Secure client-server communication

B Bharadwaj 21CSB0B07

Palacharla Sri Satya Naveen 21CSB0B69

**Introduction:**

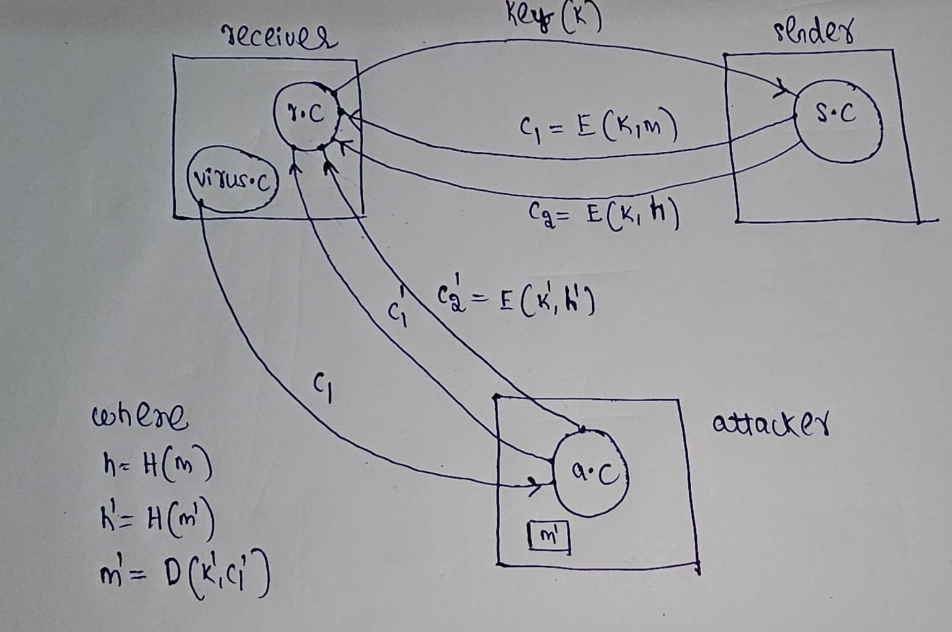
In our project, we explore a robust cryptographic communication system designed to secure message transmissions against sophisticated cyber-attacks. Initially, the communication begins with the receiver sending a secure key to the sender. Utilizing this key, the sender encrypts the message using the Advanced Encryption Standard (AES) algorithm and dispatches the ciphertext to the receiver. However, vulnerabilities arise when an attacker injects a virus into the receiver’s system, enabling them to intercept and slightly modify the ciphertext before redirecting it back to the receiver. Consequently, the receiver faces the dilemma of identifying the legitimate message, as they receive two ciphertexts – one from the original sender and another from the attacker.

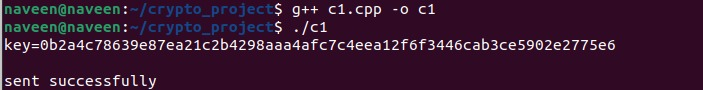
To counteract this security breach, our system integrates the use of encrypted hash. The sender generates an encrypted hash by encrypting a hash of the message, created using the SHA-256 algorithm, with their private key. As the attacker lacks access to the original sender's private key, they are forced to use an alternative key to forge a hash. Upon receipt, the receiver verifies both hash values against the known key of the sender. This verification process enables the receiver to accurately determine the authenticity of the message, effectively identifying the intended sender and mitigating the risk of manipulated messages. This approach not only enhances the integrity of the communication but also fortifies the overall security framework against potential cryptographic attacks.

**Objectives:**

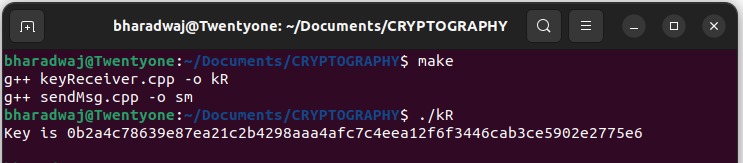
* Implement a cryptographic system using AES and SHA-256 to ensure message authenticity and prevent unauthorized modifications.
* Develop robust verification mechanisms to distinguish between legitimate and tampered messages, enhancing security against cyber-attacks.

**Implementation and Results analysis:**

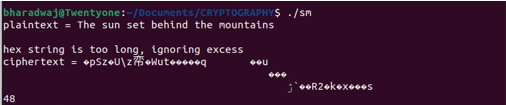
****

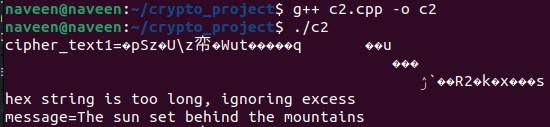
1)Receiver sending symmetric key to sender securely. ****

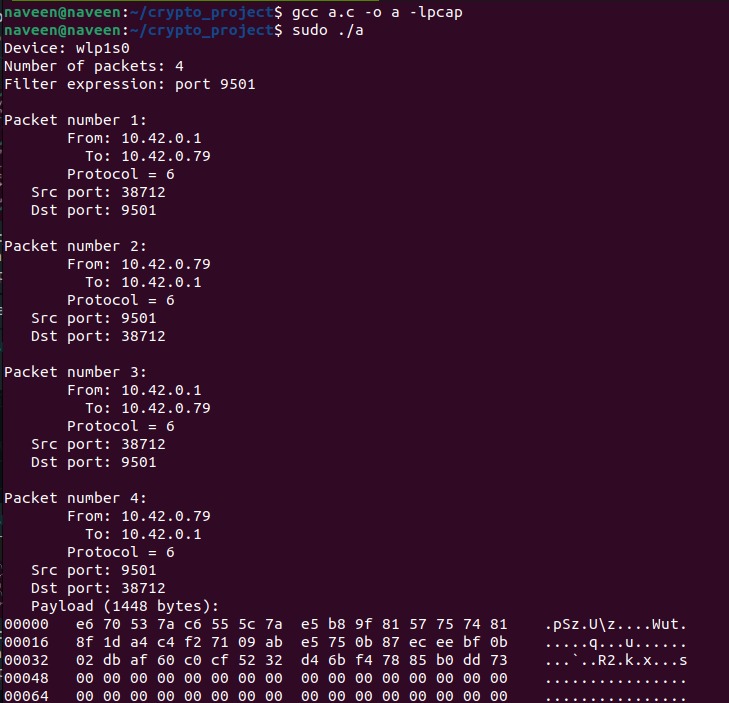
2)Sender received symmetric key from receiver.



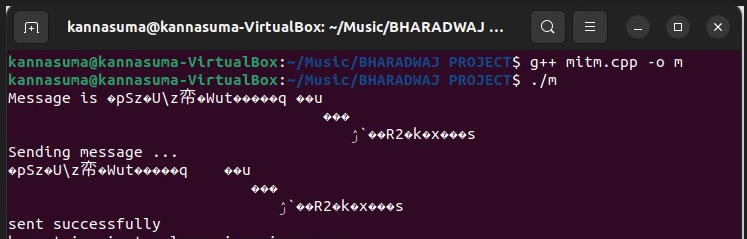
3)Sender sending the ciphertext by encrypting with symmetric key.

  
4)Receiver received the ciphertext and got plaintext by decrypting ciphertext.

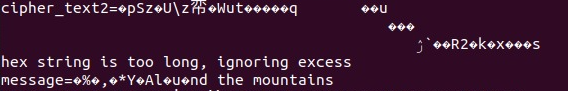


5)A virus program runs in receiver system and captures the ciphertext and sends to attacker. 

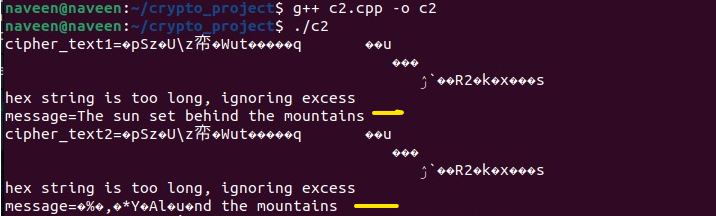
6)Attacker after receiving the ciphertext modifies it slightly and sends back to receiver.



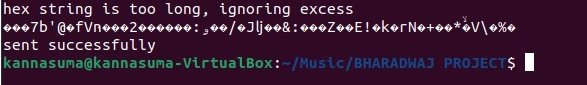
7)Now receiver gets another ciphertext and decrypts it.



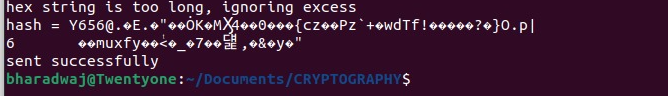
8)Now receiver has two messages and he can’t distinguish between sender and attacker.



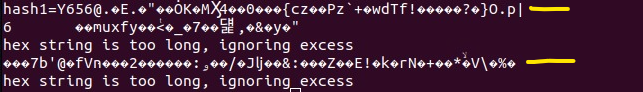
9)Now in order to prevent this attack we use the idea of encrypted hash using sha256 and symmetric key used for encryption. Since attacker don’t know the key he produces the encrypted hash by encrypting hash with his own key and sends to the receiver.



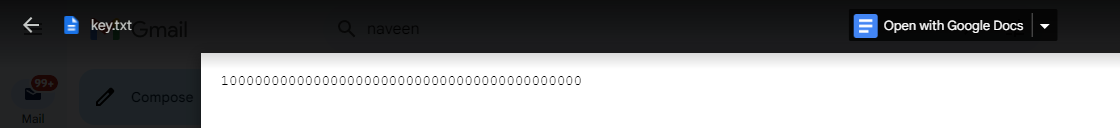
10)Now sender will send the encrypted hash to the receiver by encrypting hash with symmetric key.



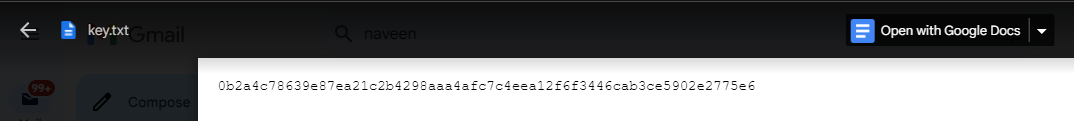
11)Receiver receives both the encrypted hash values. Now receiver will decrypt both encrypted hash values using the symmetric key.



12)Since the attacker’s key is different from the symmetric key receiver finds the hash computed from plaintext sent by attacker is different from the hash found by decrypting the encrypted hash sent by attacker.

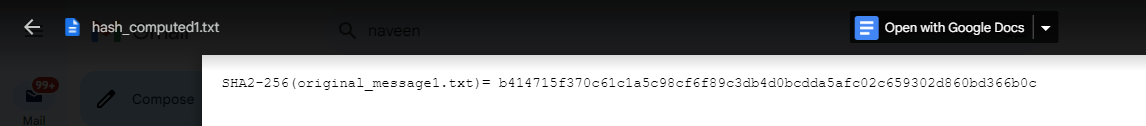


Attacker key



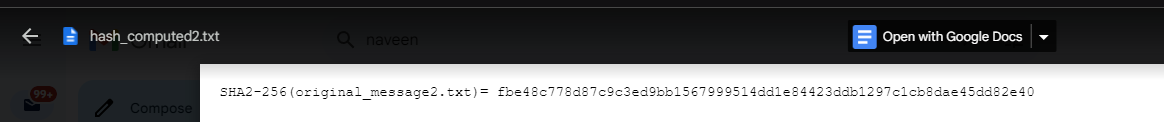
Symmetric key

13) Decrypted hash value1 of encrypted hash1 and Computed hash value from decrypted message of the received cipher text1. 



14) Decrypted hash value2 of encrypted hash2 and Computed hash value from decrypted message of the received cipher text2.





**Conclusion:**

Since receiver finds difference in hash values from one of the sender so he concludes that this corresponding sender is attacker.

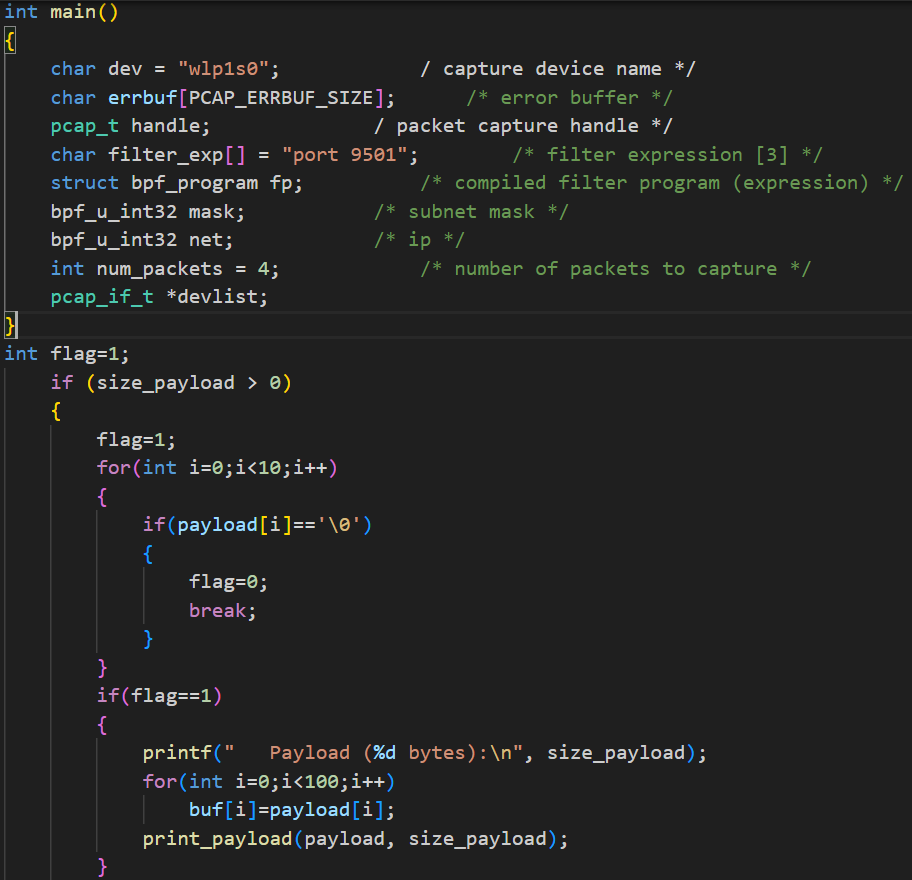
In conclusion, our project has successfully addressed the vulnerabilities in cryptographic communication systems by integrating AES encryption and SHA-256 hashed signatures. By employing these techniques, we have enhanced message authenticity and integrity while mitigating the risk of manipulation by cyber attackers. The combination of encrypted hash and key verification ensures that only legitimate messages from the intended sender are accepted, bolstering overall security against potential cryptographic attacks. This comprehensive approach underscores our commitment to developing robust solutions for secure communication in the face of evolving cyber threats.

**Learning Outcomes:**

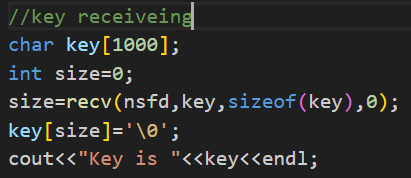
* Gained insights into how Advanced Encryption Standard and Secure Hash Algorithm 256 work to ensure secure and reliable message encryption and hashing.
* Learned to implement encrypted hash to verify message authenticity and integrity, enhancing security protocols.
* Developed a deeper understanding of the role of cryptography in protecting against cyber-attacks, particularly in communication systems.

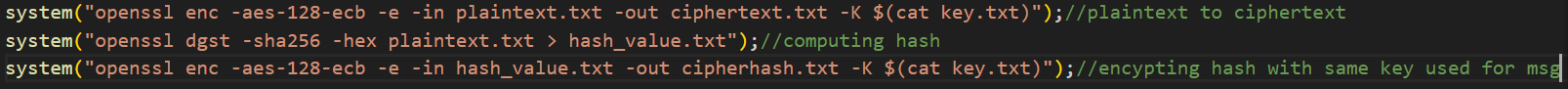
**Source codes:**

Code at attacker side:

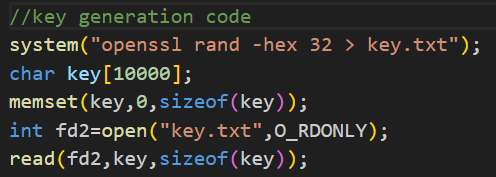


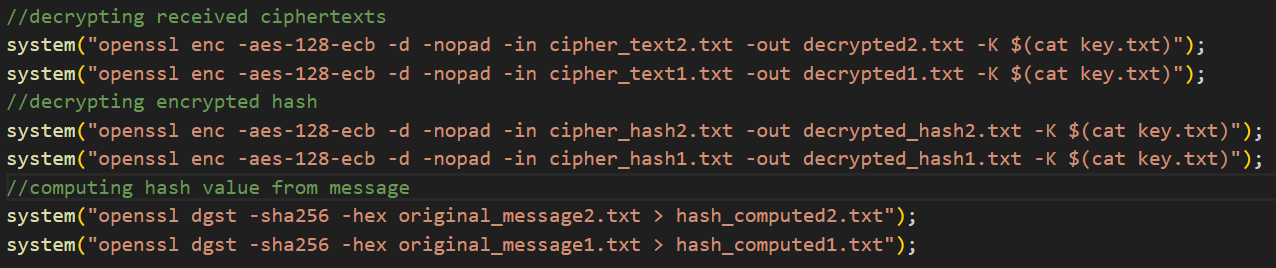
Code at sender side:





Code at receiver side:





**References:**

1)Used inbuilt commands of OPENSSL.

2)Used some code of tcpdump for capturing packets.