Network and Computer Security

Retail: GrooveGalaxy

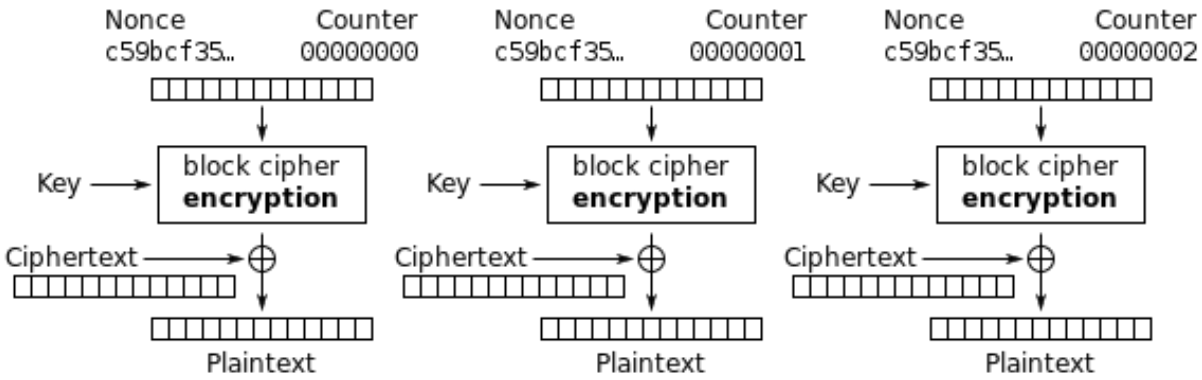
99236 Inês Pissarra
99261 Juliana Marcelino
99275 Mário Santos

Secure Document Library and Tool

Secure Document Library and Tool

- Protect with CTR

  This encryption method allows you to decrypt content that is in the middle of the file.

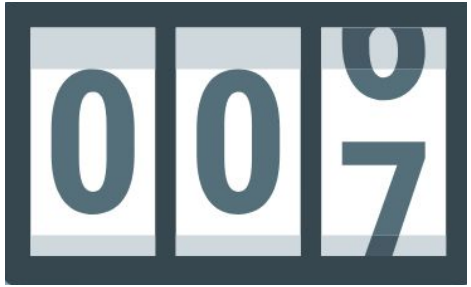


Counter (CTR) mode decryption

Secure Document Library and Tool

- Protect with Nonce

  To ensure the freshness, a nonce composed of a counter and a timestamp is implemented. This prevents replay attacks and old messages from being processed.



Secure Document Library and Tool

- Protect with MAC

  To ensure the integrity of the file, we used a MAC (with 256 bits) algorithm.

- Encrypt-then-MAC:

  It was used EtM method so that we can test the integrity of the file without having to decrypt it

Secure Document Library and Tool

- Check

  Uses MAC algorithm and checks the freshness of the file by comparing the nonce components, counter and timestamp with the current ones.

- Unprotect

  Reverses the protection process. Calls the check class to verify the integrity, and decrypts the file content using AES in CTR mode with the key and initialization vector (this last provided on the JSON).

Secure Document Library and Tool

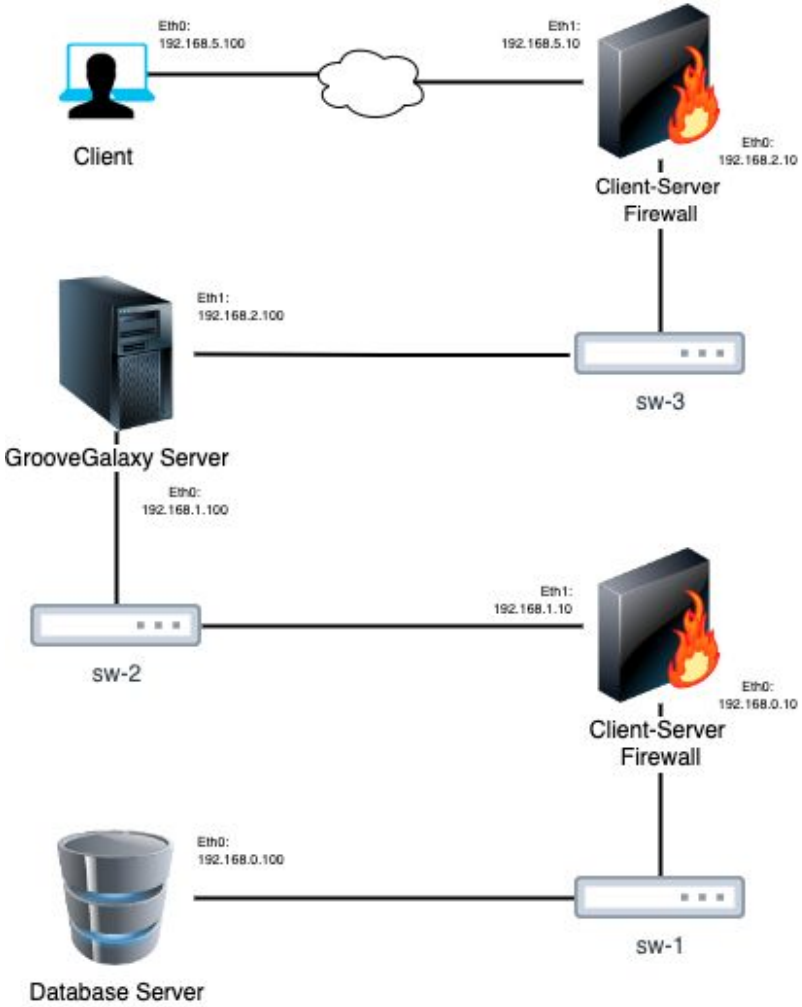
```
Encrypted File Structure:

iv: _________

encrypted File: _________

Nonce:

      Counter: _________

      Timestamp: _________

MAC: (all previous data encrypted)
```

Structure Of The System

Structure Of The System

Virtual machines each with one of the following (total of 5 VMs):

- 1 Client
- 2 Firewalls
- 2 Servers (1 Main and 1 Database)



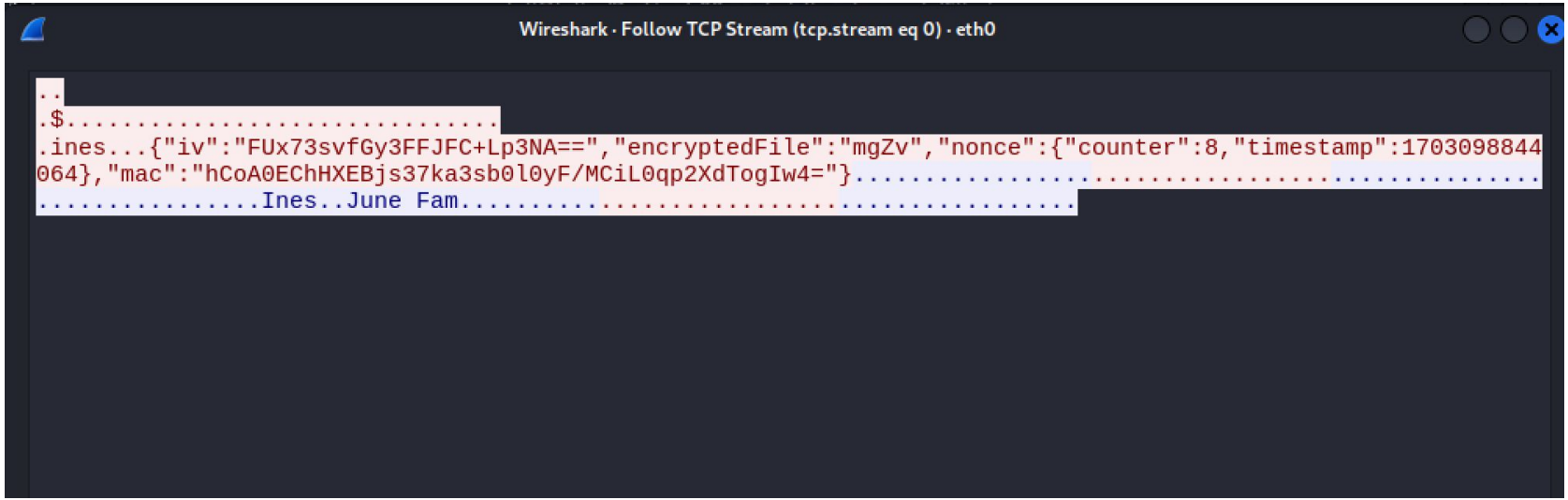
Secure Channels

Secure Channels

- Client and the server communicate via gRPC
- Both client-server and server-database communications use Transport Layer Security (TLS) and one CA for each communication.

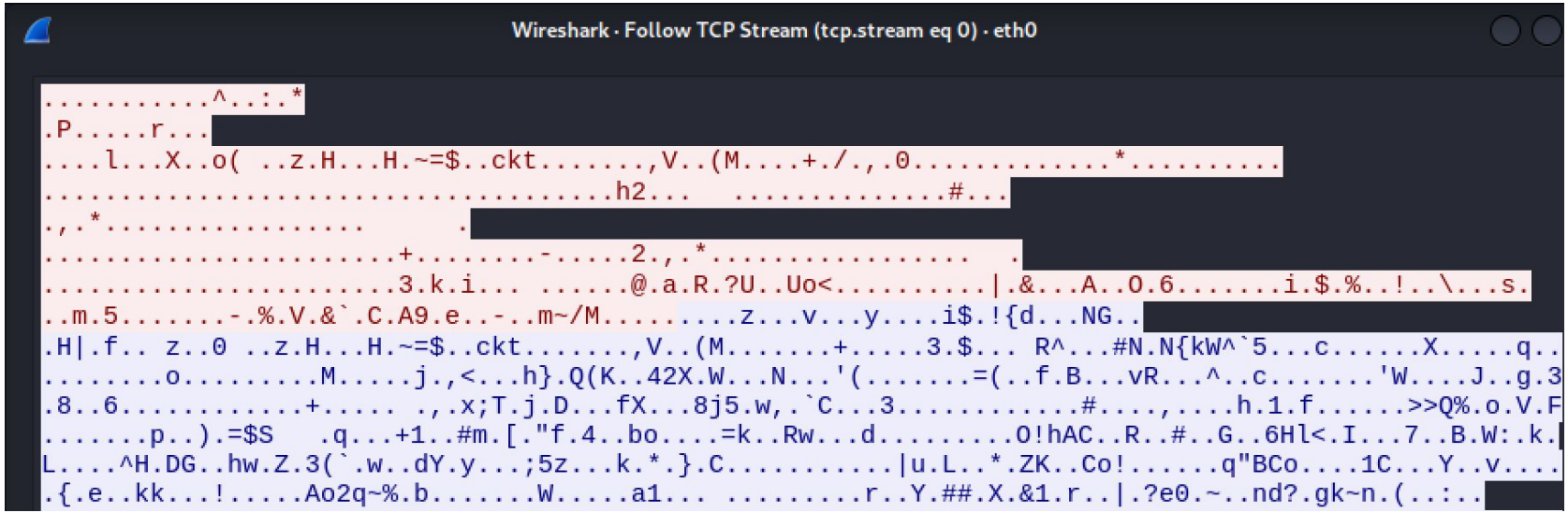
Secure Channels

Encryption without TLS (client-server)



Secure Channels

Encryption with TLS (client-server)



Security Challenge

Family sharing

Each family has its own key that is sent to the family members when they join the family. The keys are encrypted with the member’s key when distributed.

This way, each family member has their own key and the family key.

Playback in the middle of an audio stream

Using CTR we can decrypt from the middle of a file, so it’s possible to decrypt the song from any place we want.

It works like a normal command “play” but when unprotecting the file for the client, we securely decrypt the part from where the client wants until the end, leaving the beginning encrypted.

Demonstration