**Applied Cryptography (CMPS 381)Course Project**

Selected Topic: Password Store

Submission Date: 10/24/2021

PHASE II

Participated student’s information:

|  |  |  |
| --- | --- | --- |
| Names: | Student QU number | QU-email |
| Mohammed Omar | 201911057 | [Mo1911057@qu.edu.qa](mailto:Mo1911057@qu.edu.qa) |
| Ibrahim Demdoum | 201701515 | [Id1701515@qu.edu.qa](mailto:Id1701515@qu.edu.qa) |
| Talha Abdullah | 201903446 | [Tp1903446@qu.edu.qa](mailto:Tp1903446@qu.edu.qa) |

**Section A Threat model**:

**Assumptions about the hacker:**

Every system has their own advantages and challenges. We assume the hacker who is trying to exploit our system vulnerabilities have motives like stealing data, bank details, holding secret files for ransom or altering important information. We make few assumptions about the hacker:

1. Hacker is smarter than our system. As good and secure our system might be, there is always a hacker who is smarter out there. It is close to impossible to create a 100% secure system. The main reason is that there are a lot of aspects to securing our system, while the hacker can focus only on a single part of the system to break into. There are at times where group of hackers come together to break into our system by working on different segments of our network such as databases, servers, etc.
2. Our server is always a matter of interest for the hacker to break into. Breaching passwords can lead to a dangerous situation for the user. For instance, access to bank password can lead to hacker stealing money from the user or changing passwords to another password to cause trouble to the users.
3. Hacker can attack any time. We must expect the attack to take place any moment, now or then. This will help us to always make our service available for the users. In case, we do not have this in mind, an attack even if it is easy to fix can disturb users of our service.
4. Hacker can be someone who has experience in outsmarting the same system security that we are using. His experience dealing with system security is much more than other hackers. Hence, it is more likely possible for him to break into our system than a normal hacker.

Assumptions about the hacker give us all the aspects and challenges that our system can face.

**Threats Faced by our System:**

To counter this, we first investigate some of the threats the hacker can inject into our system to provide challenges to our system. A threat can affect one or more assets and manipulate it.

Our system needs to address all basic threats such as:

1. Viruses and worms – Viruses and worms can be injected into our system which may cause damages such as large scale password leaks, data loss or theft, reputational damage as well as expensive repair costs.
2. Phishing attacks – The style of identity theft is more popular and many fall victims easily to it. Main focus of phishing attacks is that it can cause a leak of credit card numbers, high-profile passwords used in banks by the user, leading to substantial financial loss.
3. Distributed Denial-of-service (DDOS) attack – DDOS will damage system’s availability. When a hacker attacks using DDOS, our server is likely to fall due to low performance or even a server crash. This will deny access of users to our system during the phase of attack and until the issue is fixed.
4. Ransomware – It is a type of malware that can hijack crucial information from our system. Using this method, the hacker can hold the user to pay for a ransom in exchange of his personal details. The hacker earns a financial gain by doing ransomware attacks
5. Dictionary Attacks - This is an attack used by hacker known as Brute Force Attack limited to dictionary words and common passwords kept in general. It is a possibility that the hacker can somehow break into the system using every word in the dictionary and common passwords kept by user. The hacker can then access personal passwords saved by the user to gain an advantage
6. Rootkit Attack – These types of attacks are especially hard to detect. The hacker disables user’s security software and track keys entered by the user to gain his login information. Hence, breaking into his password store and stealing data
7. Brute Force Attacks – The hacker uses a method brute force cracking which involves using all combinations of credentials. This might take a long time based on different passwords kept by different users. Hackers use automated tool, script or bot to run through every possible combination possible.
8. Social Engineering – This attack is carried out by direct human interaction. They are socially skilled to extract information about any organization. The attacker may seem respectable and unassuming, possibly joining our system as a new Employee, admin, repairer, or researcher, even offering his own credentials to support his identity.

**Addressing Issues of our System:**

It is necessary to fix and address system security issues. It is also a very important part of risk resolution. Different methods can be used to make our system stronger. They are:

1. Introducing Multi-Factor Authentication for our system. The method will use user’s phone number as a second piece of information. For example, a code is generated and sent on user’s phone while the user logs in. There are many other forms of Multi-Factor Authentication such as getting code via SMS, personal security keys, etc.
2. Getting the user to have a stronger and unique password to access our server. For instance, they must have longer passwords, mixture of different characters, and numbers. A password check will be implemented to check if the password entered by user is effectively unique or has a certain level of unpredictability.
3. Have a guidance for users informing them types of phishing attacks they can face, educating them on it and handle it in case any user is a victim of phishing. In this way, more users cannot be an easy target for the hacker
4. Updating security measures daily. There are always new types of attacks discovered daily, to which new security measures are built up. Therefore, we will keep our security systems updated to help us fight new types of attacks and prevent any major damage to our system.
5. Ask user to change his/her password once in a while (once in a month/ once in two months). This will ensure more security for the user.
6. Our system will interact with the user whenever he is entering a password to store into our system. The user who creates the digital signature will use a private key to encrypt his password data, while the decryption and storage will be done in our system using user’s public key. Digital signature will boost a high standard security
7. Address issues such as multiple invalid logins by a user. This will make sure once a user enters invalid login 3 times, there will be a timeout where the user will not perform anything. This will work specifically when a hacker is trying to break into a user’s login. A timeout will be passed along with an email to the designated user about the invalid attempts.
8. Establishing tracing technique of the whole system. Whenever there is an attack or an attack happened, it is easier to view the root cause and vulnerability in the system and fix/upgrade it.

**Section B Cryptographic Design**:

**Scenario Descriptions:**

**1)**

**Name:** Get stored passwords

**Description:** Attacker gains access to the database system containing the user’s passwords

**Threat Agent:** External threat

**Threatened Entities:** User Passwords, Database

**Assumptions:**

1. Attacker is well versed in SQL.
2. There are vulnerabilities in the database security and can be penetrated

**Main Stream –**

1. Attacker accesses the web-application login interface
2. Attacker performs SQL Query to retrieve relations/tables from the database.
3. Attacker gains encrypted user passwords from the database
4. Attacker tries to decrypt and is successful

**Alternative Flows –**

2.1 Attacker installs an automated tool (example: SPI Dynamics' SQL Injector) and retrieves the tables from the database.

**2)**

**Name:** Get the user password

**Description:** Threat Agent can gain user password by being able to read transferred data on an exposed network

**Threat Agent:** Internal threat

**Threatened Entities:** User Password, Network

**Assumptions:**

1. Since the attacker is from the same organization (internal threat agent), he has access to the internal network and the private keys.
2. The attacker can read and capture the data that is being transferred through the network

**Main Stream** –

1. Attacker installs an IP listener (example: Port Listener)
2. Attacker obtains and captures the packets that are being transferred on the network
3. Attacker evaluates the obtained packets and gains access to a set of username and password
4. The attacker tries to log in with the username and password.
5. The login is validated by the web-application and is granted access/entry

**Alternative Flows –**

5.1 The web-application notices unusual login attempt from a different device and denies access. Therefore, the attacker’s system mimics the actual user’s device MAC address and eventually is granted access/entry.

**Description of Cryptographic algorithm/protocol used:**

1. **Hashing (Used SHA-2)**

To Allow the user to safely communicate with our system, we use a method to verify integrity of communication between the user and our system known as hashing. They use Asymmetric cryptography to allow key exchange. Thus, both system and the user have information regarding the symmetric key. The user appends message which consist of his password with the hash and send it to our system. The system verifies by generating its own hash with the message and the key and compare it with the one sent by the user. If it matches, the system will store the password sent by the user. But if the system finds any fault while comparing both hashes, it will abort the communication as it is likely that a hacker is manipulating the communication or impersonating the user. The transfer of hash and message between the user and the system is done through AES encryption.

* 1. **Salted Hashing –** Stored Hashed password with salt. When a user enters a password, the hash of that password is compared to the stored hash value which is used for verification. Password from storage is hard to be retrieved by the hacker

1. **Asymmetric Cryptography –** Key exchange uses an asymmetric cryptography method known as RSA (RSA One-way function). This is mathematically impossible for a hacker to crack and thus a common key (symmetric key) is present in between the
2. **AES Encryption –** It is essential to encrypt the message and hash using the AES encryption as it is impossible to crack and thus, improves security in the communication process.

**Main Use Cases:**

**Use Case Diagram for Our System**

Diagram

Description automatically generated

**References:**

Some Basic Threats:

<https://searchsecurity.techtarget.com/feature/Top-10-types-of-information-security-threats-for-IT-teams>

General Solutions against threats:

<https://www.wired.com/story/how-to-prevent-getting-hacked/>

<https://auth0.com/blog/hashing-passwords-one-way-road-to-security/>

Hashing:

<https://www.2brightsparks.com/resources/articles/introduction-to-hashing-and-its-uses.html>

<https://auth0.com/blog/hashing-passwords-one-way-road-to-security/>

Salt Hashing:

<https://auth0.com/blog/hashing-passwords-one-way-road-to-security/>