Aggressive attacks are achieved by editing hacked data.

v) IP spoofing : Hacker uses tool to modify source address in packet header.

Secuing against attacks

i) Router Security : enable packet filtering enable intrusion detection and prevention, block unused ports.
ii) Log and audit unusual activity
iii) Disable unused interface
iv) Firewall is up to date
v) Place firewall between untrusted networks
vi) Switch software is up to ~~date~~ date
vii) Switch traffic is encrypted
viii) Use authentication header in IP SEC

b) Security association in IPSEC
c) Encapsulation security protocol in IPSEC

Q4) Q3) A software design is not secure by hiding it from potential attackers or obscure, encryption system should be able to withstand the attack

Secure software development principles

i) Economy of mechanism: Security mechanism should be small and simple so that they can be easily implemented and verified. eg Security Kernel.
Complex design increase the likelihood that errors will be made

ii) Fail safe defaults: Basing access decisions on permission rather than exclusion, meaning, the access is denied and protection scheme identifies conditions under which access is permitted. If access granting fails, situation can be detected and corrected.

iii) Complete mediation: Every access to every object must be checked for authority. Source of every request must be verified. OS should mediate access process.

iv) Open design: Software design is not secure by hiding it from attacker. Encryption design should be strong enough to withstand an open attack.

v) Least privilege: Every program and every user of

system should operate using least set of privileges necessary to finish a job.

vi) Least common mechanism: Minimize the amount of mechanism common to more than 1 user and depended on by all users.

vii) Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply protection mechanism.

viii) Compromise recording: Mechanisms should record the compromise of information that has occured and can be used in place of more elaborate mechanisms that completely prevent loss