
看雪·第七届安全开发者峰会
车联网-站在研发视角挖漏洞
陈迎澳 小米
COURSE
Android
KCTF
2023
SDC

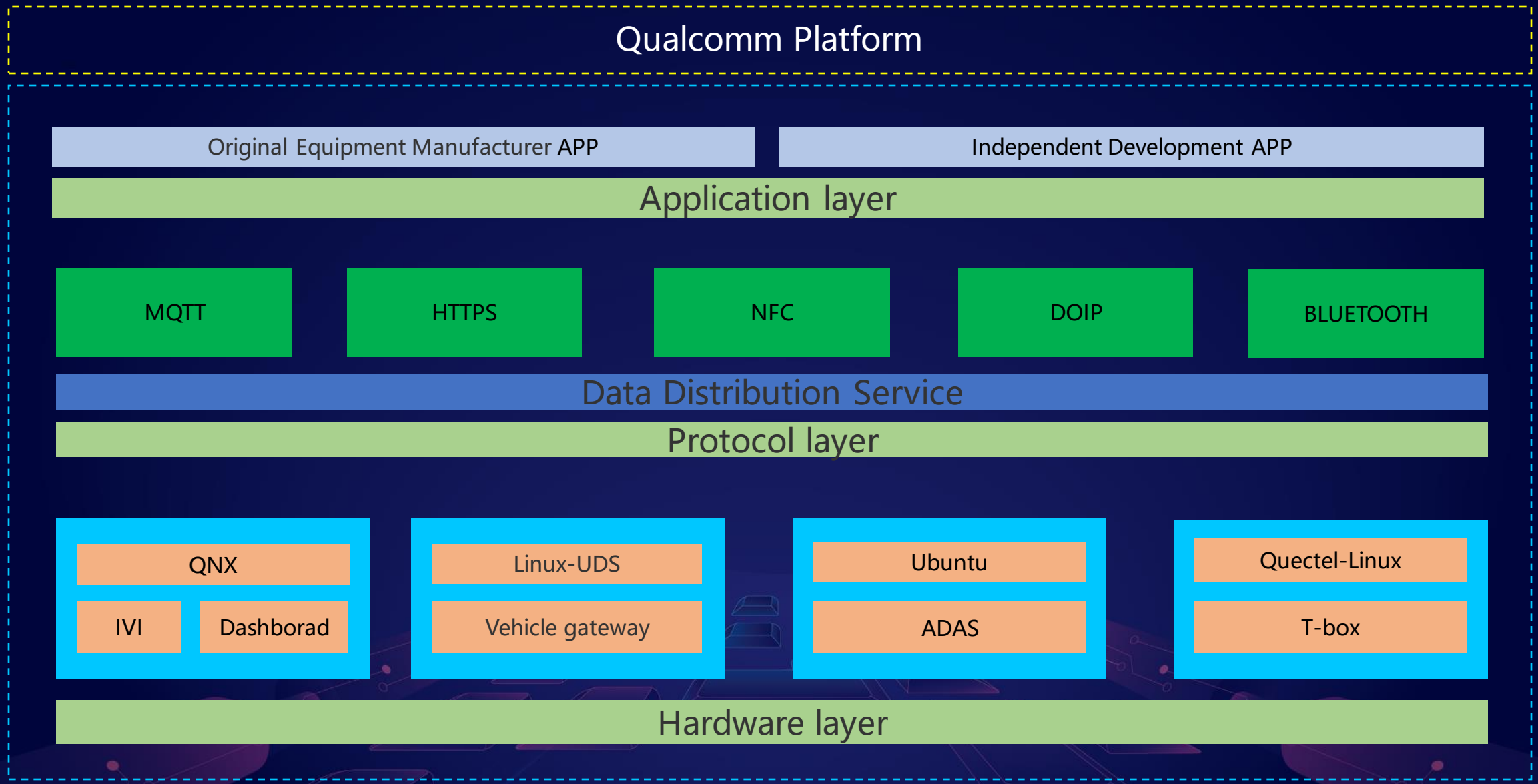
小米智能终端安全实验室

小米旗下的安全团队，实验室致力于研究行业安全技术和实践、研发自动化平台、并对智能终端产品进行安全评估和防护，提升小米产品安全性。团队成员曾多次参加 Geekpwn 天府杯 补天杯等赛事并获大奖

- 汽车网络架构
- 固件提取
- 寻找控车目标
- 寻找突破口
- 研发过程中出现的问题
- 控车案例—Geekpwn2022
- 漏洞成果

先从汽车网络架构讲起


燃油车架构
QNX
RTOS
移远Linux
Vehicle gateway
仪表盘
IVI
T-box
RTOS
TSP
日志上传
PKI认证
远程控车
车辆位置监控


Qualcomm Platform
Original Equipment Manufacturer APP
Independent Development APP
Application layer
MQTT
HTTPS
NFC
DOIP
BLUETOOTH
Data Distribution Service
Protocol layer
QNX
IVI
Dashborad
Linux-UDS
Vehicle gateway
Ubuntu
ADAS
Quectel-Linux
T-box
Hardware layer

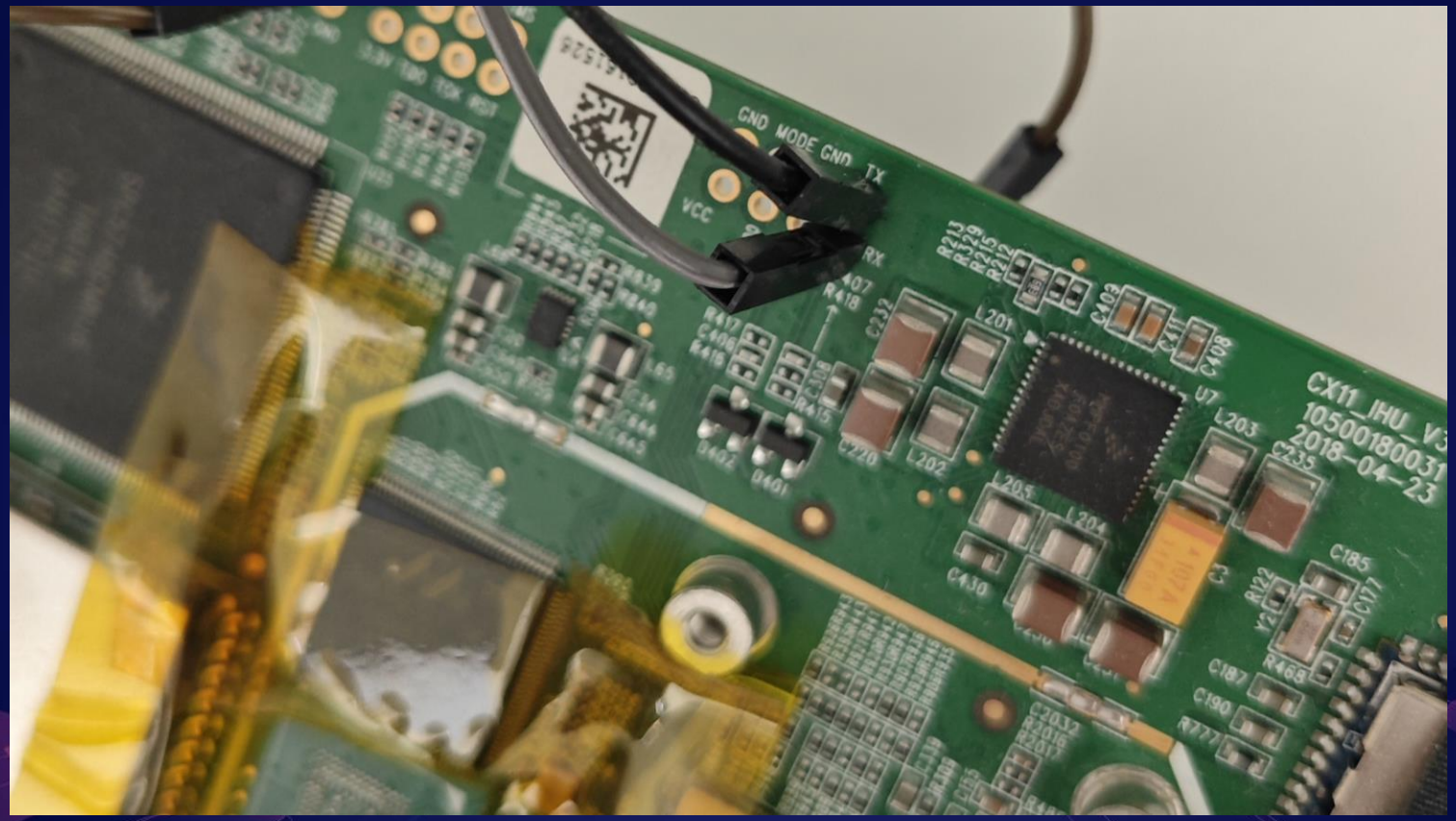
	燃油车架构	新能源架构
IVI	QNX	基于QNX虚拟机的Android
Dashborad	QNX	QNX or Android
T-box	Quectel Linux	Quectel Linux
Vehicle gateway	RTOS UsbCan	Embedded Linux Doip
ADAS	Null	Ubuntu

一切分析的开始，拿固件

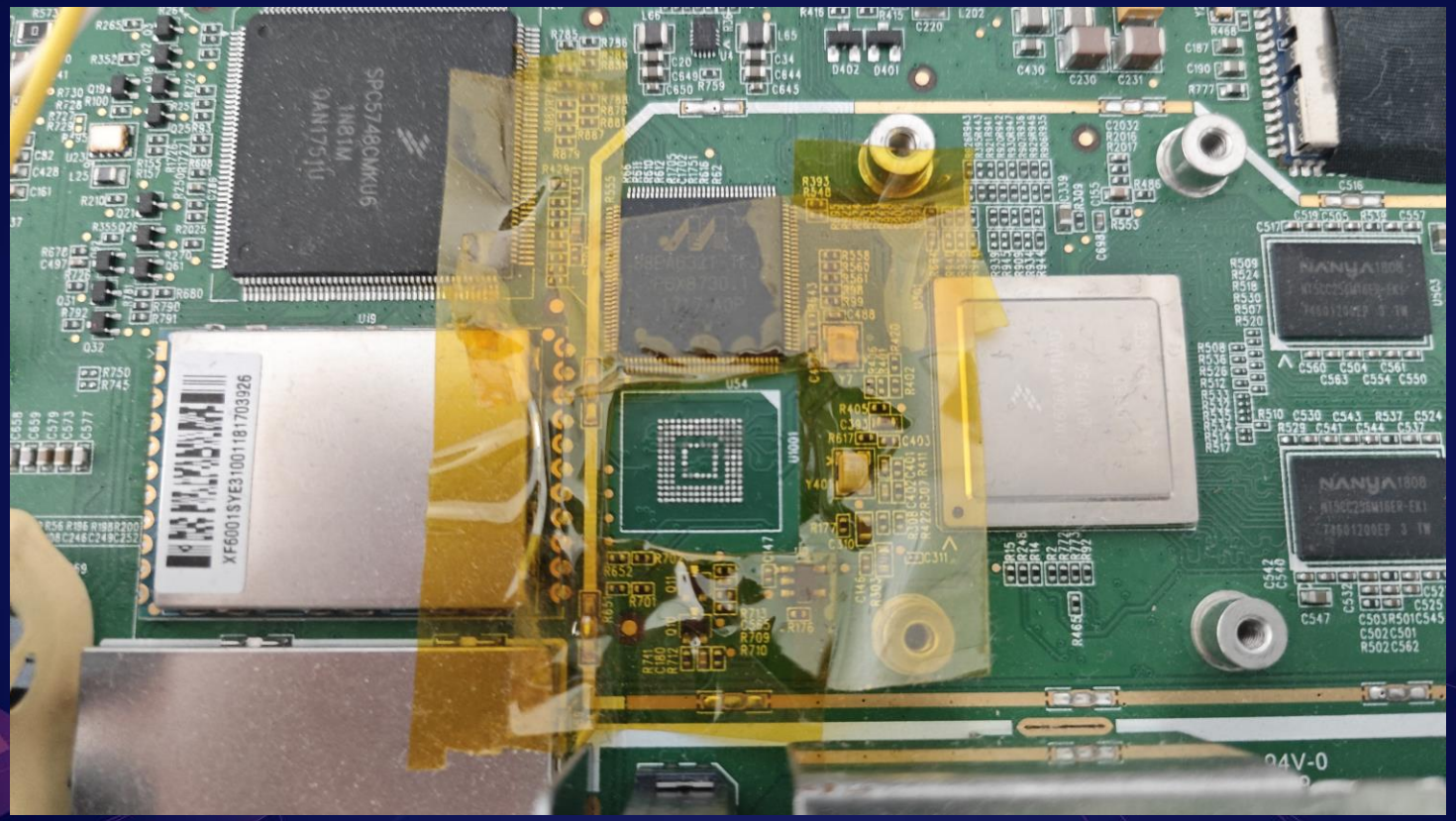
固件提取

<table>
<tr><td>IVI</td><td>Dashborad</td><td>T-box</td><td>Vehicle gateway</td><td>ADAS</td></tr>
<tr><td colspan="5">热风枪吹取Flash，通过底座进行读取</td></tr>
<tr><td colspan="5">找到引脚定义，通过调试引脚飞线进入调试进行提取</td></tr>
<tr><td rowspan="2">工程模式开启ADB提取</td><td colspan="4">使用IVI热点，无任何网段隔离，弱口令或供应商通用口令进各组件SSH</td></tr>
<tr><td colspan="4">使用IVI热点，除T-box外存在网段隔离，以T-box为跳板进各组件SSH</td></tr>
</table>

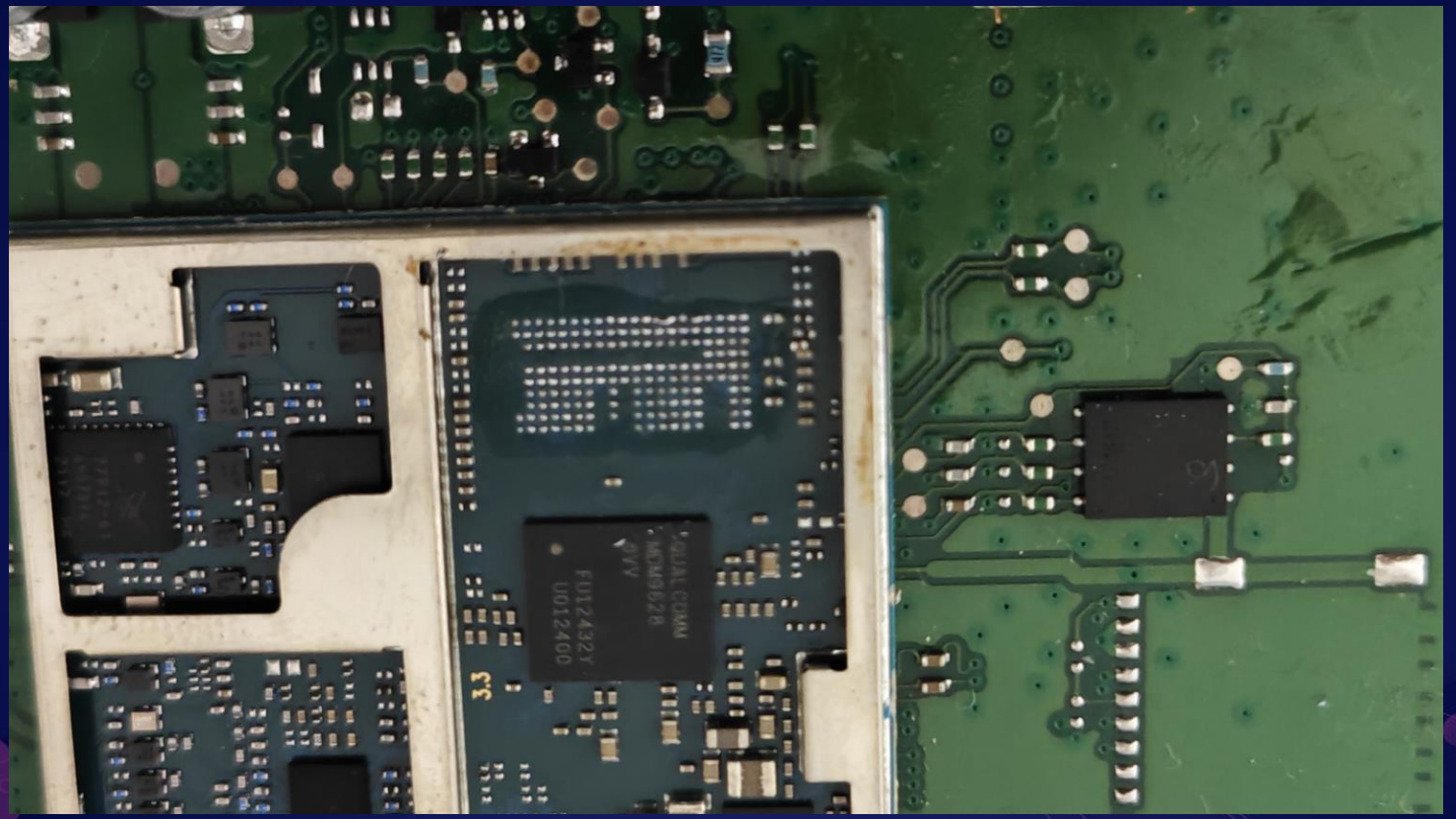
调试串口



EMMC芯片吹取

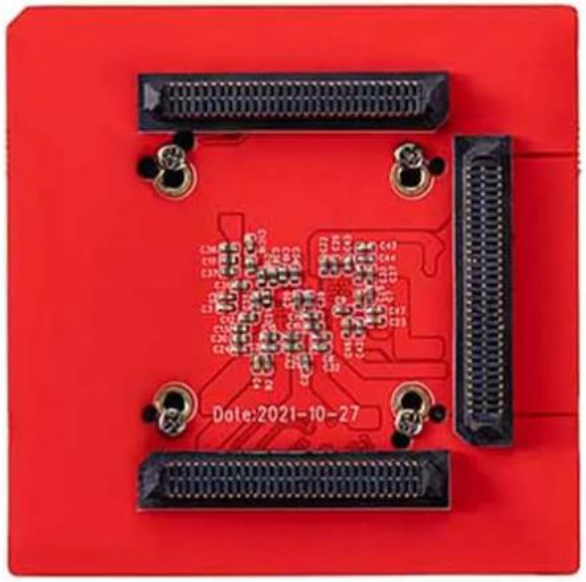


EMCP芯片吹取



编程器


UFS-BGA-153
WWW.ICFRIEND.COM
UFS-BGA-297
ICFRIEND
NB-HS-BGA 4 in 1
ICFRIEND
UFS-EMMC-BGA254


Date:2021-10-27

OEM登陆口令

oelinux123

quectel123

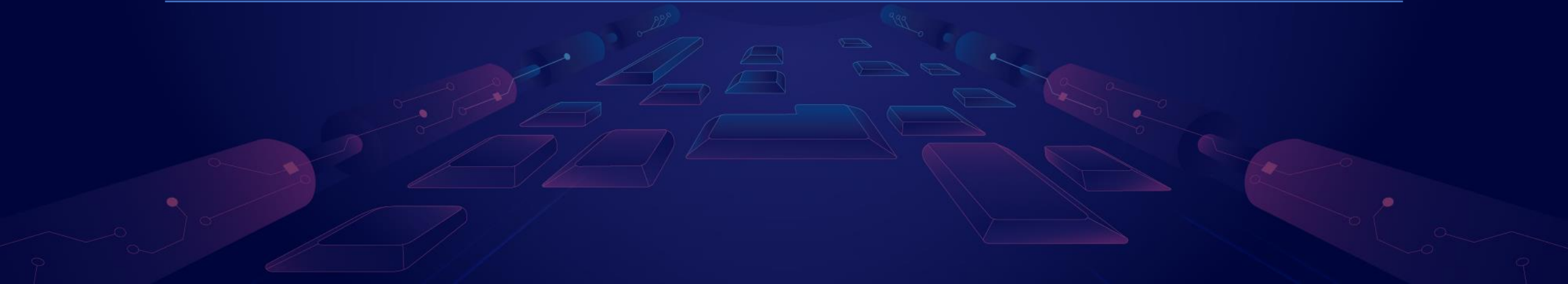
如何寻找目标

信息收集

1.该品牌有无信息安全团队，是否正在招聘信息安全人员

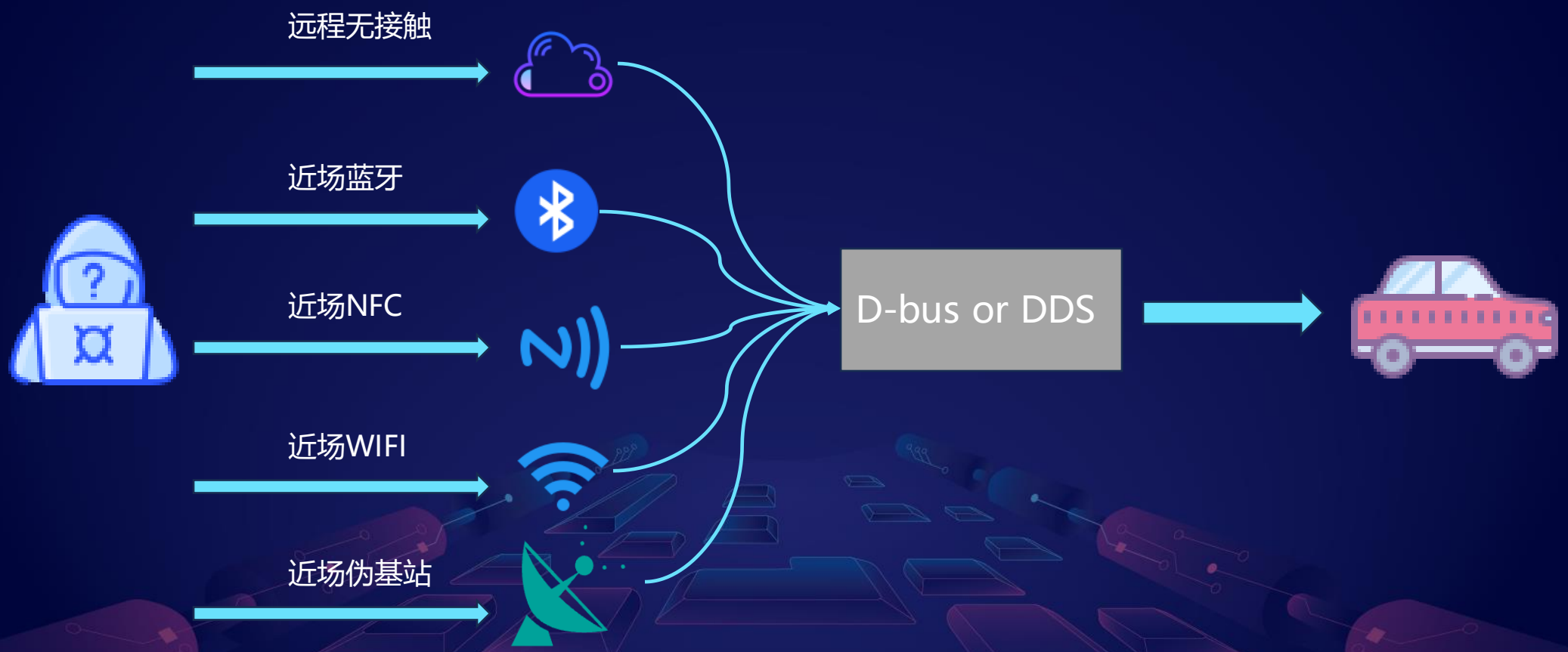
2.该品牌供应商为几家，这几家供应商供应几家车厂

3.通过供应商情况与车厂情况判断是否重视安全

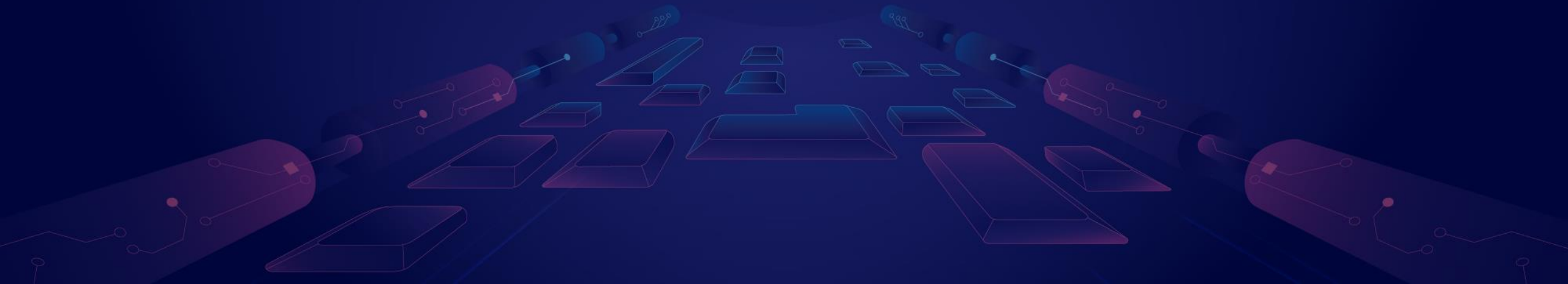


确立目标后如何寻找突破口

“一远四近”



研发过程中出现的问题

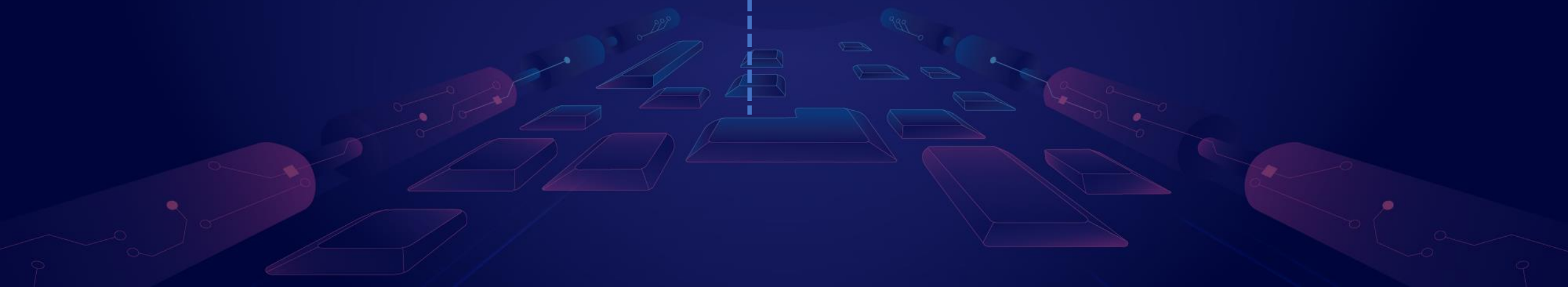


总体设计

- 上百页的技术文档
- 充分的调研论证
- 多次的安全评审

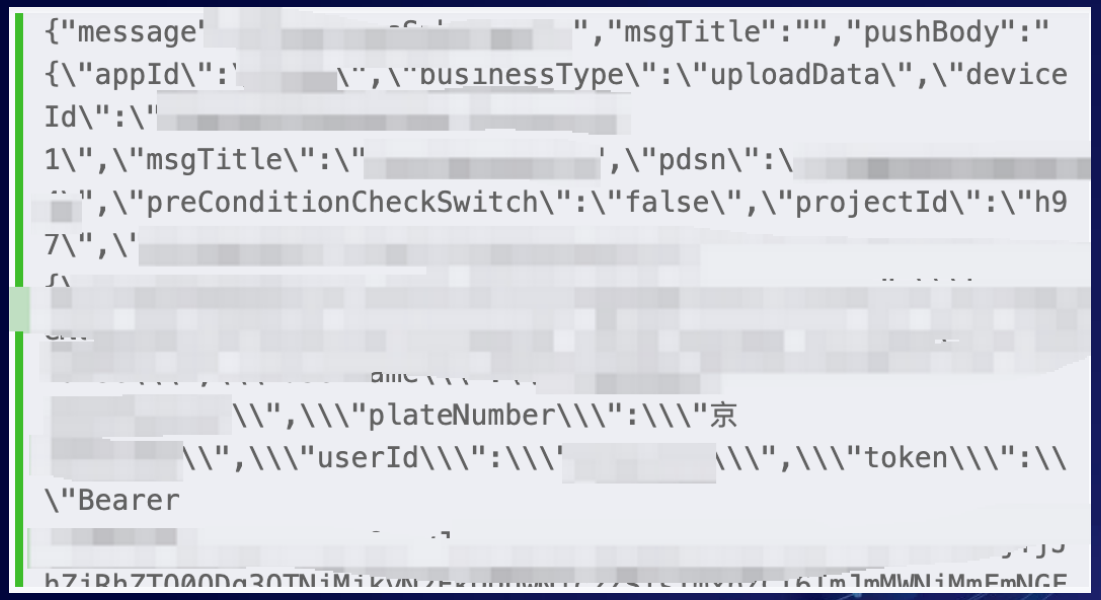
编码

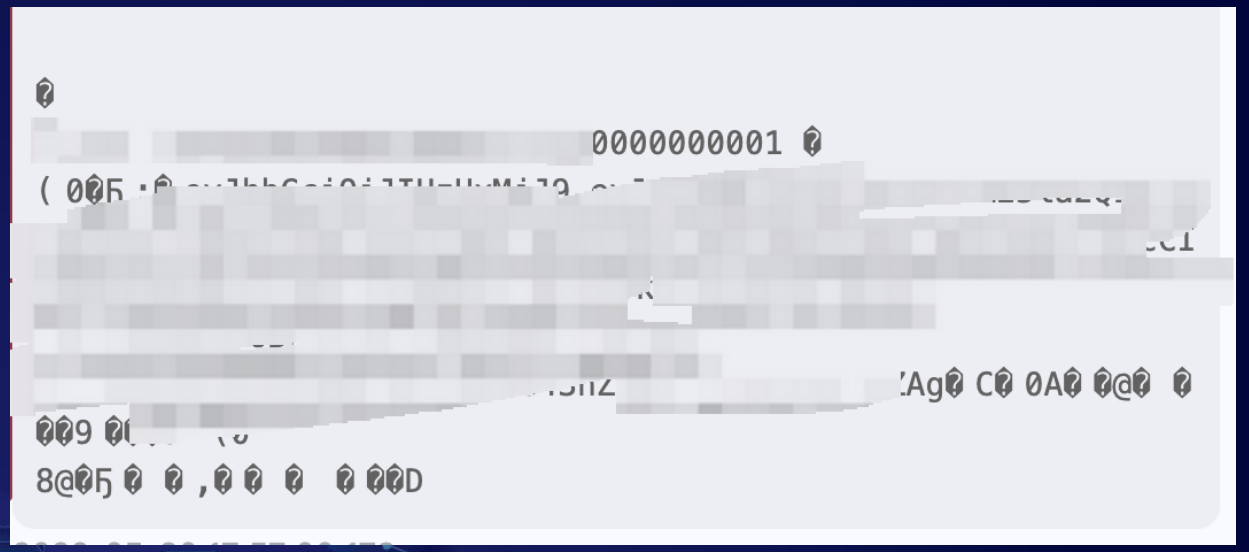
- 研发人员项目上线压力
- 研发人员安全意识不高
- 实施时不重视安全，对设计阶段的蓝图打折扣完成



控车案例—MQTT的问题

MQTT





OEM的MQTT服务供应ABCDE五个车厂，想要控A车，在无A车硬件前提下，调研B车APP发现，可通过B车泄漏TLS证书，打入A车MQTT服务，使用A系车VIN控A系其他汽车，**实现多点收集，一点爆破。**

TSP地址在私网怎么办

私网突破

首先需要台架先上网，使用贴片天线，成本低廉

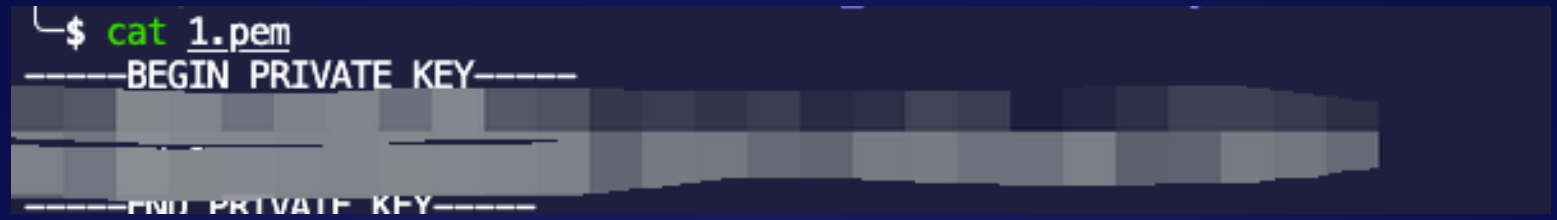
配置文件中泄漏地址

conUrl	
dataMiningUrl	
ipChannel	
dataMiningEnable	1
numberBcallLocation	
numberEcallLocation	
numberIcallLocation	
lastLat	
lastLon	
groupId	
pkiUrl	
username	
pwd	

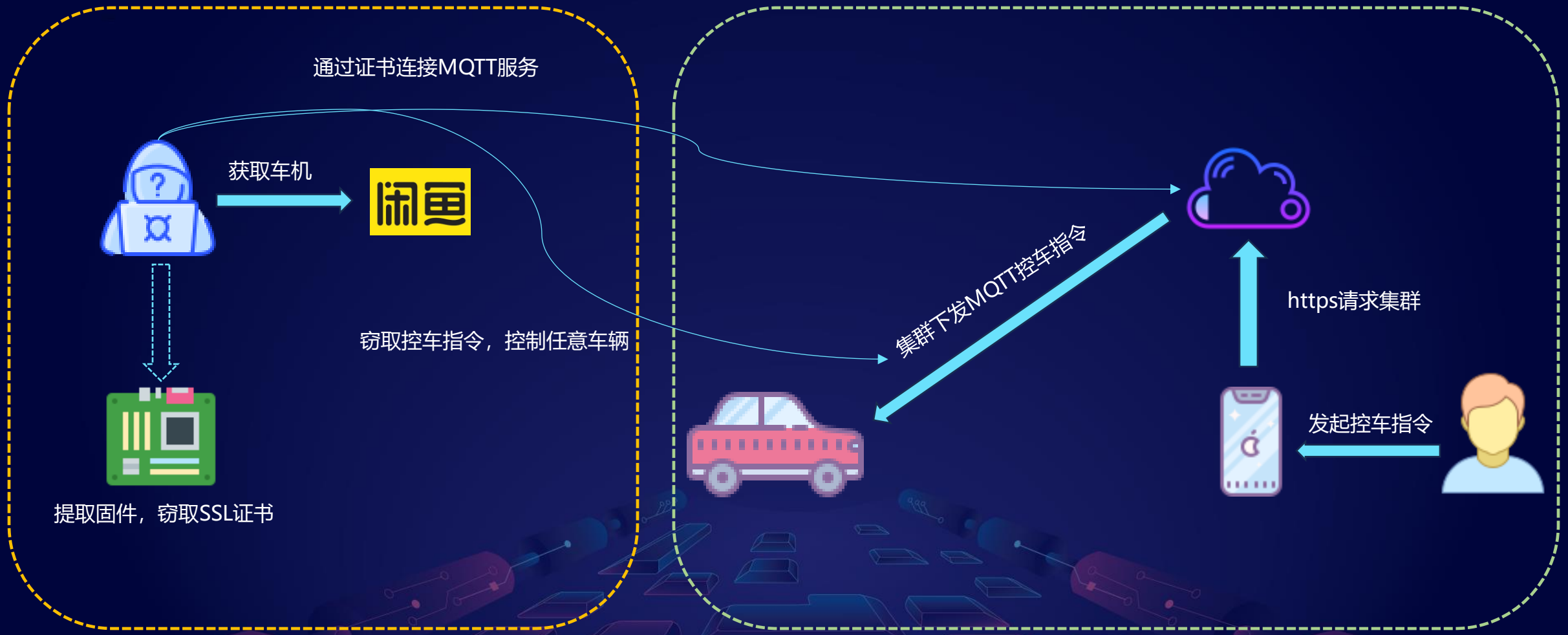
cm_provision_rsm
call_auto_dial_attempts
mqtt_server_ip_address
mqtt_server_address
netprot_tsp_port
mqtt_bypass_server_address
mqtt_bypass_server_port
sms_number
public_apn_param
netprot_apn_name
msg_timeout
msg_retry_numbers

其次泄漏服务地址，并在固件中泄漏证书

固件中泄漏证书



动态调试或静态分析进行证书提取


通过证书连接MQTT服务
获取车机
闲鱼
窃取控车指令，控制任意车辆
集群下发MQTT控车指令
https请求集群
发起控车指令
提取固件，窃取SSL证书
攻击侧
用户侧

漏洞成果

IVI APP使用公开签名且无签名校验

```
Valid APK signature v2 found

    Signer 1

        Type: X.509
        Version: 3
        Serial number: 0xb3998086d056cffa
        Subject: EMAILADDRESS=android@android.com, CN=Android, OU=Android, O=Android, L=Mountain View, ST=California, C=US
        Valid from: Wed Apr 16 06:40:50 CST 2008
        Valid until: Sun Sep 02 06:40:50 CST 2035

        Public key type: RSA
        Exponent: 3
        Modulus size (bits): 2048
        Modulus: 19752360514994145315516200922626500113201095930210877139293882360491442085478786151541720152971477143983881863321664523422547611110099273765224120568364777034650912678907821093580890163251737414924

        Signature type: MD5withRSA
        Signature OID: 1.2.840.113549.1.1.4

        MD5 Fingerprint: 8D DB 34 2F 2D A5 40 84 02 D7 56 8A F2 1E 29 F9
        SHA-1 Fingerprint: 27 19 6E 38 6B 87 5E 76 AD F7 00 E7 EA 84 E4 C6 EE E3 3D FA
        SHA-256 Fingerprint: C8 A2 E9 BC CF 59 7C 2F B6 DC 66 BE E2 93 FC 13 F2 FC 47 EC 77 BC 6B 2B 0D 52 C1 1F 51 19 2A B8

Valid APK signature v3 found
```

安装system权限app

T-box MQTT不存在有效认证

单纯的将TEE作为密钥存储的工具是不可靠的

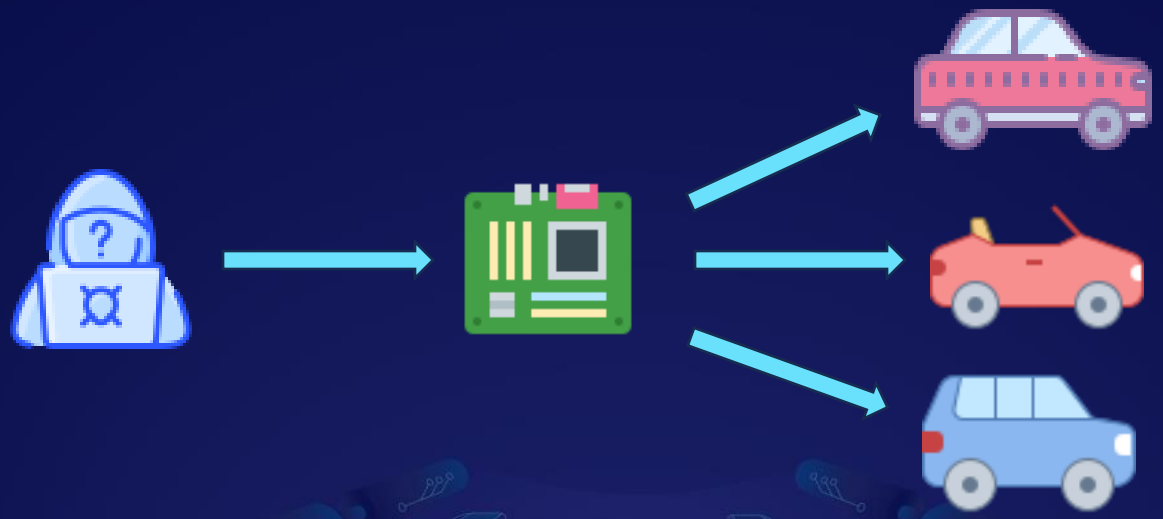
T-box 本地提权

```
  while ( v34 < 0 );
  v36 = read(v34, cmd_str, 2047u);
  if ( v36 > 4 )
    break;
  shutdown(v35, 2);
  close(v35);
  (0, 4, , v36);
}
*((_BYTE *)cmd_str + v36) = 0;
v37 = (0, 4, cmd_str[0]);
switch ( cmd_str[0] )
{
  case 1:
    sub_160FC(v37);
    if ( (unsigned int)(dword_3B300 - 1) > 1 )
    {
      dword_3B300 = cmd_str[0];
      v58 = (void *)operator new[](v36 + 1);
      memcpy(v58, cmd_str, v36);
      pthread_attr_init(s);
      pthread_attr_setdetachstate(s, 1);
      v59 = pthread_create(&newthread, s, (void *(*)(void *))sub_162B4, v58);
      v60 = v59;
      if ( v59 )
      {
```

```
switch ( cmd_str[0] )
{
  case 1:
    sub_160FC(v37);
    if ( (unsigned int)(dword_3B300 - 1) > 1 )
    {
      dword_3B300 = cmd_str[0];
      v58 = (void *)operator new[](v36 + 1);
      memcpy(v58, cmd_str, v36);
      pthread_attr_init(s);
      pthread_attr_setdetachstate(s, 1);
      v59 = pthread_create(&newthread, s, (void *(*)(void *
  case 42:
    shutdown(v35, 2);
    close(v35);
    system((const char *)&cmd_str[67]);
    goto LABEL_150;
  case 43:
```

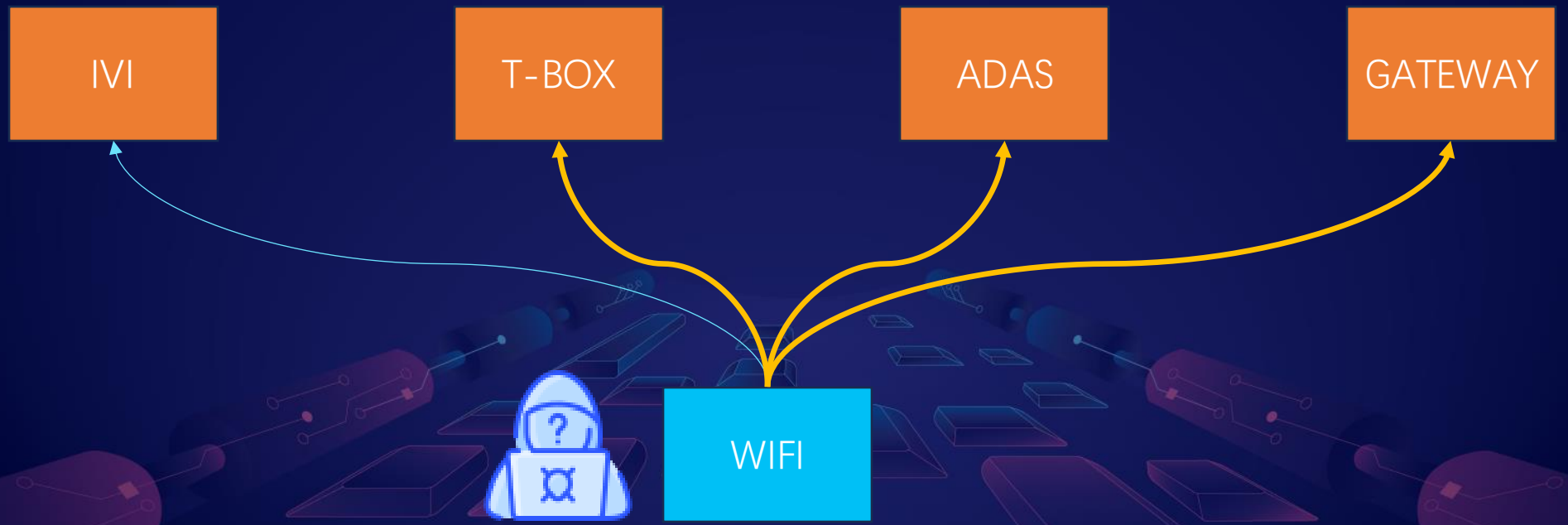
用户可控，cmd_str控制case，传入相应偏移，将case置为42触发漏洞

T-box 运营商网段未隔离



通过A车T-box的网络攻击其他A车，同时B车与A车在一个运营商网段，可从A车打入B车

车域之间不隔离

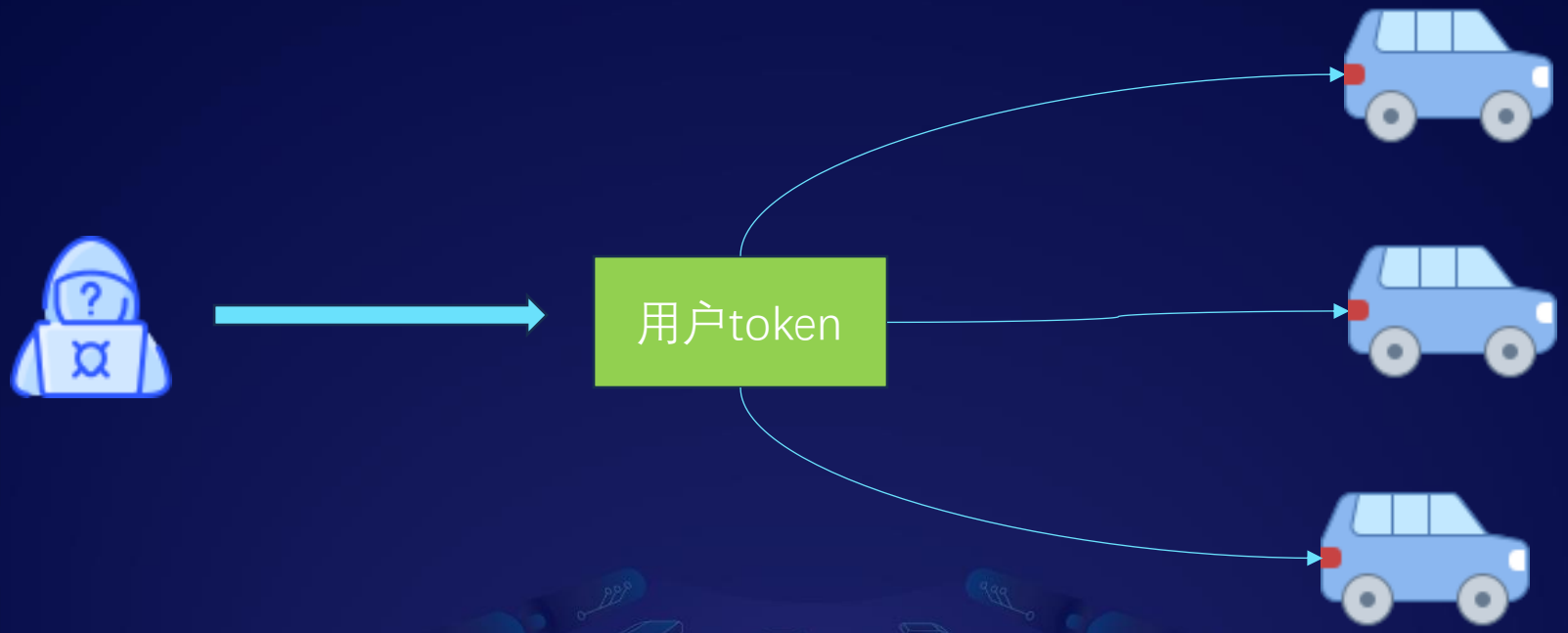


USB工程模式

```
v22 = strcmp("0529", sysattr_value) == 0;
if ( !v9 )
  v22 = 0;
if ( v22 && (!strcmp("0001", v9) || !strcmp("0003", v9)) )
{
  *(_QWORD *)argv = 0x703914007044C8LL;
  v38 = 0;
  v23 = fork();
  if ( !v23 )
  {
    v23 = execve("/usr/bin/hasplmd", argv, (char *const *)environ);
    if ( v23 < 0 )
      sub_48F04();
```

检测Vender Id 与 Product Id

云端平行越权



通过A车token可控该品牌下任意一款汽车

谢谢