Network and Computer Security

Retail: GrooveGalaxy

Group A16

João Leitão - 93088
Daniel Gomes - 99195
Simen Myrrusten - 108924

Project Advisor: David R. Matos
Project Evaluator: Miguel Filipe Leitão Pardal

Outline

- Secure document
- Message format
- Architecture
- Router rules
- Security challenge
- Conclusion

Secure document

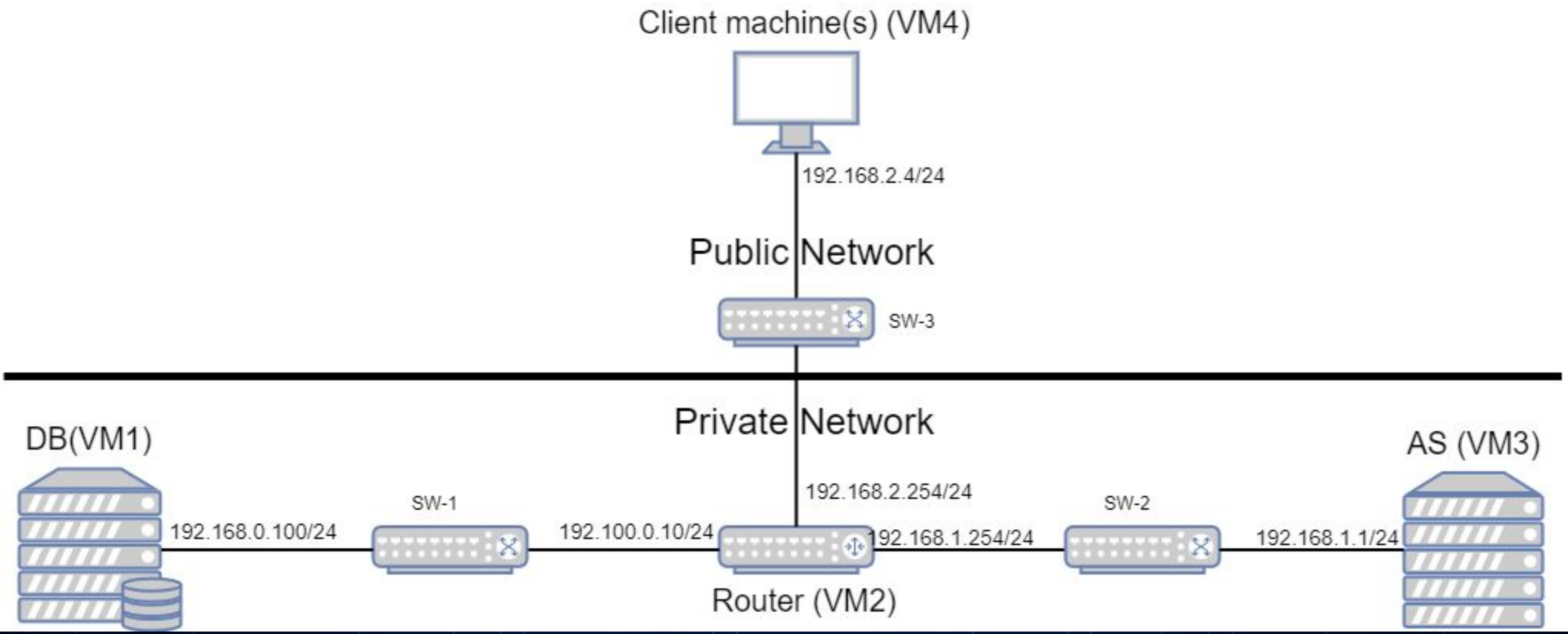
- Provided a single shared secret
- Task: Provide authenticity and confidentiality
- AES/CTR/NoPadding
- AES recognized symmetric encryption
- CTR enables parallel encoding
- HMAC for authenticity

Message format

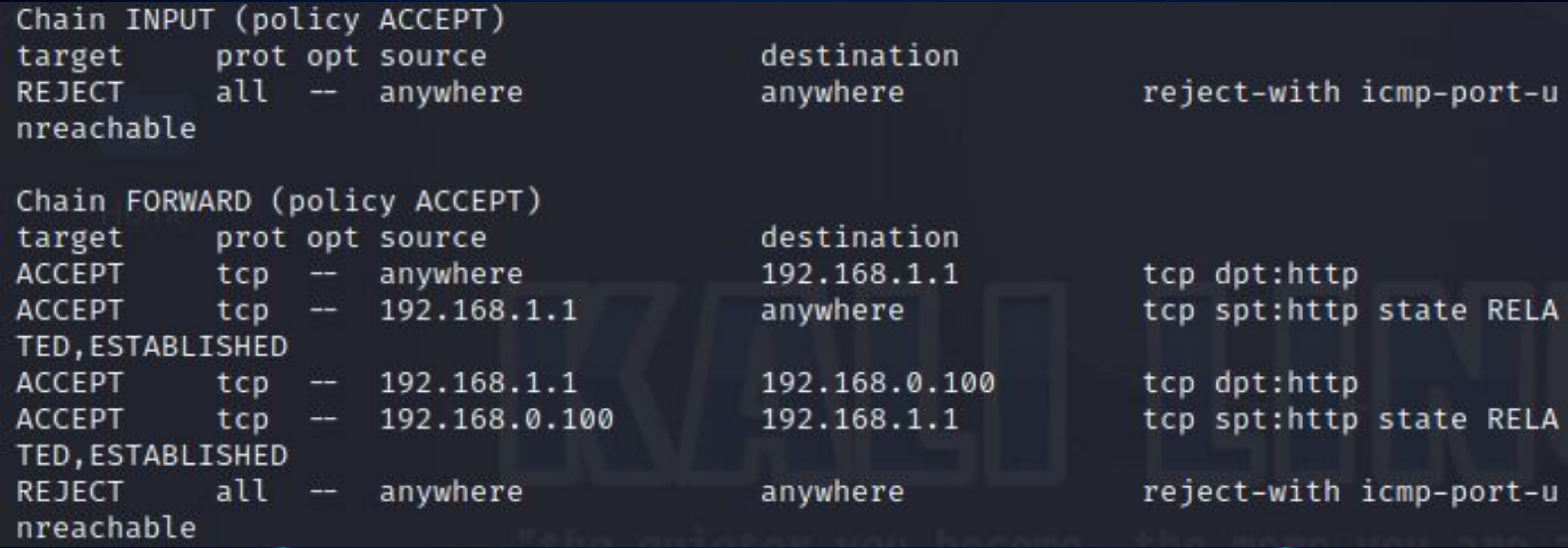
- $\{Tag, \{ProtectedDoc\}_{Klt}, IV_{lt}\}_{Ks}, IV_s$
- $HMAC(\{ProtectedDoc\}_{Klt}, K_{lt})$
- Variables:

- Ks = session key
- Klt = Long-term key (initial shared secret)
- IV_{lt} = IV used for CTR mode in the inner encryption
- IV_s = IV used for CTR Mode in the outer encryption
- HMAC() = the function creating the Tag.

Architecture

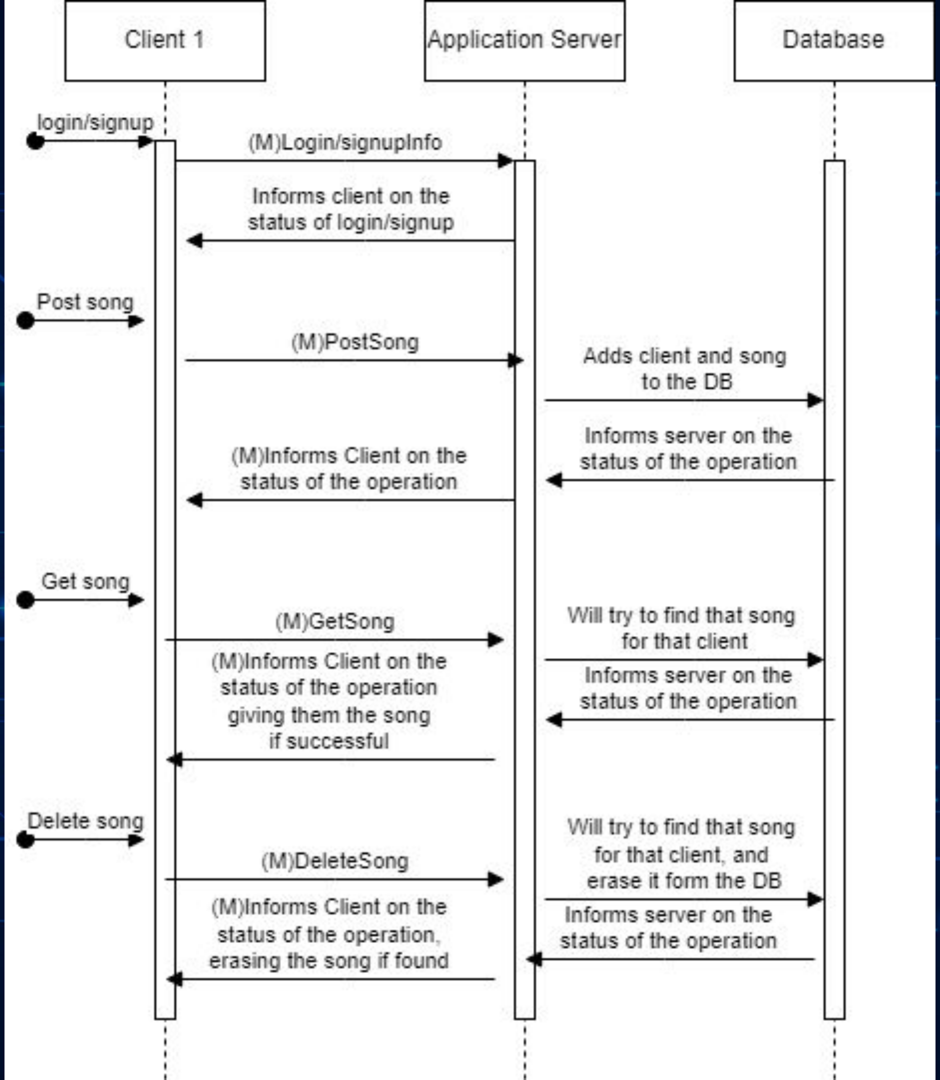


Router rules



```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-u
nreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.1.1          tcp dpt:http
ACCEPT     tcp  --  192.168.1.1          anywhere             tcp spt:http state RELA
TED,ESTABLISHED
ACCEPT     tcp  --  192.168.1.1          192.168.0.100        tcp dpt:http
ACCEPT     tcp  --  192.168.0.100        192.168.1.1          tcp spt:http state RELA
TED,ESTABLISHED
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-u
nreachable
```



Client 1

Application Server

Database

login/signup

(M)Login/signupInfo

Informs client on the status of login/signup

Post song

(M)PostSong

Adds client and song to the DB

Informs server on the status of the operation

(M)Informs Client on the status of the operation

Get song

(M)GetSong

Will try to find that song for that client

Informs server on the status of the operation

(M)Informs Client on the status of the operation giving them the song if successful

Delete song

(M)DeleteSong

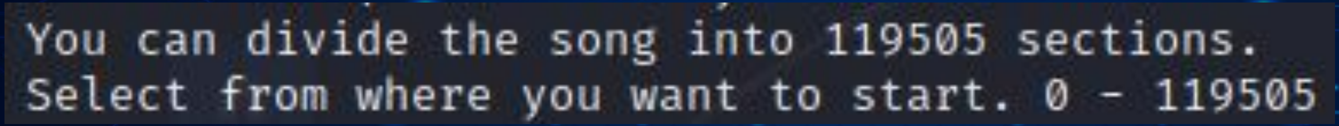
Will try to find that song for that client, and erase it form the DB

Informs server on the status of the operation

(M)Informs Client on the status of the operation, erasing the song if found

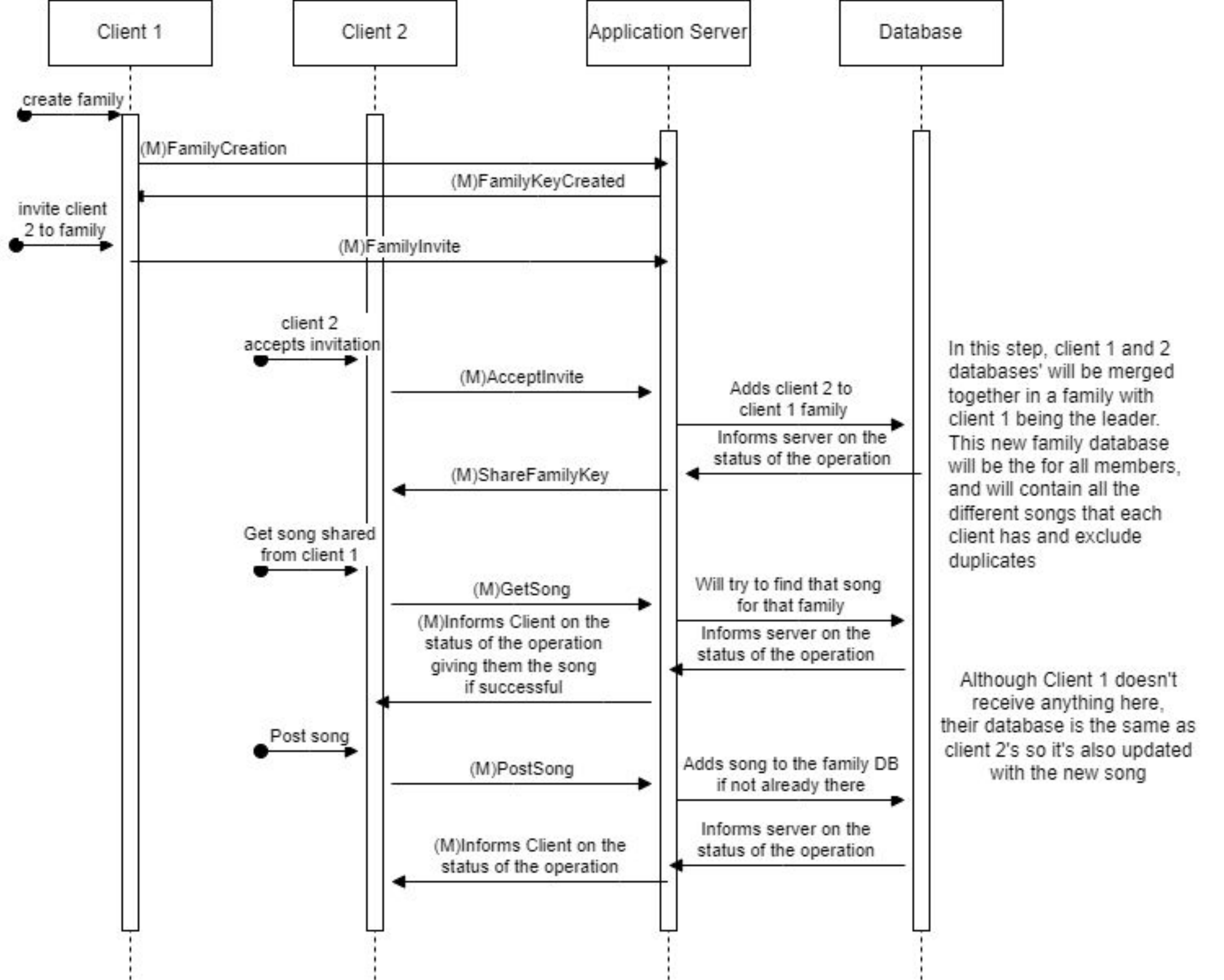
Security challenge

- Fast decryption and family sharing
- Use properties of CTR to encrypt certain parts at client side:



```
You can divide the song into 119505 sections.
Select from where you want to start. 0 - 119505
```

- Select where you want to start in the song. Sections are the blocks of encryptions in CTR.
- More user friendly adaptations could be implemented


Client 1
Client 2
Application Server
Database
create family
(M)FamilyCreation
(M)FamilyKeyCreated
invite client 2 to family
(M)FamilyInvite
client 2 accepts invitation
(M)AcceptInvite
Adds client 2 to client 1 family
Informs server on the status of the operation
(M)ShareFamilyKey
Get song shared from client 1
(M)GetSong
Will try to find that song for that family
Informs server on the status of the operation
(M)Informs Client on the status of the operation giving them the song if successful
Post song
(M)PostSong
Adds song to the family DB if not already there
Informs server on the status of the operation
(M)Informs Client on the status of the operation

In this step, client 1 and 2 databases' will be merged together in a family with client 1 being the leader. This new family database will be the for all members, and will contain all the different songs that each client has and exclude duplicates

Although Client 1 doesn't receive anything here, their database is the same as client 2's so it's also updated with the new song

When a family key is introduced, it is used instead of the initial shared secret in the encryption.

Conclusion

Achievements:

- Working application with client(s), application server and database.
- Integrity
- Authenticity
- Restrictive access of private network
- Family sharing
- “Fast decryption”

Improvements:

- User friendliness
- HTTPS
- Perfect forward secrecy
- Replay attacks protection