



COSC340 - Assessment 4

Report

16.05.2024

—

Bart Stolarek
220178419

Executive Summary

This report presents an assessment of the security, privacy, and trust issues identified in the previous version of our messaging application (Assessment 2) and outlines the measures implemented to address those issues in the current secure messaging application (Assessment 4). The report highlights the key findings, recommendations, and future considerations for enhancing the overall security and privacy of the application.

Background

In the previous iteration (Assessment 2), several security and privacy vulnerabilities were identified. This report aims to provide an overview of those issues and present the solutions implemented in the current version (Assessment 4) to mitigate the risks and improve the application's security posture.

Security and Privacy Issues Identified

Lack of User Authentication

Finding: The previous application lacked a proper user authentication mechanism, allowing unauthorised access to user accounts and messages.

Impact: Unauthorised individuals could potentially impersonate legitimate users and access confidential information.

Unencrypted Communication

Finding: All communication between the client and server was transmitted in plaintext, making it susceptible to interception and unauthorised access.

Impact: Sensitive information, including user messages, could be compromised if intercepted by malicious actors.

Absence of Message Integrity and Authentication

Finding: The previous application did not implement mechanisms to ensure the integrity and authenticity of messages, leaving them vulnerable to tampering and spoofing.

Impact: Malicious actors could potentially modify or forge messages, leading to misinformation and loss of trust among users.

Implemented Security Measures

To address the identified security and privacy issues, the following measures have been implemented in the current secure messaging application (Assessment 4):

User Authentication

Solution: Implemented a robust user registration and login system utilising password-based authentication. User passwords are securely hashed using the SHA-256 algorithm along with a randomly generated salt before storing them on the server.

Benefit: Ensures that only authorised users can access their accounts and messages, preventing unauthorised access and impersonation.

Encrypted Communication

Solution: All communication between the client and server is now encrypted using the Fernet symmetric encryption algorithm. The encryption key is securely shared between the client and server during the initial setup process.

Benefit: Protects the confidentiality and privacy of user messages by preventing unauthorised access and interception of sensitive information.

Message Integrity and Authentication

Solution: Implemented HMAC (Hash-based Message Authentication Code) signatures for each message exchanged between the client and server. The HMAC signature is computed using a shared secret key and the message content, ensuring the integrity and authenticity of the messages.

Benefit: Detects any unauthorised modifications or tampering of messages, maintaining the trustworthiness of the communication channel.

Digital Signatures

Solution: Introduced the use of RSA key pairs for digital signatures to provide message authentication and non-repudiation. The server signs each message using its private key before sending it to the client, allowing the client to verify the signature using the server's public key.

Benefit: Ensures that messages originate from the intended sender (server) and have not been tampered with, establishing trust and accountability.

Secure Password Storage

Solution: Implemented secure password storage by hashing user passwords using the SHA-256 algorithm along with a unique, randomly generated salt for each user. The salt is stored alongside the hashed password on the server.

Benefit: Protects user passwords from being easily cracked or reversed, even if the server is compromised, enhancing the overall security of user accounts.

4. Recommendations and Future Considerations


While the implemented security measures significantly improve the security and privacy of the messaging application, there are still areas for further enhancement:

- **Recommendation 1:** Implement a secure key exchange mechanism, such as Diffie-Hellman, to strengthen the security of the shared encryption key and HMAC secret key.
- **Recommendation 2:** Explore the integration of client-side certificates or other authentication mechanisms to provide an additional layer of security and verify the identity of users.
- **Recommendation 3:** Investigate the implementation of perfect forward secrecy to protect past messages in case of key compromise.
- **Recommendation 4:** Consider implementing key revocation and user account deletion functionalities to enhance user control over their data and privacy.

Conclusion

The security and privacy assessment of our messaging application has revealed several vulnerabilities and areas for improvement. By implementing user authentication, encrypted communication, message integrity and authentication, digital signatures, and secure password storage, we have significantly enhanced the security posture of the application.

However, it is crucial to recognize that security is an ongoing process, and continuous monitoring, evaluation, and improvement are necessary to stay ahead of evolving threats. By adhering to industry best practices and regularly updating our security measures, we can ensure the confidentiality, integrity, and privacy of our users' data.



We recommend prioritising the implementation of the aforementioned recommendations to further strengthen the security and privacy of the messaging application. By doing so, we can foster trust among our users and maintain a secure communication platform for our messaging uses.