# 车联网安全体系防护策略及建议方案

绿盟科技
资深架构师 程紫尧

2017.12.20

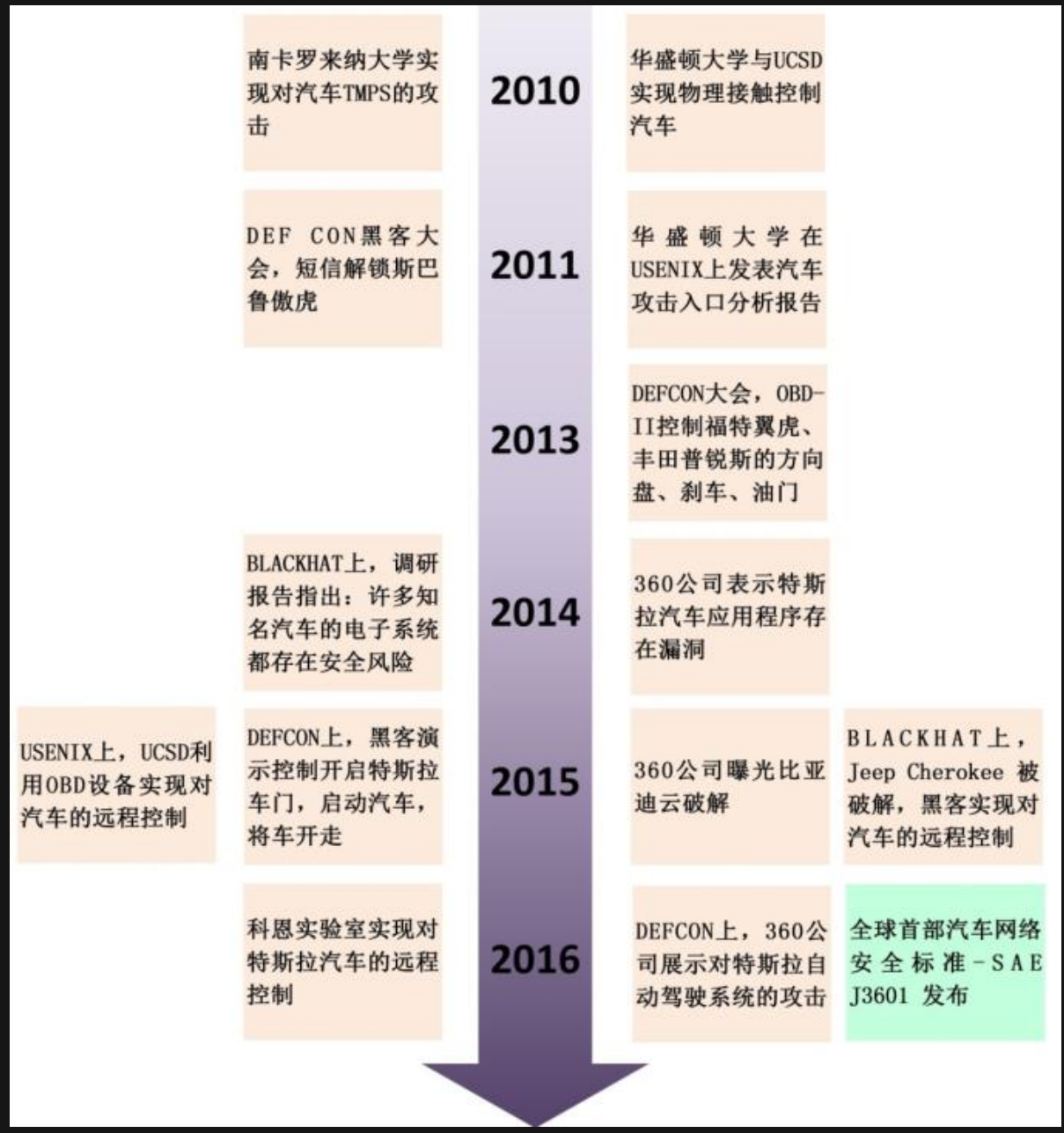
NSFOCUS

# 01

# 车联网安全体系

# 车联网安全事件

随着汽车产业正在不断的发展，增加更多的便利和个性化的驾驶体验的能力特点。
消费者希望**不断地加以连接**，这是推动汽车制造商增加车辆和个人设备之间进行更多的整合，如智能手机等。以前，汽车是孤立的，物理隔离的，因此黑客很难远程入侵汽车内部控制器，除非进行物理入侵，而这个是需要很高的犯罪成本。
随着互联网的进化，当**TSP通过T-Box 与汽车内部网络联网**之后，汽车受到的远程网络攻击就不再是猜想。



# 车联网安全事件频发原因

**传统汽车驾驶**

L0：完成人类驾驶

L1：辅助驾驶

**互联汽车驾驶**

L2：部分自动驾驶

L3：有条件自动驾驶

L4：高度自动驾驶

L5：完全自动驾驶

**高度、完全自动驾驶**

## 智能化

**更多软件代码**

- 最新汽车上至少100台车载电脑，运行6000万行代码
- 无人驾驶2亿行以上

**更多漏洞BUG**

- CNNVD发布近3年漏洞数量每年20%以上的增长，全球态势更加严峻
- 企业纷纷推出漏洞收集与响应平台
- 厂商定期发布修复补丁：MS、Google

## 网联化

**更多接入途径**

- T-BOX、IVI、OBD、USB、USB、充电接口、GPS、摄像头
- 汽车中使用的计算和联网系统沿袭了既有的计算和联网架构，也继承了这些系统天然的安全缺陷

**更大攻击面**

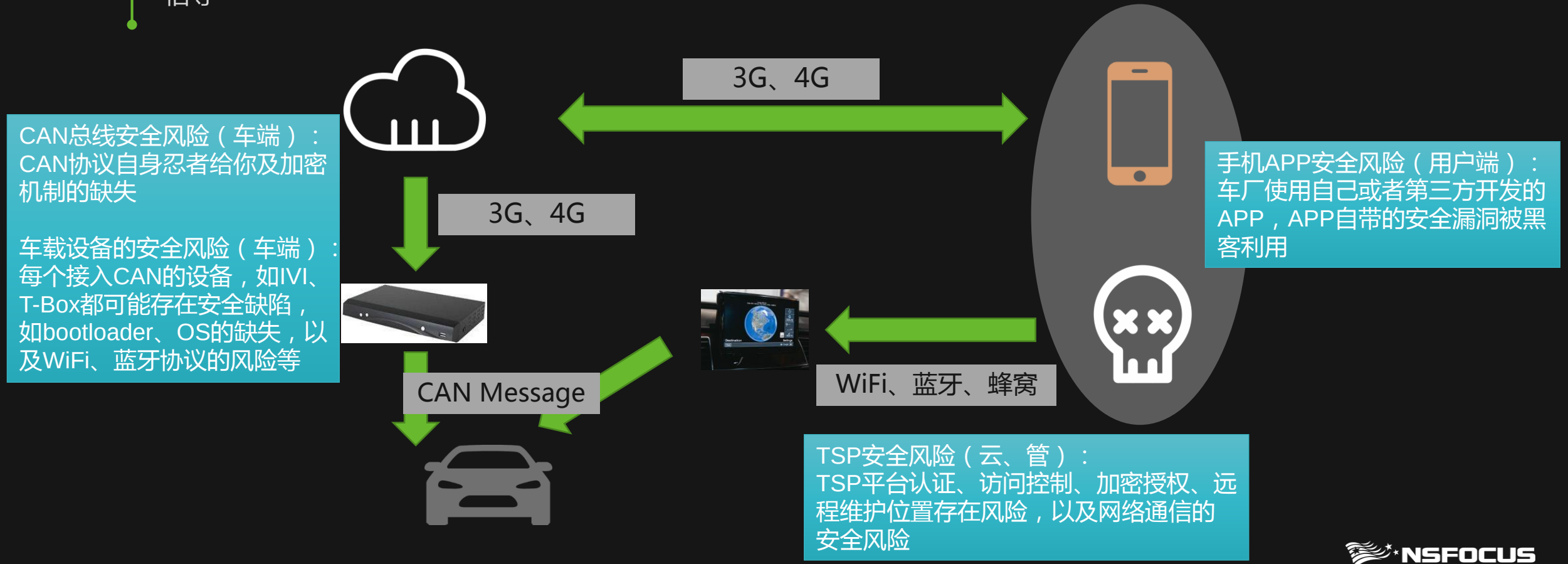
- 直接攻击：破坏安全功能、传动系统、安全控制件、动力、转向、制动、仪表等
- 便携设备攻击：车载APP、OBD接口、导航设备、娱乐信息设备等
- 无线攻击：智能钥匙、TPMS系统、V2X通信设备、WIFI、蓝牙、Telematics等

NSFOCUS

# 车联网安全体系——云、管、端

对于车联网安全体系的理解有助于快速找到安全的切入点。车联网体系结构通常认为有3个层面，包括：云侧、管侧和端侧。

云侧实现后台大数据分析和车辆特定服务；管侧提供通信连接管道；端侧实现车辆控制、车辆对周边环境的感知和通信等



02

# 车联网安全建议方案

# 云端安全


| | |
|---|---|
| 应用安全 | SDLC，敏感文件保护，漏洞检测，应用防护，交易安全 |
| 信息安全 | DLP，数据库活动监控，加密，APT攻击检测，恶意行为分析，攻击溯源 |
| 安全管理 | 病毒/漏洞管理，补丁管理，配置管理，身份识别与访问管理，组织管理 |
| 网络安全 | 部署防护设备（IPS，NF，Anti-DOS），QOS |
| 可信计算 | 可信软件，可信硬件以及接口，可信接入与数据传输 |
| 计算存储 | 安全加固，HA，访问控制，恶意代码防护，日志，完整性管理 |
| 物理安全 | 物理访问控制，物理状态监控，安全值守 |

预测　防御　检测　修复

NSFOCUS

# 通信安全


加密通讯

数据中增加随机因子签名认证

接入设备和接入系统安全认证

服务质量保障

# 车端安全


## 概念阶段

- 汽车材料安全
- 芯片及其系统安全
- 功能风险面评估
- 环境对车辆的影响
- 无线信号干扰容错

## 设计阶段

- 防撞工程设计
- 芯片及其系统安全
- 分级安全管理
- 安全隔离设计
- 异常状态、行为检测上报
- 可信认证
- FOTA可信升级
- 通讯协议完整性设计
- 加解密算法复杂度分析
- 核心器件物理安全
- 设计安全标准

## 实施阶段

- 安全编码规范
- 代码安全评估
- 系统软件安全评估
- APP代码加固
- 核心数据加密存储
- APP软件可信认证
- 畸形数据的容错处理
- CAN总线实现符合AutoSAR标准
- CAN总线数据干扰容错
- ECU硬件、固件、更新安全检测
- 防止固件逆向安全检测
- 证书固化在芯片中
- 校验算法由独立硬件完成

## 生产阶段

- 传感器失效模式验证与分析
- 对相关安全指标进行逐项测试

# 终端方案


核心数据加密存储

接入口令复杂化和随机化，阻止暴力破解

数据校验与认证，阻止数据包重放攻击

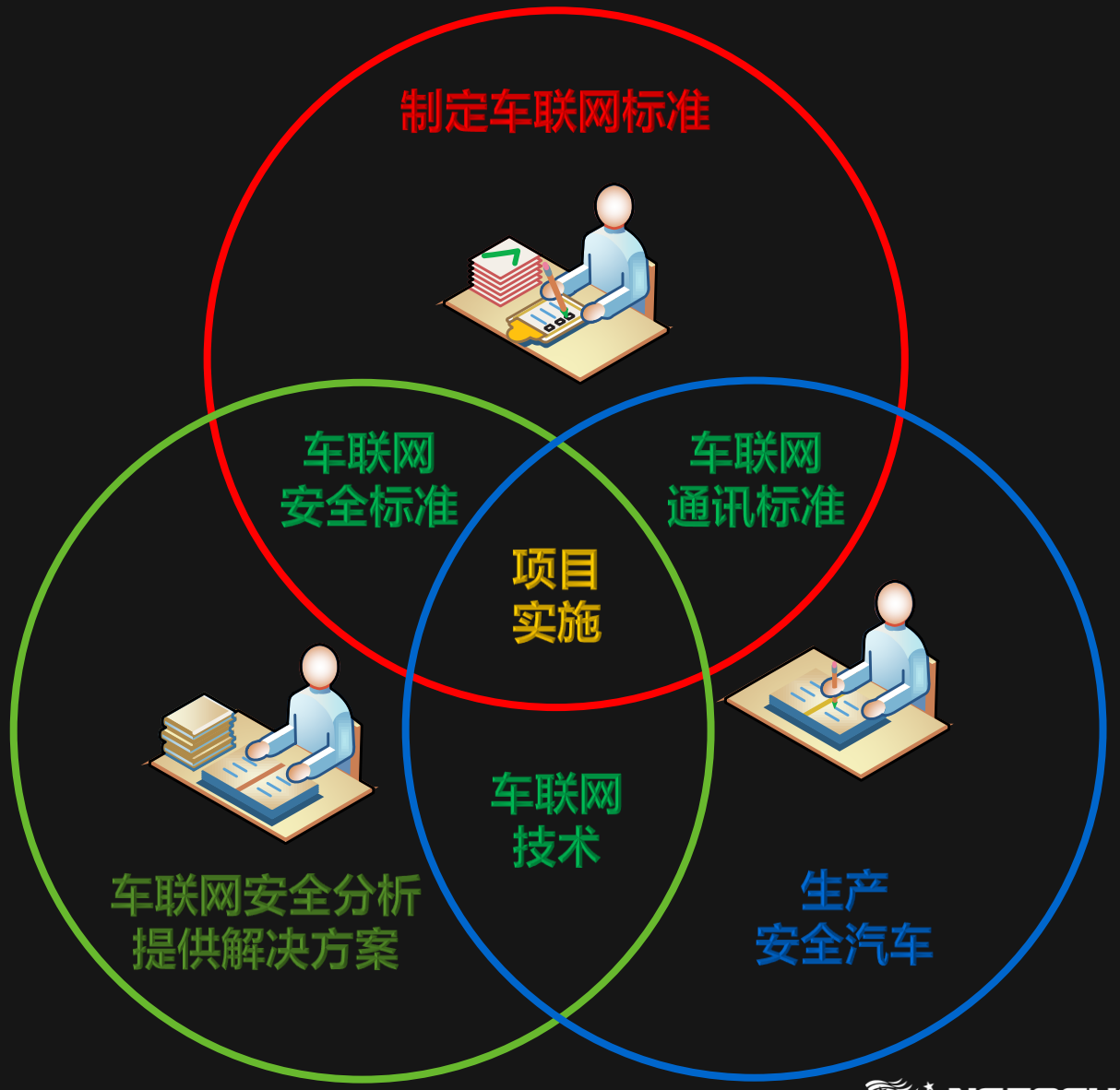
App代码加固以及通讯数据加密与签名认证

内置防护系统

及时更新系统和软件

# 总结


业务
分析
data


制定车联网标准
车联网
安全标准
车联网
通讯标准
项目
实施
车联网
技术
车联网安全分析
提供解决方案
生产
安全汽车

# 谢谢！

NSFOCUS