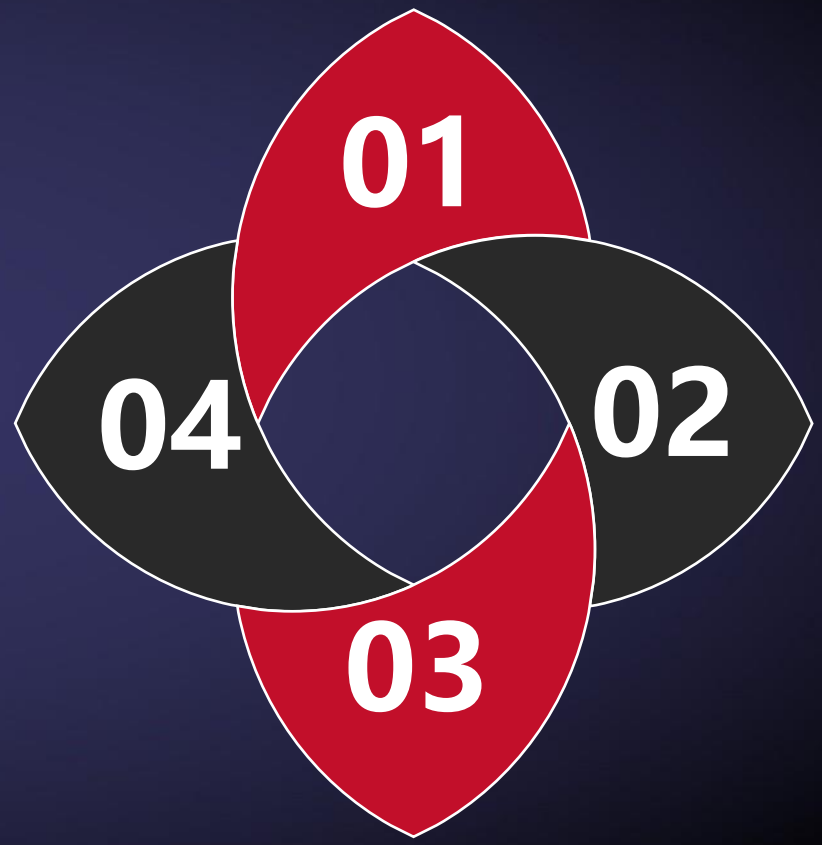
C3安全峰会
CYBER | CLOUD | COMMUNICATION

车联网之边界安全

国家互联网应急中心
王永建

目录

C3安全峰会
CYBER | CLOUD | COMMUNICATION



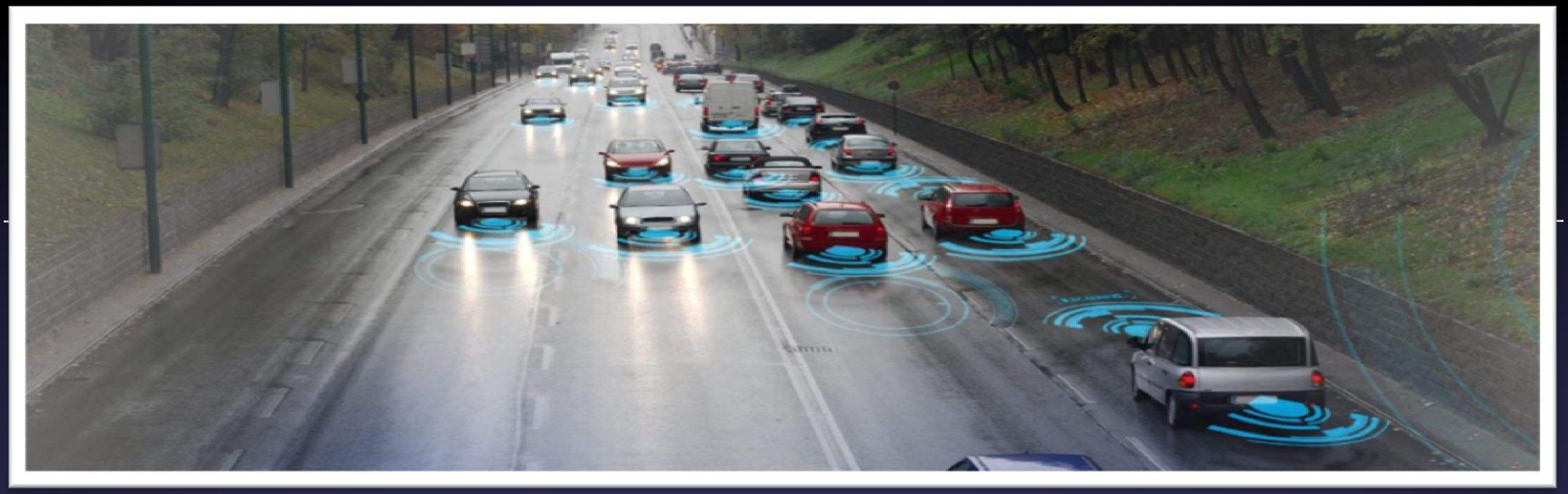
车联网介绍

★传统车联网：车辆信息的提取与利用。

★现代车联网：车辆智能化控制、智能交通、智能信息服务。

智能汽车趋势

智能汽车的趋势如何？



汽车不可缺少性

- 汽车已经成为人们生活中不可缺少的交通工具
- 传统机车的概念渐渐被模糊化，人们开始重视汽车的智能、交互、便捷性

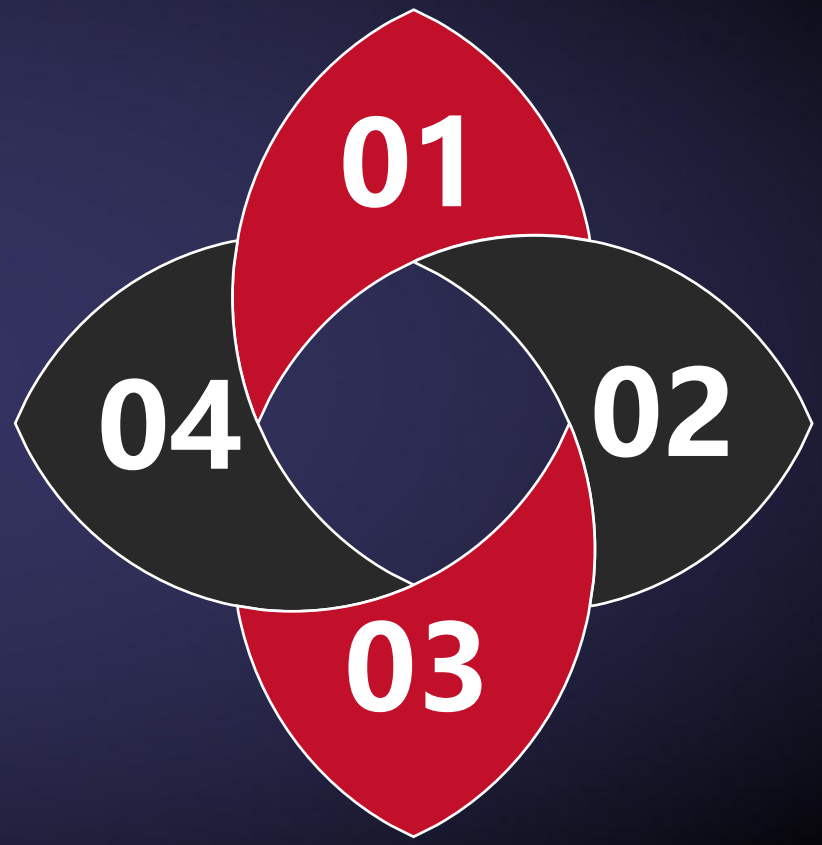
互联网公司的选择

- 百度、谷歌、腾讯等大型互联网公司开始进军车联网
- 百度、谷歌无人驾驶

汽车厂商的重视

- 厂商对自产车辆添加更多智能化服务产品
- 针对自产车辆研发相对应APP辅助功能

目录



车联网的边界定义

车联网边界定义

❑ 成功的攻击

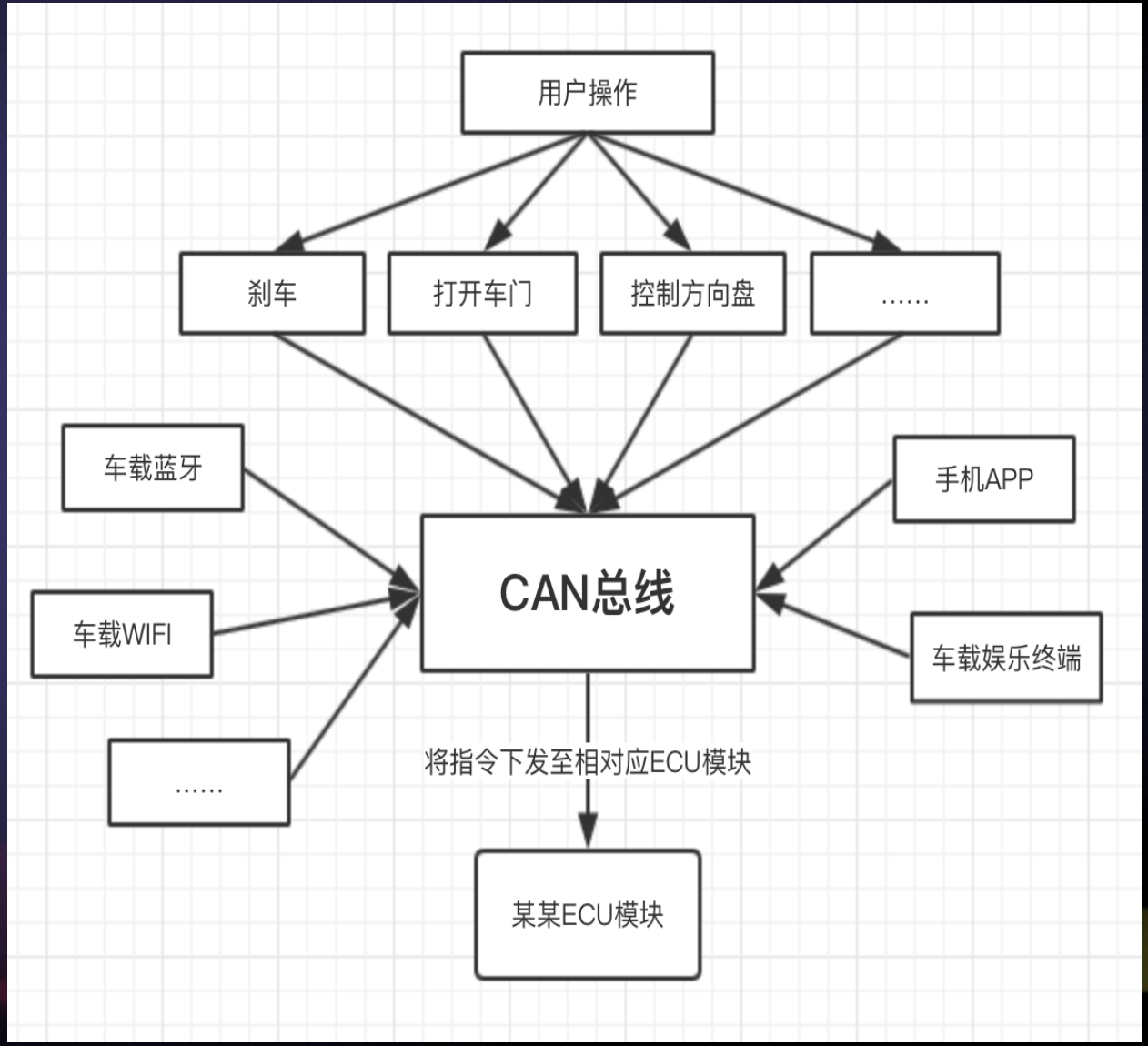
• 达到控制车内刹车、车窗、车门等模块功能，

我们视其为成功的攻击

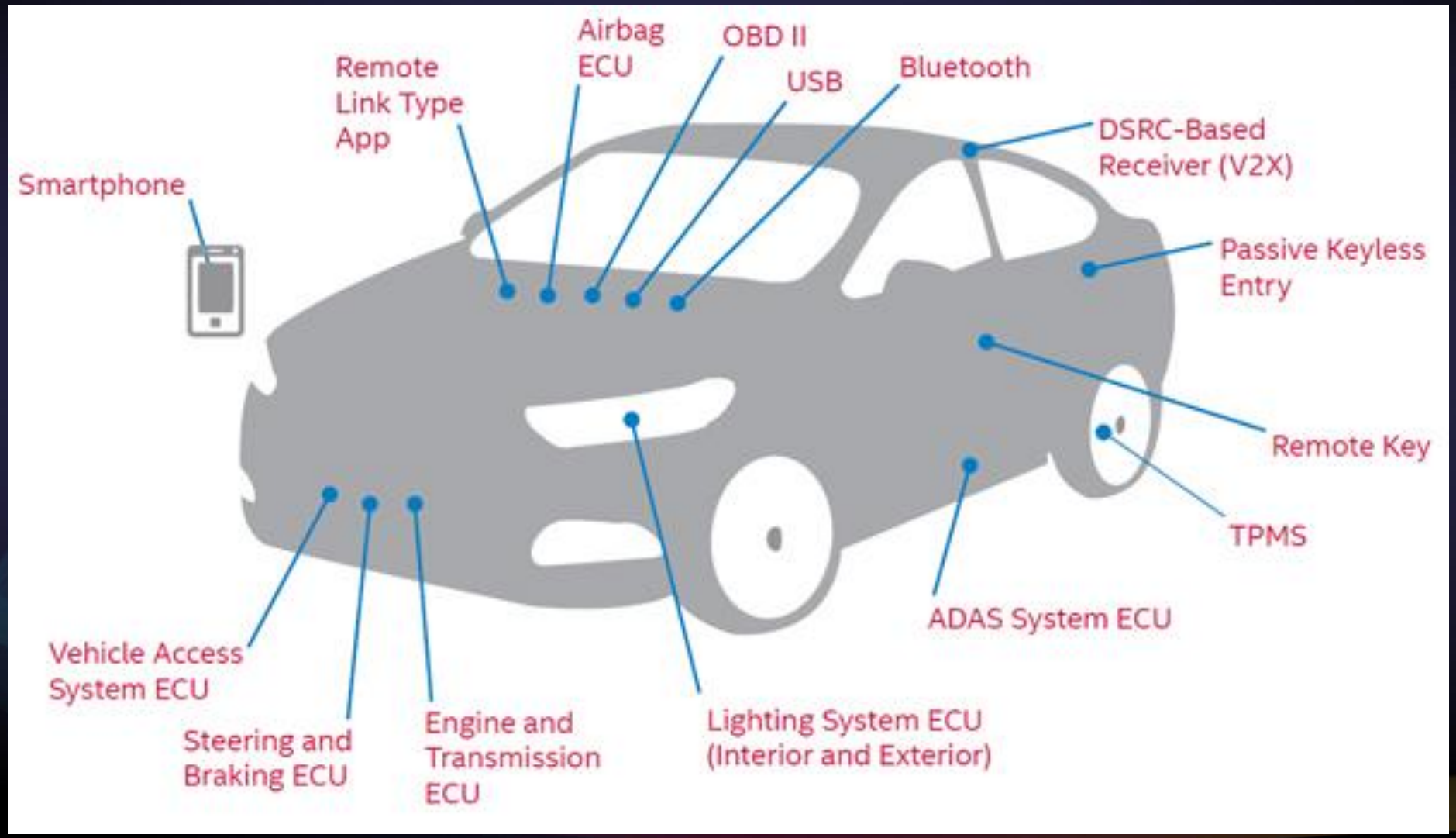
❑ 边界中心点

•为保证CAN总线安全，凡是最终接入CAN总线的

模块均处于边界范围内



车联网边界总览


Airbag ECU
OBD II
Remote Link Type App
USB
Bluetooth
DSRC-Based Receiver (V2X)
Smartphone
Passive Keyless Entry
Remote Key
TPMS
ADAS System ECU
Vehicle Access System ECU
Steering and Braking ECU
Engine and Transmission ECU
Lighting System ECU (Interior and Exterior)

车联网边界安全

蓝牙 *边界安全*

传统用途

- 方便接听、拨打电话
- 播放手机音乐

现代用途

- 方便接听、拨打电话
- 播放手机音乐
- 连接手机，通过指定APP对车载模块进行控制

边界安全

- 蓝牙开车门功能需要连接动力CAN、舒适CAN两个CAN总线
- 大多蓝牙与车辆内部网络通信处于同一个网络内

车载WIFI *边界安全*

边界安全

- 车载WIFI与车辆内部网络通信处于同一个网络内
- 通过车载WIFI可向CAN总线内发送伪造、虚假命令

汽车钥匙 *边界安全*

传统用途

- 开车门
- 钥匙功能键支持开后备箱、天窗等

边界安全

- 使用车钥匙执行功能时，信号被录下进行重放攻击
- 车钥匙滚码算法出现安全漏洞

车联网边界安全之——云端

OEM服务

1、诸多智能汽车在出厂后带有实时天气信息、前方路况、车辆定位等服务。

2、这些服务均为汽车生产商或服务商为其提供，车辆出厂后嵌入车载本身。增加用户体验度等众多因素。

手机APP

1、手机APP越来越流行，这些应用可以帮助用户通过手机定位车辆位置、追踪汽车等常见功能。

2、而部分APP甚至支持远程锁车、远程启动发动机、远程打开一些辅助设备等等，像一些受欢迎的汽车品牌动辄就有超过上百万用户。

供应商网络

1、供应商网络是类似一个中转平台。用户由汽车将上传的数据、执行的命令上传至供应商提供的网络（如国内的移动、电信等），然后在由供应商转发数据给OEM厂商、服务商。

2、一旦供应商出现问题，那么将可产生远程控制汽车执行危险动作等。

供应商网络

1、著名2015年的Jeep被远程攻破就是这样的原因，供应商网络被攻破，导致攻击者可以局域网内横向移动，根据车辆唯一特征码定位车辆，远程下发危险指令。

车联网边界安全之——组件安全

ECU

1、ECU一般被称为“行车电脑”、“车载电脑”等。

2、ECU会将执行由CAN总线发送过来的指令，如关闭引擎或开启引擎,关车门开车门等等。

3、ECU为最后一层防御，如果本身没有对执行命令进行合法性效验，则不能达到有效安全性。

CAN总线

1、CAN总线是用来与ECU进行通讯的，例如刹车、发动机、开车门等。

2、CAN自判断命令执行模块如果是开启发动机的，就传给发动机的ECU来进行处理。

3、CAN总线使用多数厂商的私有协议，如果CAN数据未加密，一旦被破解，攻击者则可以根据相关私有协议，伪造下发虚假命令。

OBD接口

1、OBD接口本来是用于车载诊断使用的，可以有效返回出当前车辆油量损耗、汽车尾气排放等情况。

2、研究发现，大量OBD接口直接连接到CAN总线而且可以向CAN总线发送数据。这表示一旦控制OBD接口，也就可以向ECU内发布危险指令。

车联网边界安全之——组件安全

娱乐系统

1、很多智能汽车现在都有一套娱乐系统，大多数采用嵌入式Linux、QNX、Android。

2、由于娱乐系统的代码量、系统复杂度高，从而经常存在安全漏洞。

3、因为娱乐系统默认也是连接到CAN总线的，所以一旦娱乐系统被恶意软件、攻击者接管，那么就可以向CAN总线发送任意伪造危险数据。

U盘等外置设备

1、如果U盘等外置设备经过修改，如BadUSB等，一旦U盘插入MP3音乐播放口，即可执行恶意操作。

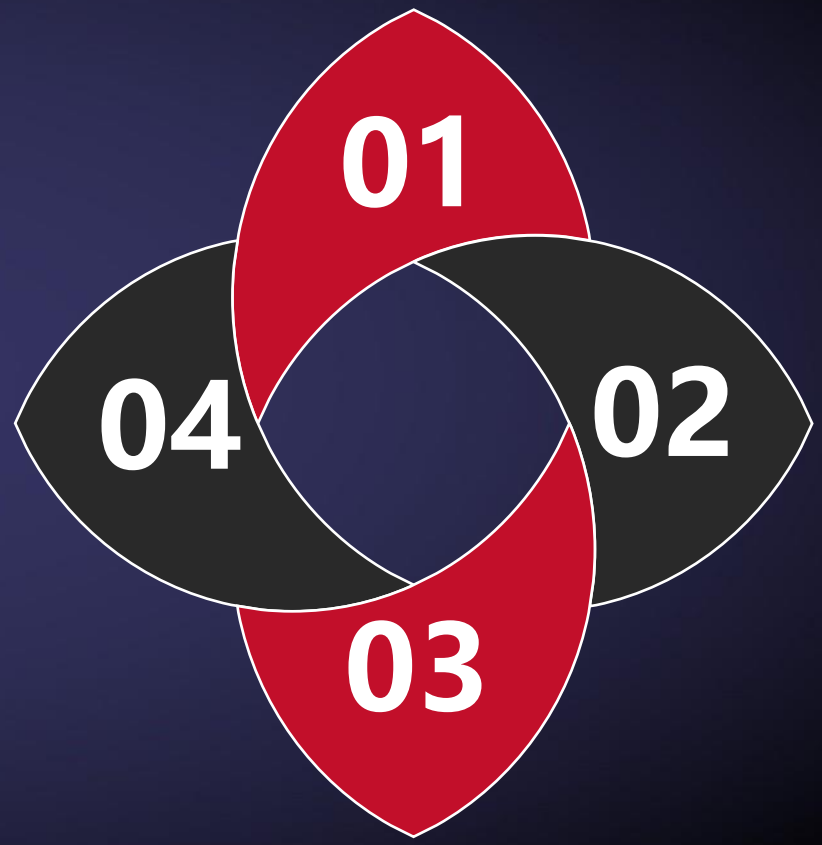
2、一旦接管了娱乐终端，其接下来步骤与上面相类似，接下将可以攻击CAN总线等高危险操作。

不明应用程序

1、配备了车载电脑的汽车可以执行安装或下载应用程序，不明应用程序嵌入恶意代码

2、攻击者可以将恶意代码假装成更新程序，通过这种方式使未授权的软件获取其所需的权限

目录



车辆体系架构

★网络划分和网段隔离

对不同的网段（例如车载WIFI、蓝牙、与APP通讯等）进行隔离划分区别，每个网网段不可互相接入，不必要的网络不要加入CAN总线接口。

★对流量进行安全分析与阻断

★在ECU、CAN总线添加相应网关、入侵检测等系统

车辆移动设备

1、车载移动设备是指手机、USB等外置设备，需要连接车载内部网络、车载终端。

2、建议针对每个设备进行相对的安全认证机制，确保设备的安全性，避免未经允许的设备连入汽车内部网络，造成安全隐患。

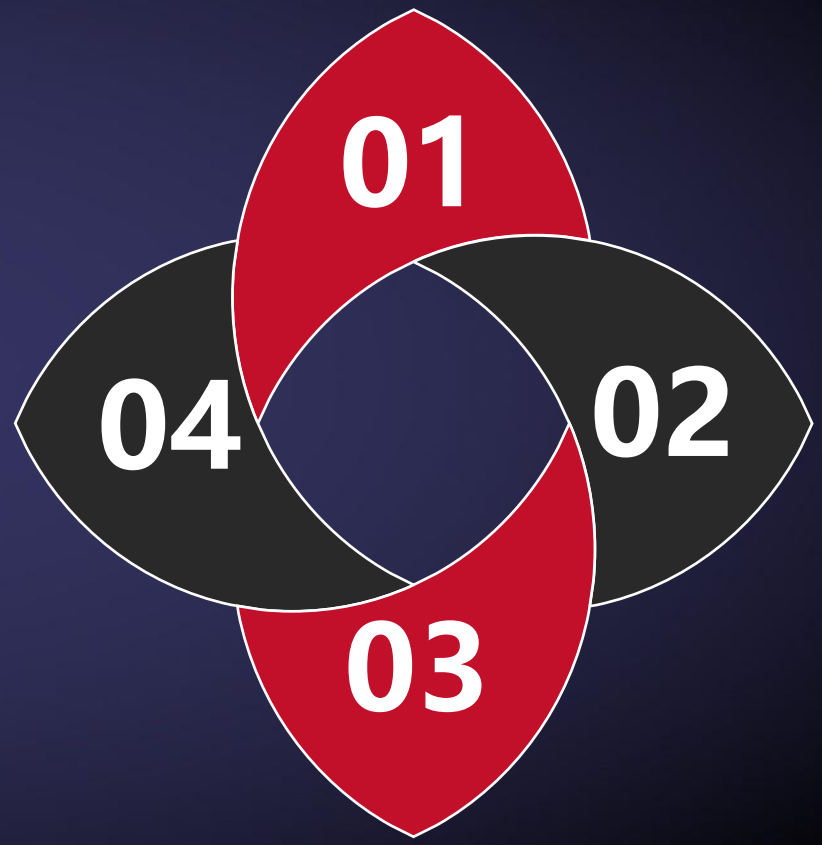
云端安全

1、在云端安全中，我们建议在车辆与云端进行通讯的过程中使用加密协议、VPN隧道等形式，确保传输安全。

2、云端设定指定信任IP访问。避免陌生IP进行访问遭安全隐患。定期进行系统代码内部安全审计。

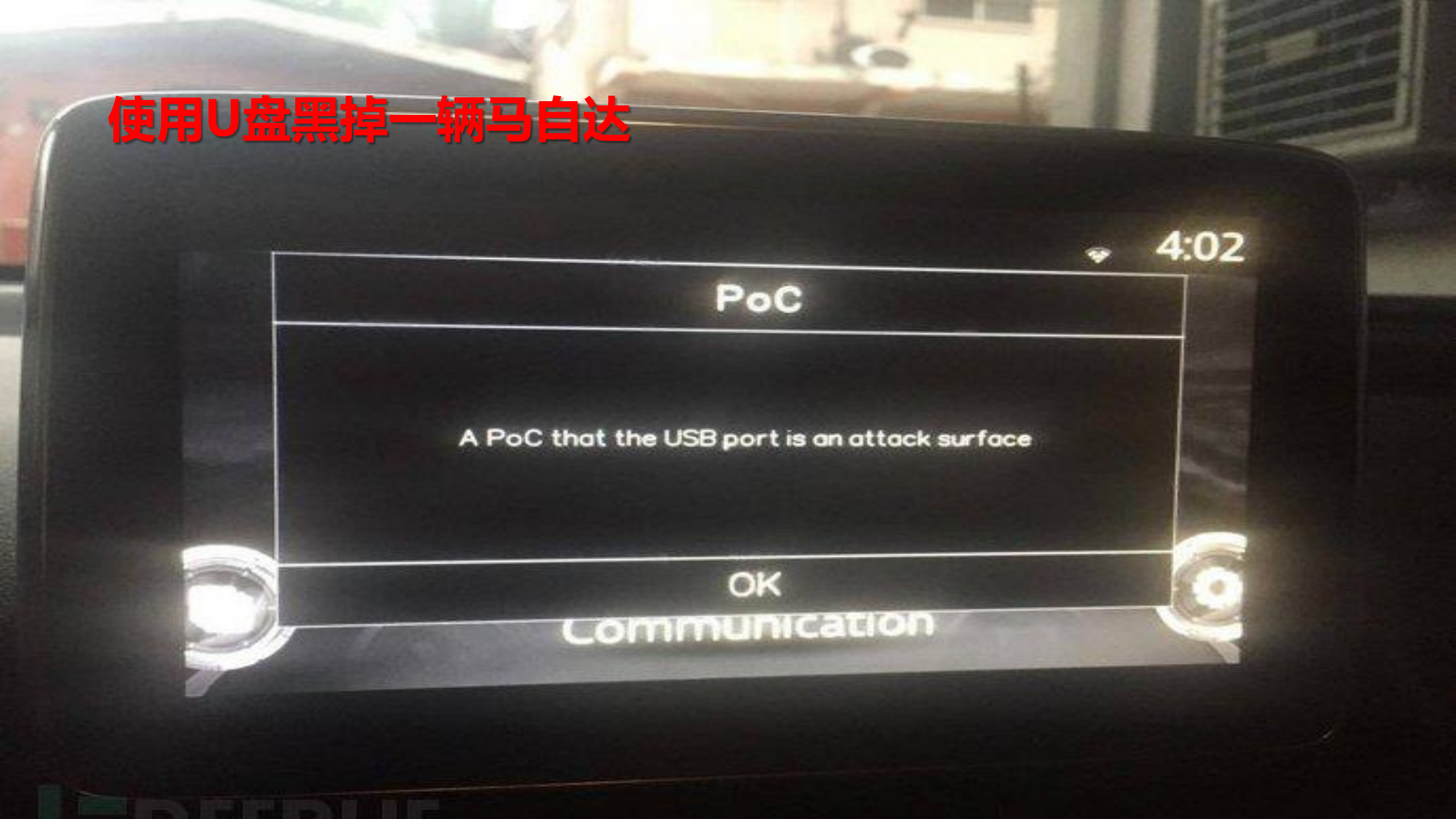
3、严格把控边界数据库、测试使用等服务器，不要将其暴露在外网环境。

目录

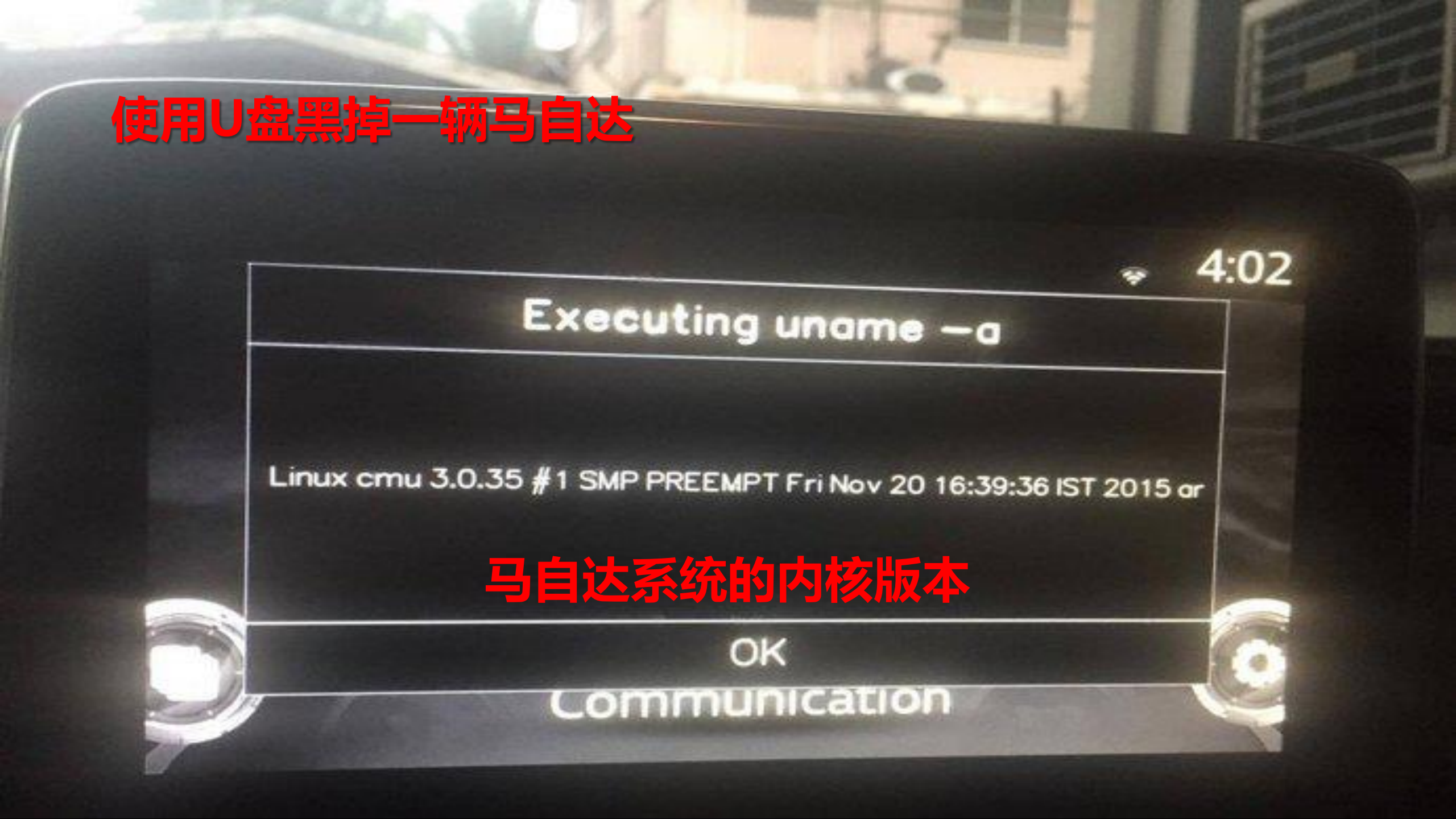


使用U盘黑掉一辆马自达

使用U盘黑掉一辆马自达



使用U盘黑掉一辆马自达



马自达系统的内核版本

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You