CSE565 Assignment 1

Name: Sri Charan Reddy Teegala

Email: teegala@buffalo.edu

UBID: teegala

UB Number: 50681752

Academic Integrity Statement:
I, Sri Charan Reddy Teegala, have read and understood the course academic integrity policy.

1. Give a brief description of HBGary Hack and list five lessons learned from this hack.

   HBGary Hack refers to the security breach in 2011, when the hacker group named Anonymous targeted the security consultant company HBGary Federal after its CEO Aaron Barr claimed to reveal leaders behind Anonymous. Anonymous broke into HBGary servers, published their emails on web, defaced their website and took Greg Hoglund' website offline and the user registration data published.

   Hackers used standard procedures to break into systems and gathered sensitive information and used it to access further systems. HBGary used a custom Content Management System (CMS) which had a SQL injection vulnerability which was used to exploit user data (usernames and password hashes). Using sources like rainbow table they were able to crack passwords of most of the users as HBGary was using MD5 for hashing which is one of the most common hash functions. Some of the employees, including CEO re-used the same passwords which helped hackers to get full access to the HB Gary's system and deleted gigabytes of backups and research data. It also led to access to the e-mail system of the company with the administrator account. Hackers also used social engineering attack to get direct ssh access with the root account using Greg's Gmail account. This incident highlighted weakness in both technical defenses and organizational practices. From which, several lessons can be learnt:

   1. Always ask users to create strong passwords for their accounts
   2. Do not reuse passwords in multiple accounts.
   3. Always patch servers to keep them free of known security flaws.
   4. Always delete emails containing passwords and other sensitive information.
   5. Educate employees against social engineering attacks.

   HBGary hack shows that even security firms are vulnerable to basic flaws, highlighting the importance of strong passwords, proper system patching and employee awareness to prevent similar breaches.

2. Consider an automated teller machine (ATM) to which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement. Include as many resources (data, metadata, equipment, etc.) as you can think of which are worth protecting in the context of this problem.

   Confidentiality:

   - PIN numbers of the customers must be protected using encryption. (*Critical*)
   - Personal Information and account balances should not be leaked. (*High*)
   - ATM Transaction logs should not expose sensitive details. (*Medium*)

   Integrity:

   - Account closing balances must be updated correctly after withdrawals/deposits. (Critical)
   - Transaction records must be accurate (*High*)
   - ATM software should not be altered with malware. (*Critical*)
   - Communication between ATM and bank servers must not be modified during transit. (*High*)

   Availability:

   - ATMs must be accessible for customers to withdraw or deposit money when needed. (*Critical*)
   - Bank servers must have a reliable connection to the ATMs. (*High*)
   - Hardware like keypad, cash dispenser, card reader must function properly. (*Medium*)

3. What are the major attacks? Which security objective(s) does each attack affect?

   Major attacks in computer security include:

   Eavesdropping:

   - Attackers gain access to unauthorized information which is intended for someone else when it is being transmitted. For example, packet sniffers capture information passing over a computer network.
   - It affects confidentiality.

   Alteration:

   - Attackers modify data or programs without authorization. For example, man-in-the-middle attack intercepts a network stream, modifies it and retransmits the modified information.
   - It affects integrity.

Interruption:

- Attackers make the resources/services unavailable to authorized users. For example, Distributed Denial-of-service disrupts network traffic of a targeted server/service.
- It affects availability.

4. What is the difference between passive and active security threats?

   Passive security Threats:

   - They involve monitoring or observing information without altering the system or data
   - Examples: Wiretapping, Security objective affected: Confidentiality

   Active Security Threats:

   - These involve modifying or injecting data into the system resources for corrupting it or changing them.
   - Examples: Corrupting users, Security objective affected: Integrity and Confidentiality

5. Compare and contrast symmetric encryption with public-key encryption, including the strengths and weaknesses of each.

   Symmetric Encryption:

   Uses the same key (public key) to decrypt and encrypt.
   Strengths:

   - Much faster and efficient when processing large amounts of data.
   - Less computational effort required.

   Weaknesses:

   - Key distribution is an issue (both sender and receiver must securely exchange the secret key).
   - When one key is leaked, the entire communication is at risk.

   Public-Key Encryption:

   Uses two keys a public key (for encryption) and a private key (for decryption).
   Strengths:

   - Resolves key distribution problem since the public key can be publicly available.
   - Provides digital signatures for authentication.

   Weaknesses:

   - Much slower than symmetric encryption.
   - Needs more computational resources.

6. Give an example to explain the substitution cipher.

   A substitution cipher is a method where we replace each letter in plain text by another letter with a fixed mapping or system. For example, let's consider the word CHARAN to encrypt this we follow a fixed rule to shift every letter by 3 positions in the alphabet (Caesar cipher). Therefore, the substitution will be:

   C – F, H – K, A – D, R – U, A – D, N – Q

   The encrypted word will be FKDUDQ which will be unreadable and can be safely transmitted.

7. What are possible ways to break an encryption scheme?

   These are the possible ways to break an encryption scheme:

   1) **Ciphertext-only attack:**
      Only cipher text is available for analysis. Two common approaches:
      - Brute Force key search – trying all keys and choosing a plain text.
      - Statistical analysis – using frequency patterns and structure to infer plain text or the key.
   2) **Known-plaintext attack:**
      Attackers have some plaintext-key pairs, these pairs will be used to deduce the key and decrypt the other ciphers.
   3) **Chosen-plaintext attack:**
      The attacker can obtain ciphertexts for plaintexts they choose (encryption oracle) which will reveal the structure of the key.

8. Explain the differences between Electronic Code Book (ECB) Mode and Cipher Block Chaining (CBC) Mode and the strengths and weaknesses of each mode.

   Electronic Code Book (ECB) Mode:
   Each plaintext block will be encrypted using the same key independently in a sequence and will be decrypted in the same manner.
   Strengths:
   - Very simple to implement
   - Allows parallel encryption/decryption of blocks of plaintext
   - Loss or damage of a block can be tolerated.

   Weaknesses:
   - Not suitable for large, structured data like documents and images since patterns in plaintext will be repeated in ciphertext

   Cipher Block Chaining (CBC) Mode:
   Each plaintext block will be XORed with the previous ciphertext block before encryption.

A random block separately transmitted will be encrypted known as IV (Initialization Vector).

Strengths:

- Patterns are not shown in the plaintext.
- More secure
- CBC is the most common mode.

Weaknesses:

- Encryption cannot be parallelized easily (sequential).
- Requires a random IV for security
- Not suitable for applications that allow packet losses. E.g. Streaming services

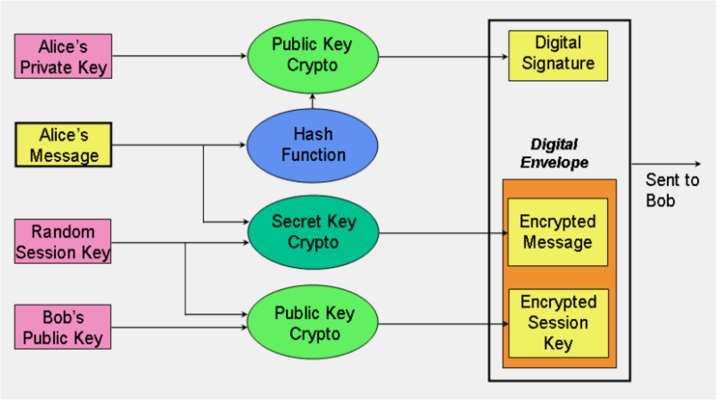
9. Explain why we need public-key certification and how we can verify others' public keys through certificate authorities.

- Public-key certification is necessary to prevent attacks where attackers can create a fake message and lead other people to believe that it comes from someone else by sending their own public key impersonating the victim.
- Certification Authorities (CAs) prevent this by attaching a public key to a verified identity.
- A CA issues a digital certificate containing the public key and entity identity, which is signed with the CA private key.
- It is verifiable by others with the CA public key to establish that the public key is indeed owned by the claimed entity.

10. What are the major security issues that cryptography can solve? Describe how to address those issues in a secure communication depicted in slide #41 of the PPT presentation on Cryptography.

Major Security issues solved by cryptography:

- Confidentiality – Ensures that only the intended recipient can read the message.
- Integrity – Guarantees the message was not altered during the transmission.
- End-Point Authentication – Confirms identity of the sender.



In the slide these issues are addressed as follows:

- The message is encrypted with a random session key, and the session key is encrypted using Bob's public key. (Confidentiality)
- Hash value of Alice's message is stored. (Integrity)
- Only Bob can decrypt the session key using his private key (Bob's side authentication)
- We can ensure that the message is sent by Alice because we need to decrypt the digital signature with Alice's public key. (Alice's side Authentication)

References:

Week-3_Class-1-2_Cryptography.pptx

Week-2_Class-2_Overview.pptx

Week-1_Class-1-2_Introduction.pptx

Anonymous speaks: the inside story of the HBGary hack - Ars Technica

https://www.geeksforgeeks.org/computer-networks/cryptography-and-its-types/