UNIVERSITÀ DI PISA

Secure Bank application

Foundation of Cybersecurity project

Fabio Piras
Giacomo Volpi

Introduction and assumption

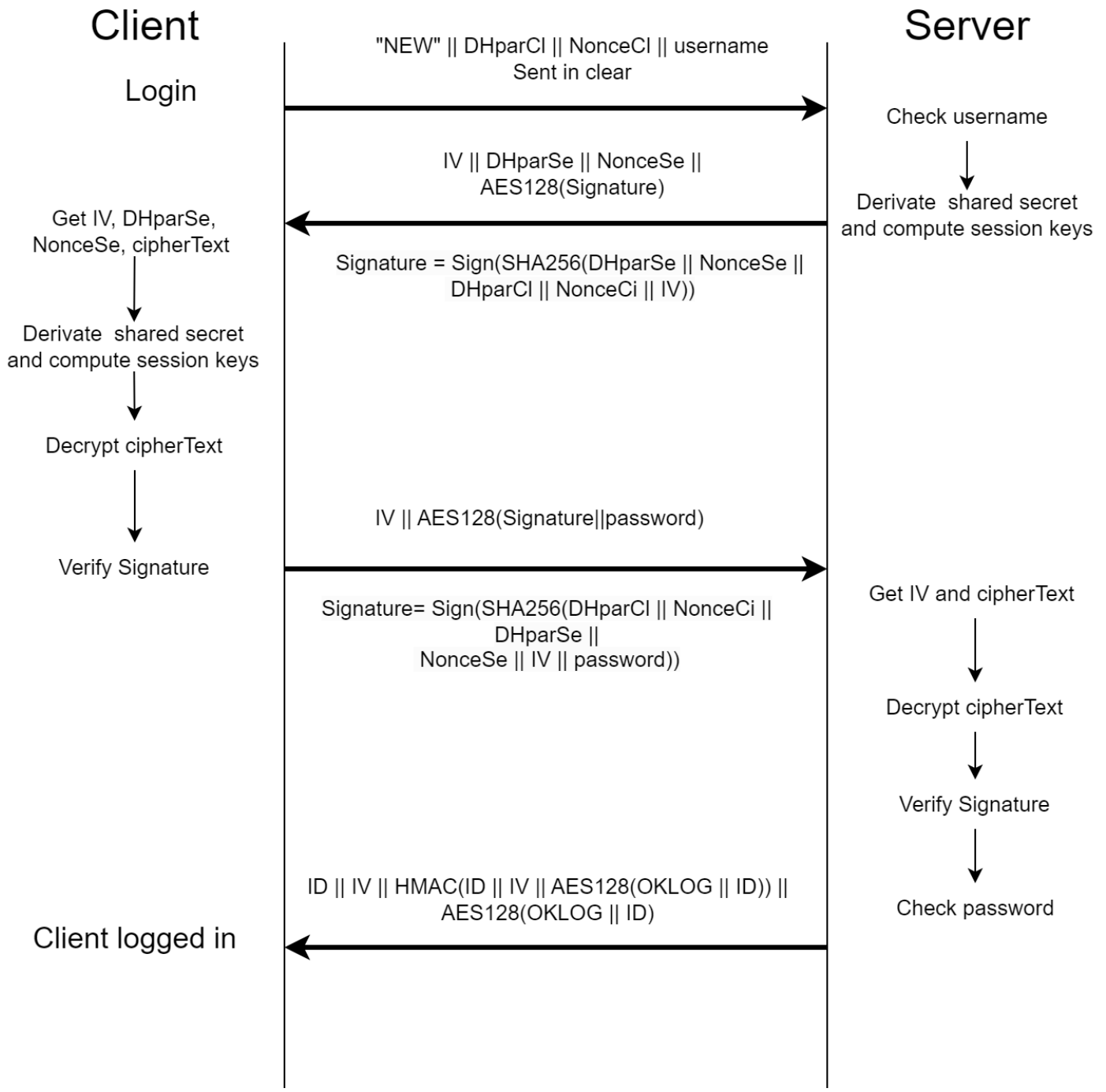
A Secure Bank Application (SBA) is a client-server application that allows users to issue operations on their own bank accounts.

- The SBA server maintains the public key of every user, each user maintains the public key of the server.
- No registration functionality
- Session ids are just one byte (for simplicity)
- There are only two users (f and g) registered
- Balance/Password/History are encrypted, but filesystem must be protected

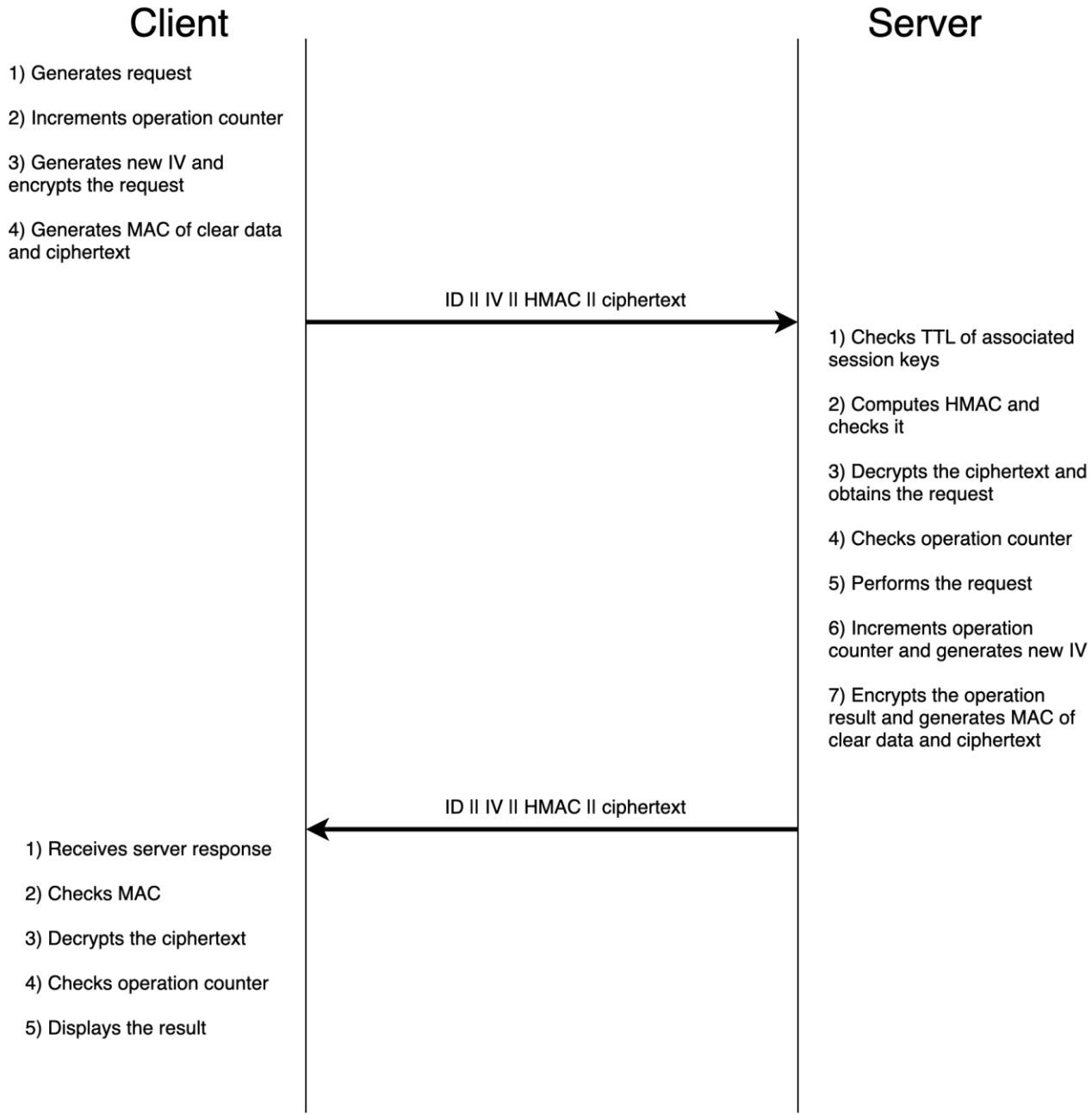
Handshake

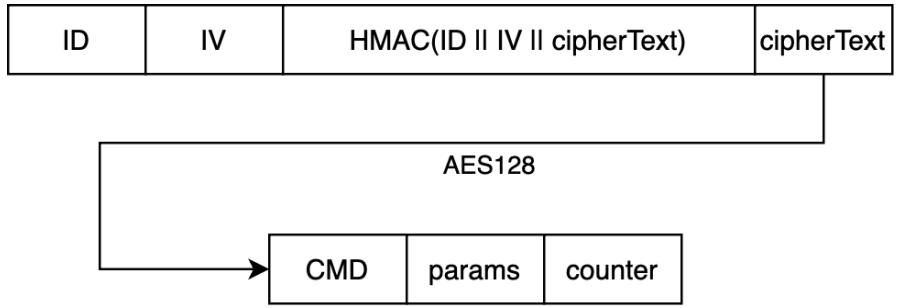
Points of interest:

- Protocol fulfills perfect forward secrecy and direct authentication (use station to station structure)
- The first msg is in clear
- The session keys are computed by hashing the Diffie Hellman shared secret and the nonces
- The Sign process use the private key of the relative actor to sign the hash
- IV are always sent in clear, but the integrity is guaranteed by the hash/HMAC
- If the client or server encounters an error (decrypt failure/verify signature failure) sends “ERR” in clear to the other party (not shown)
- The last msg is always encrypted even in case of error
- Private elements (e.g. DH parameters) are freed after final use (not shown)



Session protocol and message format





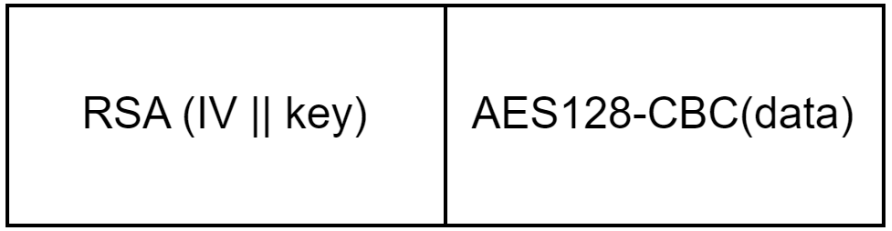
Points of interest:

- Use EtM scheme
- TTL checks are used to prevent «too long» use of the same session keys
- Counters are used to prevent replay attacks inside the session

File encryption

Points of interest:

- Files are encrypted with the digital envelope
- The IV and the key of the symmetric cipher are encrypted with RSA (with secure padding) using the server public key
- The IV and the key are randomly generated each time



Example of file management during a transfer operation:

1. Decrypt sender balance
2. Decrypt receiver balance
3. Check if there is enough balance
4. Update balances
5. Decrypt history
6. Add transaction to history
7. Newly encrypt the files (new IV and key)