Alex Liang

2018年7月3日

SHOW CHAIN
ShortVideoProtocol 0.1

1. 数据结构：

Access_Key：

{

 'id' : $USER_ID,

 'name' : $RES_NAME,

 'encrypt_key' : $ENCRYPT_KEY,

 'md5' : $RES_MD5,

 'transfer_md5' : $RES_TRANS_MD5,

 'size' : $RES_SIZE,

 'transfer_size' : $RES_TRANS_SIZE,

 'length' : $RES_PLAY_LENGTH

}

2. 文件加密传输编码：

源文件 —> 提取md5 —> LZ4 —> DES (encrypt_key) —> 提取md5 —>base64

3. 发布内容：

Request：

```
{
 'op_code' : 0x201,
 'access_key' : $Access_Key,
 'access_key_md5' : $Access_Key_md5,
 'thumbnail' : $Access_Key,
 'seq' : $CLIENT_PACKET_SEQUENCE,
 'ts' : $CLIENT_TIMESTAMP,
 'sign' : [op_code, access_key_md5, seq, ts] RSA Signature
}
```

Response:

```
{
 'op_code' : 0x202,
 'access_key_md5' : $Access_Key_md5,
 'res_uid' : $GENERATE_UUID,
 'seq' : $CLIENT_PACKET_SEQUENCE,
 'ts' : $CLIENT_TIMESTAMP,
 'sign' : [op_code, access_key_md5, res_uid, seq, ts] RSA Signature
}
```

4. 请求内容：

Request：

```
{
 'op_code' : 0x203,
 'target' : $TARGET_ID,
 'id' : $USER_ID,
 'md5' : $RES_MD5,
 'session' : $GENERATE_SESSION_ID,
 'seq' : $CLIENT_PACKET_SEQUENCE,
 'ts' : $CLIENT_TIMESTAMP,
 'sign' : [op_code, target, md5, seq, ts] RSA Signature
}
```

5. UDP文件传输协议：

Transfer Data :

```
{
 'op_code' : 0x204,
 'id' : $USER_ID,
 'session' : $REQUEST_SESSION_ID,
 'num' : $FILE_PACKET_NUM,
 'data' : $FILE_PACKET,
 'seq' : $CLIENT_PACKET_SEQUENCE,
 'ts' : $CLIENT_TIMESTAMP
}
```

Request Transfer Data :

```
{
 'op_code' : 0x205,
 'id' : $USER_ID,
 'session' : $REQUEST_SESSION_ID,
 'page' : $FILE_PACKET_PAGE,
 'map' : $FILE_PACKET_MAP,
 'seq' : $CLIENT_PACKET_SEQUENCE,
 'ts' : $CLIENT_TIMESTAMP
}
```