Security Weaknesses Table

Shira Gamliel

Vulnerabilities and Recommendations

Weakness	Affected Component	Vulnerability Type	Description	Potential Attack	Proposed Fix
Use of CRC for Integrity Verification	Integrity Verification Mechanism	Weak Integrity Verification	The use of CRC does not provide adequate security for file integrity checks.	Attackers could alter files without detection.	Implement a strong cryptographic hashing algorithm, like SHA-256.
Lack of Identity Authentication in RSA Key Exchange	Key Exchange Mechanism	Man-in-the-Middle (MITM)	There are no mechanisms to verify the identity of the client and server during RSA key exchange.	MITM attacks could intercept and modify sensitive information.	Integrate digital signatures into the key exchange process.
Use of Constant IV in AES-CBC	Encryption Mechanism	Weak Initialization Vector (IV)	A constant IV in AES-CBC encryption reduces the effectiveness of encryption.	Attackers could analyze encrypted packets to infer data structure.	Use a unique, random IV for each encryption instance.
Absence of Replay Attack Prevention Mechanism	Security Mechanism	Replay Attack	The protocol lacks measures to prevent replay attacks.	Attackers could resend intercepted messages, leading to vulnerabilities.	Implement sequence numbers or timestamps for each message.

Use of 1024-bit RSA Keys	Encryption Mechanism	Insufficient Key Length	1024-bit RSA keys are increasingly considered insecure.	Attackers may decrypt communications and expose sensitive data.	Upgrade to at least 2048-bit RSA keys.
Use of Fixed Keys	Encryption Mechanism	Lack of Key Renewal	Relying on a fixed key without renewal makes the encryption vulnerable.	An exposed key allows unlimited access to encrypted data.	Periodically renew keys or generate unique keys for each session.
Lack of DoS Attack Prevention Mechanism	Server Mechanism	Excessive Load	The protocol lacks mechanisms for managing server load effectively.	Attackers could overwhelm the server, leading to service outages.	Implement rate limiting to restrict excessive requests.
No Signature or Password for Client Authentication	Client Authentication	Impersonation	A malicious client could impersonate another by obtaining unencrypted credentials.	Impersonation attacks could occur, compromising security.	Implement digital signatures or password-based authentication methods.
Client Can Skip Reconnection Step	Session Management	Session Bypass	Clients can bypass the reconnection process and send requests directly.	Unauthorized actions could be performed without re-establishing a session.	Require clients to reconnect and re-authenticate before taking actions.

Client Cannot Change RSA Key (Private Key Exposure)	Key Management	Private Key Exposure	If a client reveals their private key, it cannot be changed.	An attacker with the private key can decrypt future messages.	Allow the server to generate and rotate RSA key pairs for the client.

Use of CRC for Integrity Verification

Affected Component: Integrity Verification Mechanism

Vulnerability Class: Weak Integrity Verification

Description: CRC does not provide adequate security for verifying file integrity due to its susceptibility to attacks.

Result: Attackers can alter files without detection, leading to data tampering.

Prerequisites: Attacker has access to the network or communication channel.

Business Impact: Undetected tampering with files can lead to data corruption or unauthorized modifications.

Proposed Remediation: Replace CRC with a stronger cryptographic hashing algorithm, such as SHA-256.

Lack of Identity Authentication in RSA Key Exchange

Affected Component: Key Exchange Mechanism

Vulnerability Class: Man-in-the-Middle (MITM)

Description: There is no mechanism to verify the identity of the client and server during RSA key exchange.

Result: MITM attackers can intercept and alter sensitive information.

Prerequisites: Attacker can position themselves between the client and server.

Business Impact: Compromise of sensitive information and data privacy.

Proposed Remediation: Integrate digital signatures to authenticate both parties during key exchange.

Use of Constant IV in AES-CBC

Affected Component: Encryption Mechanism

Vulnerability Class: Weak Initialization Vector (IV)

Description: A constant IV in AES-CBC reduces encryption effectiveness, allowing patterns in encrypted data to be identified.

Result: Attackers can infer data structure by analyzing repeated patterns in encrypted packets.

Prerequisites: Attacker has access to multiple encrypted messages.

Business Impact: Potential data leakage due to predictable encryption patterns.

Proposed Remediation: Use a unique, random IV for each encryption instance.

Absence of Replay Attack Prevention Mechanism

Affected Component: Security Mechanism

Vulnerability Class: Replay Attack

Description: The protocol does not have measures to prevent replay attacks.

Result: Attackers can resend intercepted messages, potentially performing unauthorized actions.

Prerequisites: Attacker can intercept and resend messages.

Business Impact: Risk of unauthorized access or actions by resending valid requests.

Proposed Remediation: Implement sequence numbers or timestamps for each message to prevent replay.

Use of 1024-bit RSA Keys

Affected Component: Encryption Mechanism

Vulnerability Class: Insufficient Key Length

Description: 1024-bit RSA keys are considered insecure due to advancements in cryptographic attacks.

Result: Attackers could decrypt communications and access sensitive data.

Prerequisites: Attacker has sufficient computational resources.

Business Impact: Loss of confidentiality of sensitive data.

Proposed Remediation: Upgrade to at least 2048-bit RSA keys for improved security.

Use of Fixed Keys

Affected Component: Encryption Mechanism

Vulnerability Class: Lack of Key Renewal

Description: Using a fixed key for encryption without renewal makes it vulnerable to exposure.

Result: An exposed key compromises all encrypted data protected by that key.

Prerequisites: Attacker obtains the encryption key.

Business Impact: Loss of data security and potential unauthorized access to sensitive information.

Proposed Remediation: Implement periodic key renewal or generate unique keys for each session.

Lack of DoS Attack Prevention Mechanism

Affected Component: Server Mechanism

Vulnerability Class: Excessive Load

Description: The server lacks mechanisms for managing high traffic or malicious requests.

Result: Attackers could overwhelm the server, resulting in a denial of service.

Prerequisites: Attacker sends numerous requests to overload the server.

Business Impact: Service disruption and potential loss of availability.

Proposed Remediation: Implement rate limiting to restrict excessive requests and manage load effectively.

No Signature or Password for Client Authentication

Affected Component: Client Authentication

Vulnerability Class: Impersonation

Description: Lack of authentication allows any client to impersonate another.

Result: A malicious client could impersonate another client and access unauthorized data.

Prerequisites: Malicious client knows or intercepts credentials.

Business Impact: Potential unauthorized access and data breach.

Proposed Remediation: Integrate digital signatures or password-based authentication.

Client Can Skip Reconnection Step

Affected Component: Session Management

Vulnerability Class: Session Bypass

Description: The protocol allows clients to bypass the reconnection process.

Result: Unauthorized actions can be taken without re-establishing a session.

Prerequisites: Malicious client is connected but attempts to bypass reconnection.

Business Impact: Unauthorized actions may compromise security or data integrity.

Proposed Remediation: Require clients to reconnect and re-authenticate before taking actions.

Client Cannot Change RSA Key (Private Key Exposure)

Affected Component: Key Management

Vulnerability Class: Private Key Exposure

Description: If a client's private key is exposed, it cannot be changed.

Result: An attacker with the private key can decrypt future messages.

Prerequisites: The private key is exposed to a malicious entity.

Business Impact: Decryption of sensitive data by unauthorized entities.

Proposed Remediation: Allow the server to generate and rotate RSA key pairs for the client.