Network and Computer Security
GrooveGalaxy Project

André Torres - 99053
Gonçalo Nunes - 99074
Pedro Lobo - 99115

GROUP 52

Outline

- Secure Document Format
- Infrastructure
- Secure Channels and key distribution
- Security Challenge
    - Playback in the middle of an audio stream
    - Family Sharing
- Live Demo
- Conclusion

Outline

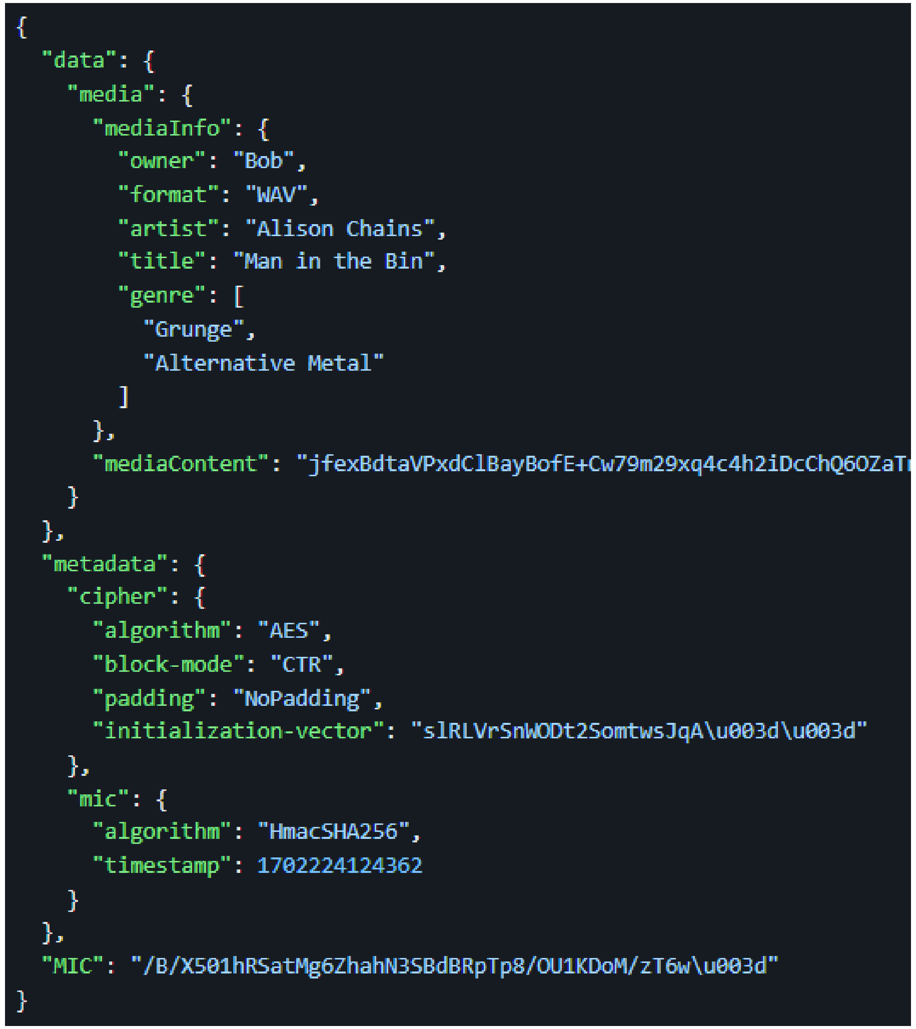
- Secure Document Format
- Infrastructure
- Secure Channels and key distribution
- Security Challenge
    - Playback in the middle of an audio stream
    - Family Sharing
- Live Demo
- Conclusion

Secure Document Format

- Our cryptographic library supports three main operations: protect(), check() and unprotect().

- To ensure **confidentiality**, the application ciphers the song's data with the shared key.

- To achieve **authenticity**, an HMAC-SHA256 is computed over the song data and metadata, using the shared secret key. A timestamp is added to the message to guarantee freshness.



```
{
  "data": {
    "media": {
      "mediaInfo": {
        "owner": "Bob",
        "format": "WAV",
        "artist": "Alison Chains",
        "title": "Man in the Bin",
        "genre": [
          "Grunge",
          "Alternative Metal"
        ]
      },
      "mediaContent": "jfexBdtaVPxdClBayBofE+Cw79m29xq4c4h2iDcChQ6OZaT
    }
  },
  "metadata": {
    "cipher": {
      "algorithm": "AES",
      "block-mode": "CTR",
      "padding": "NoPadding",
      "initialization-vector": "slRLVrSnWODt2SomtwsJqA\u003d\u003d"
    },
    "mic": {
      "algorithm": "HmacSHA256",
      "timestamp": 1702224124362
    }
  },
  "MIC": "/B/X501hRSatMg6ZhahN3SBdBRpTp8/OU1KDoM/zT6w\u003d"
}
```

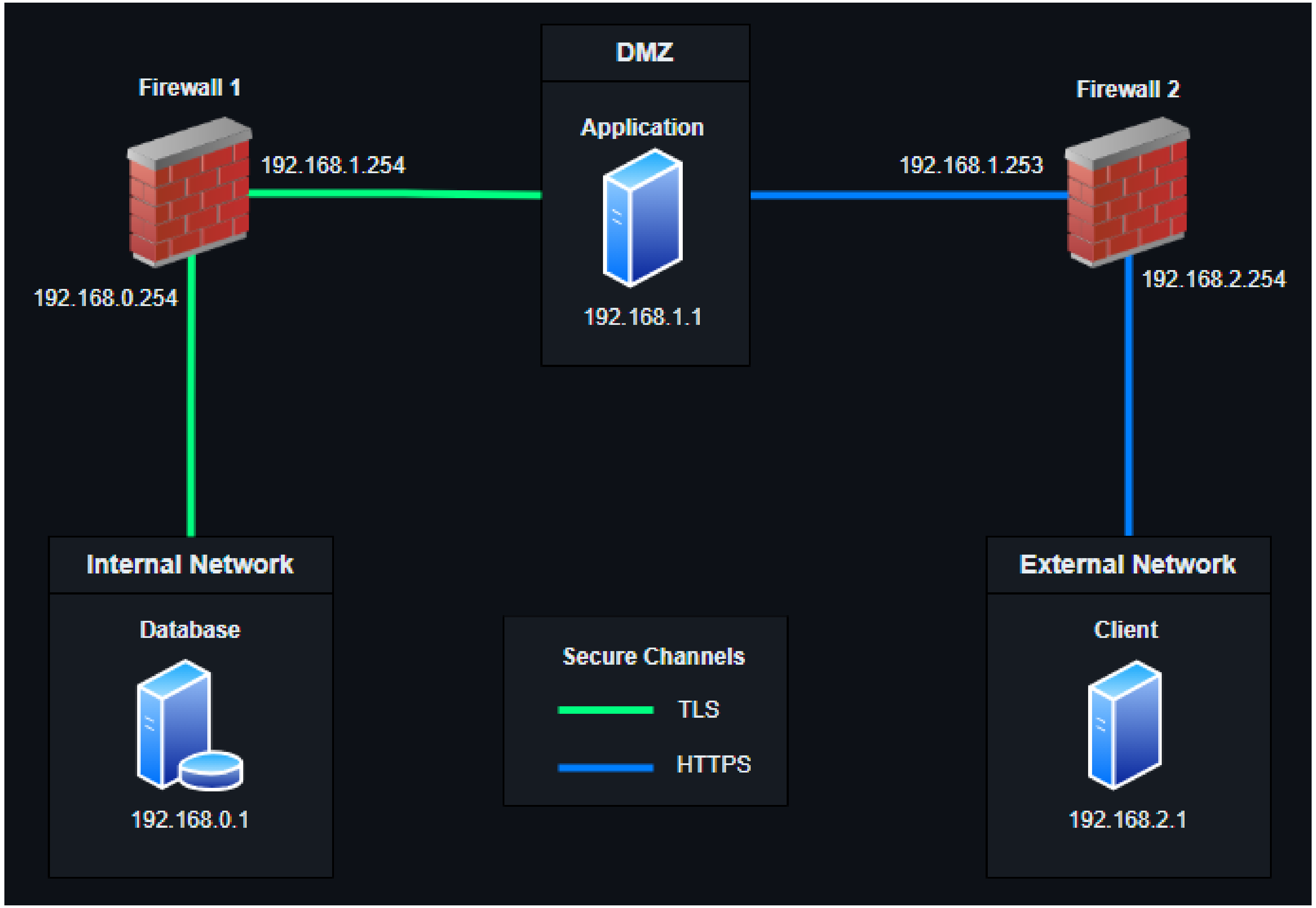
Outline

- Secure Document Format
- Infrastructure
- Secure Channels and key distribution
- Security Challenge
  - Playback in the middle of an audio stream
  - Family Sharing
- Live Demo
- Conclusion

Infrastructure

- Consists of a set of main machines, in three distinct networks, and two firewall machines.

- The main machines include a database machine, an application machine and a client machine that interacts with the application through a command-line interface.



Outline

- Secure Document Format
- Infrastructure
- Secure Channels and key distribution
- Security Challenge
  - Playback in the middle of an audio stream
  - Family Sharing
- Live Demo
- Conclusion

Secure Channels and Key Distribution

- The communication between the internal network (the database server) and the DMZ (the application server) is secured by TLS.

- To secure the communication between the external network (the client) and the DMZ (the application server), HTTPS (HTTP over TLS) was used.

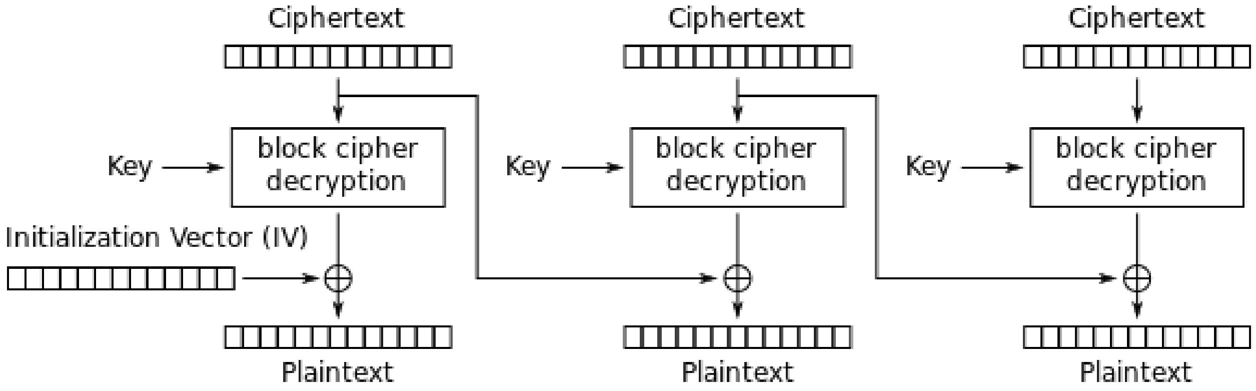
- The keys necessary for the TLS/HTTPS configuration are generated while setting up the machines. The generated keys on the three machines are RSA key pairs. The keys are used to generate a certificate sign request and, in the case of the application server, a self-signed certificate. The certificate requests and copies are then distributed using *scp.*

Outline

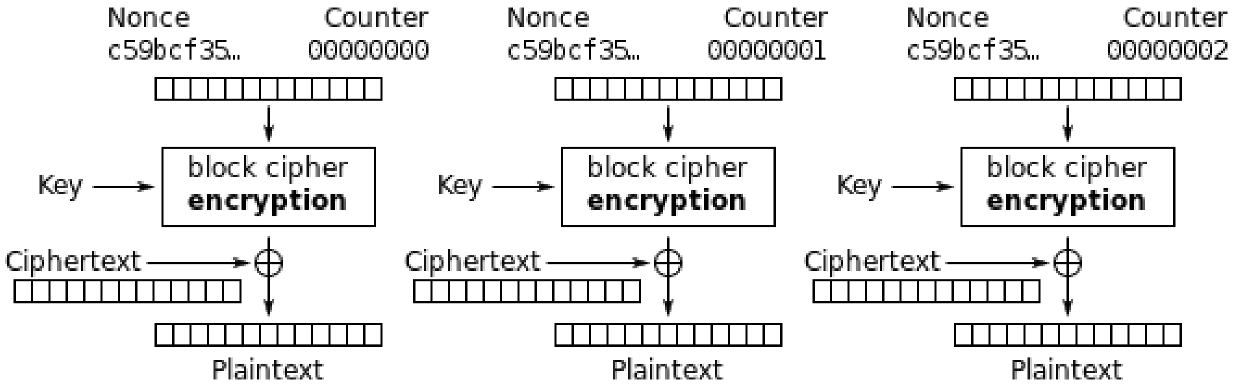
- Secure Document Format
- Infrastructure
- Secure Channels and key distribution
- Security Challenge
    - Playback in the middle of an audio stream
    - Family Sharing
- Live Demo
- Conclusion

Security Challenge: Playback in middle of a stream

- The first security challenge consisted of allowing playback to quickly start in the middle of an audio stream.
- The solution is achieved by using **CTR** cipher mode which allows for random access, unlike in the original implementation which used CBC.



Cipher Block Chaining (CBC) mode decryption

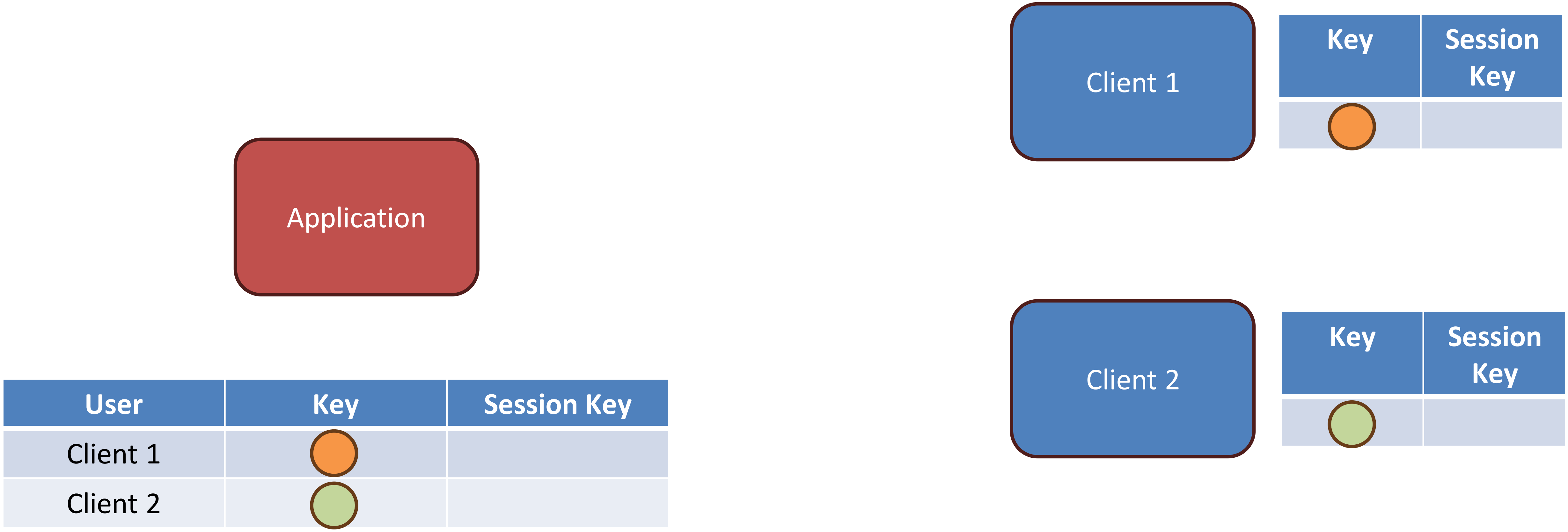


Counter (CTR) mode decryption

Security Challenge: Family Sharing

- Dynamic key distribution.
- Modifications to cryptographic tool to support this feature:
  - Three new operations were added: protect_key(), check_key(), unprotect_key(), generate_key().

Security Challenge: Family Sharing



Application

Client 1

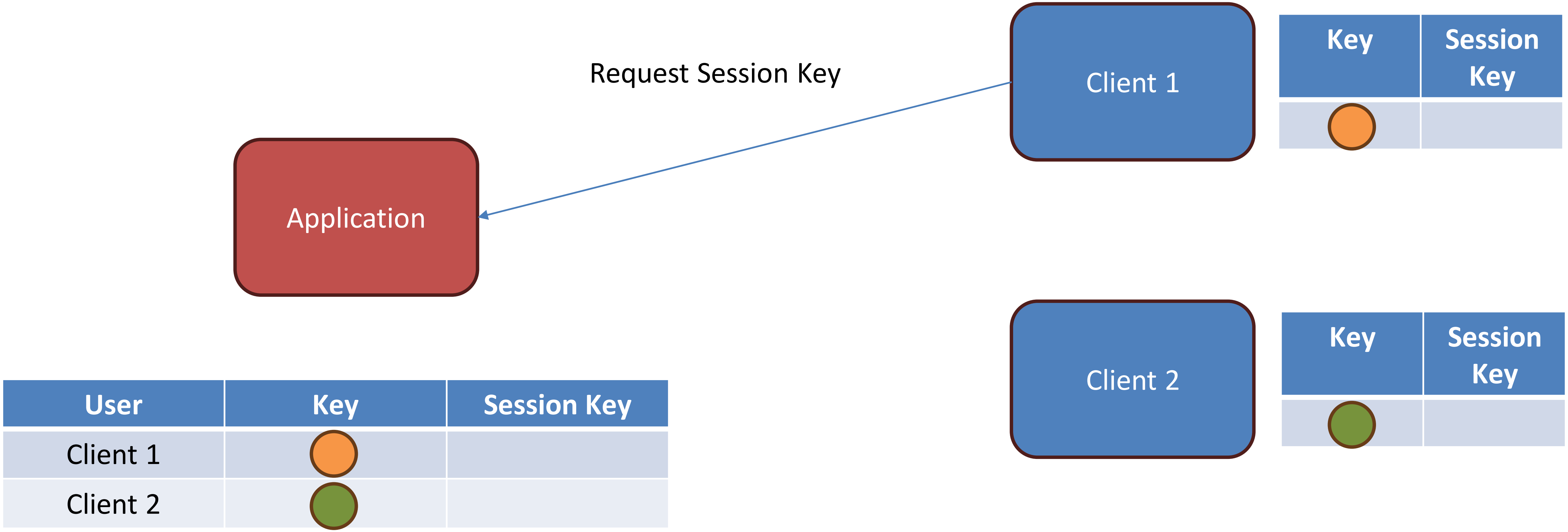
Key	Session Key
🟠	

Client 2

Key	Session Key
🟢	

User	Key	Session Key
Client 1	🟠	
Client 2	🟢	

Security Challenge: Family Sharing

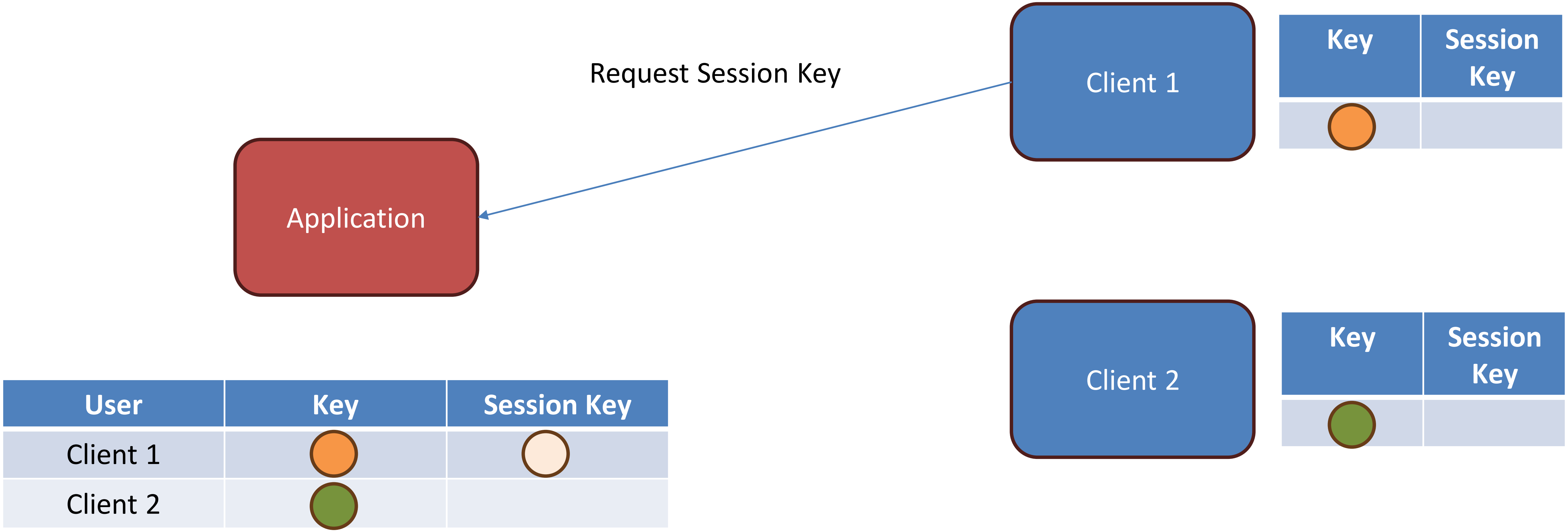


Key	Session Key
🟠	

Key	Session Key
🟢	

User	Key	Session Key
Client 1	🟠	
Client 2	🟢	

Security Challenge: Family Sharing

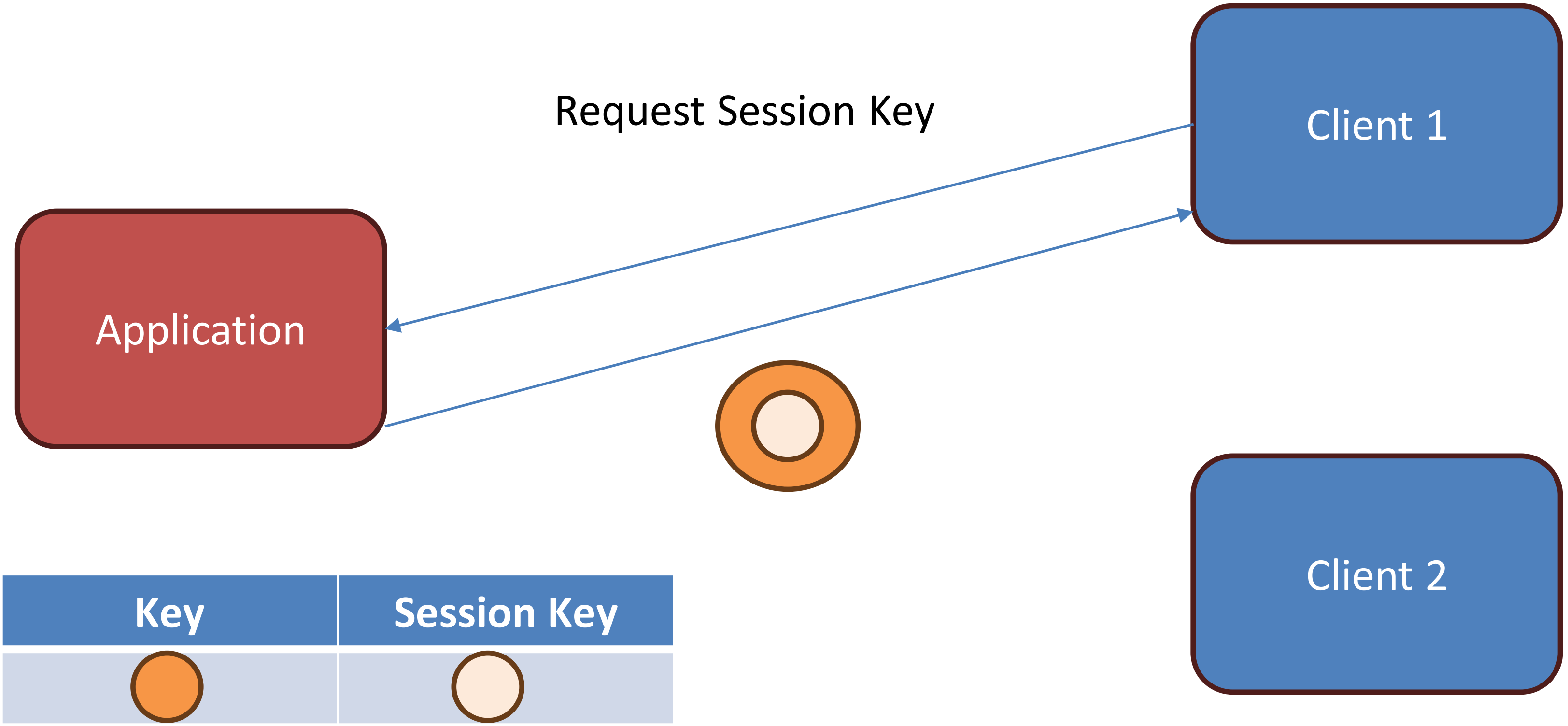


Key	Session Key
●	

Key	Session Key
●	

User	Key	Session Key
Client 1	●	○
Client 2	●	

Security Challenge: Family Sharing

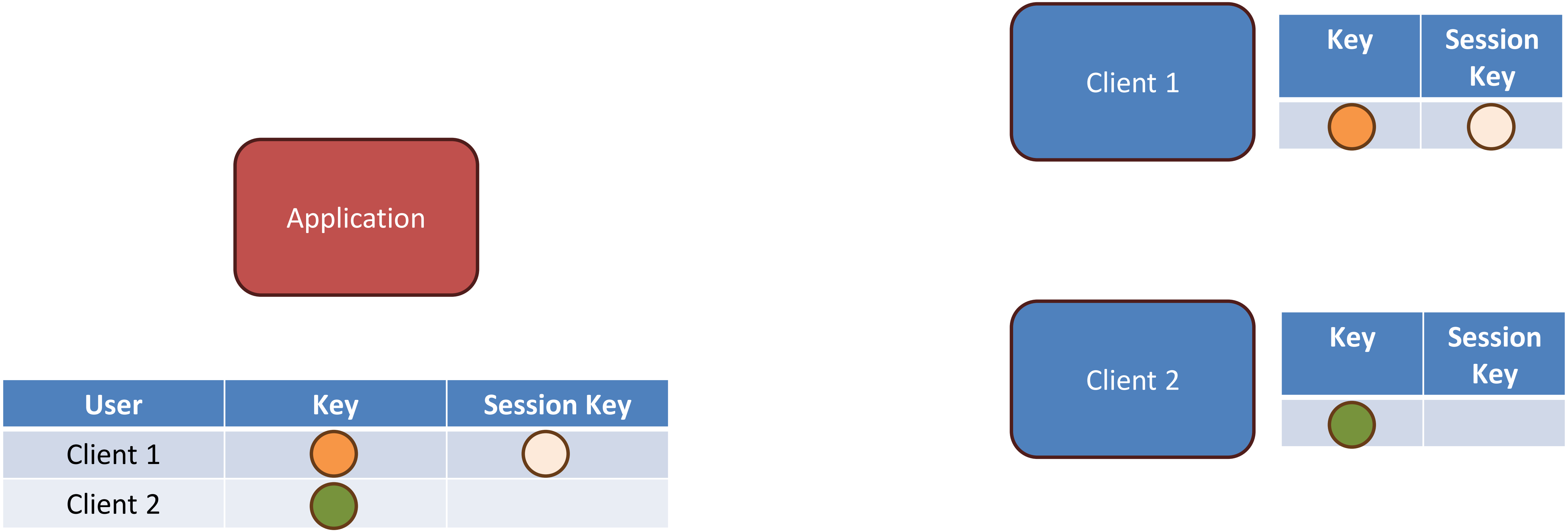


Key	Session Key
🟠	

Key	Session Key
🟢	

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	

Security Challenge: Family Sharing



User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	

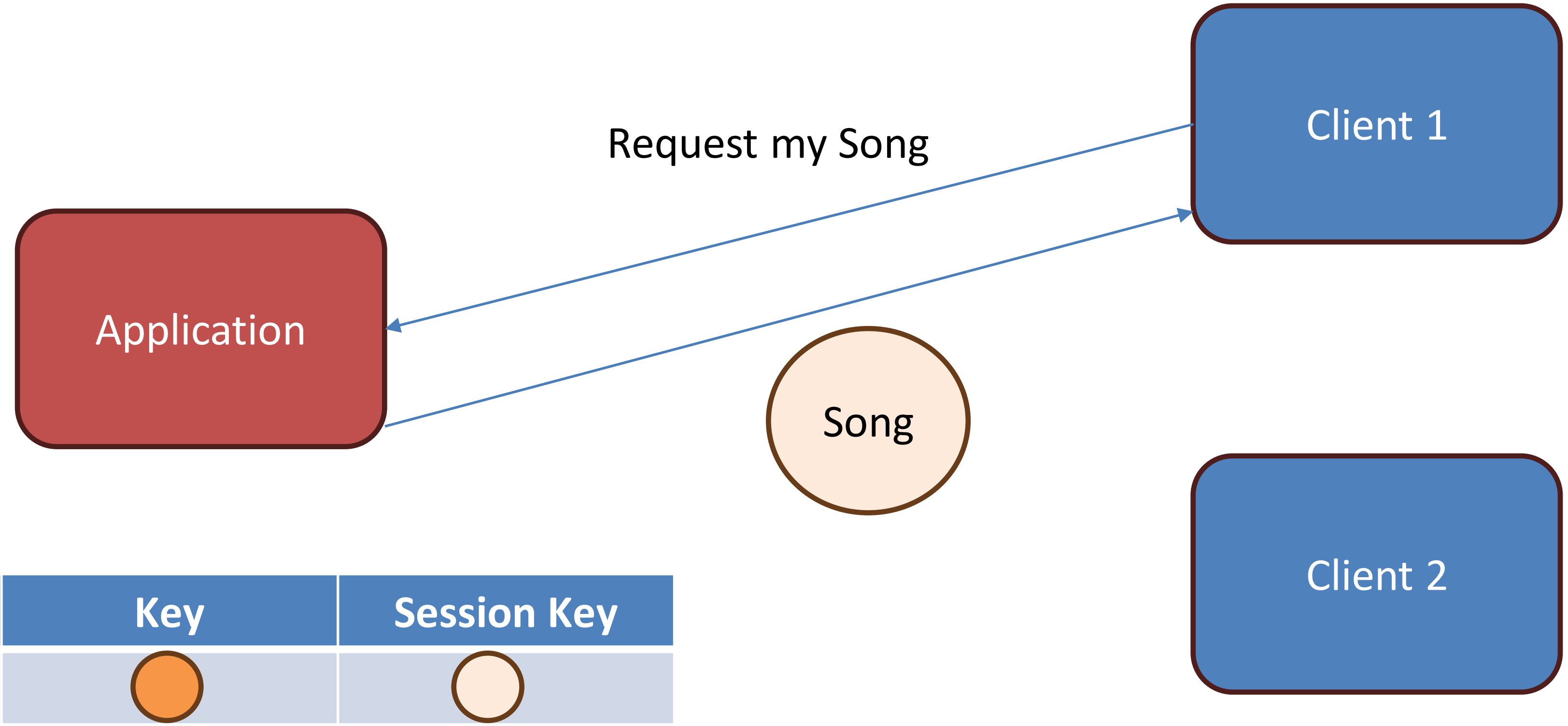
Client 1:

Key	Session Key
🟠	○

Client 2:

Key	Session Key
🟢	

Security Challenge: Family Sharing

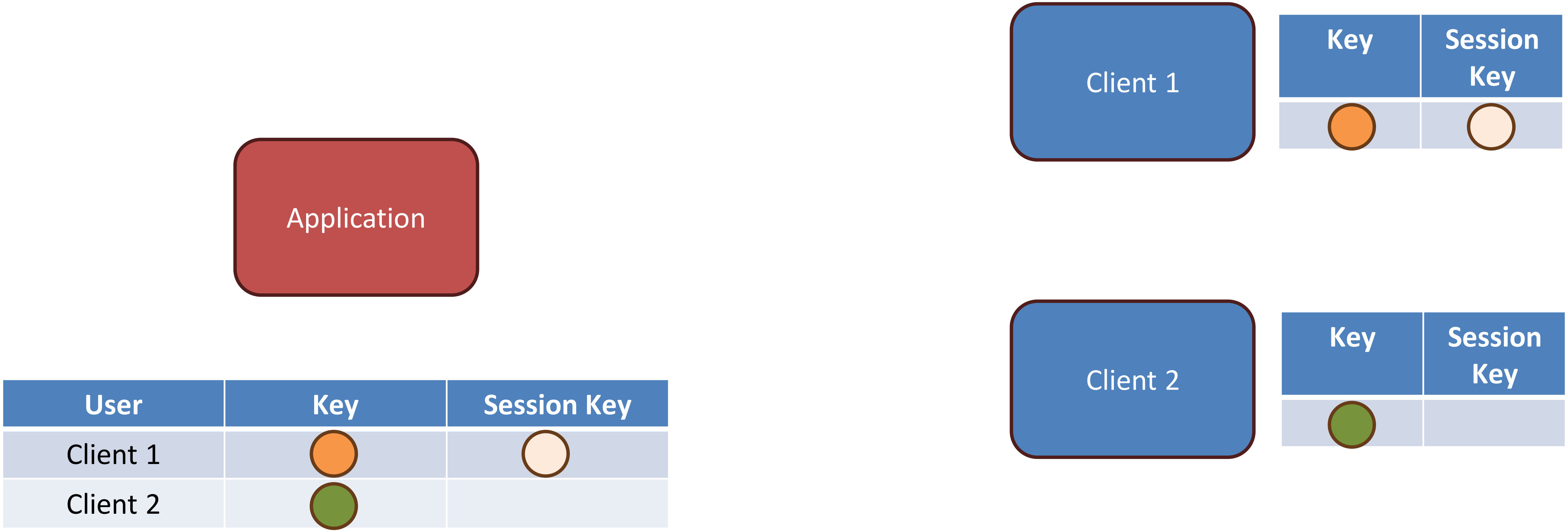


Key	Session Key
🟠	○

Key	Session Key
🟢	

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	

Security Challenge: Family Sharing



Application

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	

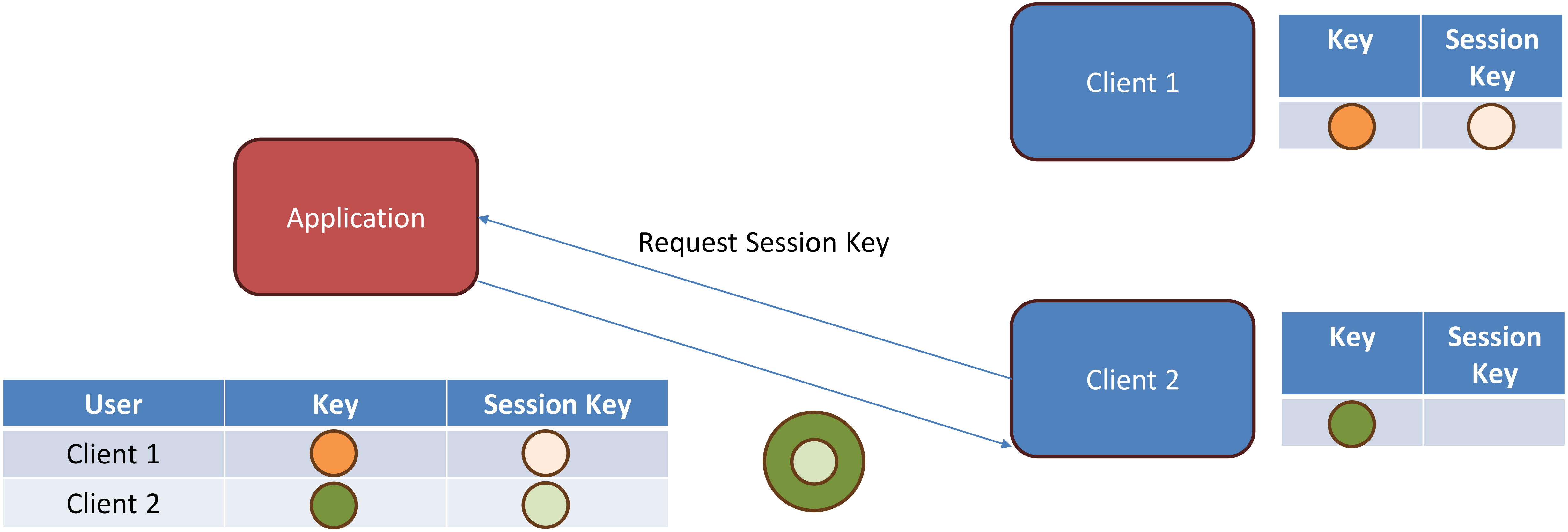
Client 1

Key	Session Key
🟠	○

Client 2

Key	Session Key
🟢	

Security Challenge: Family Sharing



Key	Session Key
●	○

Key	Session Key
●	

User	Key	Session Key
Client 1	●	○
Client 2	●	○

Security Challenge: Family Sharing

Application

User	Key	Session Key
Client 1	🟠	⚪
Client 2	🟢	○

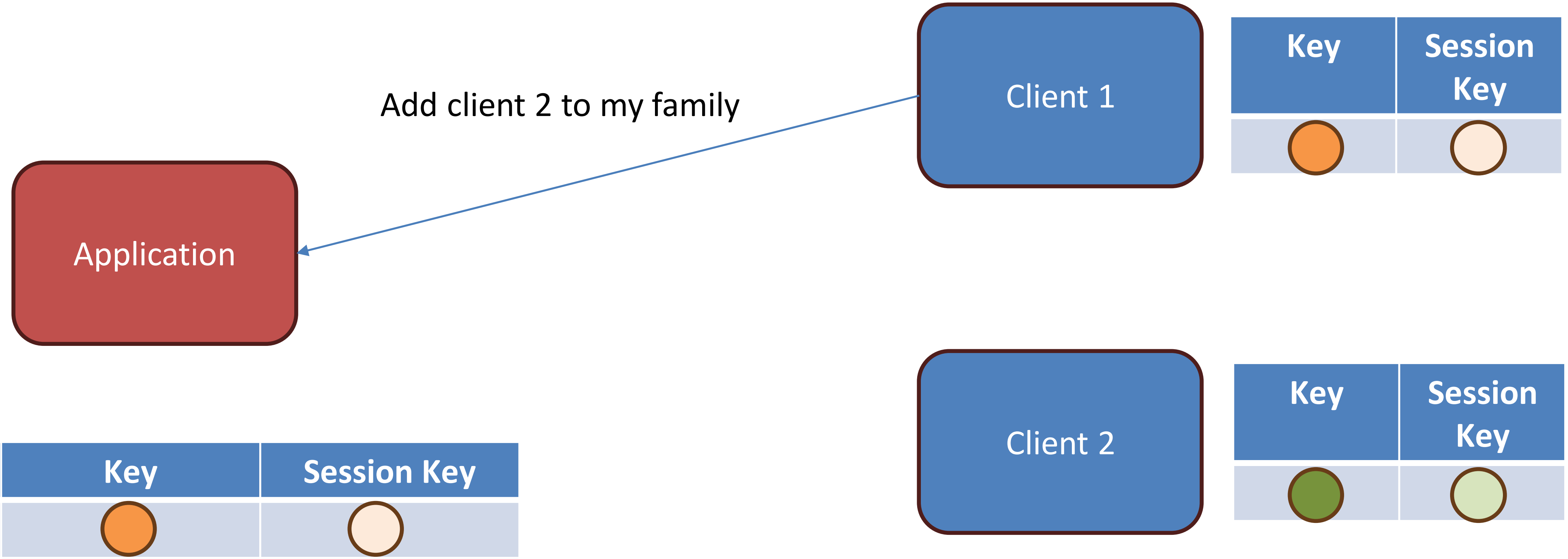
Client 1

Key	Session Key
🟠	⚪

Client 2

Key	Session Key
🟢	○

Security Challenge: Family Sharing

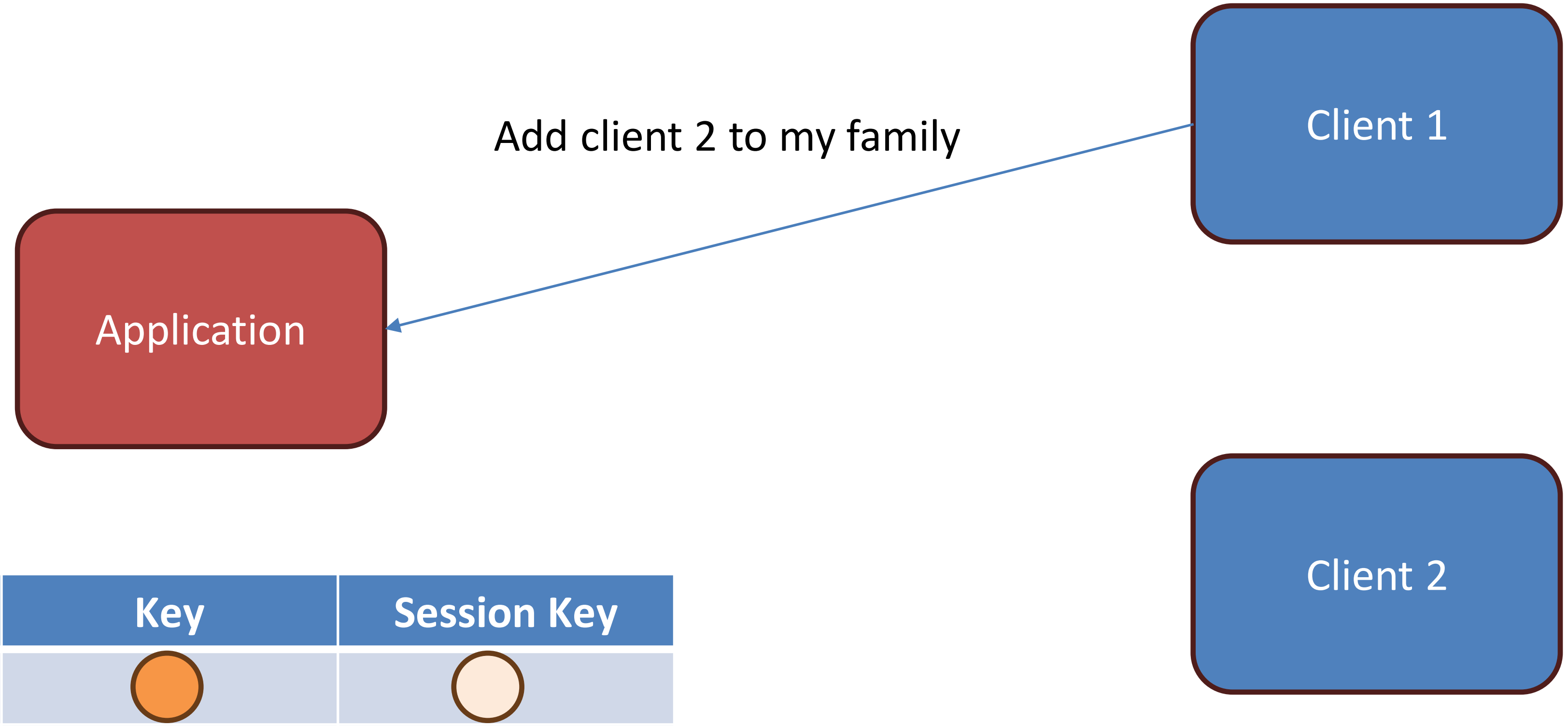


Key	Session Key
🟠	○

Key	Session Key
🟢	○

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

Security Challenge: Family Sharing

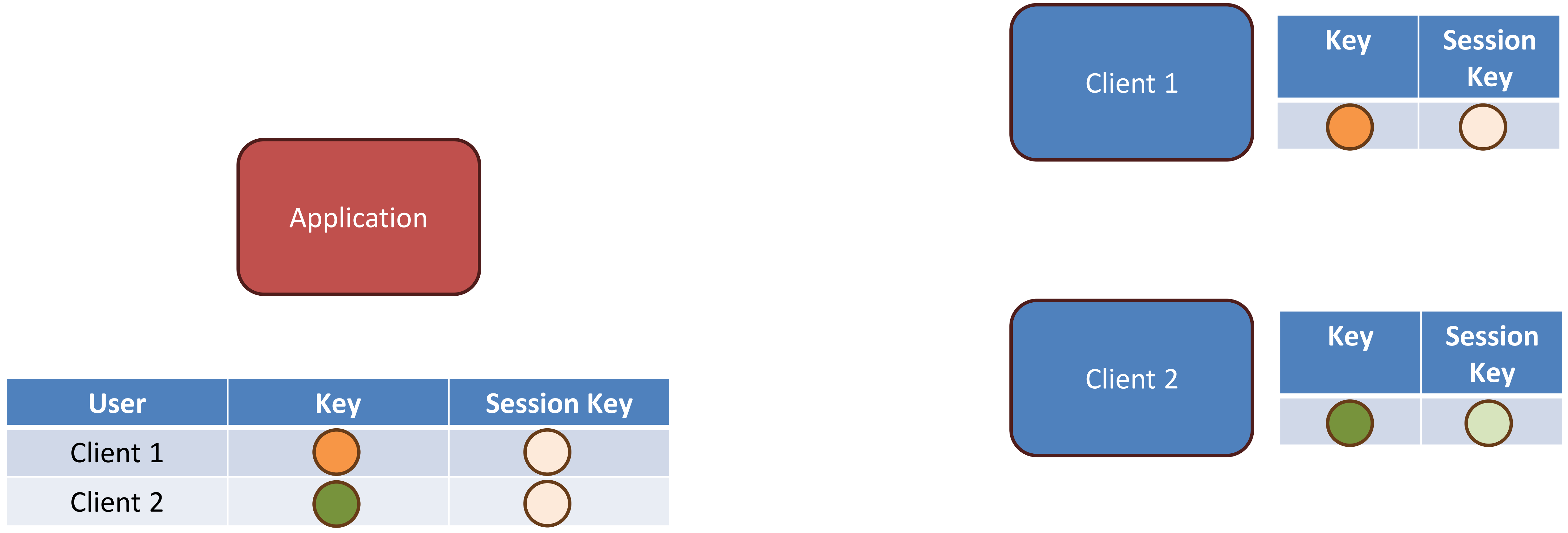


Key	Session Key
🟠	○

Key	Session Key
🟢	◎

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

Security Challenge: Family Sharing



User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

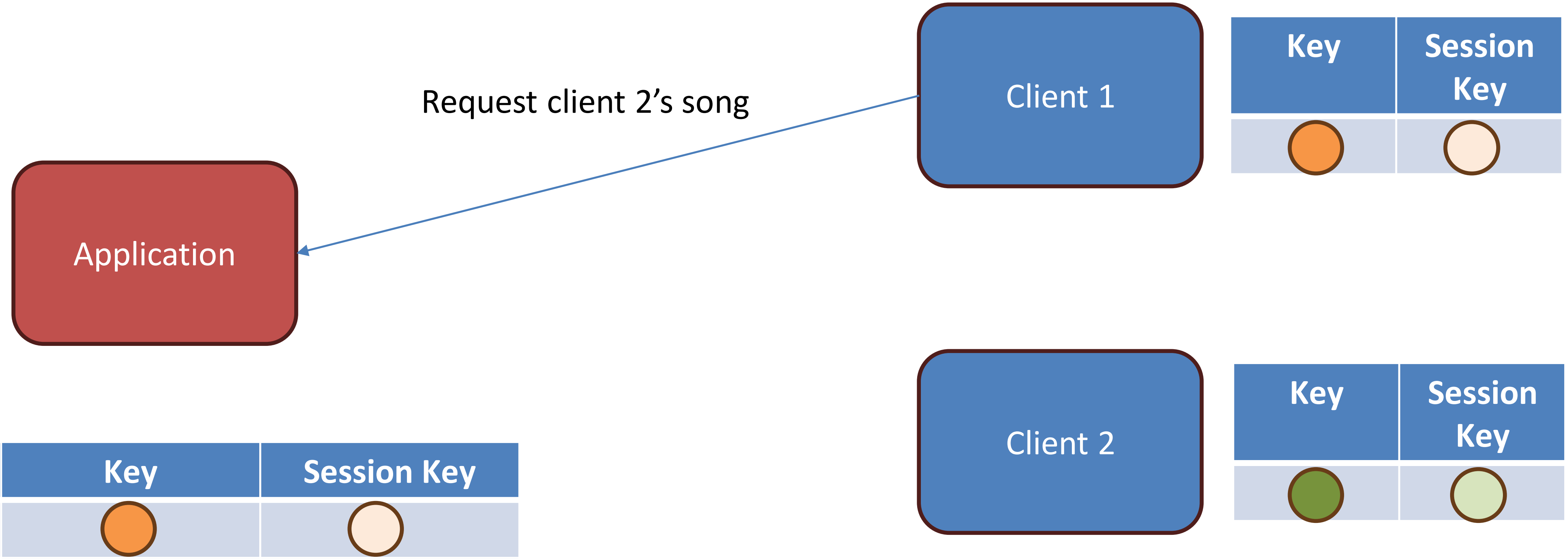
Client 1

Key	Session Key
🟠	○

Client 2

Key	Session Key
🟢	○

Security Challenge: Family Sharing

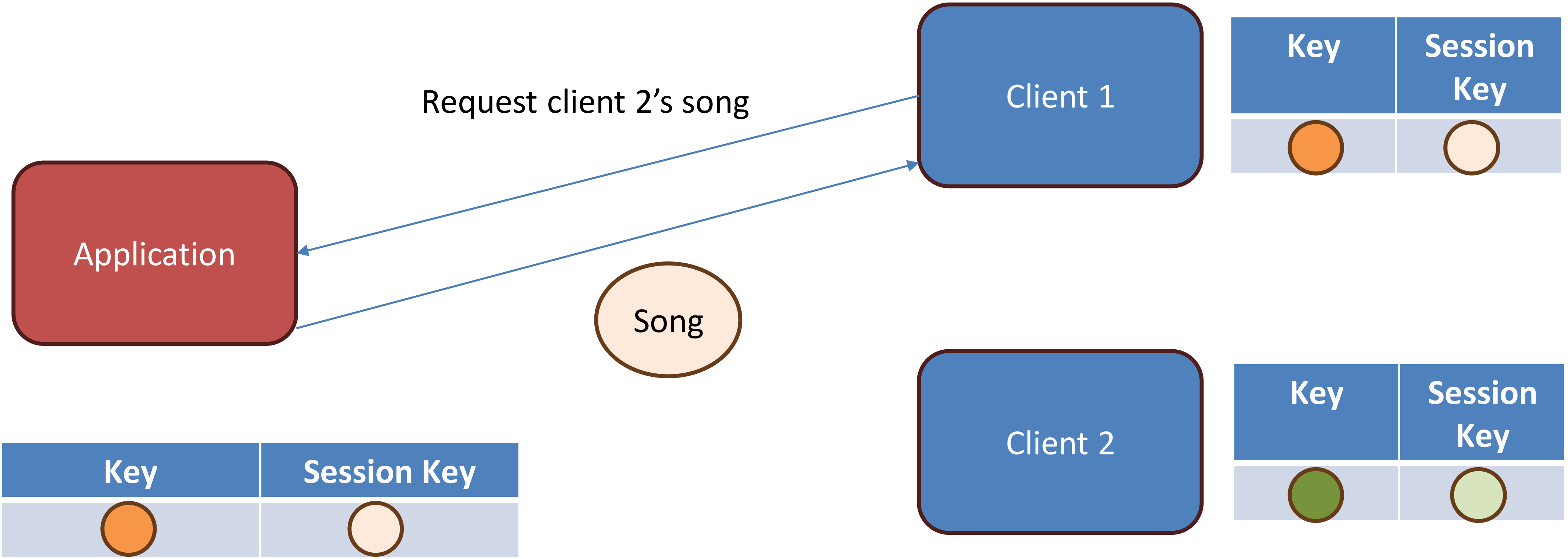


Key	Session Key
🟠	⚪

Key	Session Key
🟢	🟢

User	Key	Session Key
Client 1	🟠	⚪
Client 2	🟢	⚪

Security Challenge: Family Sharing

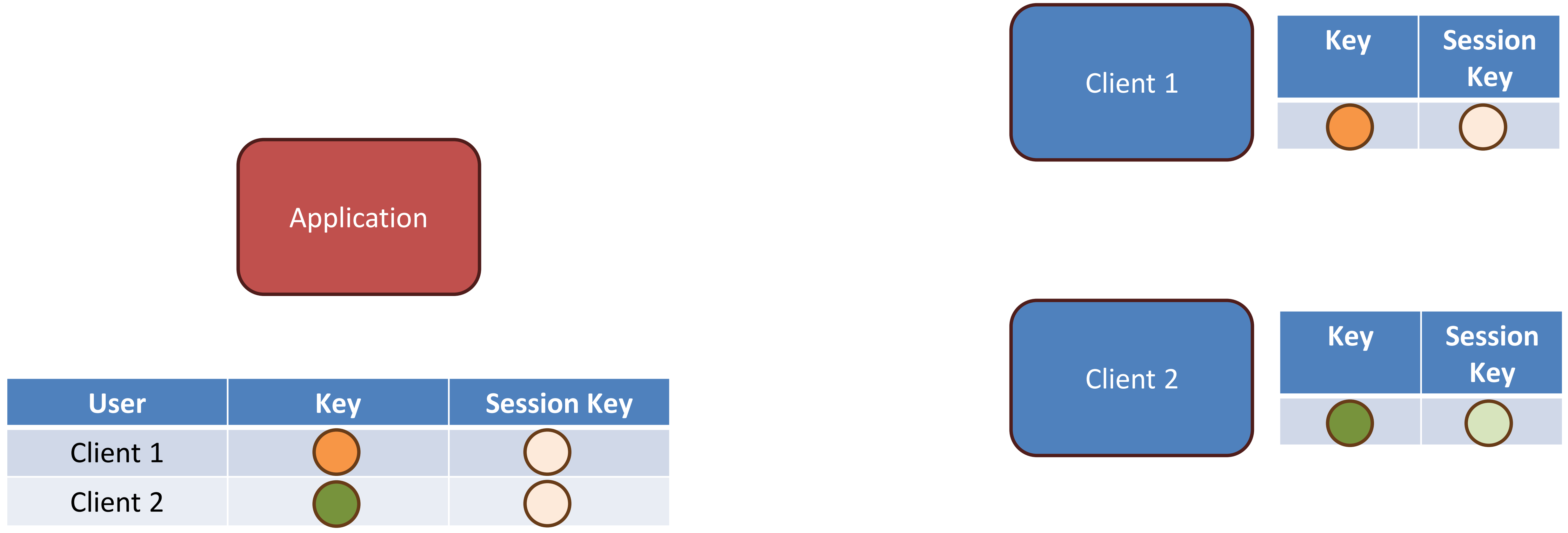


Key	Session Key
🟠	○

Key	Session Key
🟢	◍

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

Security Challenge: Family Sharing



User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

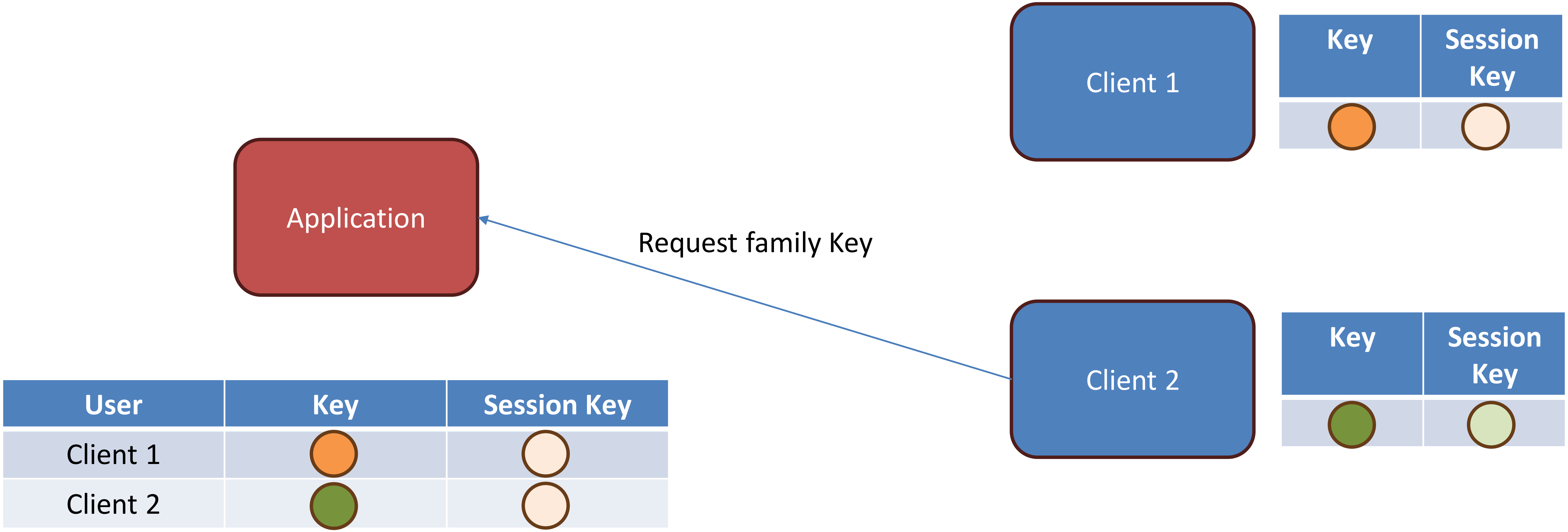
Client 1

Key	Session Key
🟠	○

Client 2

Key	Session Key
🟢	○

Security Challenge: Family Sharing

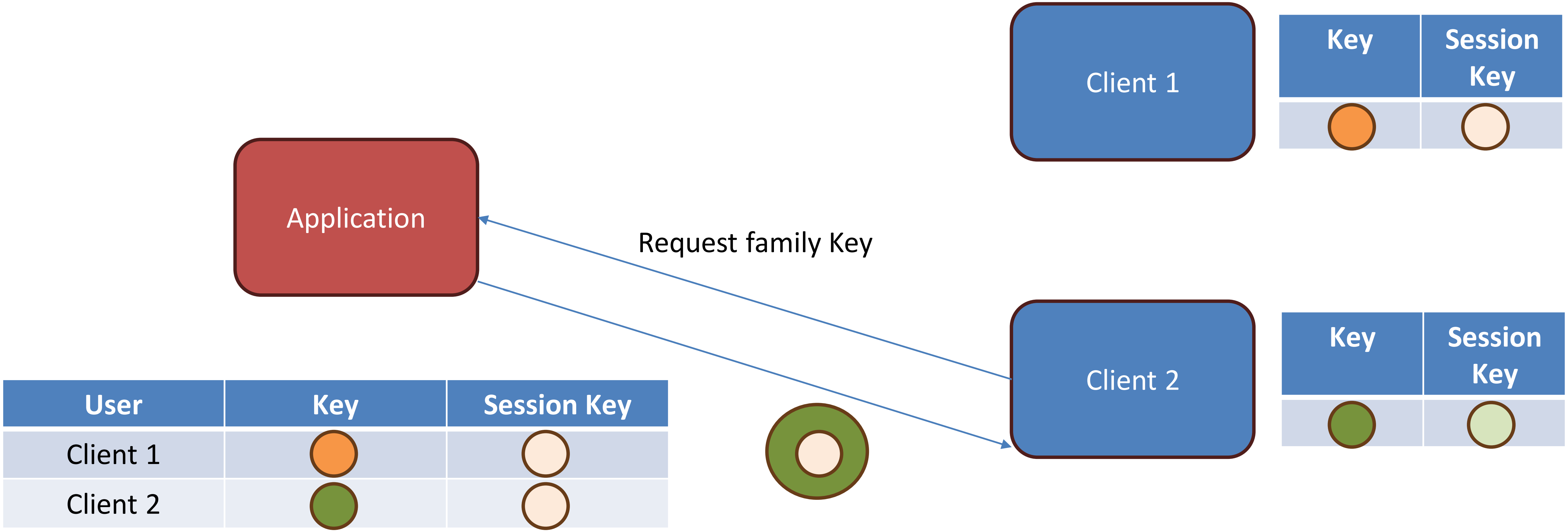


Key	Session Key
🟠	○

Key	Session Key
🟢	○

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

Security Challenge: Family Sharing

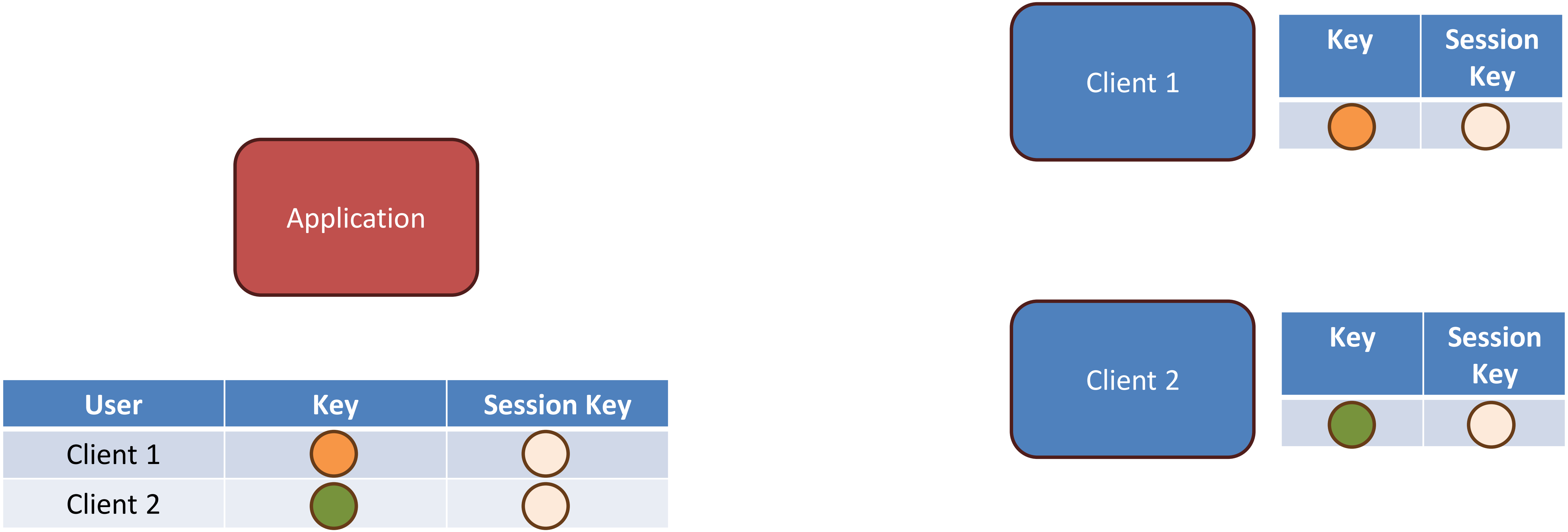


Key	Session Key
🟠	○

Key	Session Key
🟢	○

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

Security Challenge: Family Sharing



User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

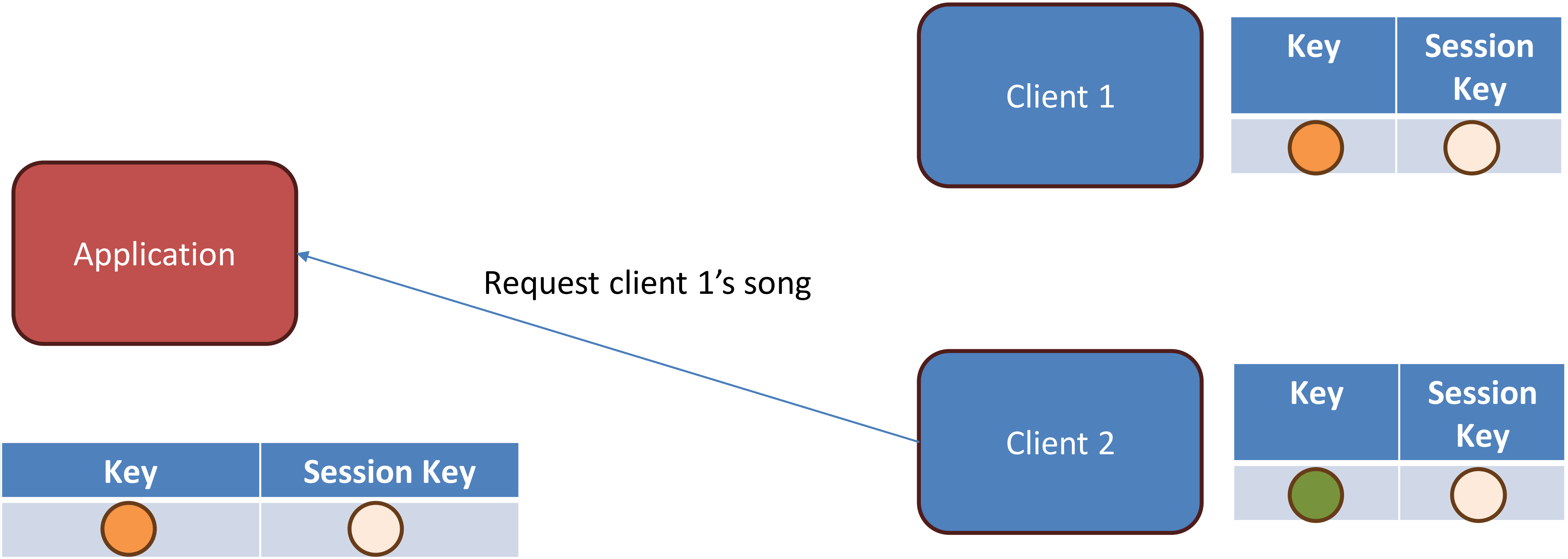
Client 1

Key	Session Key
🟠	○

Client 2

Key	Session Key
🟢	○

Security Challenge: Family Sharing

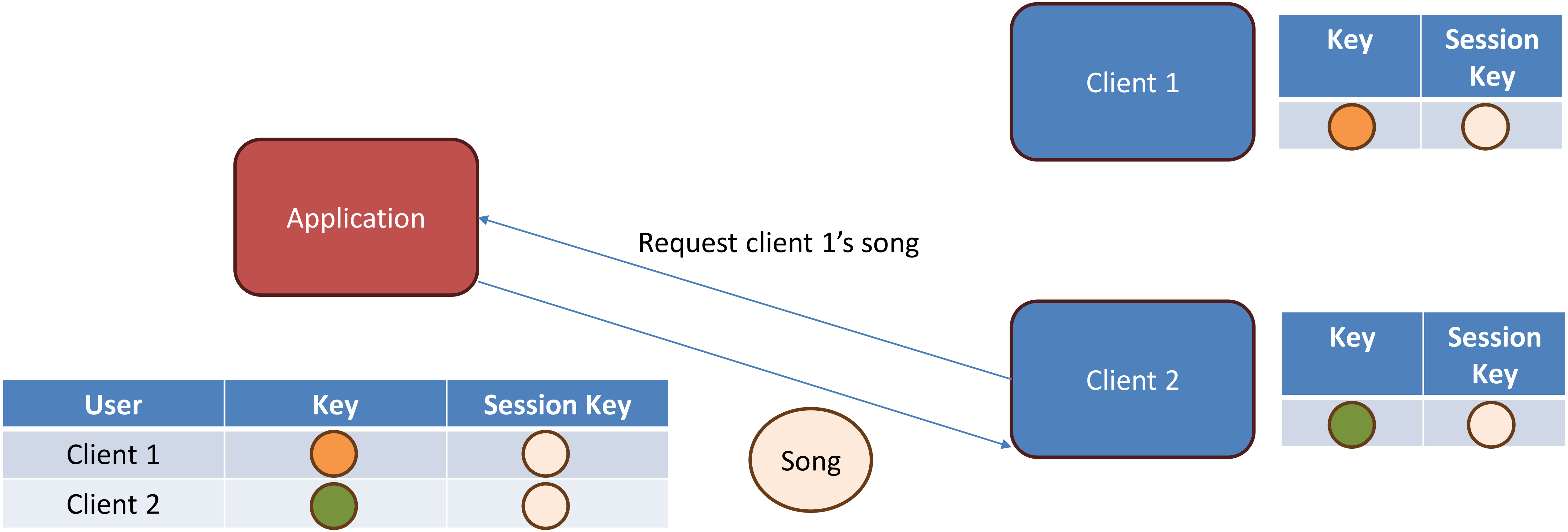


Key	Session Key
🟠	○

Key	Session Key
🟢	○

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

Security Challenge: Family Sharing

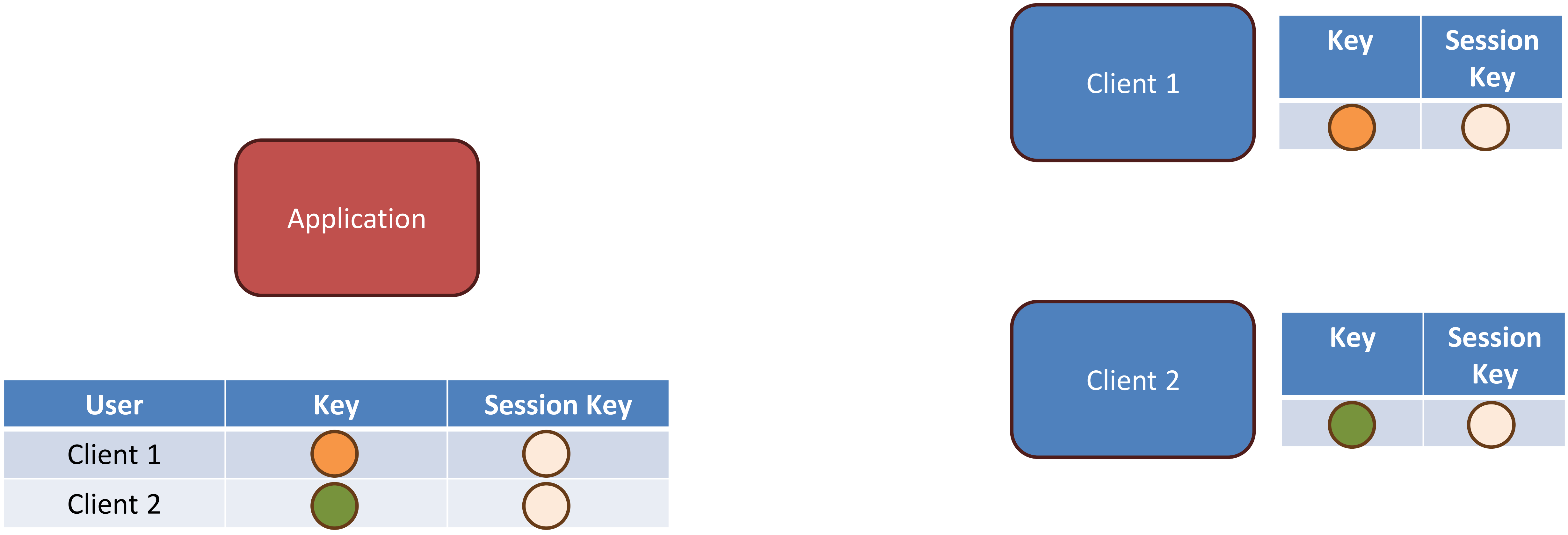


Key	Session Key
🟠	○

Key	Session Key
🟢	○

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

Security Challenge: Family Sharing

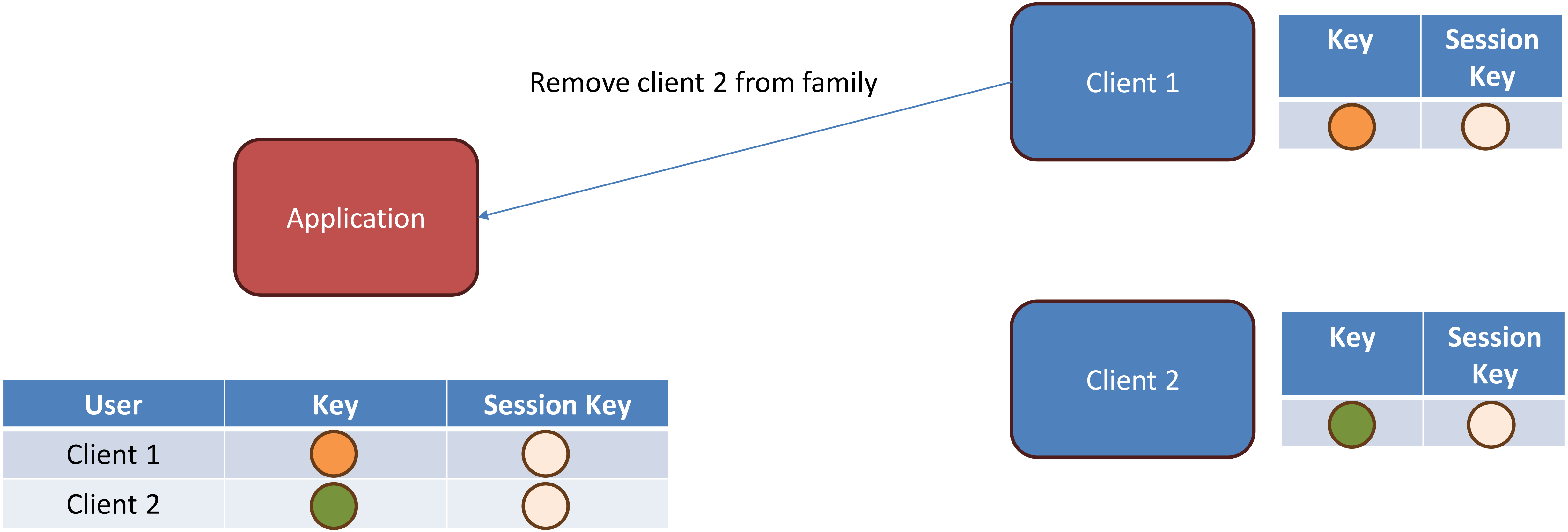


Key	Session Key
🟠	○

Key	Session Key
🟢	○

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

Security Challenge: Family Sharing

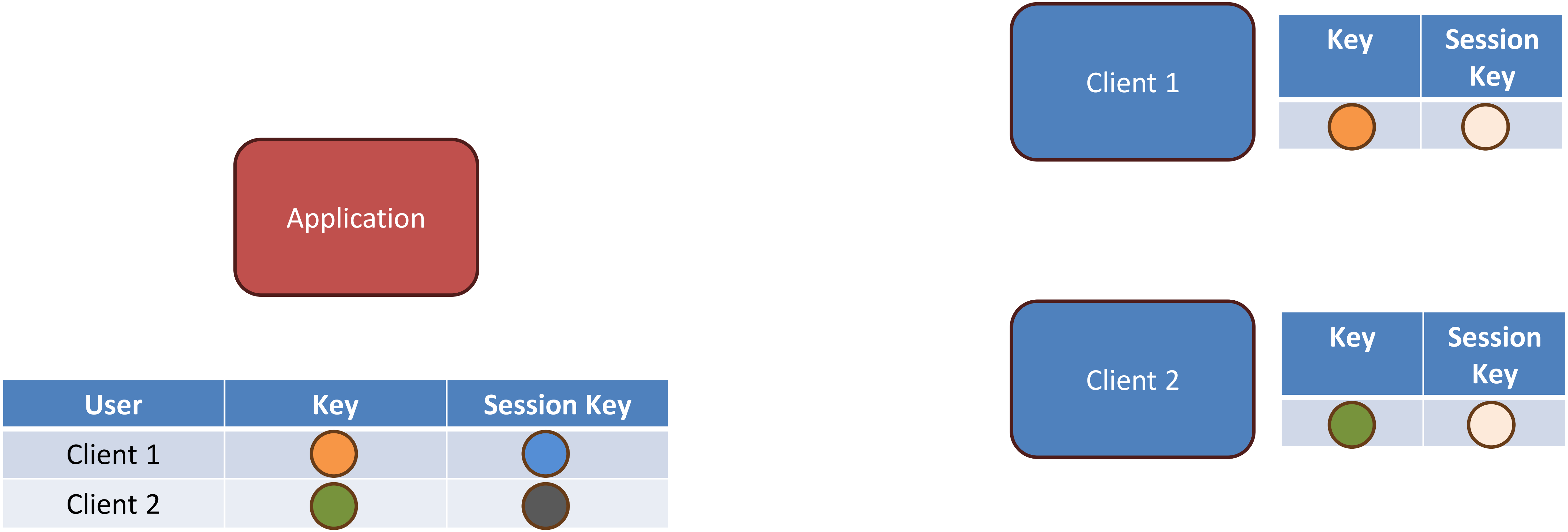


Key	Session Key
🟠	○

Key	Session Key
🟢	○

User	Key	Session Key
Client 1	🟠	○
Client 2	🟢	○

Security Challenge: Family Sharing



Application

User	Key	Session Key
Client 1	🟠	🔵
Client 2	🟢	⚫

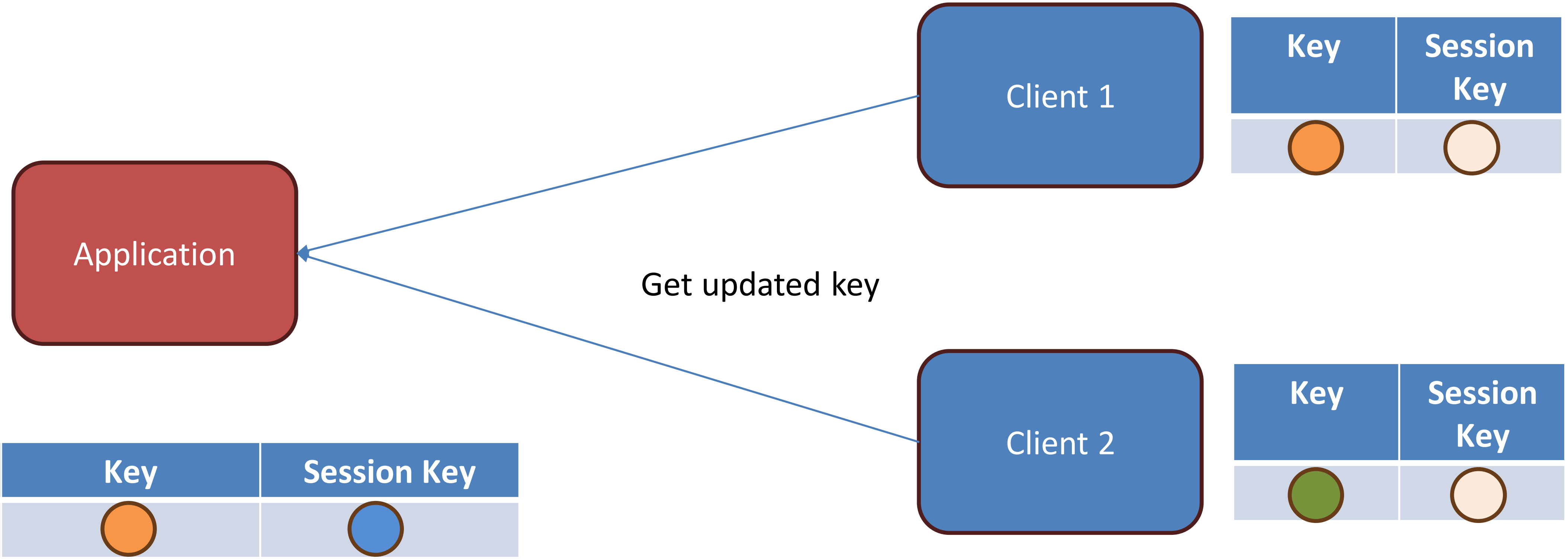
Client 1

Key	Session Key
🟠	⚪

Client 2

Key	Session Key
🟢	⚪

Security Challenge: Family Sharing

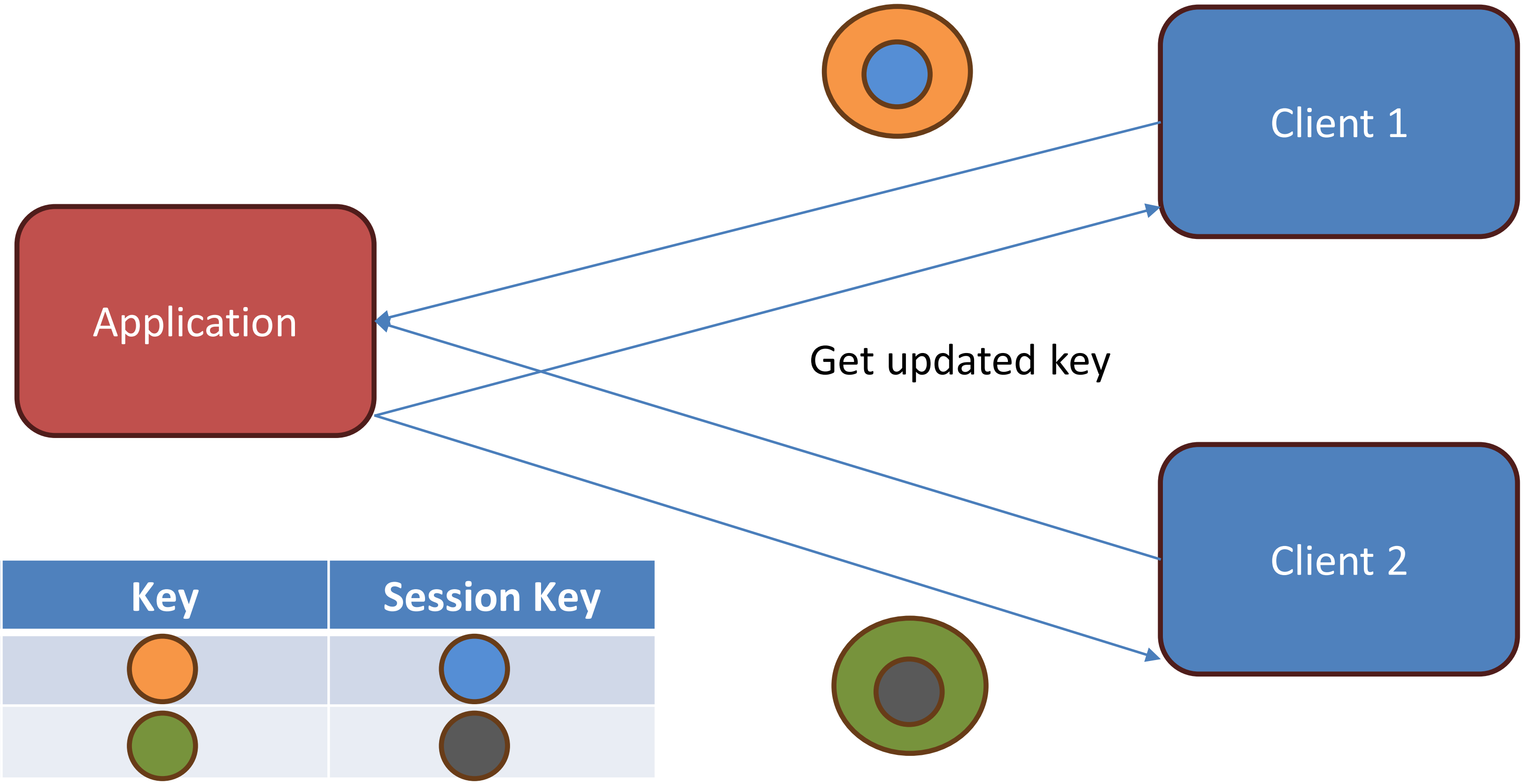


Key	Session Key
🟠	⚪

Key	Session Key
🟢	⚪

User	Key	Session Key
Client 1	🟠	🔵
Client 2	🟢	⚫

Security Challenge: Family Sharing



Key	Session Key
🟠	○

Key	Session Key
🟢	○

User	Key	Session Key
Client 1	🟠	🔵
Client 2	🟢	⚫

Security Challenge: Family Sharing

Application

User	Key	Session Key
Client 1	🟠	🔵
Client 2	🟢	⚫

Client 1

Key	Session Key
🟠	🔵

Client 2

Key	Session Key
🟢	⚫

Outline

- Secure Document Format
- Infrastructure
- Secure Channels and key distribution
- Security Challenge
    - Playback in the middle of an audio stream
    - Family Sharing
- Live Demo
- Conclusion

Outline

- Secure Document Format
- Infrastructure
- Secure Channels and key distribution
- Security Challenge
  - Playback in the middle of an audio stream
  - Family Sharing
- Live Demo
- Conclusion

Conclusion

- We implemented a cryptographic library to protect, unprotect and check the integrity of Json documents.
- We built our own infrastructure that best suited our needs. Having to configure firewalls and networks.
- Secured channels and communication assured by using HTTPS and TLS.
- Learnt about different cypher modes and which one to choose according to our needs.
- Implemented dynamic key distribution to help solve the family sharing challenge.