Chapter 5:
Mobile Security

ATTA CKS on Information Security

ATTACK:
An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations. There are many different kinds of attacks, including but not limited to passive, active, targeted, clickjacking, botnet, phishing, spamming, inside and outside. It is classified in two types:
1. **Active Attack:** An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data in route to the target.

Types of active attacks:
1. **Masquerade Attack:** In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.
2. **Session Replay Attack:** In a session replay attack, a hacker steals an authorized user’s log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.
3. **Message Modification Attack:** In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

- **DoS Attack:** In a denial of service (DoS) attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.

Passive Attack:
A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target. In passive attack, an intruder monitors systems for vulnerabilities without interaction, through methods like session capture. Also the intruder engages with the target.
system through methods like port scans. Types of passive attacks:

1. **War driving**: War driving detects vulnerable Wi-Fi networks by scanning them from nearby locations with a portable antenna. The attack is typically carried out from a moving vehicle, sometimes with GPS systems that hackers use to plot out areas with vulnerabilities on a map. War driving can be done just to steal an Internet connection or as a preliminary activity for a future attack.

2. **Dumpster diving**: In dumpster diving, intruders look for information stored on discarded computers and other devices or even passwords in trash bins. The intruders can then use this information to facilitate covert entry to a network or system.

3. **Intruder attack**: An intruder might masquerade as an authorized network user and spy without interaction. With that access, an intruder might monitor network traffic by setting the network adapter to promiscuous mode.

**COMPONENTS of INFORMATION SECURITY**

- Information security is an art of keeping the message secret ie to encrypt and hide it from others getting to know it.

- The components are:  (CIANATA)
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation
  - Authorization
  - Trust
  - Accounting

**COMPONENTS of INFORMATION SECURITY**

- **Confidentiality**: It is the property where the information is kept secret so that unauthorized persons cannot get at the information.

- **Integrity**: Integrity is the property of keeping the information intact.

- **Availability**: It is essential to ensure availability of service to legitimate users.

- **Non-repudiation** is the property by which the identity of both sender and receiver of the message can be identified and verified.

- **Authorization**: Authorization deals with privileges. The subjects (person) can
read, write or execute an object (data items/file) based on their assigned privileges.

- **Trust**: Trust involves developing a security policy, assigning credentials to entities, verifying that credentials fulfill the policies.

- **Accounting**: It is the process by which usage of service is metered. Based on the usage, the service provider collects the fees either directly from the customer or through home network. This will be true even if the user is roaming in a foreign network and using the services in a foreign network.

Security Techniques and Algorithms

Encryption Algorithms are divided into two main groups:

- Symmetric Key Encryption: In a symmetric key encryption the key used for decryption is the same as the key for encryption.

- Public Key Encryption: In case of public key algorithms the key used for decryption is different from the key used for encryption.

1) Symmetric Key Cryptography
2) Asymmetric Key Cryptography:

Comparison

<table>
<thead>
<tr>
<th>Symmetric Key Cryptography</th>
<th>Public Key Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is also known as private key cryptography</td>
<td>It is also known as asymmetric encryption</td>
</tr>
<tr>
<td>Only one key is used: Private key</td>
<td>Two Keys are used: Public and Private</td>
</tr>
<tr>
<td>The key is kept secret</td>
<td>Public key is freely available to all, while</td>
</tr>
<tr>
<td></td>
<td>private key is a secret key</td>
</tr>
<tr>
<td>Same key is used for encryption and decryption</td>
<td>One key is used for encryption while other is</td>
</tr>
<tr>
<td></td>
<td>decryption.</td>
</tr>
<tr>
<td>Faster than Public key Cryptography</td>
<td>Slower than symmetric key cryptography</td>
</tr>
<tr>
<td>It is used for encrypting small or large message</td>
<td>It is used for encrypting small messages</td>
</tr>
</tbody>
</table>

There are two types of Algorithm Types

1. Block Cipher:

   • Block Cipher technique involves encryption of one block of text at a time. Decryption also takes one block of encrypted text at a time.

   • The blocks used in block ciphers generally contain 64 bits or more
There are two types of Algorithm Types
2) Stream Cipher
Stream Cipher technique involves the encryption of one plain text byte at a time. The decryption also happens one byte at a time
In text format In binary format
Pay 100 010111001 Plain text
100101011 XOR operation with key
ZTU91^%D 11001001 Cipher Text

Public Key Cryptography
• Two keys : private key and public key
• Asymmetric Key Cryptography
• Public Key Cryptography Algorithms are:
  • RSA Algorithm
  • Diffie Hellman Algorithm

RSA Algorithm
• Choose two large prime numbers P and Q.
• Calculate N=P x Q
• Select the public key (Encryption Key ) E such that it is not a factor of (P-1) and (Q-1).
• Select the private key (Decryption Key ) D such that following equation is true
(D x E) mod (P-1) x (Q-1) = 1

5) For encryption calculate the ciphertext CT from the Plaintext PT as follows:
   \[ CT = PT^E \mod N \]
6) Send CT as the Ciphertext to the receiver.
7) For decryption, calculate the plaintext from the ciphertext CT as follows:
   \[ PT = CT^D \mod N \]

Diffie Hellman Algorithm

1. Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.
   Let \( n = 11, g = 7 \).
2. Alice chooses another large random number \( x \), and calculates \( A = g^x \mod n \).
   Let \( x = 3 \). Then, we have, \( A = 7^3 \mod 11 = 343 \mod 11 = 2 \).
3. Alice sends the number \( A \) to Bob.
   Alice sends 2 to Bob.
4. Bob independently chooses another large random integer \( y \) and calculates \( B = g^y \mod n \).
   Let \( y = 6 \). Then, we have, \( B = 7^6 \mod 11 = 117649 \mod 11 = 4 \).
5. Bob sends the number \( B \) to Alice.
   Bob sends 4 to Alice.
6. Alice now computes the secret key \( K1 \) as follows:
   \( K1 = B^x \mod n \)
   We have, \( K1 = 4^3 \mod 11 = 64 \mod 11 = 9 \).
7. Bob now computes the secret key \( K2 \) as follows:
   \( K2 = A^y \mod n \)
   We have, \( K2 = 2^6 \mod 11 = 64 \mod 11 = 9 \).

Example of Diffie-Hellman key exchange
Multifactor Security

• Multifactor security implies to a system that requires more than one method of authentication from independent categories of credentials to verify the user’s identity for a login or other transaction.

• Multifactor Security can be a combination of any of the following factors:

1. What You Know

• The idea here is that you know a secret often called a password that nobody else does. Thus, knowledge of a secret distinguishes you from all other individuals. And the authentication system simply needs to check to see if the person claiming to be you knows the secret.

  • Password
  • Pass Phrase
  • PIN
  • Answer to some personal question
  • Sequence of a Number
  • Predetermined events

Multifactor Security

2. What You Have

• Instead of basing authentication on something a principal knows and can forget, maybe we should base it on something the principal has.

  • Magnetic Stripe Card
  • Smart Card
  • Hardware token
  • Physical Key
  • Private key protected by password.

3. Who YOU Are

• Authentication based on "something you are" will employ behavioral and physiological characteristics of the principal. For example, we might use

  • Retinal scan
  • Fingerprint reader
  • Handprint reader
  • Voice print
  • Keystroke timing
  • Signature
Face (picture in passport)

Biometrics

3GPP Security

- **3GPP**: It is 3rd Generation Partnership Project.
- 3rd Generation Partnership Project (3GPP) is a collaborative project aimed at developing globally acceptable specifications for third generation (3G) mobile systems.
- 3GPP Specifications are also referred to as UTRAN, UMTS (in Europe) and FOMA (in Japan).
- The telecommunications standards bodies that make up the 3GPP are known as Organizational Partners (OP) and those are:
  - Japan"s Association of Radio Industries and Businesses (ARIB)
  - Japan"s Telecommunications Technology Committee (TTC),
  - China Communications Standards Association (CCSA),
  - South Korea"s Telecommunications Technology Association (TTA),   European Telecommunications Standards Institute (ETSI), and   Alliance for Telecommunications Industry Solutions (ATIS).
- GSM, GPRS, CDMA are designed primarily keeping the operator in mind to protect an operator from fraud and network misuse.
- None of these procedures address the security concerns of user information or the application. Hence users cannot feel confident enough to place sensitive information over these networks.
- 3GPP looked into these concerns and proposed a new architecture through following important changes:
  - Changes were made to defeat the false base station attack. It is now capable of identifying the network.
  - Keylengths are increased to allow stronger algorithms for encryption and integrity.
  - Mechanisms are included to support security within and between networks.
• Security is based within the switch rather than the base station to ensure that links are protected between station and switch.

• The authentication algorithm has not been defined but guidance on choice will be given.

Mobile Virtual Private Network

• Mobile VPN is a private network over a public network (usually the Internet) to connect two endpoints.

• Instead of using a dedicated physical connection such as leased line, a VPN uses “virtual connections routed through the Internet from the enterprises’s private network to the remote mobile device.

• VPN implements this through an encrypted private connection between nodes.

• It generally uses IPSec and other PKI frameworks to offer confidentiality, authentication, non-repudiation and Integrity.

• With Mobile VPN mobile workers have the freedom to safely use wireless applications on their handheld devices in the field as Information Technology they are in a private network.

SMART CARD Security

• Smart card is called “smart” because it contains a computer chip.

• Indeed, smart card is often referred to as “chip card” or integrated circuit card. It provides not only memory capacity, but computational capability as well.

• The self-containment of smart card makes it resistant to attack, as it does not need to depend upon potentially vulnerable external resources.

• Because of this characteristic, smart cards are often used in different applications, which require strong security protection and authentication.

• In same way, one more example of smart card is SIM in mobile phone. SIM card (also known as a subscriber identity module) is a smart card with a microprocessor and it consists of the following modules:

• CPU

• Program memory (ROM)

• Working memory (RAM)

• Data memory (EPROM or E2PROM)
• Serial communication module

• SIM stores subscriber data that includes user identity, network authorization data, personal security keys, contact lists and stored text messages.

• Factors which make SIM secure are:
  1. Cryptographic algorithm

• The presence of cryptographic algorithm and secret key in SIM card makes the SIM card secure.

• The most sensitive information of SIM card is the cryptographic algorithm A3, A8, secret Ki, PIN, PUK and Kc. A3, A8 algorithm were written into the SIM card in the producing process, and most people could not read A3, A8 algorithm.

• PUK code is held by the operator. Kc was derived in the process of encryption from Ki. Many of SIMS have RSA, DES, 3DES cryptographic algorithms implemented.

SMART CARD Security

2. Secret key:

• PIN and PUK

• PIN – Personal Identification Number.

• 2 PINs exist (PIN1 and PIN2).

• Limited attempts on PIN access.

• PUK-PIN Unblocking Code.

• Resetting PUK, resets PIN and the attempt counter.

• Too many attempts on PUK blocks use permanently.

3. SIM files system:

• SIM is organized in a hierarchical tree structure; it consists of the following three types of elements:

  • Master File (MF).
  • Dedicated File (DF).
  • Elementary File (EF).

• These file systems have stringent security controls. These files are even protected through password known to user or operator.

Mobile Virus

• Viruses are common in the PC and desktop environment.

• Things are changing as the mobile device become more intelligent and higher capabilities viruses are surfacing.
In June 2004 a virus called Cabir was developed to exploit Bluetooth vulnerability.

In Nov 2004 mobile virus called Skull.A was reported for some models of Nokia phones.


Commwarrrior.A virus uses a combination of Bluetooth and MMS to propagate.

Stagefright Android OS Virus

Mobile Worm

- A worm needs to propagate, execute and reproduce in an automated fashion.
- To reproduce and then propagate, the worm needs to execute a piece of code on the target system.
- It is necessary to have an execution environment available to the worm code on the target mobile device.
- On a mobile equipment today we have various environments like –
  - WAP/WML Script
  - Java Phone/Personal Java
  - J2ME
  - Symbian
  - WindowsCE
  - Android
- These can access both the TCP/IP and SMS interfaces. Therefore worms can replicate and propagate through both TCP/IP and SMS interfaces of Javaphone, personal Java or J2ME framework.
- Javacard facility is also available on the SIM Cards.
- Using all these technologies it will be possible to develop viruses, worms and Trojan horses for mobiles.
- These viruses and worms will be able to replicate, access the address book, use the network facility and propagate.

Symmetric Key Cryptography Algorithms

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)

DES (Data Encryption Standard)
• Data Encryption Standard (DES):
• In 1977 NIST (National Institute of Standards and Technology) had adopted Feistel structure cryptography as Data Encryption Standard (DES).

• For DES,
  • It is Block cipher type.
  • Data are encrypted in 64-bit blocks using a 56-bit key.
  • The algorithm transforms 64-bit input in a series of steps into a 64-bit output.
  • The same steps, with the same key, are used to reverse the encryption.
  • It uses a Feistel structure.

• The overall scheme for DES encryption is illustrated in following

• There are two inputs to the encryption function: the plaintext to be encrypted and the key.

• In this case, the plaintext must be 64 bits in length and the key is 56 bits in length.

![Overall scheme of DES](image_url)
AES (Advanced Encryption Standard)

• **Operation of AES:**
  - AES is an iterative rather than Feistel cipher.
  - It is based on substitution–permutation network”.
  - It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).
  - AES performs all its computations on bytes rather than bits.
  - Hence, AES treats the 128 bits of a plaintext block as 16 bytes.
  - These 16 bytes are arranged in four columns and four rows for processing as a matrix.

![AES Diagram](image)

AES (Advanced Encryption Standard)

• **Stepwise procedure in AES for encryption for a 128-bit block:**
  - Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (cipher text).

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.

- The block to be encrypted is just a sequence of 128 bits.
- AES works with byte quantities so first it convert the 128 bits into 16 bytes.

**Encryption Process**

- Each round in AES comprise of four sub-processes.

- The first round process is depicted below

![AES Encryption Diagram](image)

AES (Advanced Encryption Standard)

1. **Byte Substitution (SubBytes)**
   - The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

2. **ShiftRows**
   - Each of the four rows of the matrix is shifted to the left. Any entries that "fall off" are re-inserted on the right side of row. Shift is carried out as follows –
• First row is not shifted.
• Second row is shifted one (byte) position to the left.
• Third row is shifted two positions to the left.
• Fourth row is shifted three positions to the left.
• The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

3. MixColumns
• Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

4. Addroundkey
• The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key.
• If this is the last round then the output is the ciphertext.
• Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Questions
1. Explain components of information security. (4M S-15)
2. Explain any one Symmetric key Algorithm (4M S-15)
3. Give the features of Symbian OS. (4M S-15)
4. What is multifactor security? How it is achieved in mobile Environment? (4M S-15)
5. What do you mean by attacks? Give its categories. (4M S-15)
6. Explain any one public key Cryptography algorithm (4M S-15)
7. Explain 3GPP security and smart card security (8M S-15)
8. Describe four component of information security
9. Describe Mobile VPN.
10. With the neat diagram give step by step procedure to describe DES.
11. What is 3GPP? List its four Technical specification groups
12. List four components of information security. State the features of each.
13. Write stepwise process of RSA algorithm.
15. With the neat diagram give stepwise procedure to describe AES.
17. With neat diagram describe the stepwise procedure to describe AES (4M W-15)
19. Compare between symmetric key cryptography with public key cryptography (4M W-15).
20. Write Detail Procedure of DES algorithm (8 M W-15)