# Security Vulnerabilities in the Provided Protocol – Question 2

Made by Dean Gabbai, ID 326256112

## Man-in-the-Middle (MITM) Attack

Affected Component: RSA Key Exchange

Vulnerability Class: Key Exchange Vulnerability

### Description:

This protocol is very vulnerable to MITM attacks because of how it performs an RSA key exchange. There’s no validation of the public keys exchanged between client and server. So, anyone can jump in, intercept communication and replace the real public key with theirs. Effectively, anyone can create secure tunnels to both endpoints and eavesdrop on the conversation. What is even worse, they can also change the progression of the conversation as well.

### Result:

This creates a large gap for confidentiality and integrity to be compromised. Once the invader gets in, everything that is sent between the client and the server is available for reading and editing.

### Prerequisites:

The attacker would have to compromise the client-server model at the level of communication, for instance over a spoofed network. As far as we know, there is no proper validation of the public keys during the key exchange process, so this makes it easy to attack.

### Proposed remediation:

We have to add an additional security layer here. This may be addressed by standardizing certificate-based authentication (for instance X.509 certificate). This will make sure that each party is authentic and that the public keys are real. At this point, this type of attack will no longer work.

### Risk Quantification:

- Damage Potential: 9

- Reproducibility: 7

- Exploitability: 6

- Affected Users: 9

- Discoverability: 7

- Overall Risk: 7.6

## Replay Attack

Affected Component: Client Registration and File Transfers

Vulnerability Class: Replay Vulnerability

### Description:

The problems come from the fact that it is not instructed to the DCC protocol to utilize nonces or timestamps. As a result, attackers can intercept communication and storing up valid messages and replaying them. For example, someone would want to transfer files or register – they have valid file transfer requests and so can maliciously end up accessing file by a mistaken identity.

### Result:

It is easy to notice that messages can be replied, and the system compromised which can trigger numerous effects and possible loss of information. This can be a real mess.

### Proposed Remediation:

Utilizing nonce or timestamp type mechanisms will limit the chances of message duplication and will ensure that the possibility of message replaying does not take place.

### Prerequisites:

There exists a possibility of communication intercept of the client and server enabling the attacker to perform activities desirable. The protocol should not have any nonce or timestamp mechanisms making it prone to attack Message Replay Attacks.

### Risk Quantification:

- Damage Potential: 7

- Reproducibility: 6

- Exploitability: 6

- Affected Users: 5

- Discoverability: 7

- Overall Risk: 6.2

## Weak Symmetric Encryption

Affected Component: AES-CBC Encryption

Vulnerability Class: Weakness in Encryption

### Description:

Out of all the weaknesses related to the AES-CBC encryption utilized by this protocol, the most suspicious one is that the Initialization Vector (IV) employed is set to a fixed value or its value is always zero. As a result, encryption becomes predictable in nature, which enables attackers to identify the patterns in the ciphertext and reverse engineer the plaintext with ease.

### Result:

Where the same ciphertext is repeatedly generated. An attacker will be able to determine and then divulge the plaintext, risking sensitive information. This scenario is undesirable, particularly in the event of prolonged communications whereby patterns stand the chance of being tracked.

### Proposed Remediation:

Random IVs should always be employed throughout each session of encryption. This is because even where the plaintext is unchanged, the ciphertext will always be different.

### Prerequisites:

The attacker is capable of persisting in spying on encrypted communications during the attack itself. The encryption should involve IVs that are either invariant or can be easily predicted.

### Risk Quantification:

- Damage Potential: 8

- Reproducibility: 7

- Exploitability: 5

- Affected Users: 6

- Discoverability: 7

- Overall Risk: 6.6

## Brute-forcing on Client UUID

Affected Component: Client UUID

Vulnerability Class: Brute-force Vulnerability

### Description:

There is a possibility of client identification using a 16-byte UUID dependent on the protocol that is susceptible to brute force attacks. UUID is not sufficient and is not random enough which implies that attackers can in principle try numerous combinations and eventually manage to find one or more combinations that would be used to act as if they are the real client.

### Result:

Brute force attacks would enable an attacker to take control of a communication channel to act as the client and elicit unauthorized access to the system.

### Proposed Remediation:

In order to prevent this, either the randomness and the length of the UUID can be increased or better identification techniques such as HMACs can be applied. This would make brute forcing practically impossible.

### Prerequisites:

It is a requirement that an attacker should attempt several UUID combinations in a bid to succeed with the endeavor. It should also be noted that the UUID assistance must be poor in length or randomness.

### Risk Quantification:

- Damage Potential: 7

- Reproducibility: 6

- Exploitability: 7

- Affected Users: 5

- Discoverability: 6

- Overall Risk: 6.2

## Insecure Error Handling

Affected Component: Error Messages

Vulnerability Class: Information Disclosure.

### Description:

The protocol provides quite detailed messages which can assist the attackers in knowing some components of the system. It is sufficient to show users the messages: ‘the username is already in use’ or ‘the file transfer was unsuccessful’ to assist attackers in tailoring their attacks according to the useful usernames or filenames they know.

### Result:

This kind of knowledge allows the attackers to adjust even the finer details of their attack strategies making the attacks much more potent.

### Proposed Remediation:

The recommendations are to make the system’s password recovery messages rather vague. Instead of saying: “the request has been unsuccessful because the user does not exist”, say: “the request has been unsuccessful” and leave out all other information about the system.

### Prerequisites:

The attacker must be able to generate the conditions for errors to occur and examine the response. Also, the server must be capable of providing comprehensive explanations of the error.

### Risk Quantification:

- Damage Potential: 6

- Reproducibility: 8

- Exploitability: 6

- Affected Users: 5

- Discoverability: 7

- Overall Risk: 6.4