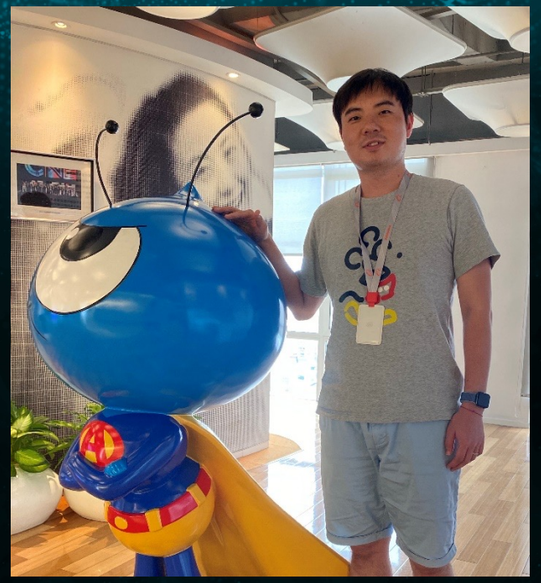
Hunting Vulnerabilities of gRPC Protocol Armed Mobile/IoT Applications

Shijie Cao & Hao Zhao

AntGroup

蚂蚁集团 ANT GROUP | 蚂蚁安全实验室 ANT SECURITY LAB

Introduction



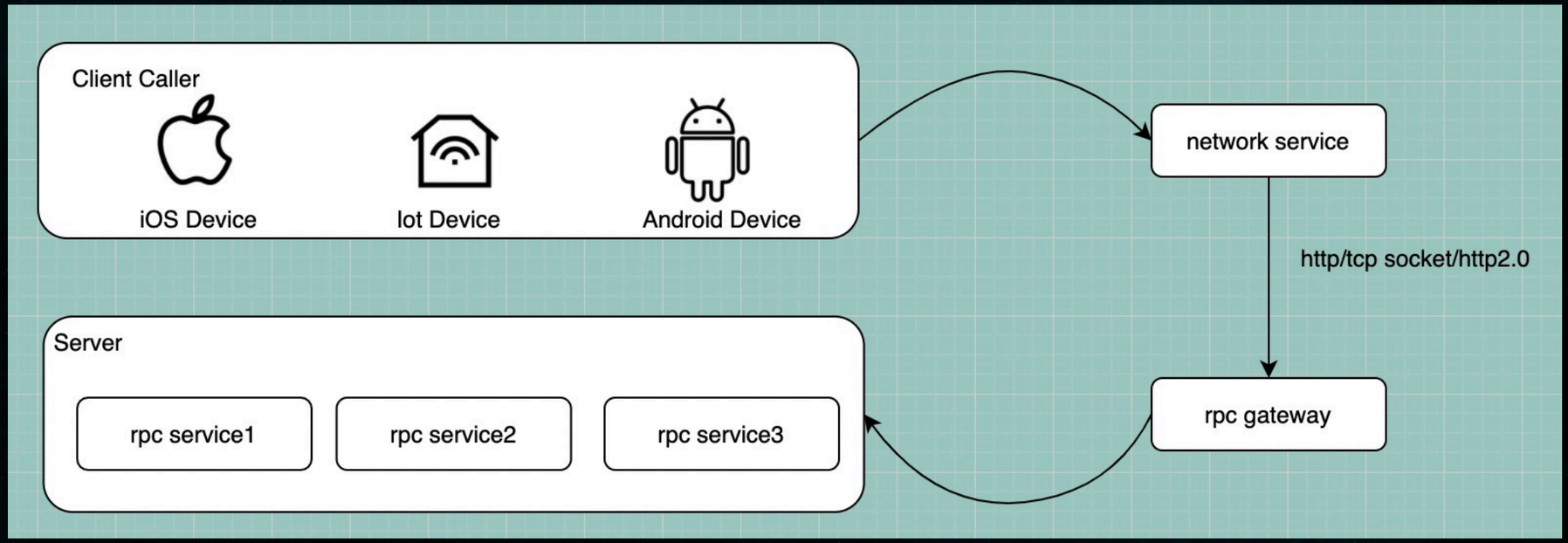
Shijie Cao: The security researcher in TianChen Lab of Ant Group. He has been engaged in mobile/Iot security for 6 years and focuses on researching mobile security architecture construction and application vulnerability fuzzing. During the past year, his research has been on automated vulnerability fuzzing on mobile applications and IoT, and hundreds of security vulnerabilities have been discovered.

Hao Zhao: The chief mobile security architect at Ant Group and the founder of Ant Group Frontage Security Lab. He has more than 8 years of experience in mobile and IoT security research. He is also responsible for Ant Group's client security defense building. He has shared many of his research results at Black Hat and RSAC.

What is RPC protocol

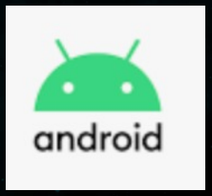
RPC is Remote Procedure Call.

Features: No need to attention network information, such as IP, port, etc., only need to pay attention to the interface name, parameters, you can get remote services .



Features of gRPC

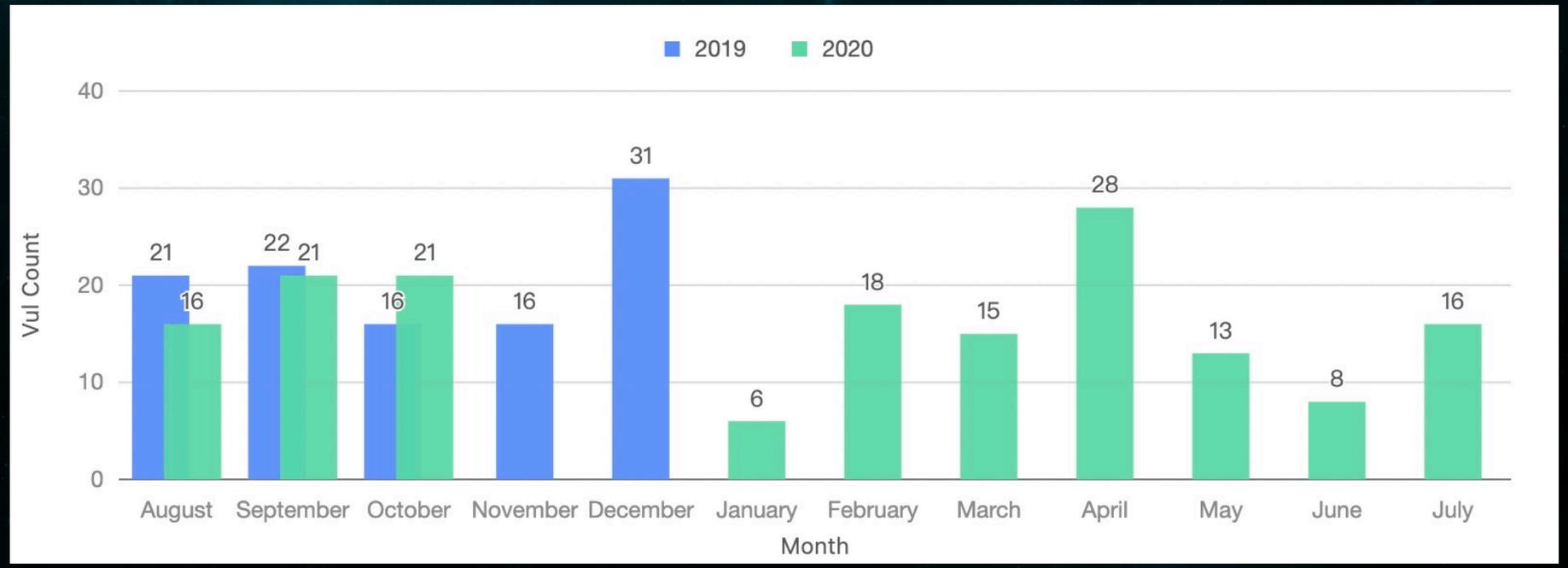
Feature 1: Can run on different platforms



Feature 2: Based on Http2.0, the network overhead is small and the expansion is higher.

Feature 3: Use Proto3 as a universal open source RPC architecture for IDL and transmission data format(Also compatible with proto2).

Statistics on the number of vulnerabilities in mobile App & IoT App based on gRPC protocol we found in the past.



Perspectives of different roles

1. From the developer's perspective, it is believed that the application of encryption, serialization, environmental verification, signature and other methods at the application level is relatively safe, and thus lacks a union defense system for the mobile application
and the cloud.

2. From the attacker's perspective, although the application will have various security mechanism to ensure the communication security, since most of the security mechanisms act on the client, once bypassed, it opens the door to app-to-cloud attacks.

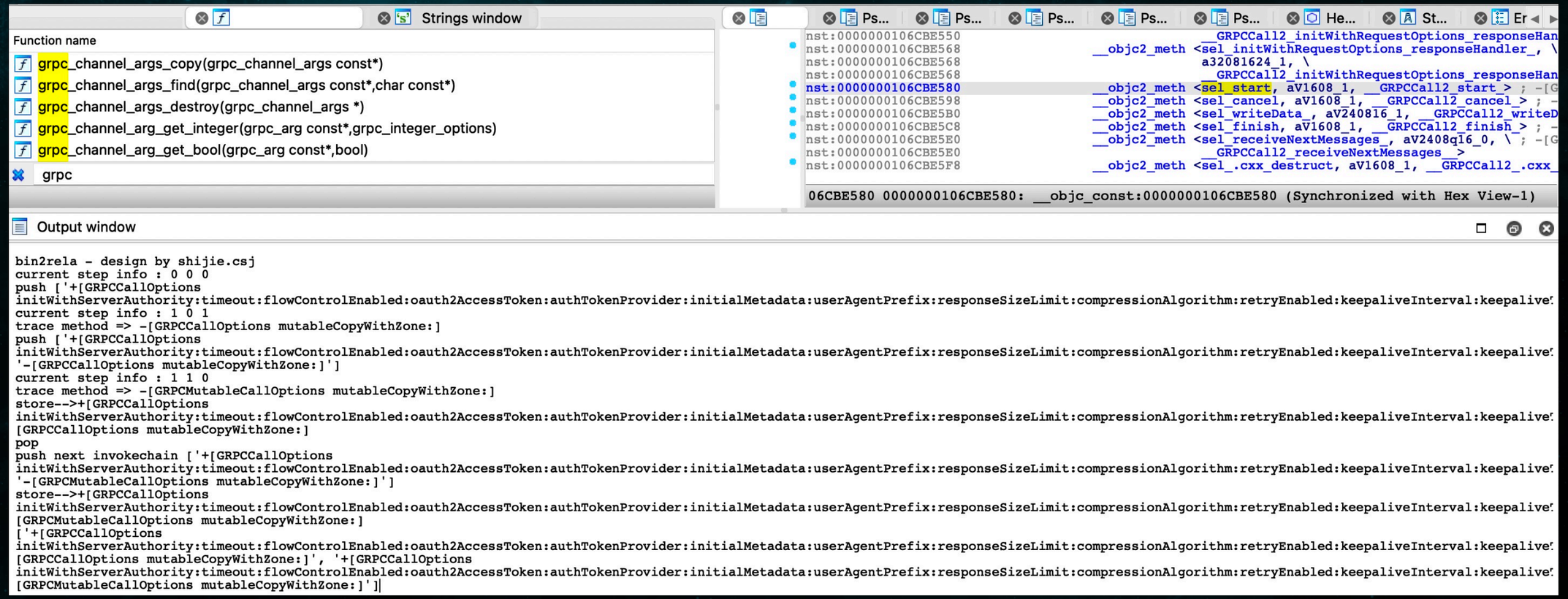
How to build a vulnerability mining platform based on grpc protocol

Grpc protocol vulnerabilities mining technical barriers ：

1. Obtain the original data of gRPC on the app and have the ability to replay gRPC data
2. Vulnerability analysis and performance improvement of different grpc requests
3. Arsenal construction

How to build a vulnerability mining platform based on grpc protocol

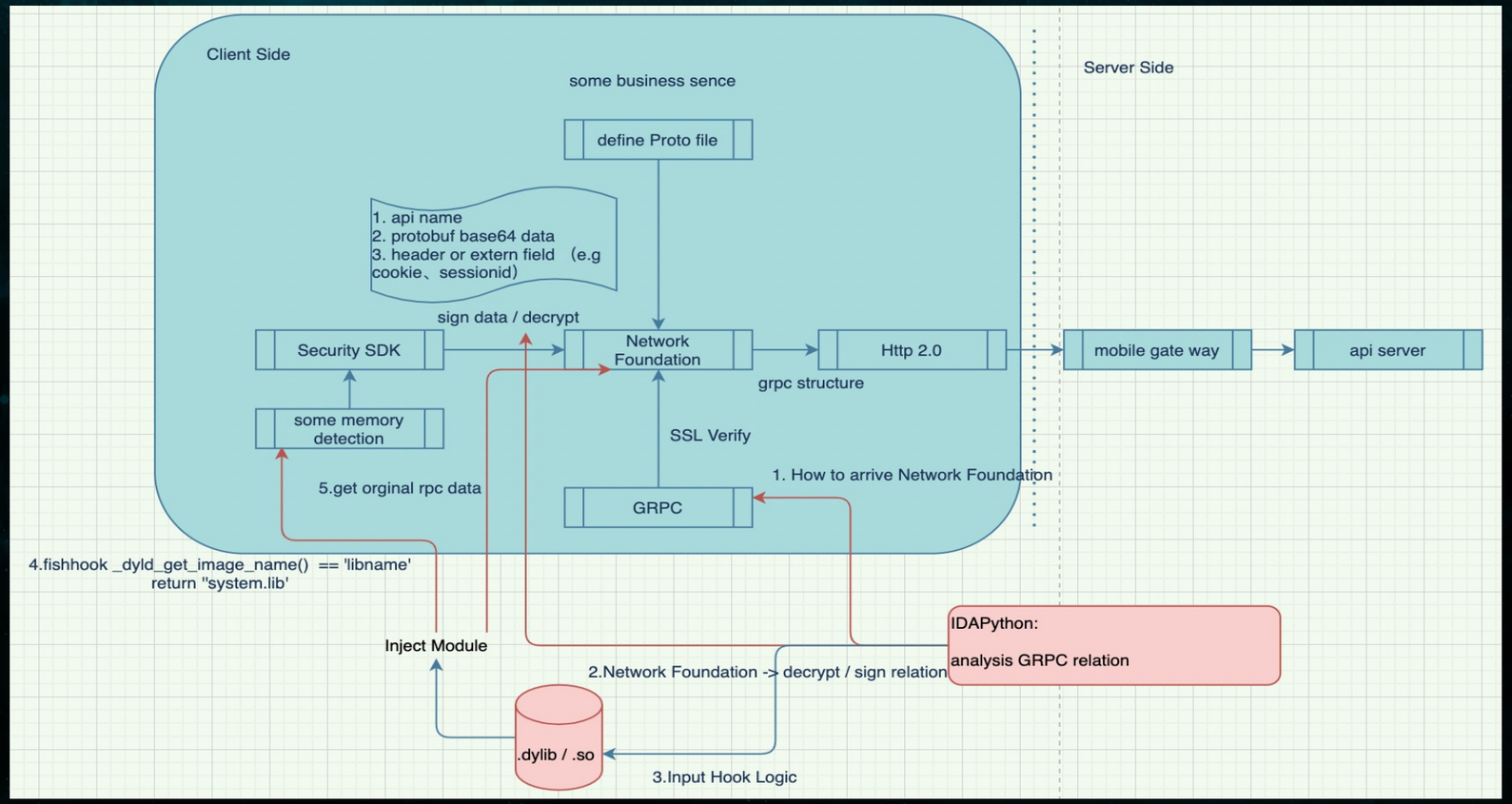
1. Understand and control the operating logic of gRPC in the application



Automatic analysis grpc relation (use push & pop trace)

How to build a vulnerability mining platform based on grpc protocol

1. Understand and control the operating logic of gRPC in the application

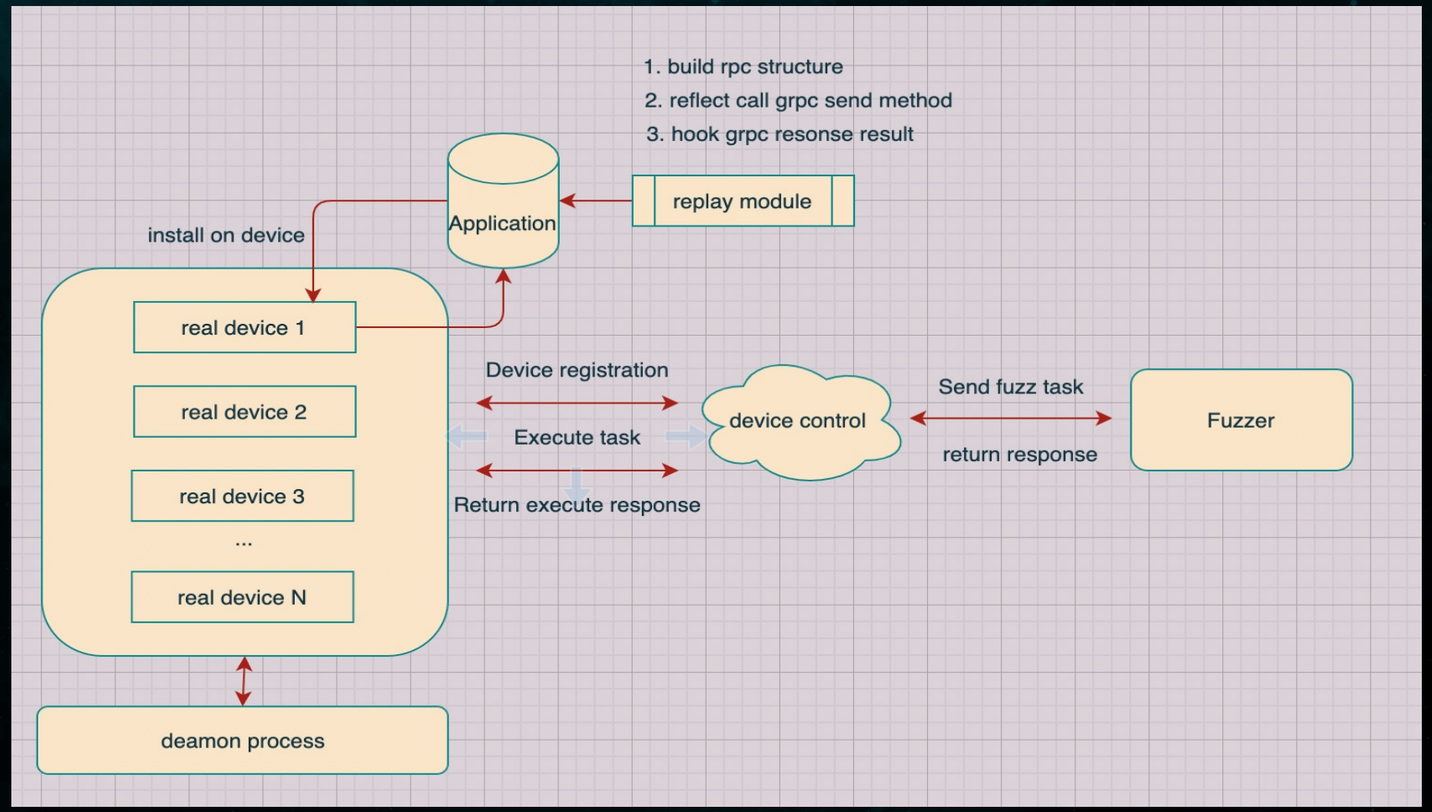


Understand the operating mechanism and interception methods of gRPC

How to build a vulnerability mining platform based on grpc protocol

1. Understand and control the operating logic of gRPC in the application

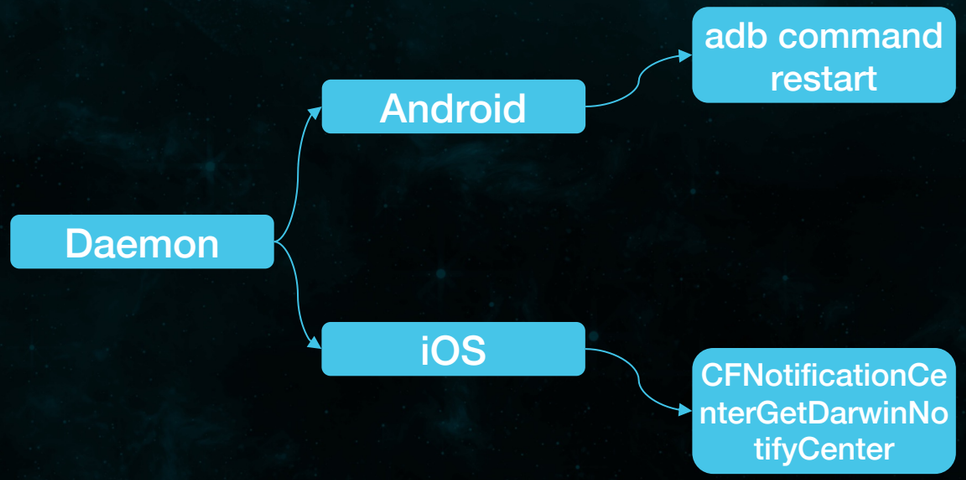
```
Client Heartbeat package :
client = GRPCAgent.instance
client.worker = nil;
client.platfrom = @"iOS/Android";
client.isHeartBeat = True;
client.isRun = FALSE;
client.taskLock = Object;


Server Side register ：
executor_info = {
            'tenant': device_tenant,
            'did': device_id,
            'type': device_type,
            'name': device_name,
            'cluster': device_cluster,
            'others': device_others,
            'last_update': now,
            'metrics': mobilegw_pb2.DeviceMetrics(),
            'last_sync_timestamp': now,
            'task_runner': 0,
            'app_version': device_app_version,
            'hook_version': device_hook_version
        }
```

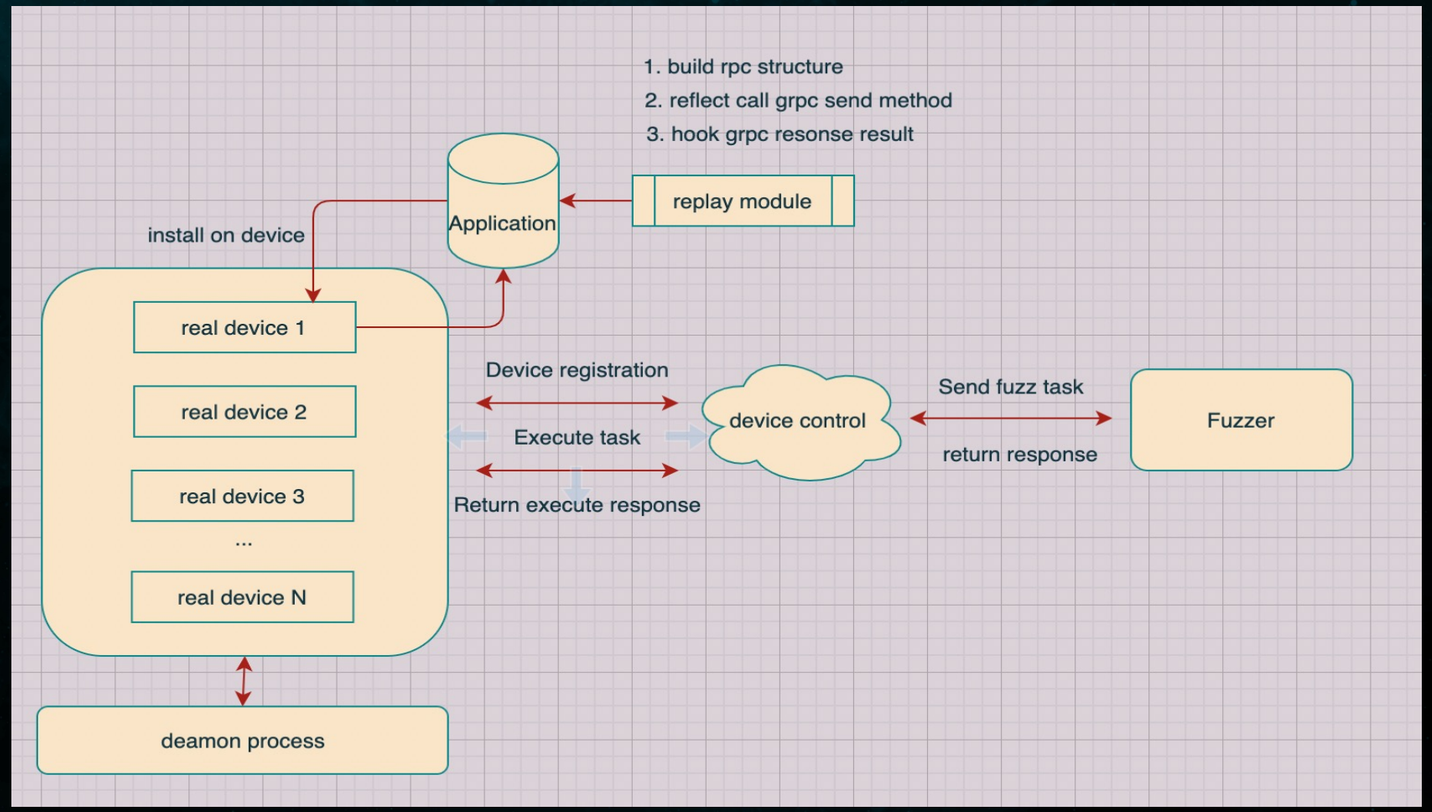


Replay ability construction

How to build a vulnerability mining platform based on grpc protocol

1. Understand and control the operating logic of gRPC in the application





Replay ability construction

How to build a vulnerability mining platform based on grpc protocol

1. Understand and control the operating logic of gRPC in the application

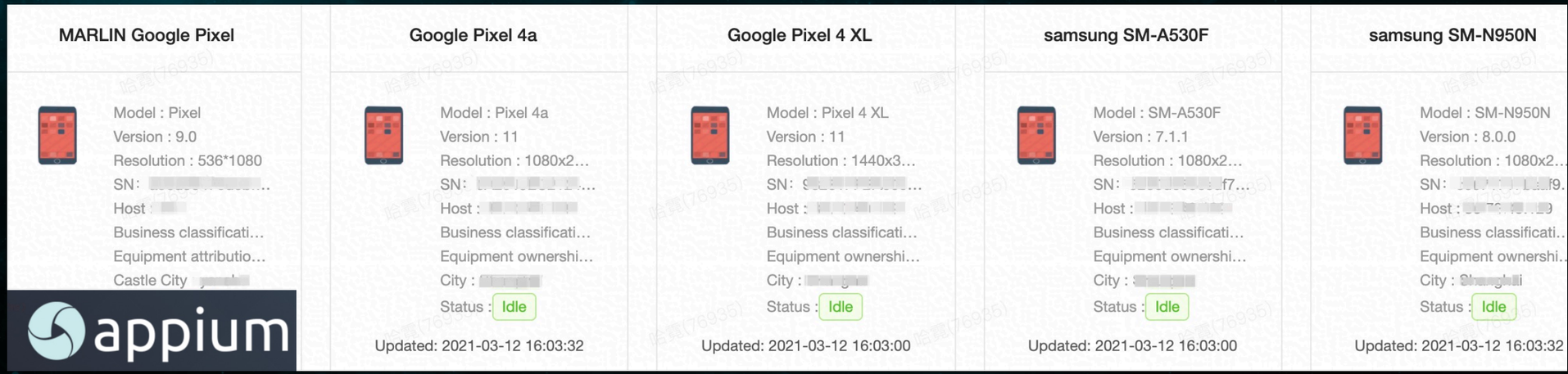
```
def getLoginState(self,appid):
    try:
        if appid == 'mobile application 1' and appid in self.loginConf.keys():
            tid = self.loginConf[appid]
            result = self.replayPlatform(appid, False, "gRPC.method.1", json.loads(tid))
            result = result.decode('utf-8')
            result = json.loads(result)
            print(result['sessionId'])
            return 'SESSIONID=' + result['sessionId']
        if appid == 'mobile application 2' and appid in self.loginConf.keys():
            tid = self.loginConf[appid]
            result = self.replayPlatform(appid,True,"gRPC.method.2",tid)
            result = protobuf().parse(result)
            all_value = data2dic_obtain_all_value(json.loads(result))
            for v in all_value:
                if type(v) == str and v.find('SESSIONID=') != -1:
                    v = json.loads(v)['set-cookies'][0].split(';')[0]
                    return v
        if appid == 'Iot device 3' and appid in self.loginConf.keys():
            tid = self.loginConf[appid]
            result = self.replayPlatform(appid,True,"gRPC.method.3",tid)
            result = protobuf().parse(result)
            result = result.replace(']\"', ']').replace('\"[', '[').replace('\"{', '{').replace('}\"', '}').replace('\\\"', '\"')
            all_value = json.loads(result)
            cookies = None
            for v in all_value:
                if type(all_value[v]) == dict:
                    for k in all_value[v]:
                        if type(all_value[v][k]) == dict:
                            c = all_value[v][k]
                            if 'cookies' in c.keys():
                                cookies = c['cookies']
            cookie = ''
            for k in cookies:
                if k == 'SESSIONID':
```

AutoLogin ability construction

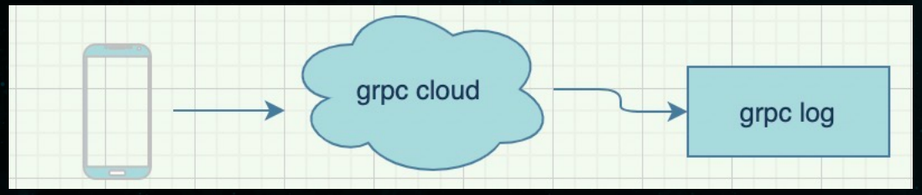
How to build a vulnerability mining platform based on grpc protocol

2. Data acquisition, parse and analysis

Method 1 ：



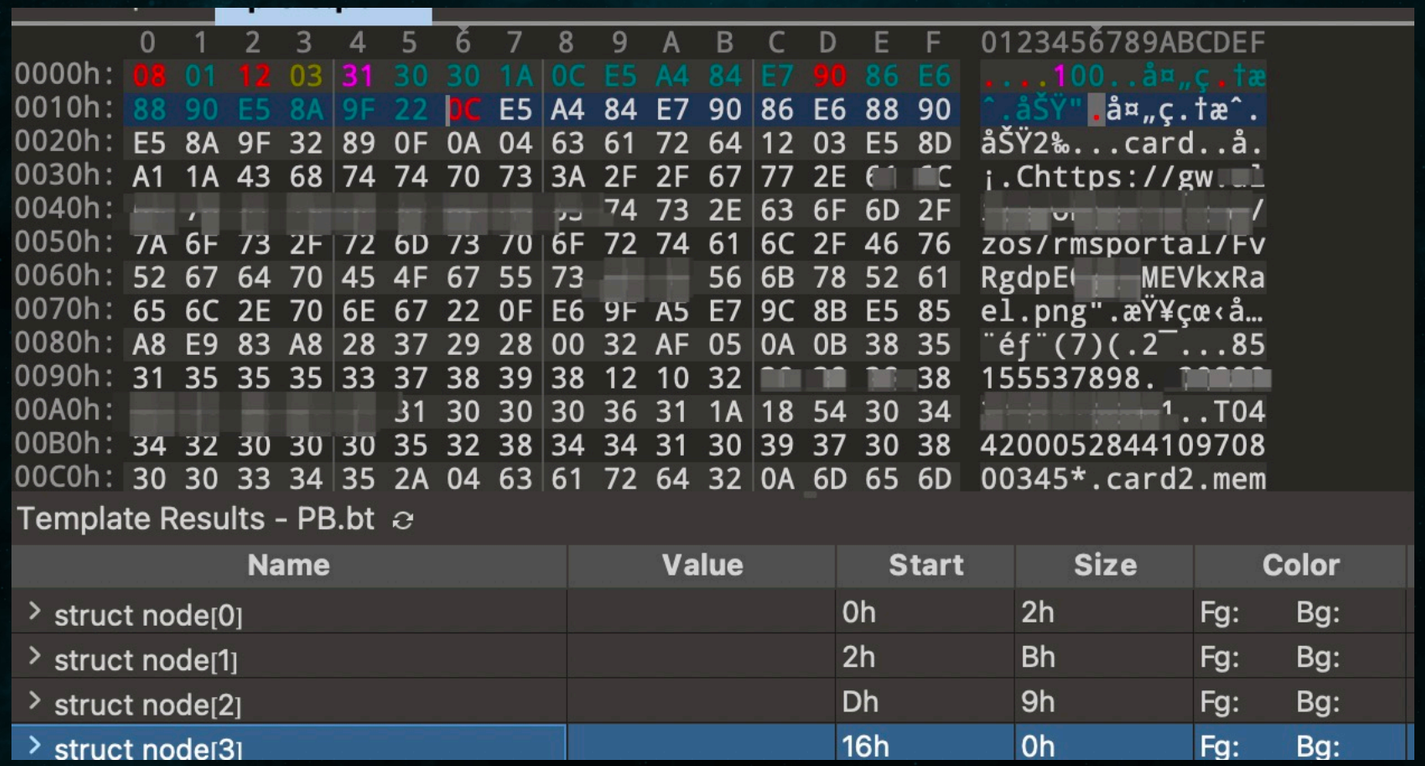
Method 2 ：



Capture the grpc flow

How to build a vulnerability mining platform based on grpc protocol

2. Data acquisition, parse and analysis




```
→  rpc_test git:(master) ✗ python3 parse_pb.py
parse original proto data:
CAESAzEwMBoM5aSE55CG5oiQ5YqfIgzlpITnkIbmiJDlip8yiQ8KBG..
proto data format json:
{"01:00:Varint": 1, "02:01:string": "100", "03:02:string
"02:01:string":  ", "03:02:string"·
int": 0, "06:05:embedded message": {"01:00:embedded mess
100061", "03:02:string": "T044200052844109708003 45", "05
om/zos/rmsportal/euoNihFudrcvNbTqlojT.png", "09:06:strin
0, "14:10:Varint": 0, "17:11:Varint": 1, "18:12:string":
```

Protobuf original data format

How to build a vulnerability mining platform based on grpc protocol

2. Data acquisition, parse and analysis

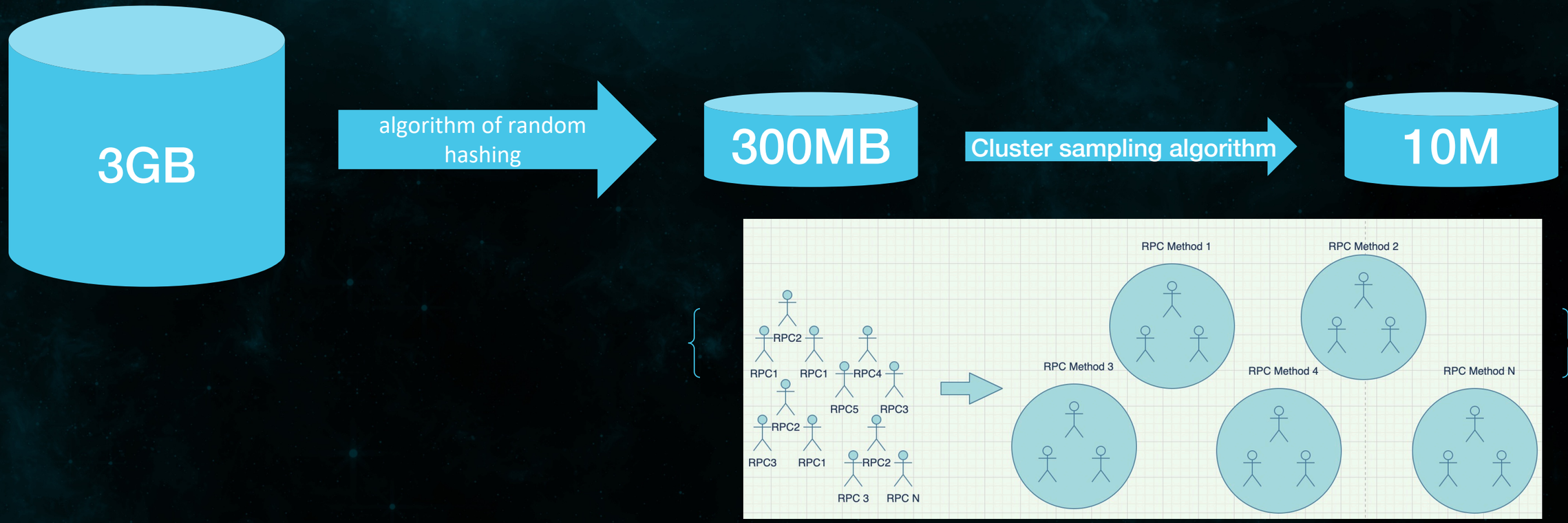
Sampling field：time，gRPC method

```
SELECT * FROM ( SELECT *
FROM grpc_table WHERE dt = '${dt}’ AND HOUR IN ( '06' , '11' , '17’ )  // time sample
) a
LEFT OUTER JOIN ( SELECT grpc_method, ,COUNT(*) AS num FROM grpc_table
WHERE dt = '${dt}’ AND HOUR IN ( '06' , '11' , '17’ ) GROUP BY grpc_method
) b on (a. grpc_method = b. grpc_method)
WHERE a.rand_num * b.num <= 100
```

Random hashing and sampling of data

How to build a vulnerability mining platform based on grpc protocol

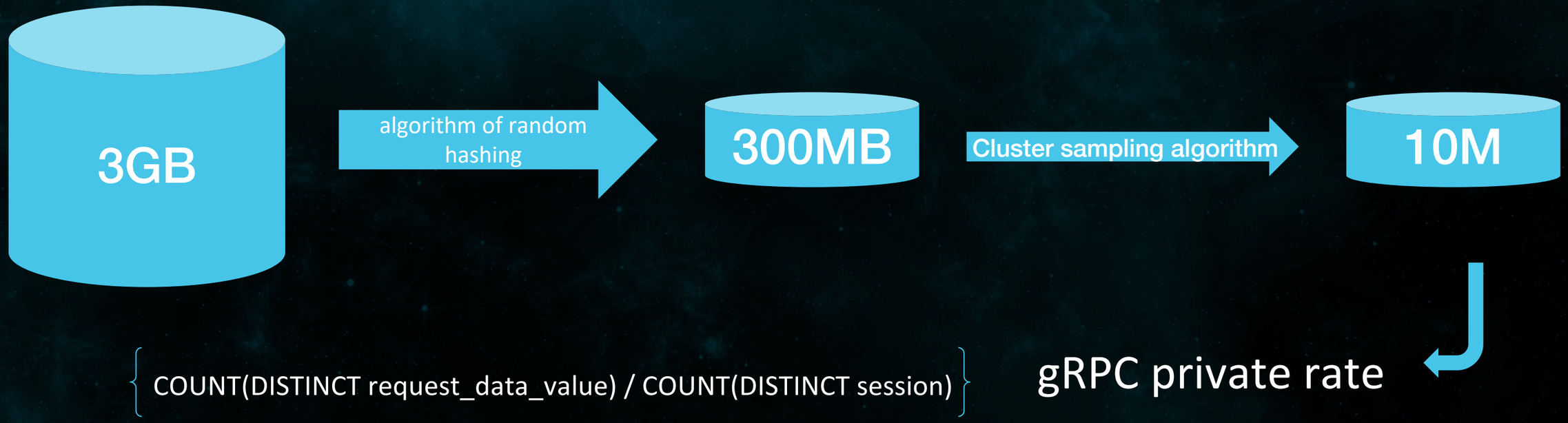
2. Data acquisition, parse and analysis



Cluster sampling

How to build a vulnerability mining platform based on grpc protocol

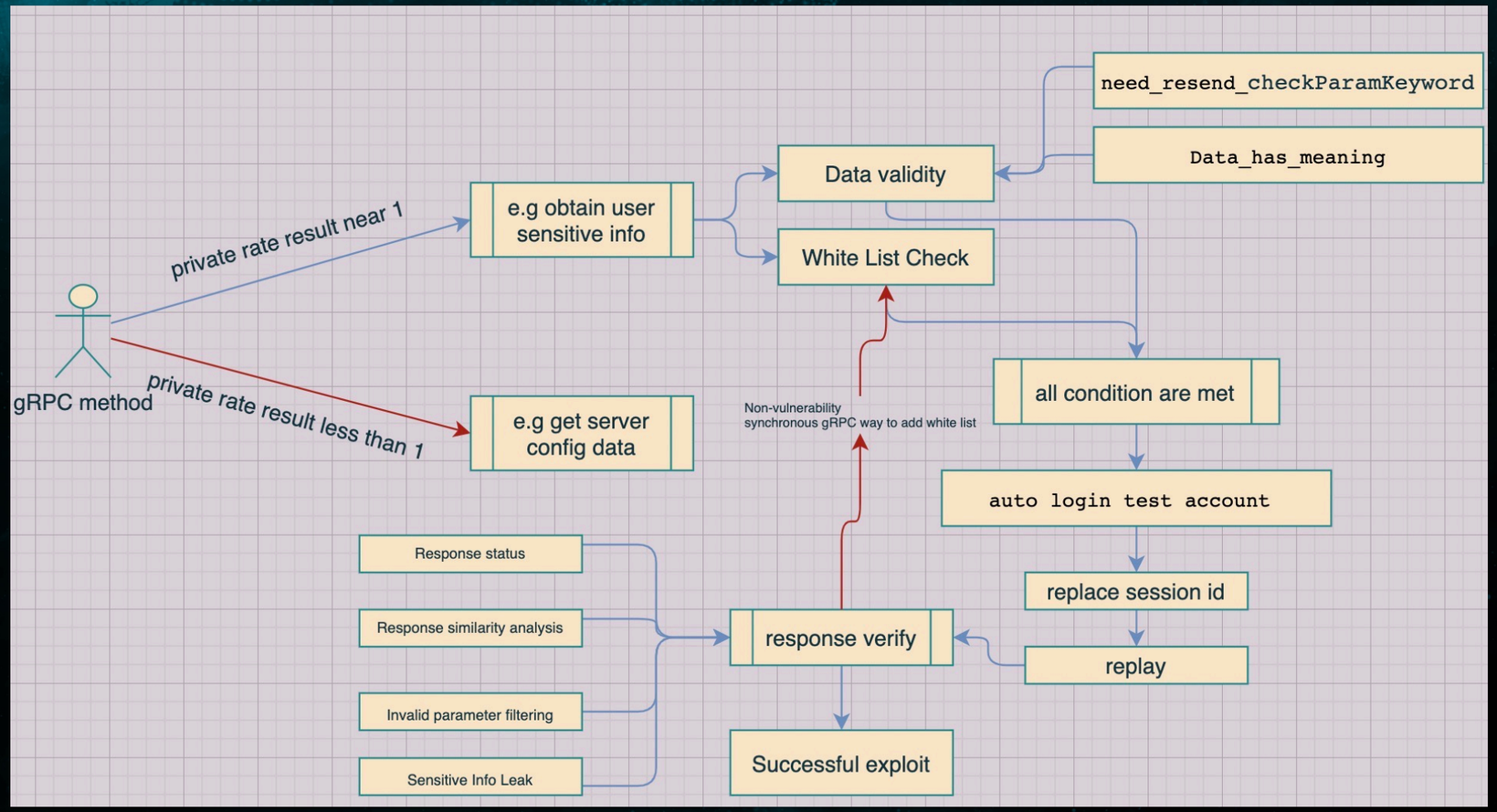
2. Data acquisition, parse and analysis



Grpc method private judgment

How to build a vulnerability mining platform based on grpc protocol

3. Arsenal construction

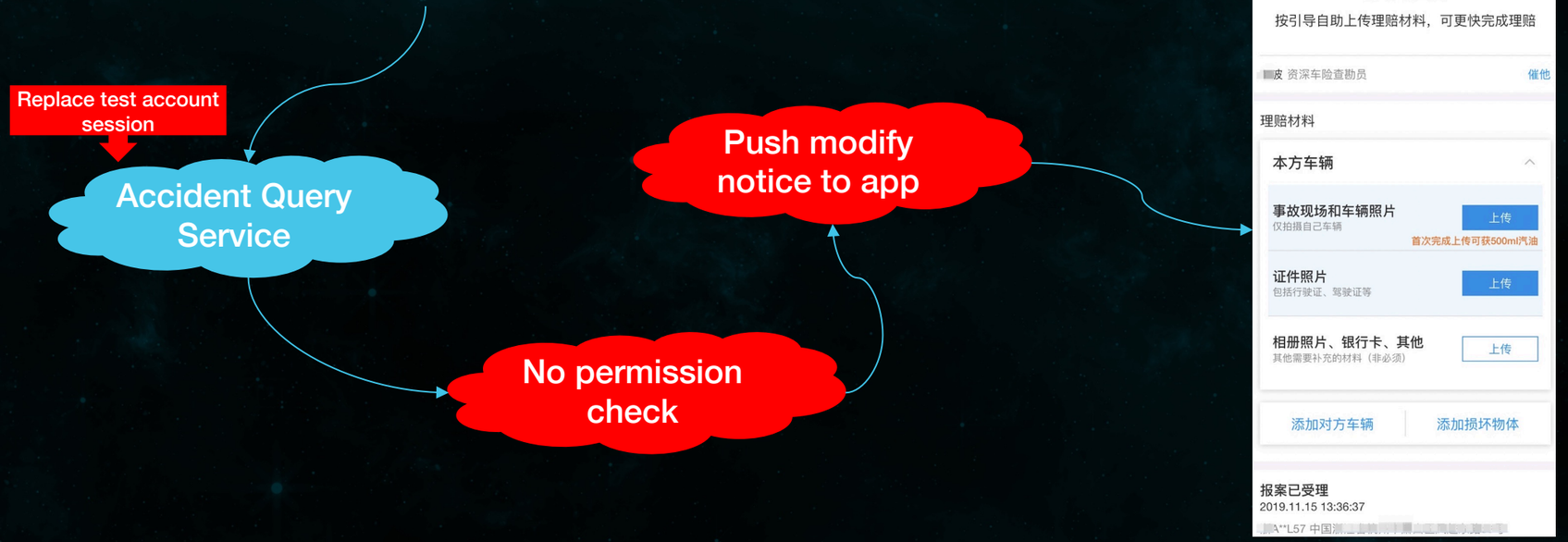


logic bypass vulnerability mining method

How to build a vulnerability mining platform based on grpc protocol

3. Arsenal construction

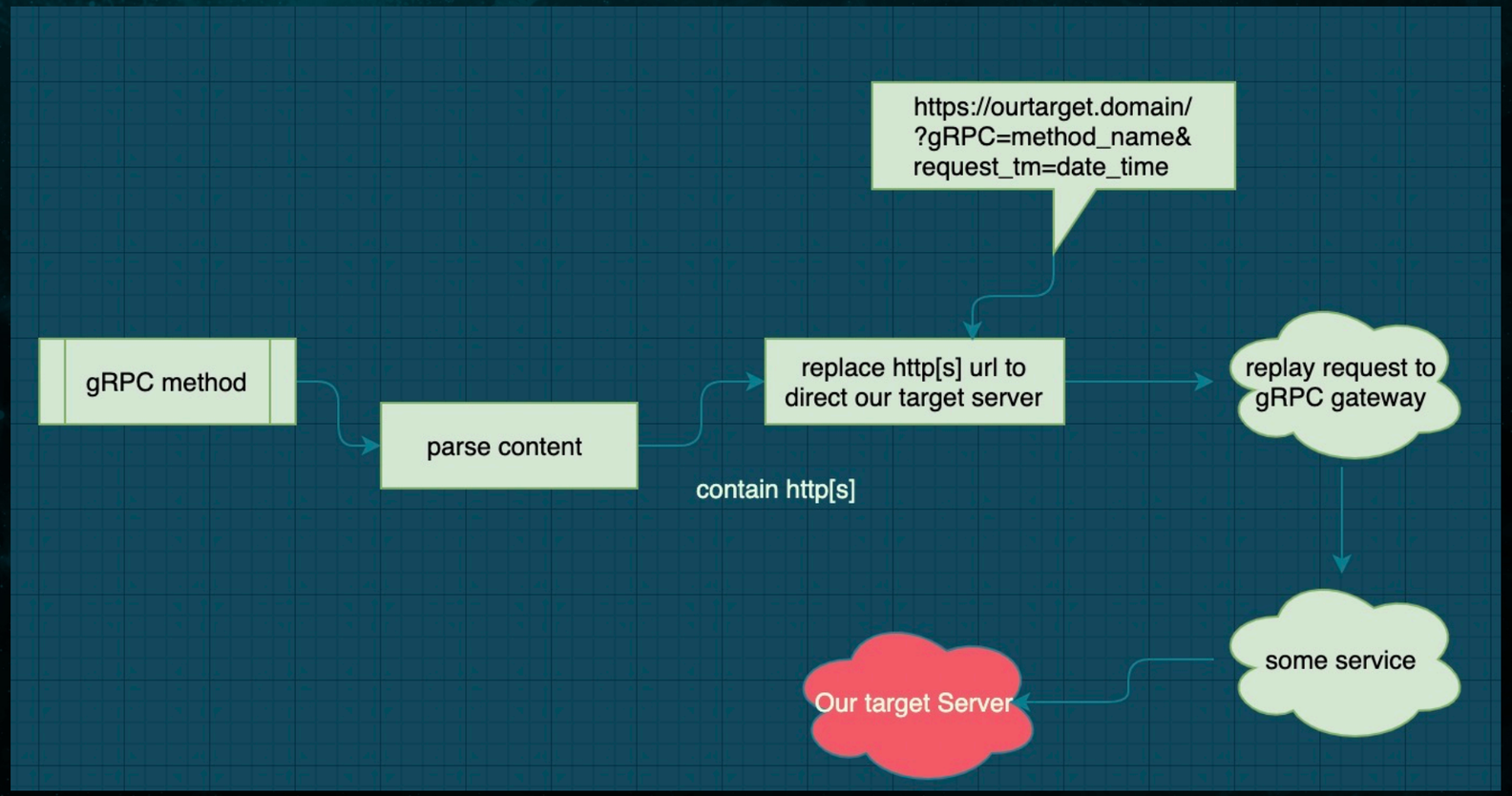
gRPC request : [{"accidentTypeId":"001","carNo":”any car number","policyList":["190412546994060105 49"],"reportAddress":"...",,"report Phone":”phone number"}]



Logic bypass vulnerability bad case

How to build a vulnerability mining platform based on grpc protocol

3. Arsenal construction



SSRF

How to build a vulnerability mining platform based on grpc protocol

3. Arsenal construction

Risk params：
[{"anonymous":true,"bizScene":"","creatorId":”xxx","creatorType":”account_id",
"creatorUserId":”xxx","poi":{},"resourceList":[{"djangoId":"A*Vk1ATJFFZgkAAAAAAAAAAAAAAAUk0AQ",
"previewUrl":"https://resource/apml567281290f65dafa15fcae0de896e8a1.image",
"resourceType":"image",**"resourceUrl":"https://cdndomain.com/afts/img/A*Vk1ATJFFZgkAAAAAAAAAAAAAAAUk0AQ/original?bz=social_content**"}],"text":" Single Wang ran out on Tanabata and ordered a drink, so he should eat and drink alone.??","title":" Life alone is wonderful ",
"topicIdList":["BC_TP_20200819000133493"],"upload_token":"",”accountid":""}]

SSRF bad case

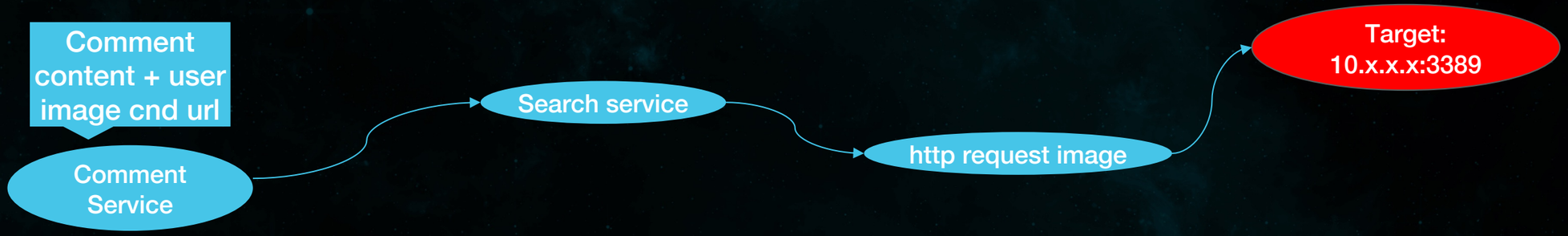
How to build a vulnerability mining platform based on grpc protocol

3. Arsenal construction

Risk params：

[{"anonymous":true,"bizScene":"","creatorId":”xxx","creatorType":”account_id",
"creatorUserId":”xxx","poi":{},"resourceList":[{"djangoId":"A*Vk1ATJFFZgkAAAAAAAAAAAAAAUk0AQ",
"previewUrl":"https://resource/apml567281290f65dafa15fcae0de896e8a1.image",
"resourceType":"image","**resourceUrl":"https://cdndomain.com/afts/img/A*Vk1ATJFFZgkAAAAAAAAAAAAAAUk0AQ/original?bz=social_content**"}],"text":"Single Wang ran out on Tanabata and ordered a drink, so he should eat and drink alone.??","title":" Life alone is wonderful ",
"topicIdList":["BC_TP_20200819000133493"],"upload_token":"",”accountid":""}]

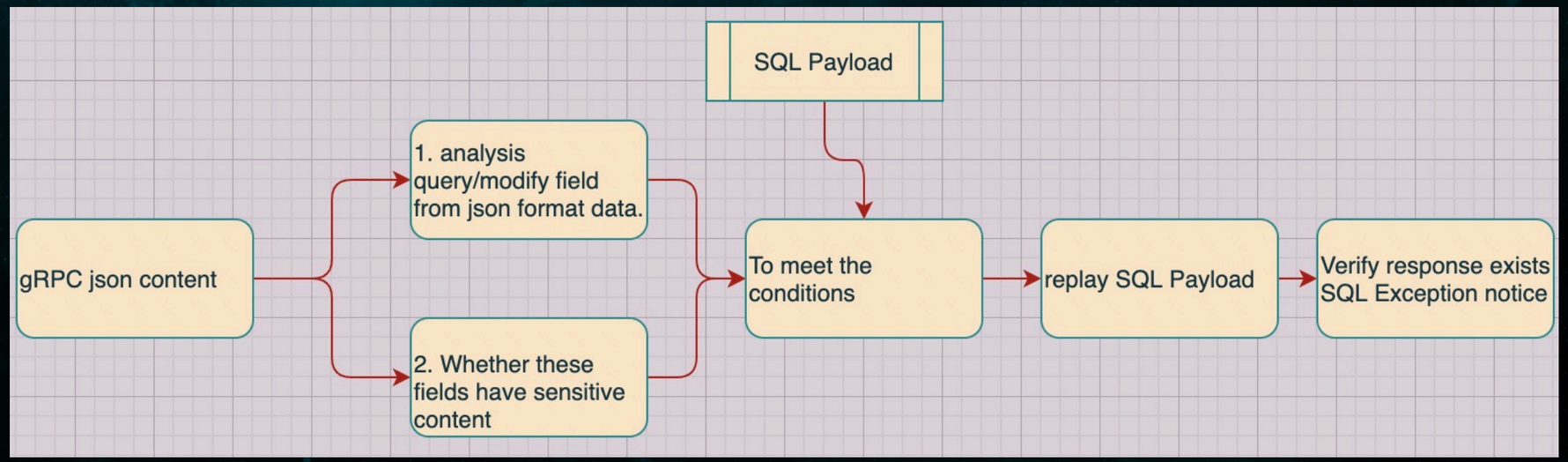
Internal service address：10.x.x.x：3389



SSRF bad case

How to build a vulnerability mining platform based on grpc protocol

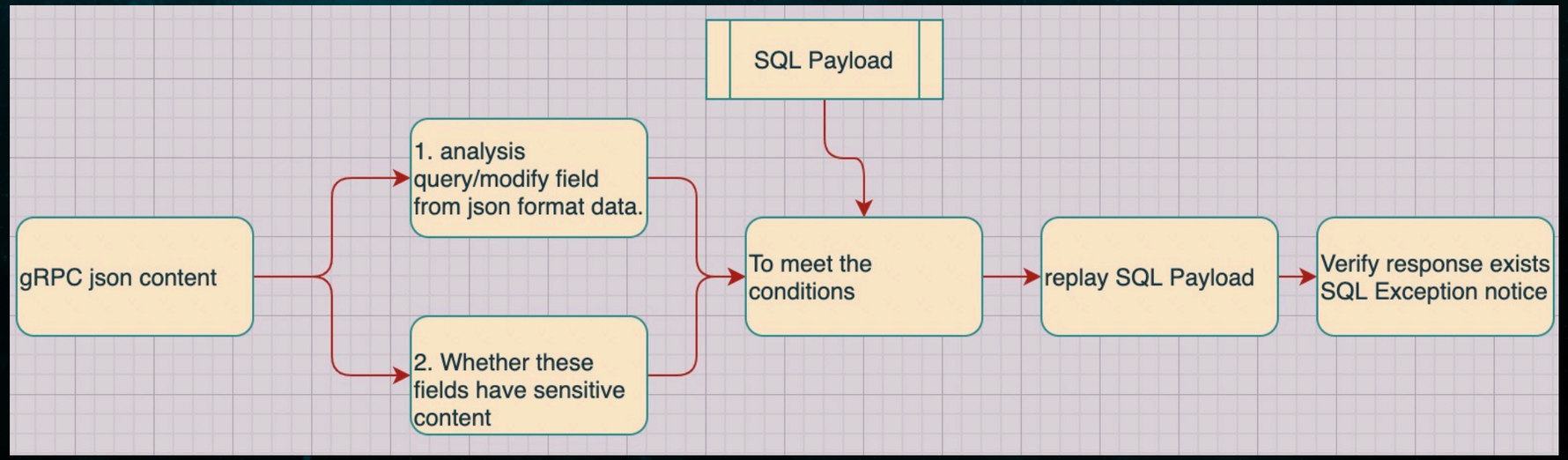
3. Arsenal construction



SQL Inject

How to build a vulnerability mining platform based on grpc protocol

3. Arsenal construction



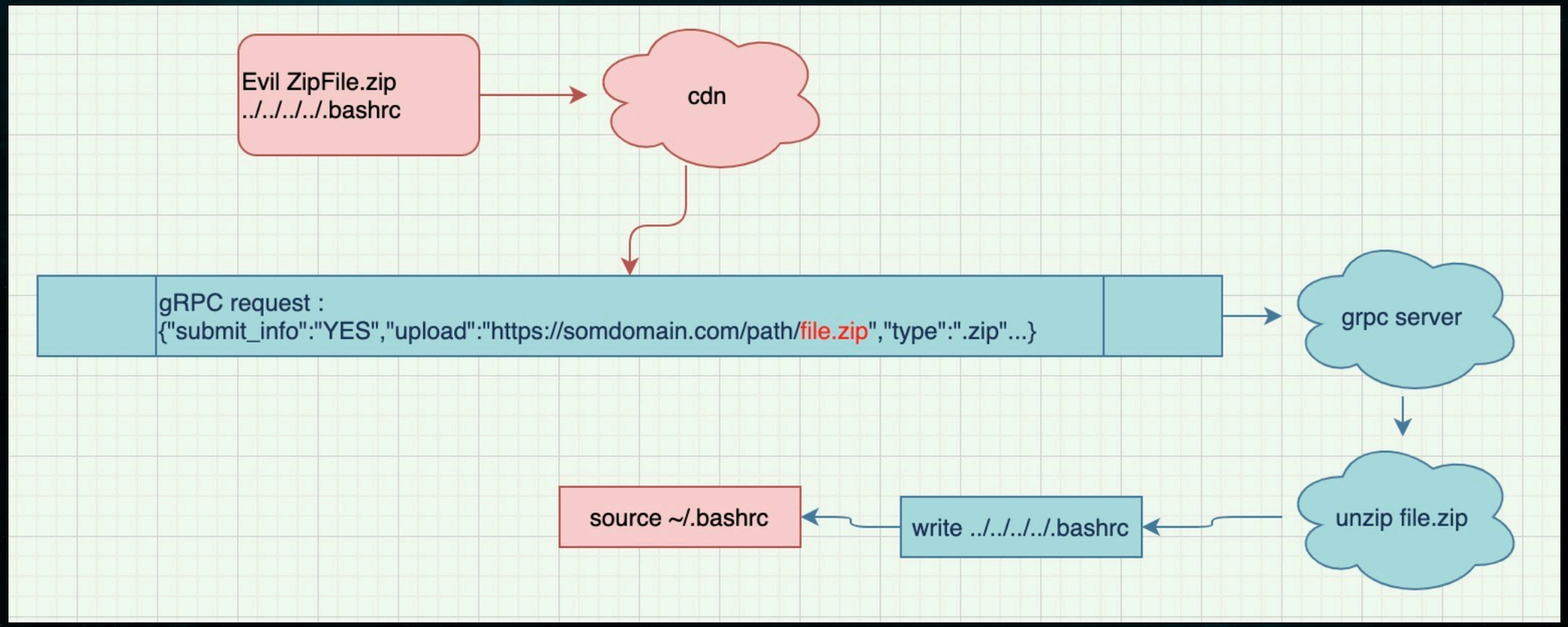
gRPC request : [{"currentPage": 1, "pageItemCount": 20, "uid": ”test@gmail.com AND 1=2"}]

gRPC response : { "success" : false, "resultCode" : "AE15073250005001", "resultView" : "system is error,please retry later!", "errorContext" : { "errorStack" : [{ "errorMsg" : "SqlMapClient operation; uncategorized SQLException for SQL []; SQL state [null]; error code [0]; … ZDAL Rule Error: bc={uid=test@gmail.com AND 1 = 2}; … nested exception is com.ibatis.common.jdbc.exception.NestedSQLException: …Check the statement (query failed). \--- Cause: com.zdal.rule.engine.exception.ZdalRuleCalculateException: ZDAL Rule …

SQL Inject Bad case

How to build a vulnerability mining platform based on grpc protocol

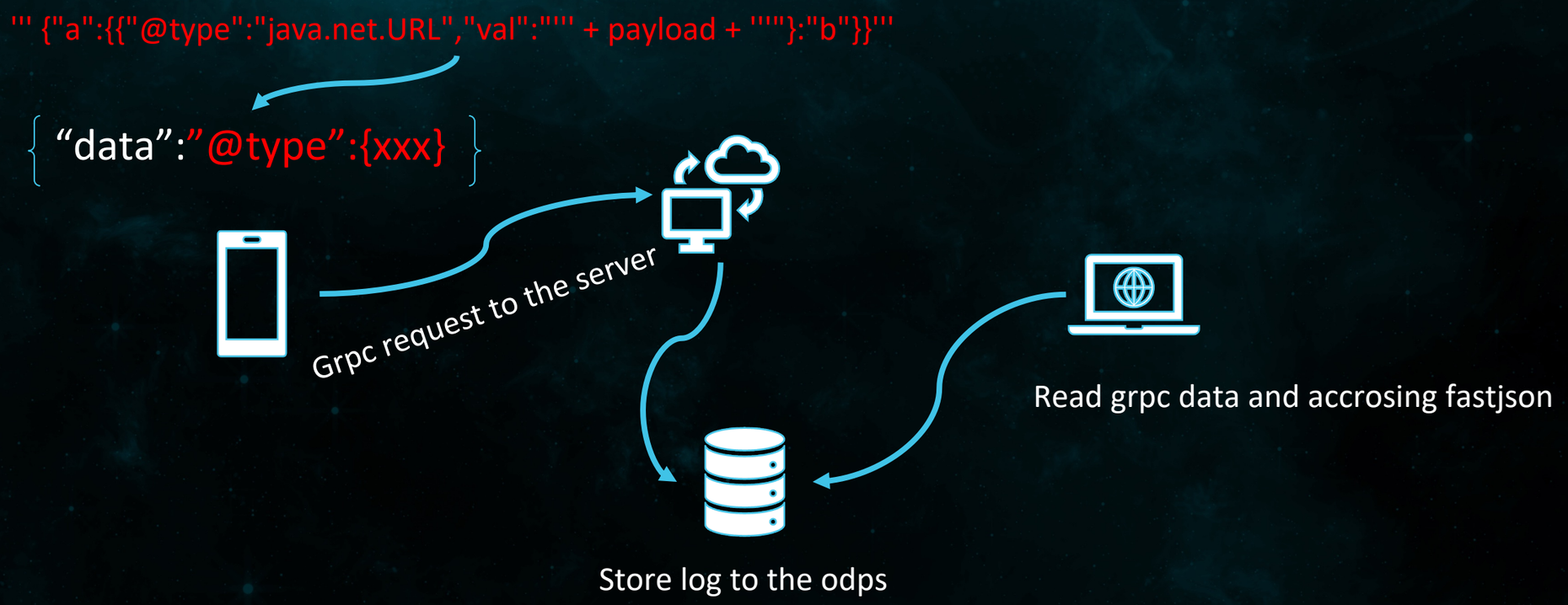
3. Arsenal construction



Command execution triggered by arbitrary path write from Unzip

How to build a vulnerability mining platform based on grpc protocol

3. Arsenal construction



gRPC Fastjson RCE

How to build a moat for gRPC applications

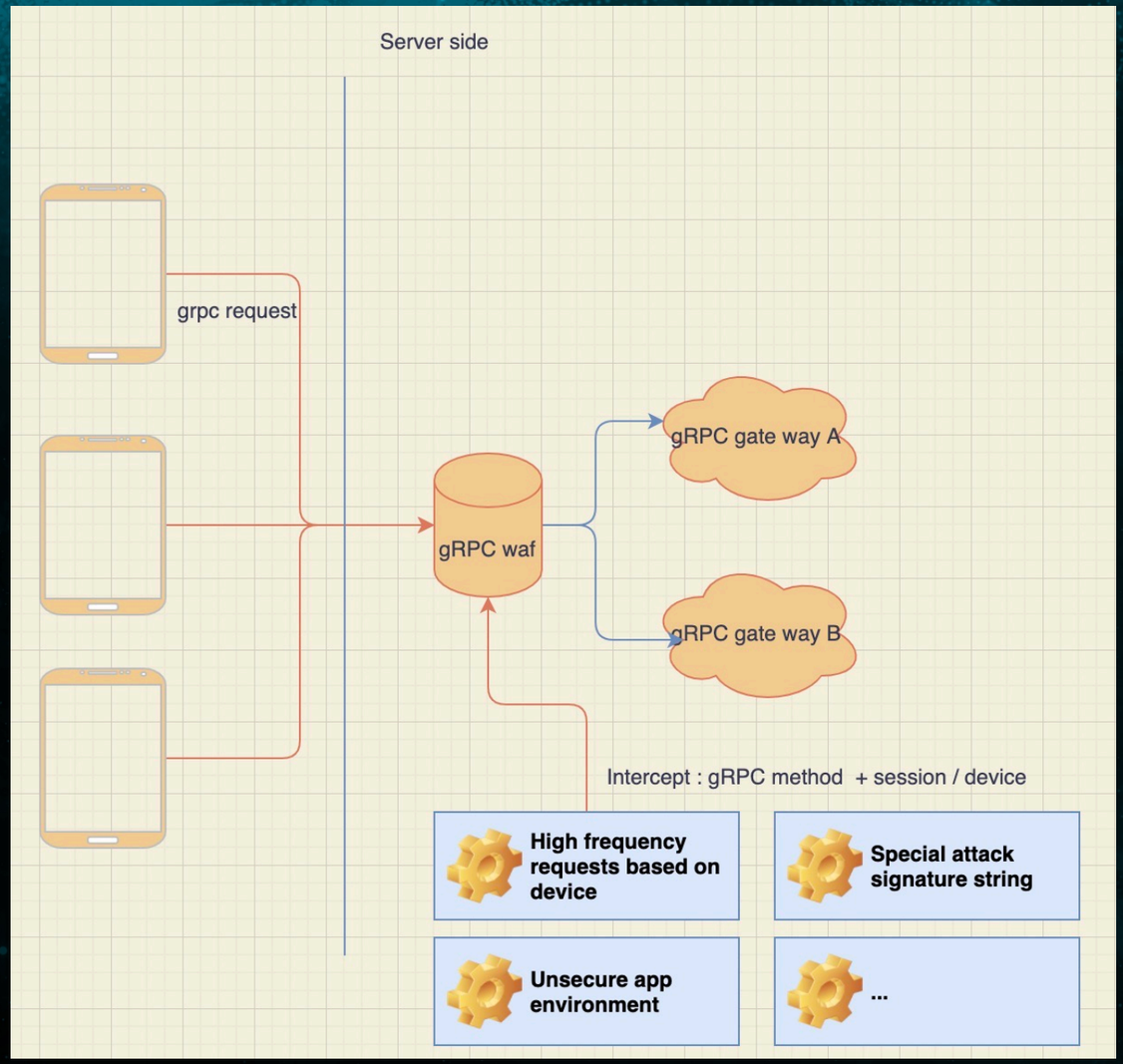
You can't just rely on the security protection mechanism on the mobile app, the server needs supporting infrastructure to build its own moat

This kind of risk confrontation is not a single defense capability, but a systematic construction of the defense-in-depth capability of the server side.

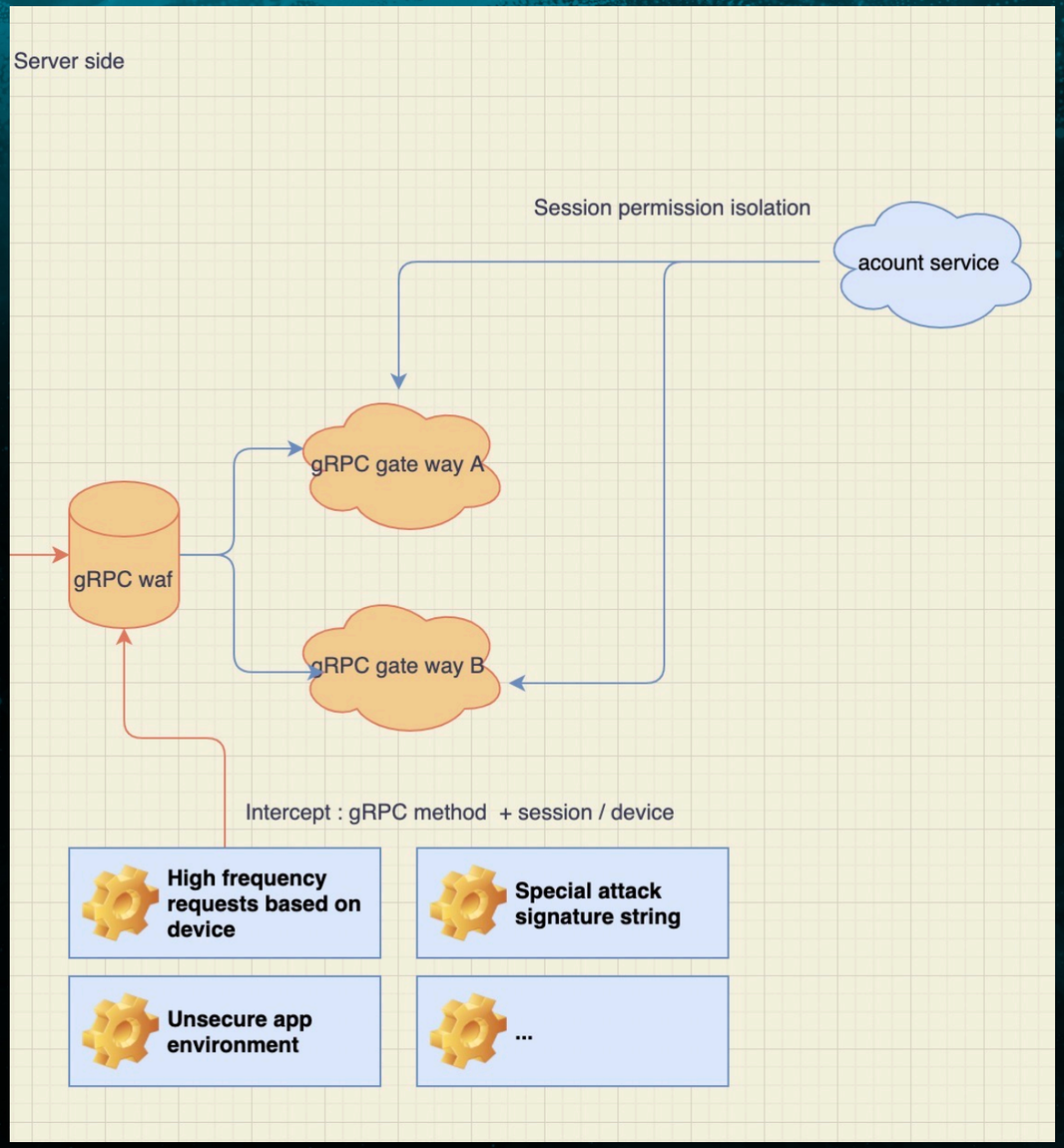
(Every piece has vulnerable.)

(Defense in depth: no vulnerable)

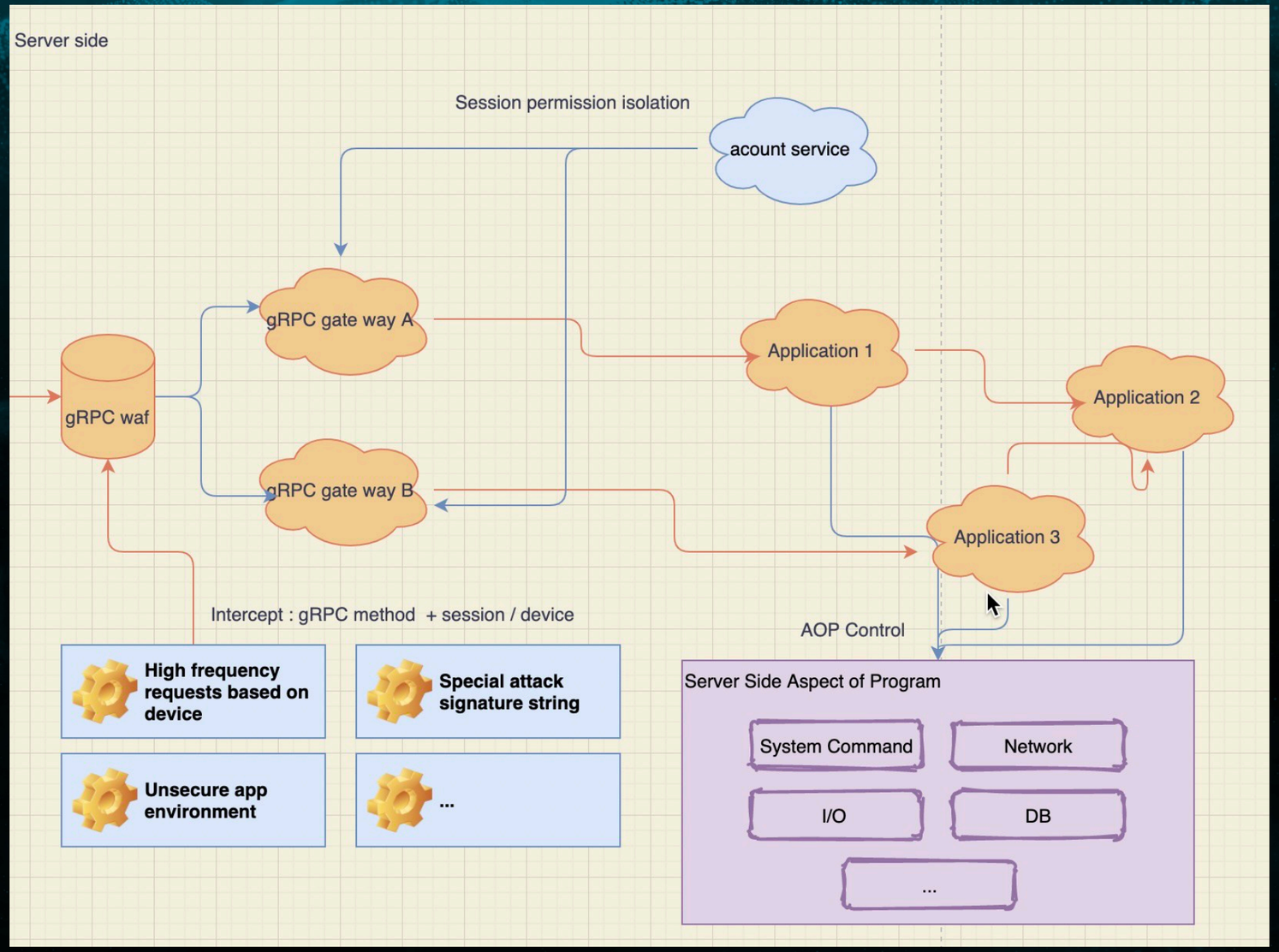
Waf based on gRPC network environment



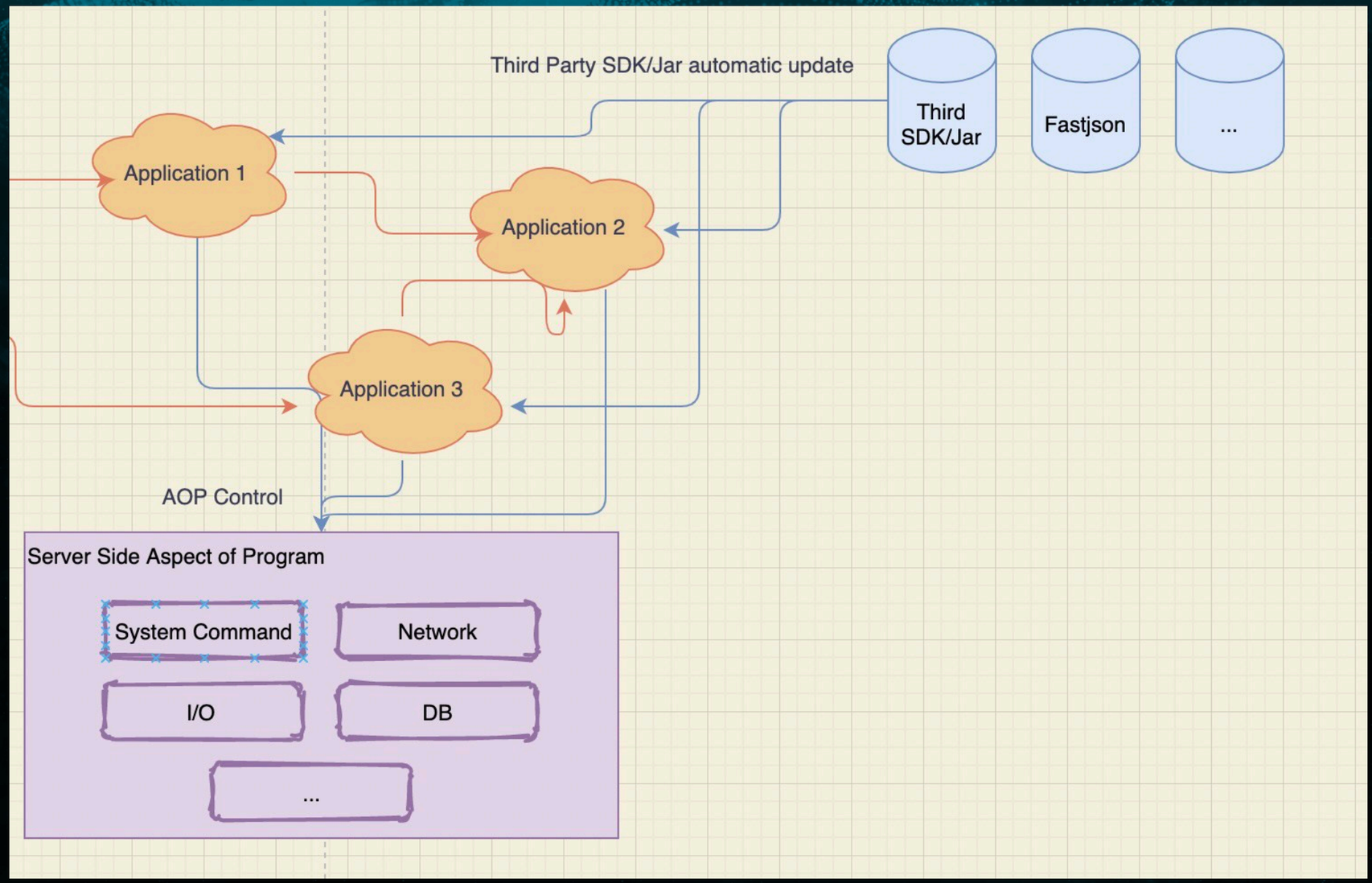
Cookie isolation for different applications



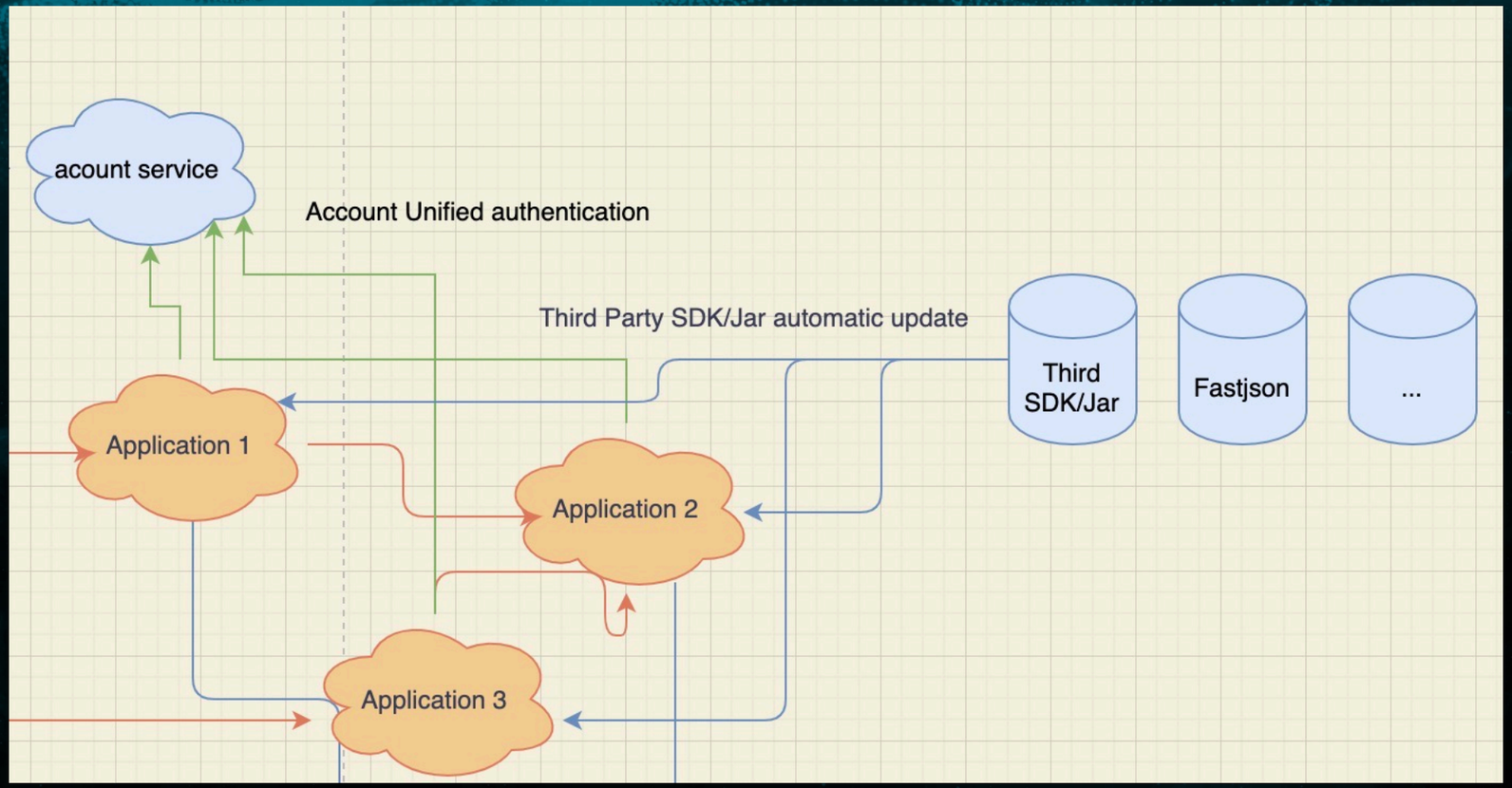
Server-side aspect defense system



Supply chain (Third Part SDK/Jar) automatic update



Unified authentication of account identity



Summary

1. In the era of mobile Internet, a large number of services rely on the gRPC protocol for data exchange.There is a huge attack surface in the middle.

2. With the rapid development of the Internet, the gRPC protocol has become the basis of network protocols facilities , need supporting defense facilities to avoid external network security risks.