
Tencent 腾讯 | 腾讯安全
CSS
互联网安全领袖峰会
Cyber Security Summit
智能网联时代，重新定义汽车安全
吕一平 | 腾讯科恩实验室

未来智能网联汽车“安全” = 功能安全 + 信息安全

大量新技术和网联功能引入，智能网联信息安全不容忽视

环境感知层
激光雷达、毫米波雷达、摄像头、传感器、红外测距、卫星导航、路侧系统等

数据采集层

信息融合层
行人障碍物识别、车辆识别、场景重构、精准定位等

智能决策层
路径规划、人机共驾等

控制执行层
自动驾驶、无人驾驶、轨迹跟踪、转向制动、耦合动力学全状态参数识别等

安全体系
功能安全（Functional Safety)和信息安全（Cyber Security)

智能控制系统架构
通讯架构和控制架构

整车集成与标定
整车硬件集成（底盘、车身、电机、电池系统等）和智能控制系统集成

测试
模块性能测试（测试机理）和整车功能测试（测试方法）

信息安全对智能网联汽车功能安全的重大影响

2015年7月，黑客可以通过远程方式入侵克莱斯勒自由光JEEP并对行车和车身进行远程控制，其中涉及了多个TSP模块、互联网通讯模块、车机模块中多个安全漏洞。
影响：克莱斯勒召回北美地区140万辆自由光

2015年7月，黑客实现对美国通用OnStar移动APP的劫持，可以远程控制车门开关、发动机启动和鸣号。主要涉及移动APP模块和TSP模块的安全漏洞。
影响：通用紧急修复相关漏洞

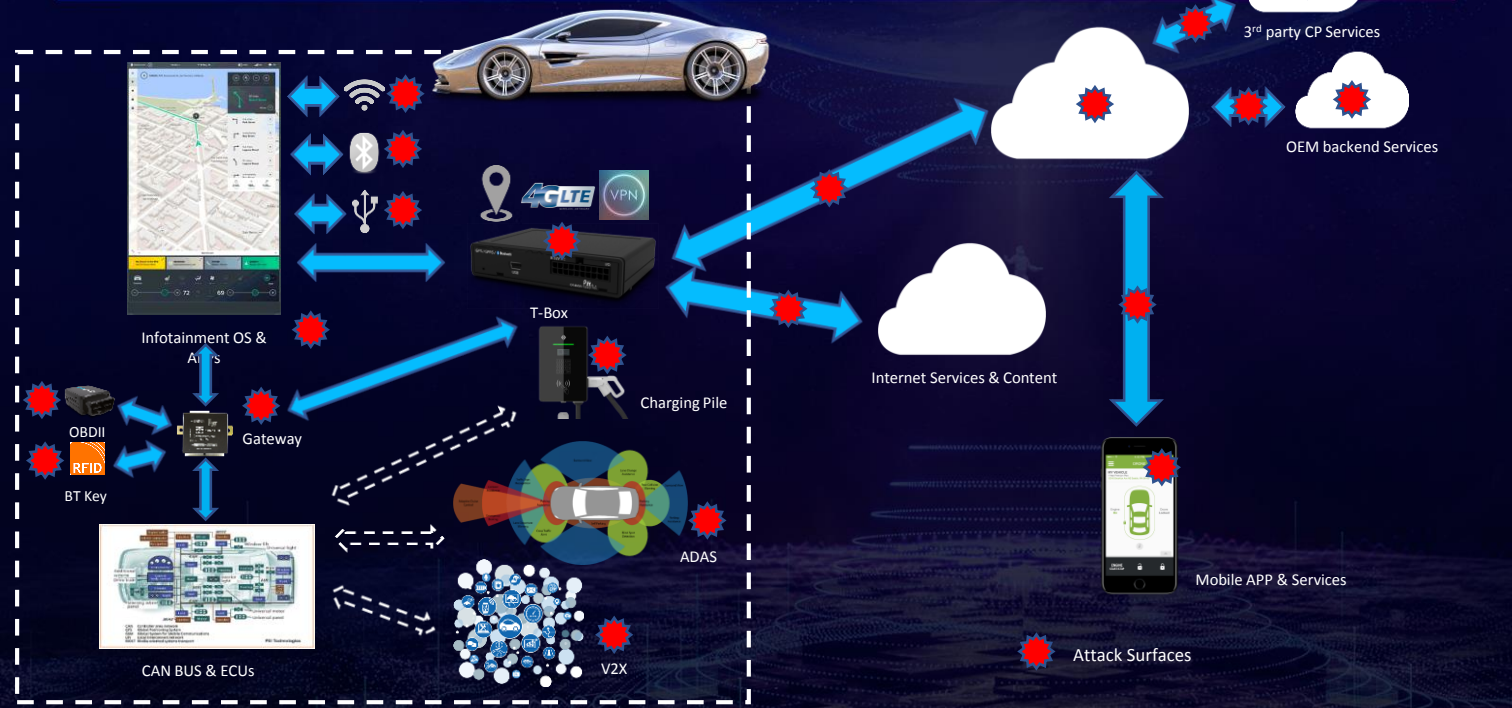
2016年2月，黑客实现对尼桑EV LEAF移动APP的劫持，可以远程控制空调开关，闪灯等。主要涉及移动APP模块和TSP模块的安全漏洞。
影响：尼桑临时关闭LEAF云端服务

2016年9月，腾讯科恩实验室实现对特斯拉Model S无物理接触远程攻击，可以对车辆在驻车状态和行车状态进行无用户授权的远程控制。主要涉及车载浏览器、车载系统、车载网关、车电网络和ECU等多个模块的安全漏洞。
影响：特斯拉在接收漏洞报告后，启动紧急修复，完成了对多个模块的漏洞修复。

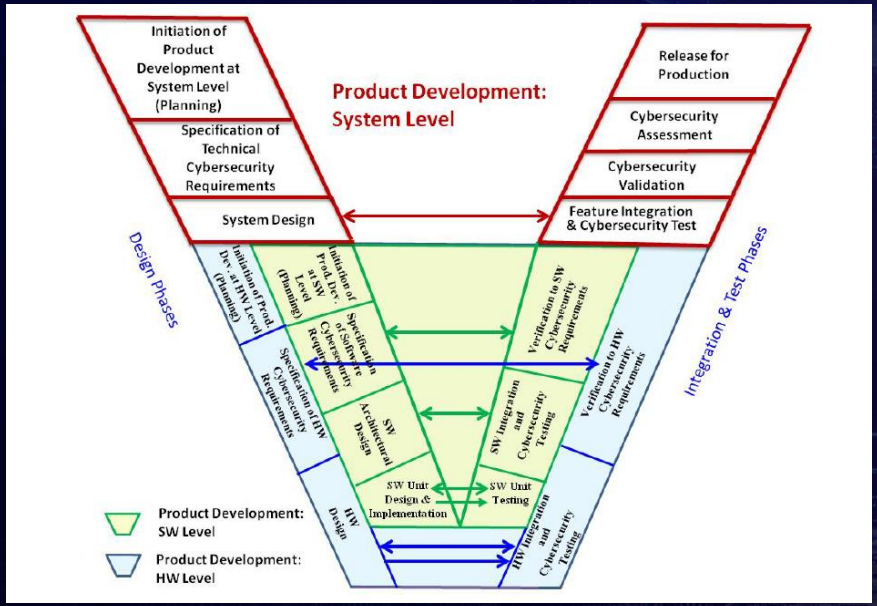
2017年7月，腾讯科恩实验室再次实现对特斯拉Model X无物理接触远程攻击。
影响：特斯拉在接收漏洞报告后，启动紧急修复，完成了对多个模块的漏洞修复。

2018年5月，腾讯科恩实验室实现对宝马系列车型无物理接触远程攻击。
影响：宝马集团在收到漏洞报告后，紧急启动全球范围内的车辆漏洞修复。

2019年3月，腾讯科恩实验室发布全球第一个面向高级辅助驾驶量产车型，Model S Autopilot的安全研究成果。验证了自动驾驶视觉技术带来新的攻击面。


3rd party CP Services
OEM backend Services
Infotainment OS & Apps
4G LTE
VPN
T-Box
Charging Pile
Internet Services & Content
OBDII
RFID
BT Key
Gateway
ADAS
Mobile APP & Services
CAN BUS & ECUs
V2X
Attack Surfaces

智能网联安全的两个层面：技术架构设计与实现



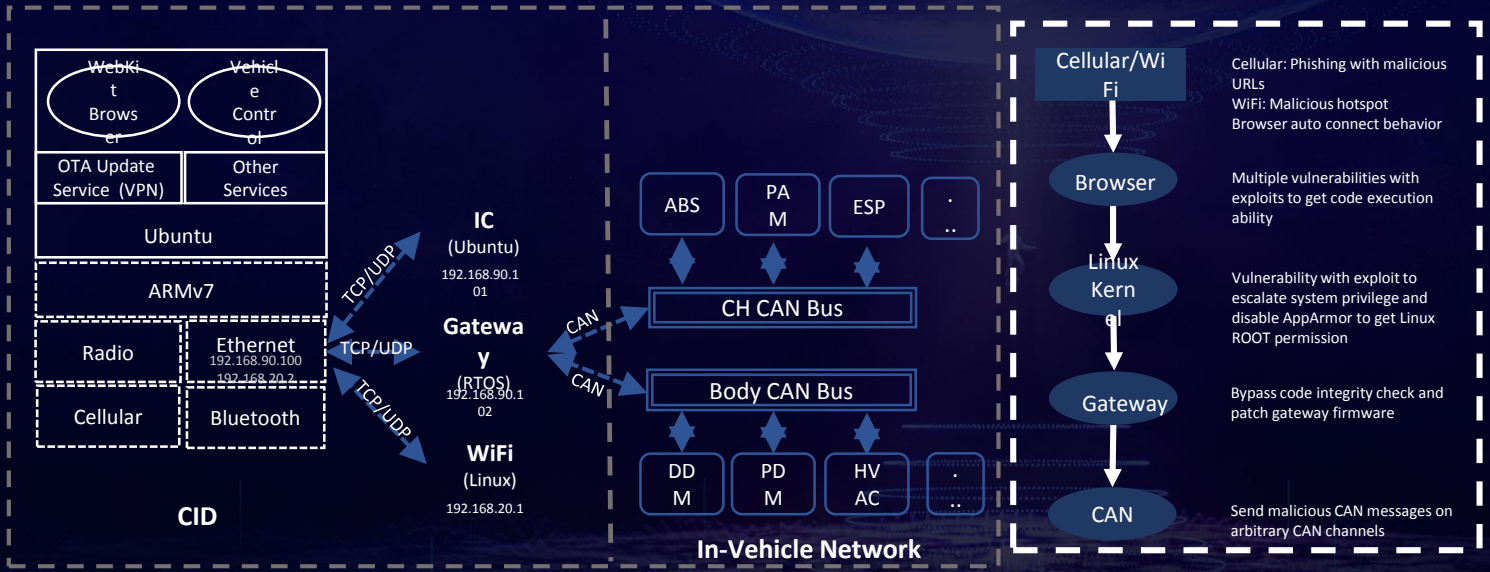
45%

技术架构设计安全FLAW

55%

技术架构代码实现中的安全BUG

腾讯科恩网联安全研究案例一：特斯拉研究2016 & 2017



特斯拉研究获得特斯拉高度认可

Tesla Security Researcher Hall of Fame

Tesla appreciates and wants to recognize the contributions of security researchers. If you are the first researcher to report a confirmed vulnerability, we will list your name in our Hall of Fame (unless you would prefer to remain anonymous). You may also be considered for an award if you are the first researcher to report one of the top 3 confirmed vulnerabilities in a calendar quarter. You must comply with our Responsible Disclosure Guidelines (above) to be considered for our Hall of Fame and top 3 awards.

2017	Keen Security Lab	Tencent
2016	Keen Security Lab	Tencent

特斯拉有史以来最高安全研究奖励

Keen Security Lab of Tencent
Tower A

Dear Keen Security Lab of Tencent,

Tesla greatly values the research of the security community. We especially appreciate when researchers help us improve the safety and security of our products. Your recent Tesla research has led to valuable improvements to the security of our vehicles.

We have enclosed Tesla security challenge coins as a token of our appreciation.

Sincerely,

Elon Musk
CEO, Tesla, Inc.

TESLA

腾讯科恩网联安全研究案例二：宝马系列车型研究2018

Software Defined
Radio Platform

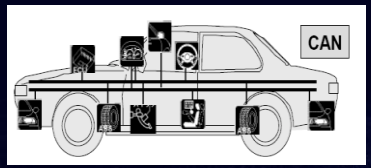
1

Simulated GSM Network

2

BMW Car

3



CAN Network

5

Central Gateway

4

T-Box

宝马研究获得宝马集团高度认可

“宝马集团认为，此项研究是迄今为止由第三方机构对宝马集团车辆进行的最全面、最复杂的测试。”

- BMW Group Press Release, May 22nd , 2018

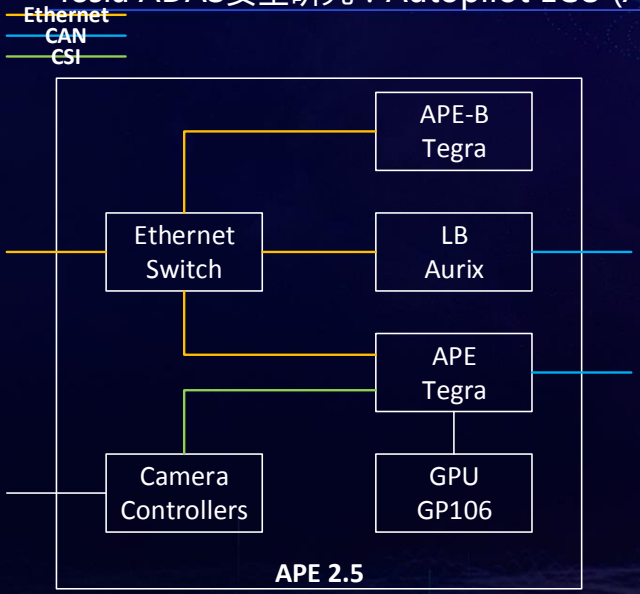
宝马研究获得宝马集团大奖

全球首个“宝马集团数字化及IT研发技术奖”以表彰腾讯科恩实验室在促进汽车安全领域所进行的杰出研究。

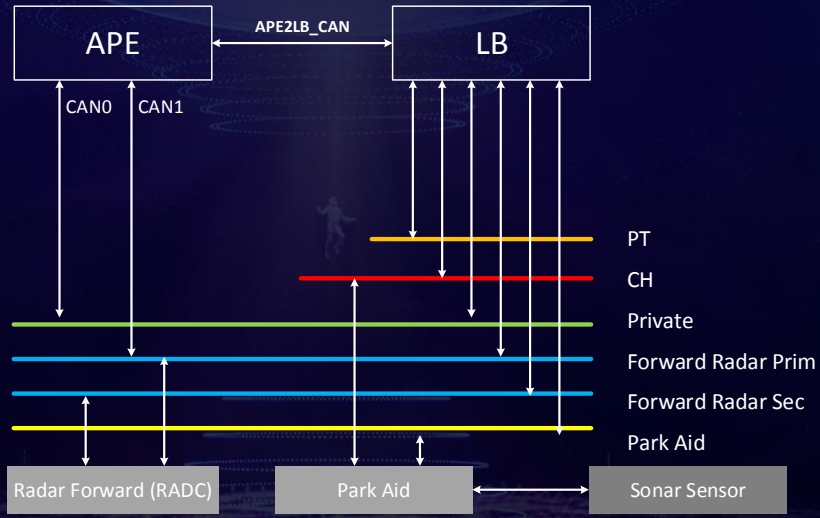
马斯克：阻止黑客对特斯拉的入侵是首要安全任务(2017.7)

“在原则上，如果有人声称自己入侵了所有特斯拉自动驾驶汽车，那么他们可以威胁‘将所有人都送到罗德岛州’，这将是特斯拉的噩梦，而罗德岛州将会聚集很多愤怒的车主。”

Tesla ADAS安全研究：Autopilot ECU (APE) 架构概览

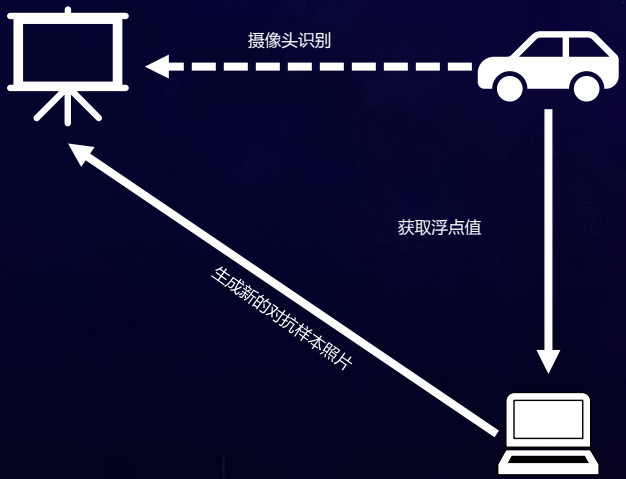


APE架构概览



APE CAN 总线图

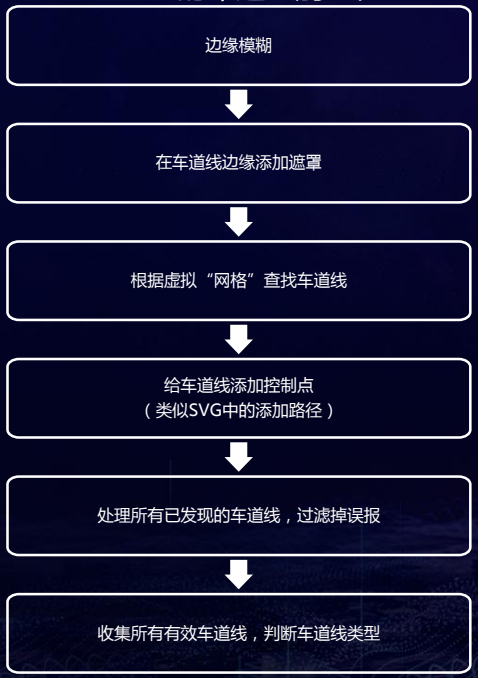
Tesla ADAS安全研究：雨刷的视觉识别缺陷



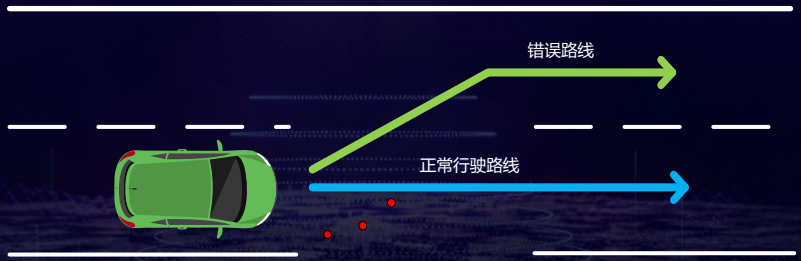
端到端（End to End）对抗样本生成

Tesla ADAS安全研究：车道的视觉识别缺陷

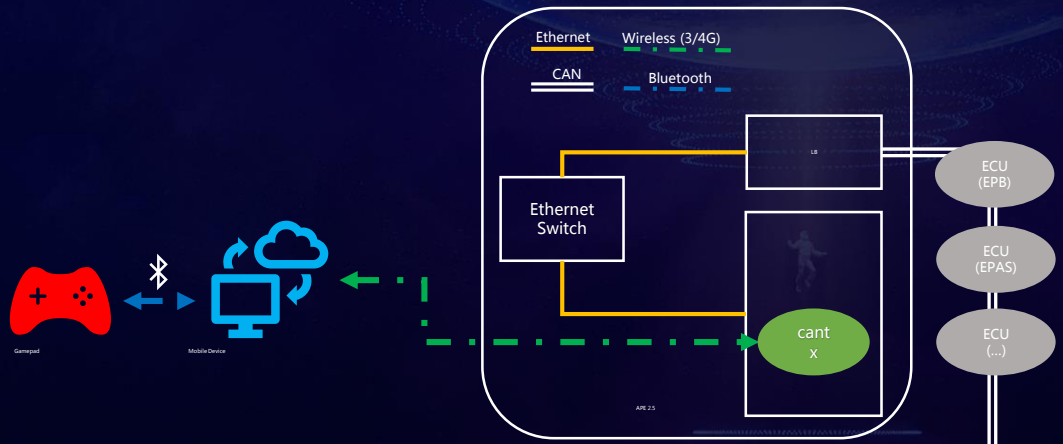
APE的车道识别过程



在路面部署干扰信息后，可导致车辆经过时对车道线做出错误判断，致使车辆驶入反向车道。



Tesla ADAS安全研究：远程控制车辆转向系统



利用已知漏洞在特斯拉Model S（版本2018.6.1）获取Autopilot控制权之后，科恩实验室通过实验证明，即使Autopilot系统没有被车主主动开启，也可以利用Autopilot功能实现通过游戏手柄对车辆行驶方向进行操控。

信息安全将成为汽车品牌的重要能力

	FCA (2015)	Tesla (2016)	BMW (2018)
首次安全响应时间	1周+	1.5小时	3小时
确认安全问题速度	1月+	1天	2周
安全问题修复速度（包括Tie-1供应商模块）	3月+	10天	3月+
修复推送周期/修复百分比	6个月/50%-	3天/90%+	2.5月/70%+
是否需要召回？	召回	FOTA	OTA+常规保养升级
修复成本	4亿美金	常规升级成本	常规升级成本
对公司品牌影响	非常负面	中性	中性

信息安全将成为智能网联汽车产品的关键属性

功能安全

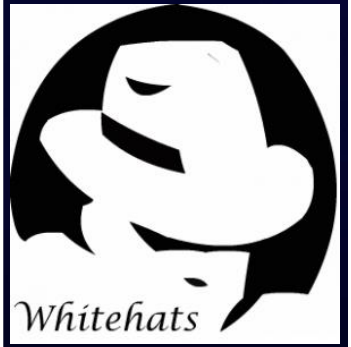
法律要求

增值业务

质量和品牌

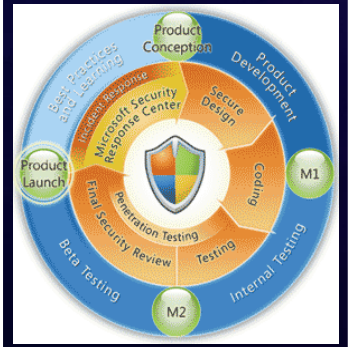
信息安全将会成为汽车行业的“国防”

专业安全团队



专业的人做专业的事
信息安全专家的引入

安全工程方法



问题尽可能多消灭在研发阶段
安全工程方法的引入

安全保护技术

做更坚固的盾，提高攻击成本
安全保护机制的引入

安全策略和流程

比攻击者更快
响应、修复、更新机制的引入

腾讯科恩，为智能网联产业升级

保驾护航

感谢聆听！
Thank You!

腾讯科恩实验室微信公众号