BFTB Banking

SEC Project Report

Group 20

89627, Gustavo Pinto

102118, Rui Costa

102146, Sebastião Sotto Mayor

April 1, 2022

Design of the Solution

For our solution we have decided to use UDP sockets for messages sent between the Bank and the client (via the API), and store the information kept by the bank in CSV files:

- One to store information on the clients
- One for each client to store information on pending transfers
- One for each client to store information on completed transfers

Each entity shall have its own key pairs in order to sign the messages it sends, and we assume public keys have already been distributed between entities. To generate these keys, we have provided a shell script (defaulted to 6 clients) which generates a certificate authority certificate, that signs the keys of the bank and client entities, also generated in this script.

Furthermore, a KeyStore object written into a file is used in order to maintain an in-memory protected storage for a user private key. Each user has his own password protected KeyStore where he can store multiple keys if wanted.

Possible system threats

Man-in-the-middle attacks

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. [1]

Replay attacks

A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. [2]

Sybil attacks

A Sybil attack is a kind of security threat on an online system where one person tries to take over the network by creating multiple accounts, nodes or computers. [3]

Implemented system protections

- Integrity and freshness checks are done in every message exchange, which ensure the authenticity of the sender, thus eliminating the possibility of man-in-the-middle and replay attacks. To achieve this, integrity guarantees have been established, which are explained in the respective subsection.
- All system users are assumed to be non-malicious. Therefore, there is no need to protect against Sybil attacks in this stage of the project.

Confidentiality Guarantees

All information is assumed to be public, so no confidentiality issues arise when sending the messages. Therefore, there is no need for confidentiality guarantees.

Dependability Guarantees

Integrity

To guarantee integrity of the system we have used:

- Message digest (hash) of the information sent between entities to prevent manipulation attacks on the message sent.
- Signing of the message digest along with a timestamp by the sender to guarantee authenticity.
- Incremental token in requests, to prevent duplicate, drop and reject attacks on messages sent through the UDP channels.

Availability and Reliability

- As there is no server replication yet in this stage of the project, there are no availability and reliability guarantees. This means that the system may stop providing its service if some unexpected event occurs.
- To prevent the system from terminating at every error (leading to a system failure), exceptions are caught and printed, and the client is returned to the bank options menu to resume the service.

Safety

The system in hand is a safety-critical one [4], because of significant financial loss in the event of a serious failure. This issue is mitigated by handling exceptions and returning the client to a safe state whenever an unexpected event occurs.

Maintainability

All significant system actions are logged to help maintainers detect errors before they cause a system failure. Also, the way the system is structured in a modularized way, permits the easy restoration of service in the event of a system failure.

References

[1] https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

[2] https://www.kaspersky.com/resource-center/definitions/replay-attack

[3] https://academy.binance.com/en/articles/sybil-attacks-explained

[4] https://www.technipages.com/definition/safety-critical-system