ACG CA2 Report

Applied Cryptography (ST2504)

DISM/FT/1B/05

Md Amirul Adeeb (2107095)

Table of Contents

1. Introduction

1.1 Overview

The goal of this report is to look into security holes and potential solutions for the team's automated menu system, SPAM2 (So Power Automated Menu 2).

Due to the system's overwhelming popularity, it has been decided to expand SPAM2 by adding new outlets outside of SP and utilizing free public WIFI like Wireless@SG.

The system is intended to be installed in a public area with an unsecured wireless connection, so it is crucial to prepare security solutions to ensure the security and privacy of the data (Wireless@SG).

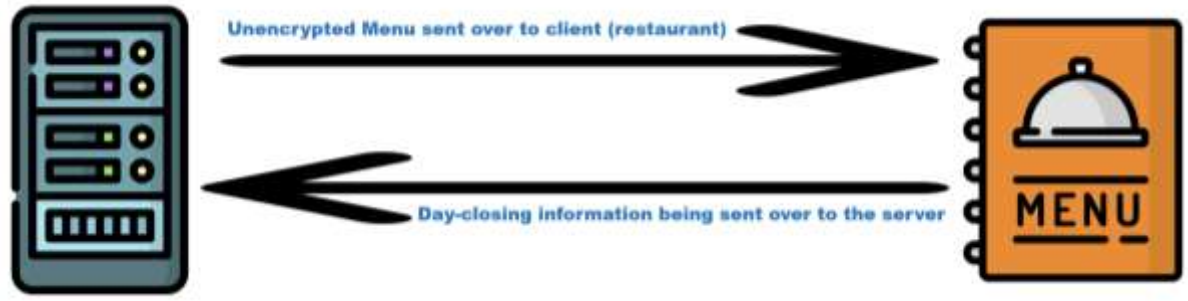
1.2 Assumptions

Assumptions that were made:

- Wireless@SG is a connection that is open and insecure, making it vulnerable to attacks and data theft.
- The SPAM2 system is regarded as being compatible with the open Wi-Fi network.

2. SPAM2 System

2.1 Illustration

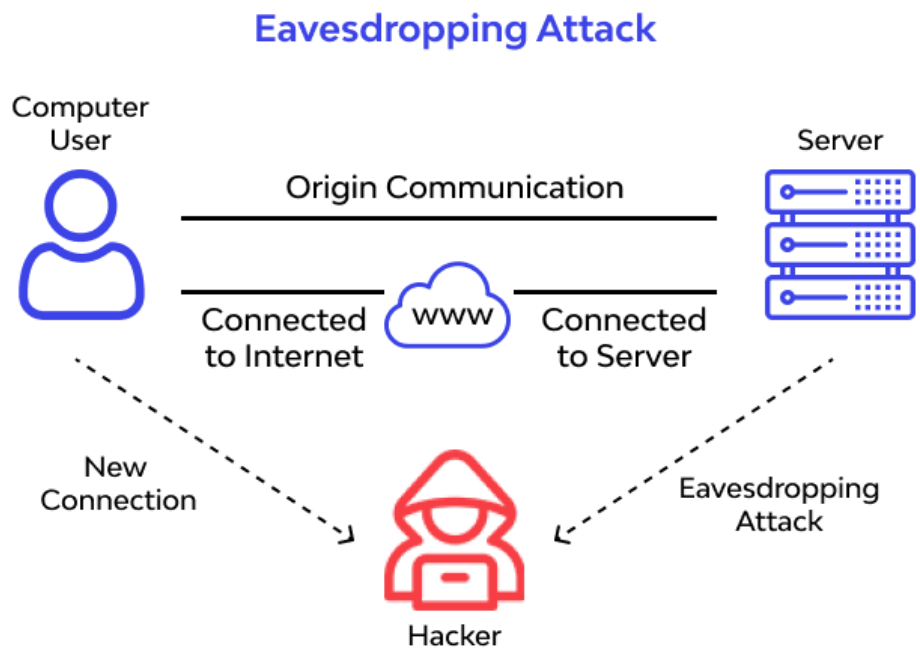


This is an illustration of the current SPAM2 system without any security features, confidentiality protection and non-repudiation.

This system cannot be implemented into an open Wi-Fi as it would pose serious security concerns since attackers can use it to carry out harmful activities like collecting business data or changing menu items, among other things.

3. Attack Scenarios & Countermeasures

3.1 Eavesdropping Attack



Eavesdropping refers to the act of secretly or surreptitiously listening to or monitoring someone's private conversation or communication without their knowledge or consent. This can include intercepting phone calls, emails, or other forms of electronic communication, or listening in on face-to-face conversations. The purpose of eavesdropping can range from gathering sensitive or confidential information for personal or commercial gain, to simply satisfying curiosity or gaining an advantage in a situation.

The Day-Closing information is sent from the client socket to the server socket at the end of each day. However, this information is unencrypted and vulnerable to eavesdropping by attackers who can easily steal sensitive business data. Competitors can use this information to gain an advantage over the SPAM2 system. To address this issue, encryption should be used to protect the confidentiality of the day-closing information. The RSA encryption algorithm can be used to encrypt the data on the server-side before it is sent.

The RSA algorithm uses a public and private key for encryption and decryption, respectively. The server and client will each have their own private key and their public key will be known to each other. The day-closing information from the client will be encrypted using the server's public key before being sent, and the server will then use its private key to decrypt it. This makes it difficult for attackers to access the information even if they intercept it.

3.2 Non-Repudiation of Day-Closing Information

Non-repudiation is a security concept that ensures that a party cannot deny having participated in a transaction or communication. It involves providing proof that a message was sent and received by the intended parties and that the content of the message has not been altered.

Non-repudiation with Alice and Bob can be demonstrated as follows:

1. Alice wants to send a message to Bob and wants to ensure that the message cannot be denied by either her or Bob in the future.
2. Alice hashes the message using a cryptographic hash function and encrypts it using her private key. This creates a digital signature.
3. Alice sends the message along with the digital signature to Bob.
4. Bob receives the message and the digital signature. He then uses Alice's public key to decrypt the digital signature.
5. Bob uses the same cryptographic hash function to hash the message that he received and compares it to the decrypted digital signature.
6. If the hashes match, Bob knows that the message came from Alice and cannot be denied by her in the future.
7. Bob can also add his own digital signature to the message, which acts as proof that he received the message from Alice and cannot deny receiving it in the future.

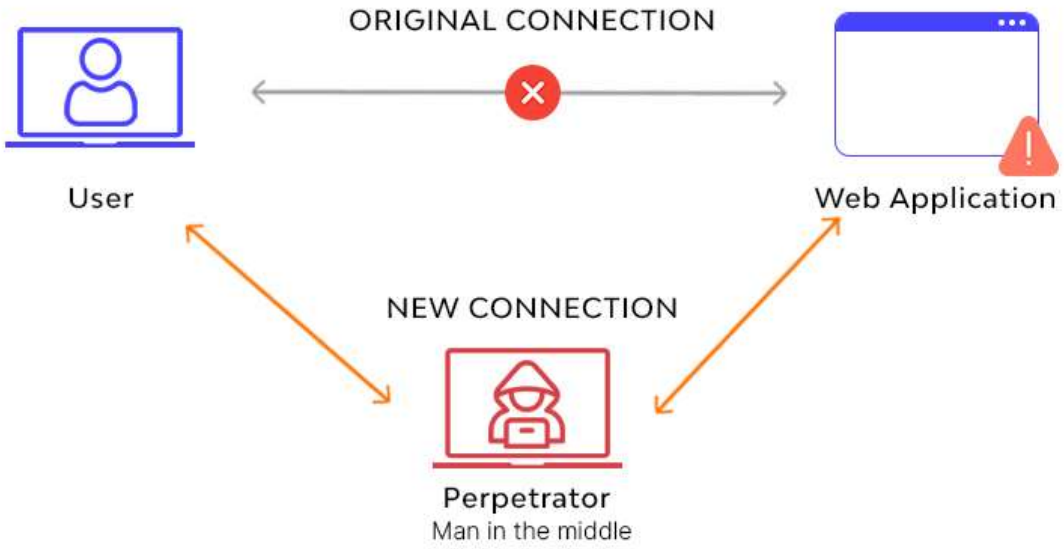
In this way, non-repudiation is achieved as the authenticity of the message can be verified and the originator of the message cannot deny sending it in the future.

At the end of each day, the client must send Day-Closing information to the server. However, there is a risk that a malicious attacker could send false information, which would negatively impact the SPAM2 system. To prevent this, the SPAM2 system will implement non-repudiation to verify the authenticity of the information being sent.

To achieve this, the client will use digital signatures to secure the Day-Closing information. The message will be encrypted and hashed using SHA-256 before being sent to the server. When the server receives the message, it will validate the signature by hashing and encrypting the message, and if the keys match, the server will send an acknowledgement with its own digital signature appended.

Once the client receives the acknowledgement and verifies the signature, it can use the acknowledgement and its own signature as proof that the correct Day-Closing information was sent and received by the server. Digital signatures are unique and secure, as only the intended recipient has the key to create the same signature, making it impossible for the server to deny receiving the correct information from the client.

3.3 Man-in-the-Middle Attack



A Man-in-the-Middle (MITM) attack is a type of cyber-attack in which the attacker intercepts and alters the communication between two parties without either of them realizing it. The attacker essentially acts as a middleman between the two parties, allowing them to read, modify, or even inject their own messages into the conversation. The goal of an MITM attack is to steal sensitive information, manipulate transactions, or gain unauthorized access to systems and networks. MITM attacks can occur in many forms, such as network-level attacks, application-level attacks, and wireless network attacks. They can be carried out through various techniques, such as packet sniffing, IP spoofing, and ARP cache poisoning.

The SPAM2 system sends daily menu information as soon as the connection between the server and client socket is established. This leaves the information open to integrity attacks like man-in-the-middle attacks, where an attacker can intercept the unencrypted data and modify it. This can lead to false menus being sent or an invalid menu, causing panic or disrupting business operations. A well-trained and well-resourced attacker could easily carry out such an attack.

To address this issue, the management has deemed it necessary to protect the integrity of the menu information in transit. As a result, a countermeasure has been proposed using SHA-256 hashing. This method verifies the integrity of messages by using a one-way function to create a hash of the message. Although it does not provide confidentiality protection, it is sufficient for integrity protection in this scenario.

The menu information will be hashed by the server before being sent to the client, where the client will recalculate the hash upon receipt to check if any data has been altered. This helps prevent any loss of integrity due to man-in-the-middle attacks or injection attacks.

4. Proposed System

4.1 The Recommendations

The server will give the client information about the menu of the day when the socket connection between the server and client is established. Before being sent, this information will be hashed on the server. To make sure the integrity of the menu information is not jeopardized, the client will recalculate the hash after receiving the hashed data.

Before the client transmits the Day-Closing data to the server at the end of the day, the file and its contents will be encrypted with RSA using the server's public key and hashed to establish a digital signature. This signature will then be time-stamped and arbitrator-verified.

The server will first receive the Day-Closing data, decode it with its own private key, and check its contents before using the AES technique to encrypt it. The encrypted data is subsequently placed into a file on the server for further storage.

5. Conclusion

With these defences in place, it adds numerous necessary safeguards to guarantee the efficient running of the SPAM2 system. Information about the daily specials has integrity protection, information about the day's conclusion has confidentiality and non-repudiation protection in transit, and information about both has confidentiality protection at rest.

6. Planned task allocation

Adeeb – Code & Report

7. Reflection

Adeeb: Through this coding assignment, I gain hands-on real-world use with encryption. I learn about various encryption methods in this module such as RSA, AES and Caesar cipher in the module. I gain real world scenarios on how a hacker could steal data from me. I had problems like my Crypto library needed to be capital letter for it to work for some reason and almost not being able to submit this report.

8.Appendix risk assessment form

Risk	Likelihood	Severity	Response Strategy	Actions required
To protect the confidentiality of the contents from compromise if the day-closing file is stolen, the data stored there must be encrypted.	medium	medium	Mitigate	Before being saved into the day-closing file, the information will first be encrypted with RSA. By doing it is ensured that the attacker will still need to decipher the cipher even if the file is stolen.
Eavesdropping. The confidentiality of the day-closing information could be jeopardized if an attacker were to intercept, read, and use it.	high	high	Mitigate	Day-closing data should be encrypted using AES before being sent through the connection, and it should only be decrypted once it has reached the server.
Man in the middle attack. The integrity of the menu would be compromised if an attacker were to intercept it and change it before it was sent from the server to the client, endangering operations.	High	High	Mitigate	To ensure message integrity, use hashing.
To demonstrate that the server received the correct day-closing information from the client, make sure the server acknowledgement is not repudiated.	low	medium	Mitigate	The server sends a confirmation to the client after receiving valid day-closing data from the client that is digitally signed by the server to show that the acknowledgement was sent.

9. References:

www.youtube.com. (n.d.). *What is non-repudiation in cyber security?* [online] Available at: https://www.youtube.com/watch?v=KshkuBDrvr0 [Accessed 21 Jan. 2023].

GeeksforGeeks. (2020). *RSA and Digital Signatures*. [online] Available at: https://www.geeksforgeeks.org/rsa-and-digital-signatures/.

Nakov.com. (2022). *RSA Signatures - Practical Cryptography for Developers*. [online] Available at: https://cryptobook.nakov.com/digital-signatures/rsa-signatures.

DuPaul, N. (2019). *Man in the Middle (MITM) Attack*. [online] Veracode. Available at: https://www.veracode.com/security/man-middle-attack.

Mutune, G. (n.d.). *Eavesdropping*. [online] CyberExperts.com. Available at: https://cyberexperts.com/encyclopedia/eavesdropping/.