Maman 15 - Research Document  
Ofir Rosner, ID number 200637494

First, I will discuss potential weaknesses in the protocol. Then, Iwill address how these weaknesses can be exploited for malicious purposes (attacks), and provide proposals for preventing any such attack.

**Potential weaknesses in the protocol**

1.No action towards the server requires authentication (neither from the server nor from the user).

2.The headers of all requests are transmitted in plain

3.Any user can request a list of all users and thereby obtain the ClientID of all other users, which is required for(possible) additional malicious actions.

4.There are requests such as Request Messages that do not have additional requirements beyond knowledge of the ClientID of the targeted user.

5.There is no limit on the number of customers or on the number of requests (provided that there is an option for sending and retrieving files - there is no limit on its size).

6.The server saves the message only until the next reading (although not problematic in itself, but problematic when combined with other weaknesses).

It is possible to send a symmetric key to customers who did not request to receive a symmetric key.

7.The size of the MessageID is 4 bytes and is not necessarily cyclic.

**Possible attacks by a malicious user**

First of all, let's emphasise that it is clear that due to the fact that there is no authentication mechanism throughout the registration process until sending and receiving messages (weaknesses 1+2), a malicious user can easily impersonate another user and perform actions on their behalf. In order to perform actions as another user, the malicious user needs to know the ClientID of the victim, but according to weakness 3, this is not a real limitation.

**DOS/DDOS Attacks**

**What are DOS/DDOS Attacks:**  
 DOS (Denial of Service) and DDoS (Distributed Denial of Service)   
 attacks are types of cyberattacks that are designed to disrupt the   
 availability of an online service, website or network by overwhelming   
 it with a flood of traffic or requests.  
  
 In a DOS attack, a single attacker sends a large volume of traffic or   
 requests to a targeted server, which can overwhelm the server's   
 resources and cause it to crash or become unavailable. This type of   
 attack is typically launched from a single computer or a small group of   
 computers.  
 In a DDoS attack, the attacker uses a network of computers or   
 devices, often referred to as a "botnet", to flood the targeted server   
 with traffic or requests. This makes it more difficult to stop the attack,  
 as the traffic is coming from multiple sources, making it harder to   
 identify and block the attack.

**Going over DOS/DDOS Attacks:**

The fact that there are no functional limitations on the user allows a malicious user to   
 make a very large number of requests to the server, and thus attempt to crash it. This   
 can be done by sending multiple requests of any type allowed by the protocol -   
 registration, client list, message sending, message reading, file sending or receiving.   
 (Weakness 5)  
 It should be noted that there are two specific types of requests that are slightly more   
 problematic (and their combination can be even more problematic)   
 1. Registration request - a request that is very easy to implement and logically the server will not want to limit the number of registrations and deny service to users.  
 2.List request - a request that returns a list of items, such as a list of users or messages. This type of request can cause a high load on the server if there are a large number of items in the list and a large number of requests are made to retrieve the list.  
 In addition, a malicious user can make requests to send messages or files of unlimited length, which can heavily overload the server. For example, the malicious user can cause the server to run many threads to handle many requests that occur in parallel and thereby try to crash the server.  
 It is also possible to send messages until the server exceeds the MessageID size limit - 4 bytes (vulnerability 8).

**Suggestions for preventing DDOS attacks:**

1.Implement a rate-limiting mechanism that limits the number of requests per unit of time from a single IP address or user account. This can prevent a single user from overwhelming the server with a flood of requests.  
2.Use content delivery networks (CDNs) to distribute the load of requests across multiple servers, rather than relying on a single server. CDNs can also offer additional security measures to help prevent DDOS attacks.  
3.Deploy intrusion detection and prevention systems (IDPS) to detect and block suspicious traffic before it reaches the server. This can help to identify and block traffic from known malicious sources, as well as traffic that exhibits suspicious behavior.  
4.Ensure that your server infrastructure is properly scaled to handle expected traffic, and that you have enough bandwidth to handle spikes in traffic. This can help prevent a DDOS attack from overwhelming your servers.  
5.Use specialised DDOS mitigation services that can help filter out malicious traffic and protect your servers from attacks. These services can often offer more advanced techniques for identifying and blocking DDOS traffic.  
6.Adding limitations on the maximum size of messages or files sent between users.

**Man in the middle attack**

**What are Man in the middle attack:**  
 A Man-in-the-Middle (MitM) attack is a type of cyberattack where an   
 attacker intercepts and alters communications between two parties   
 who believe they are communicating directly with each other. The   
 attacker is able to eavesdrop on the communication, modify it, or   
 inject new information, all while the two parties remain unaware that   
 their communication has been compromised.  
  
 In a MitM attack, the attacker typically positions themselves between   
 the two parties and intercepts the communication, which can occur in   
 various ways such as by hacking into a Wi-Fi network, exploiting   
 software vulnerabilities, or by physically inserting themselves into the   
 communication path.  
  
 Once the attacker has intercepted the communication, they can then   
 either passively monitor the exchange or actively manipulate the data   
 being exchanged. This can lead to various consequences, such as   
 theft of sensitive information, modification of data or messages, or   
 impersonation of one of the parties involved in the communication.  
  
 MitM attacks can be prevented by using secure communication   
 channels such as encrypted messaging, utilizing strong passwords   
 and multi-factor authentication, and regularly updating software and   
 security protocols to protect against vulnerabilities that can be   
 exploited by attackers.

**Going over Man in the middle attack:**  
 As I mentioned in weakness 1 - there is no authentication mechanism

against the server, and there is also no authentication mechanism against

the user. In other words, under appropriate conditions, a malicious attacker can   
 cause a legitimate user to communicate with them and transfer   
 messages and information through them as if they were the legitimate   
 server.  
 The mechanism of transferring content between clients is protected using a   
 combined mechanism of symmetric and asymmetric encryption (for   
 coordinating the symmetric keys).  
 A malicious attacker with the ability to eavesdrop and inject traffic can  
 interfere with the traffic of any legitimate user.  
 Such ability can be implemented by DNS poisoning or ARP spoofing and so   
 on.  
 In this way, a malicious attacker can actually serve as a server for the

legitimate user and transfer their traffic to the real server, thereby   
 eavesdropping on all of their traffic and even altering it.  
 An attack like this is relevant on its own and allows a malicious attacker to

interfere with traffic at the level of whether to forward messages or not, but it

does not allow the attacker to read or write the content of the messages

because they do not have the symmetric key of either party at this point.  
 In order to interfere with the traffic, the attacker needs the ability to listen   
 and inject information to both attacked users, and to interfere with the   
 reception of the asymmetric public key of both. When attacked, a public key   
 is requested from a legitimate user, and the malicious attacker will pass on   
 another public key, which will give him the private asymmetric key. Then,   
 during the transfer of the symmetric key between the users, the malicious   
 attacker can decrypt it using the same private asymmetric key (and of   
 course pass it on to the attacked users in a legitimate way so that they can   
 communicate).  
 Afterwards, a malicious attacker can also read encrypted content from the  
 users and even interfere with the traffic at the content level, altering text  
 messages or files.

**Suggestions for preventing DDOS attacks:**

1.Use encryption: Encrypting your data using protocols such as SSL/TLS, IPsec, or VPN can prevent attackers from eavesdropping on your communication and stealing sensitive information.

2.Verify the authenticity of websites: When accessing websites, make sure to check the website’s SSL/TLS certificate and ensure that it is issued by a trusted Certificate Authority (CA). Avoid accessing websites with invalid or expired certificates.

3.Secure your network: Ensure that your network is secure by using firewalls, secure Wi-Fi connections, and strong passwords. Avoid using public Wi-Fi networks, especially for sensitive activities such as online banking or accessing personal information.

4.Use two-factor authentication: Two-factor authentication (2FA) adds an extra layer of security by requiring users to provide additional information such as a password and a code sent to their phone or email. This makes it more difficult for attackers to impersonate users and gain access to their accounts.

5.Keep software up to date: Make sure that all software and applications are up to date with the latest security patches and updates. This helps to prevent vulnerabilities that attackers could exploit to perform MITM attacks.

6.Be cautious of phishing: Attackers may use phishing attacks to trick users into giving away their login credentials or other sensitive information. Always be cautious of suspicious emails or messages, and never click on links or download attachments from unknown sources.

**Interruption of communication between existing clients**

**What is Interruption of communication between existing clients** An interruption of communication between existing clients attack in   
 computers is a type of cyberattack that targets the communication   
 channels between two or more existing clients. In this attack, the attacker  
 attempts to disrupt or interrupt the normal communication flow between the  
 clients by various means, such as injecting large volumes of traffic, spoofing  
 IP addresses, or exploiting vulnerabilities in the communication protocols.  
  
   
  
 **Going over Interruption of communication between existing clients** As mentioned, a malicious attacker can impersonate any user and perform   
 actions on their behalf (weaknesses 1+2+3+4). For example, they can   
 retrieve another user's messages from the server. The server will then delete   
 the message, and thus the malicious attacker does not allow the legitimate   
 user to read messages intended for them (weakness 6).  
 This attack can also be expanded to periodically read all messages of all   
 users and thus prevent any user from receiving messages intended for them   
 (a type of DOS).  
 It is important to note that this attack is only a disruption of receiving   
 messages and does not allow for interfering with their content, such as a   
 Man in the Middle attack, for example.  
  
 **Suggestions for preventing a communication disruption attack   
 between existing customers:**  
 Verification can be required for various customer requests,   
 including a request to receive all pending messages.

**Symmetric key attack**

**What is symmetric key attack:**  
 A symmetric key attack is a type of cryptographic attack where an  
 attacker gains unauthorized access to a symmetric key used for  
 encryption and decryption. In a symmetric key algorithm, the same   
 key is used for both encryption and decryption, which makes it   
 susceptible to attacks that involve stealing or guessing the key.

**Going over symmetric key attack:**  
  
 As written in Weakness 7 - it is possible to send the symmetric key of any   
 user to a legitimate user without verification and without a request from the   
 legitimate user.  
 This means that although it depends on the implementation of the client, it is   
 possible to force it to decrypt messages or files that are sent to it, without   
 the consent of the client.  
 With this request, it is also possible to disrupt communication between   
 clients by overriding the symmetric key with an irrelevant key. Afterward, the   
 attacked user will not be able to decrypt messages from another user until a  
 a new request is sent for a symmetric key answered by the remote user. Of   
 course, any message that was received in the meantime and not decrypted   
 properly will be deleted from the server, so the attacker will not be able to   
 read it until it is re-sent.

**Suggestions for preventing a symmetric key attack:**  
 1.Use a strong symmetric key: Use a strong symmetric key that is   
 difficult to guess or crack. This includes using a key that is long and   
 random, and changing the key periodically.  
 2.Use key management systems: Implement a key management   
 system to securely generate, store, and distribute symmetric keys.   
 This includes using hardware security modules (HSMs) or trusted   
 platforms to store the key.  
 3.Use key exchange protocols: Use secure key exchange protocols   
 like Diffie-Hellman or elliptic curve cryptography to exchange   
 symmetric keys securely.  
 4.Use cryptographic algorithms: Use cryptographic algorithms that   
 are secure and resistant to attacks. This includes using algorithms   
 that are widely recognized and have been tested for their security.  
 5.Limit key access: Limit access to the symmetric key to authorized   
 users only. This includes using access control policies and limiting the   
 number of people who have access to the key.  
 6.Monitor key usage: Monitor key usage to detect any unauthorized   
 access or usage. This includes logging key usage and reviewing logs   
 periodically for suspicious activity.  
 7.Keep software updated: Keep software that uses symmetric key   
 algorithms up to date. This includes applying security patches and   
 updates to software and firmware that use the symmetric key.