ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 3, pp: (58-59), Month: July - September 2023, Available at: www.researchpublish.com

Cryptographic Key Generation for Logically Shared Data Stores

[1]Mashael Alsaleh, [2]Abdullah Aldossary

Saudi Aramco, Dhahran, Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.8185969

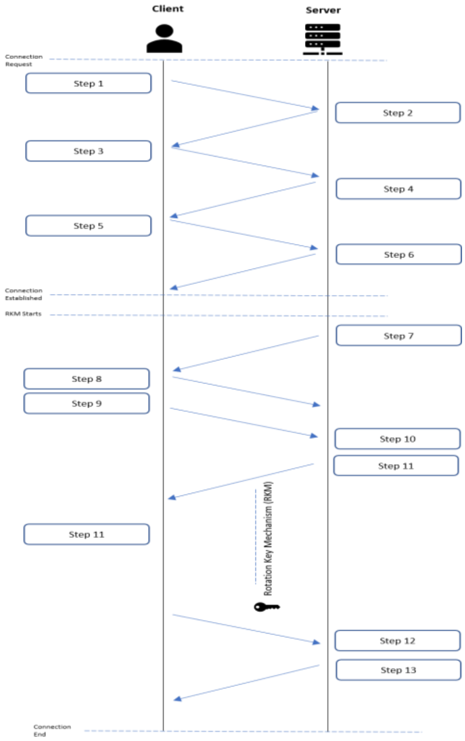
Published Date: 26-July-2023

Abstract: **This research explains a method of establishing a secure communication between a client and a server using a rotating key mechanism. The method comprises receiving a message requesting communication from a client, returning information for establishing communication to the client, including a set of cipher suites supported, receiving from the client one or more selected cipher suites from the set of cipher suites, sending rotation key mechanism attributes (RKM attributes) including a number of keys for rotation, a valid time period for each key, and a server criticality level and establishing communication between the client and server based on the rotation key mechanism attributes. The RKM attributes establish terms for key rotation when a valid time period of an active key elapses.**

Keywords: **Cryptographic Key Generation, RKM attributes, secure communication, key elapses.**

1. METHODOLOGY

This research aims to secure the communication channel between servers and clients to prevent potential security threats such as data leakage, or man-in-the middle attacks. In this research, the server will have a set of keys that will be used by the client to encrypt the communication, Moreover, the server will determine the number of keys, the time duration for each key to be valid, and its criticality. Based on this information, the client will start communicating using the information provided by the server. This process will continue until the client send a notification to the server to end the communication.



The negotiation between the client and the server starts by sending “Client-Hello”. When server sends “Server-Hello” packet which includes (session id, digital certificate, and public key, set of cipher suites supported for Rotation Key Mechanism (RKM)). The client verifies the server’s certificate with the Certificate Authority (CA), to establish trust between the client and the web server, and sends the cipher suits supported to server. The client can send one, or two cipher suits from the set of supported cipher suits from the server. Then, the server sends the Rotation Key Mechanism (RKM) attributes (number of keys, key rotation time, and system criticality categorization). After that, the client sends its private key which is encrypted by the server’s public key, and sends finished packet. When this is done, the server responds with a finished packet. The communication channel is established now. After that, the server sends the first key to the client with the time required to change the rotation of the keys. Also, it sends the category for the server criticality (critical, important, medium, and low). The time required to change the rotation of the keys is based on the server criticality (Higher criticality means key rotation time decreases, low criticality means key rotation time increases). The server criticality is based on the zone that the server is located on. For example, if the server is internet-facing then the criticality is high, if it is in intranet then the criticality is high/medium, and if it is located in isolated network, then the criticality is low. The client receives the information sent by the server and acknowledge the number of keys, the time required to change the rotation of the keys, and the server criticality. Then, the client uses the key sent by the server to encrypt its communication for the specified time agreed upon based on the server criticality. This is to prevent man-in-the-middle attack. The client keeps sending packets until the specified time agreed upon finishes. The server receives the packets from the client and decrypt them using its public key. After that, the server sends another rotation key to the client and the process starts again.

When the communication is done, the client sends a finished packet to inform the server it’s no longer sending packets, and the server sends finished packet, and the communication is terminated.

Rotation Key Mechanism (RKM):

The rotation key mechanism is to establish an agreement between the client and server of how many keys are used, how long for a key to be used in a communication until it changes, and how critical the server is. This information is provided by the server in the “server-Hello” packet (Step2), which will include:

- Supported cipher suits.
- Number of keys.
- Key Rotation time.
- System criticality.

System Criticality	Key Rotation Time
Critical	5 Minutes
Important	10 Minutes
Medium	30 Minutes
Low	1 Hour

2. CONCLUSION

In conclusion, this research article presents a robust method for establishing secure communication between clients and servers through a rotating key mechanism. The method involves a systematic process of exchanging information, selecting cipher suites, and implementing rotation key mechanism attributes (RKM attributes) to ensure a continuous and secure flow of communication. By defining key rotation terms based on the valid time period of active keys, this approach enhances the security and resilience of the communication channel. This innovative method holds great potential for strengthening data protection and safeguarding sensitive information during client-server interactions, making it a valuable contribution to the field of secure communication protocols

REFERENCES

[1] https://patents.google.com/patent/CN102510387B/en?q=TLS+Handshake&oq=TLS+Handshake

[2] https://patents.google.com/patent/US20180091483A1/en?q=TLS+encryption&oq=TLS+encryption