CAICT 泰尔终端实验室
中国信息通信研究院 China Telecommunication Technology Labs-Terminals

智能终端漏洞问题分析与检测

2017年11月

政府智库 行业平台

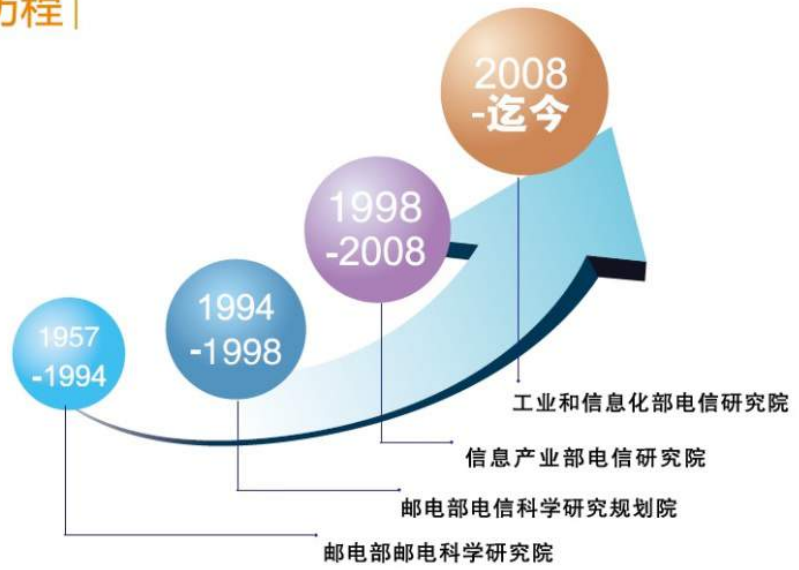
全国布局

电信研究院 （北京）
- 花园北路本部
- 阜成门驻地
- 月坛驻地
- 小西天驻地
- 大成广场驻地
- 翠湖驻地

南方分院 （深圳）
华东分院 （上海）
西部分院 （重庆）
智慧城市研究院 （广州）
抗震研究所 （保定）

发展战略、自主创新、产业政策、行业管理、规划设计、技术标准、测试认证

发展历程



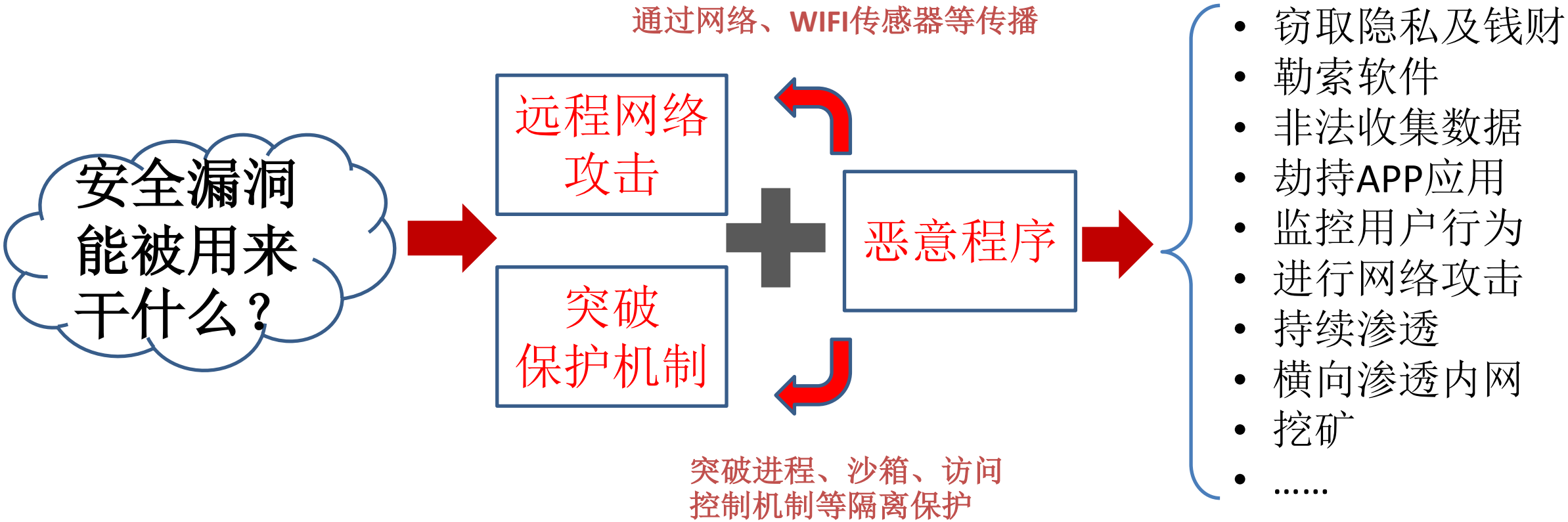
见证、参与了我国信息通信业由小到大、由弱渐强、比肩竞技、跨越发展的全过程

国内最大规模通信技术综合测试试验平台

集信息通信技术发展研究，信息通信产品标准、测试方法、通信计量标准、计量方法研究，以及国内外产品的测试、验证、技术评估、测试仪表计量以及通信软件的评估、验证为一体的高科技组织

目录

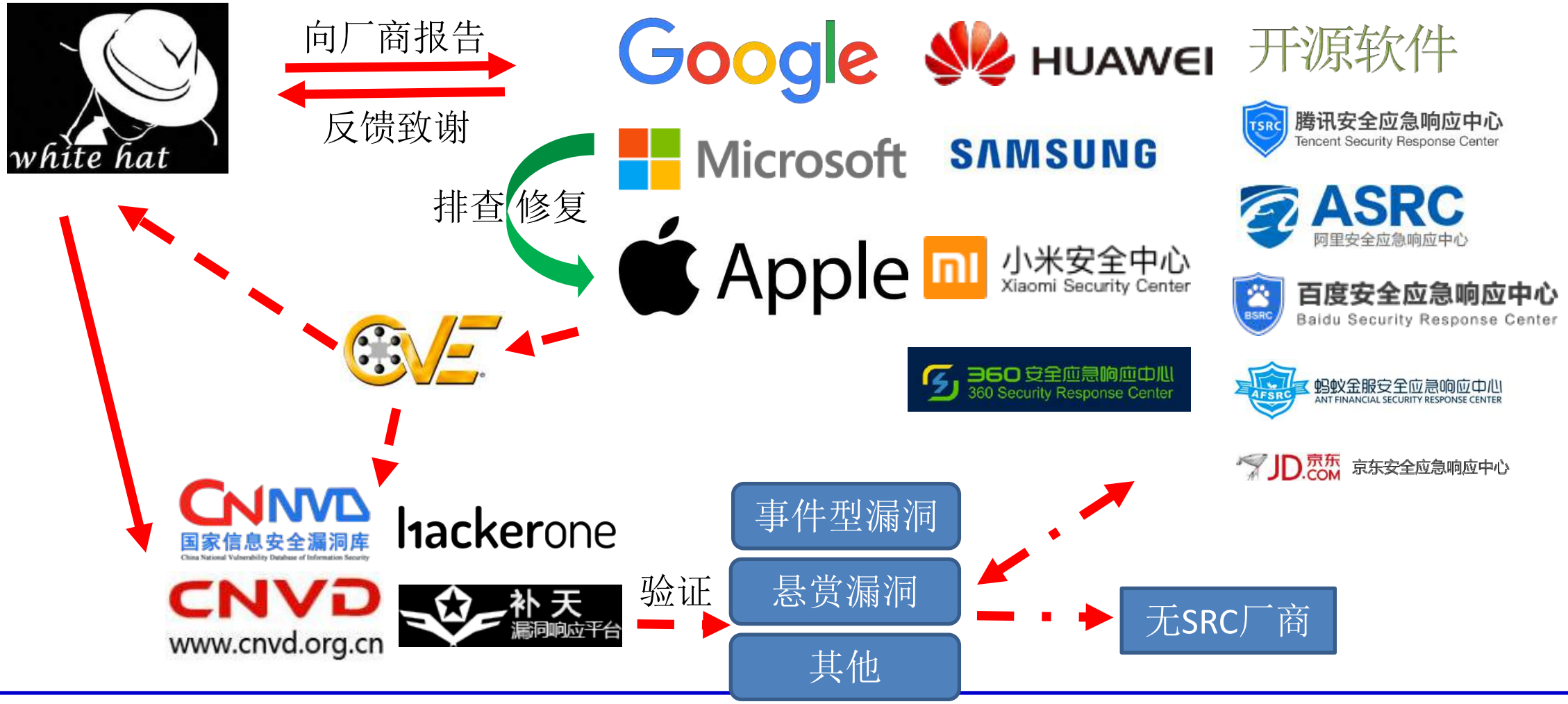
安全漏洞的危害



随着安全防护机制的逐渐增强，安全漏洞在攻击中的更显重要。

通用型漏洞报告与修复模式

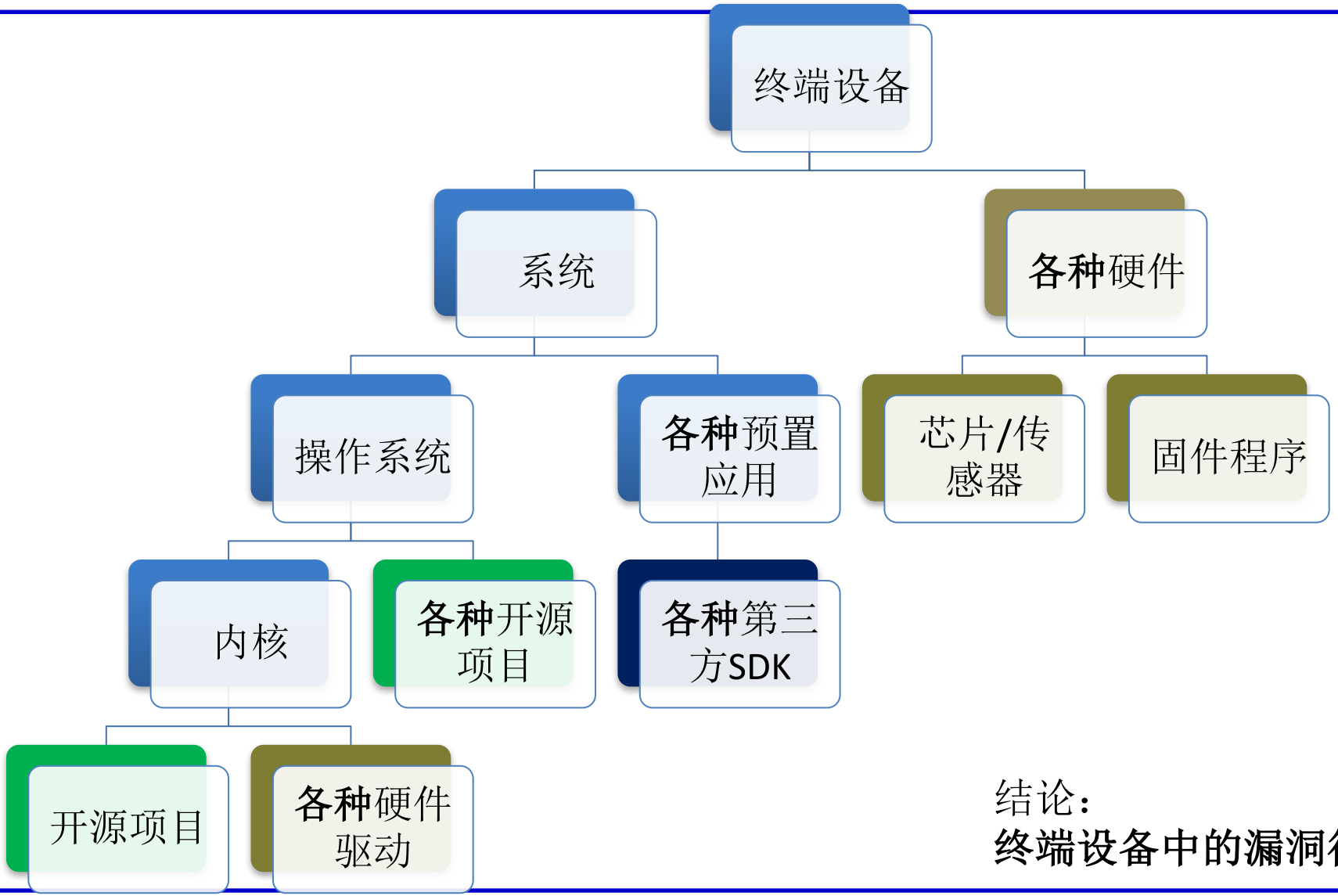
更普遍的漏洞与相关问题报告及修复模式



仍然面临的安全漏洞问题

- 提交给一个厂商的通用型安全漏洞是否影响供应链上的其他厂商
- 无安全应急响应中心厂商解决漏洞仍然困难
- 漏洞不一定容易修复
- 厂商能否认识漏洞的严重性
- 提交漏洞给第三方平台是否安全可信

移动智能终端供应链问题



特点：

- **复杂性：**终端设备，尤其是智能终端拥有庞大的供应链
- **同构性：**多款不同设备可能采用同一款底层供应链产品同
- **集成性：**与PC不同，一般移动智能终端布丁不能由供应商单独打

问题：

- **复杂性：**在复杂的设备中往往不能及时打上补丁
- **不及时性：**所有底层供应链的产品漏洞信息和布丁不能及时传递到所有上层节点
- **高权限：**供应链产品具有所在架构层级相同的权限和行为能力

结论：

终端设备中的漏洞往往不能及时消除，且危害很大

容易被低估的DirtyCow

- **漏洞分析**
  - 通过COW和madvise竞争触发的设计漏洞，满足特定时序不会产生副本内存页，直接写内存页。可通过mmap映射文件来写只读文件。
  - 很有特点，可以绕过几乎所有mitigation

- **Android端利用情况**
  - https://github.com/timwr/CVE-2016-5195
    - 写只读文件
    - 修改run-as实现root，不能改selinux domain或关闭selinux
  - https://github.com/hyln9/VIKIROOT
    - 通过vdso注入到其他进程，有一定局限性
    - 这种利用方式已经在恶意软件中被发现

- **漏洞危害**
  - 可以利用系统库注入到其他进程中，进而执行恶意行为，或作为跳板对新的接口发起攻击。

DEMO

安装器应用A权限

利用漏洞静默安装应用B权限

目录

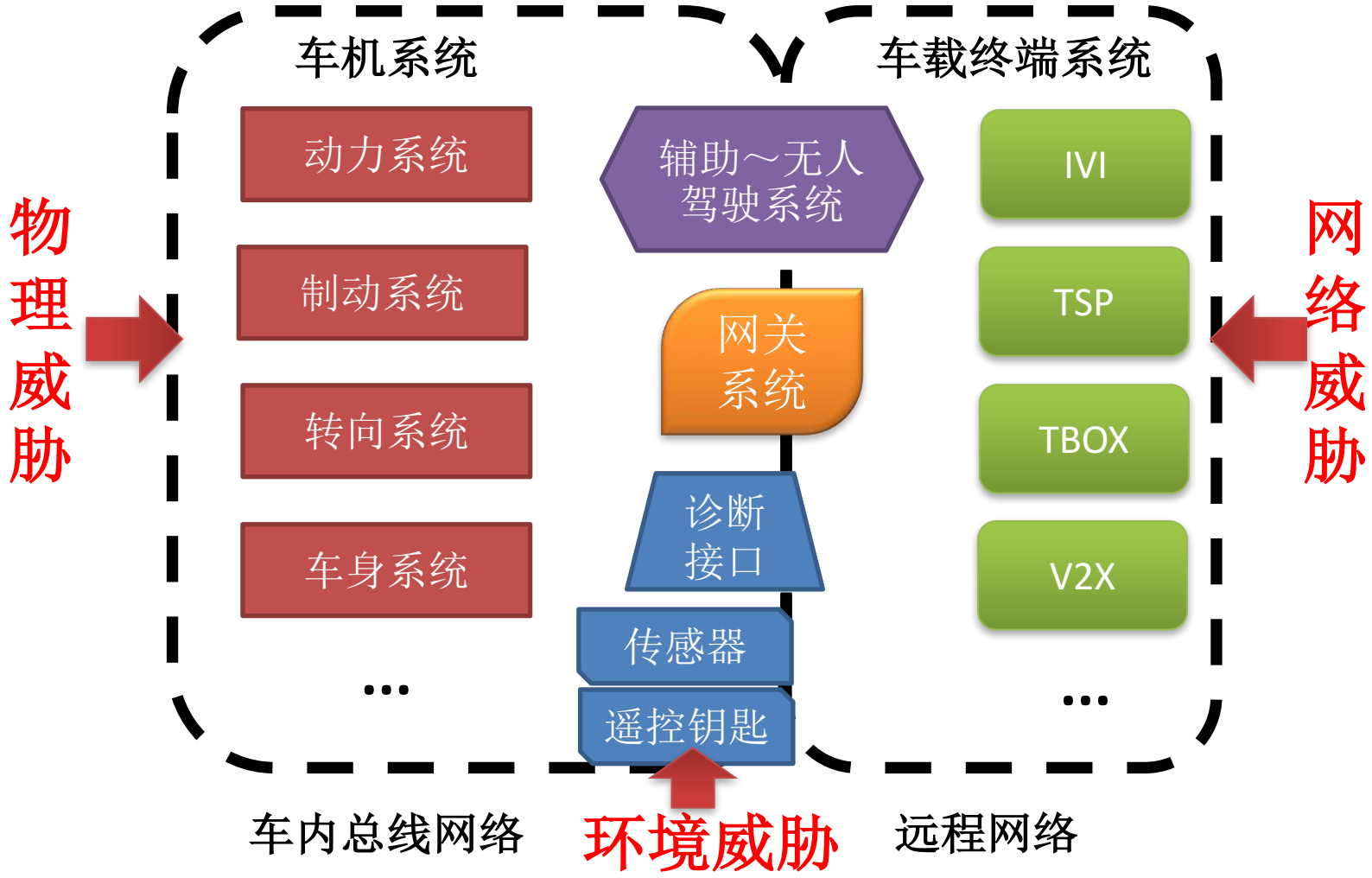
目录

智能网联汽车的智能终端演变

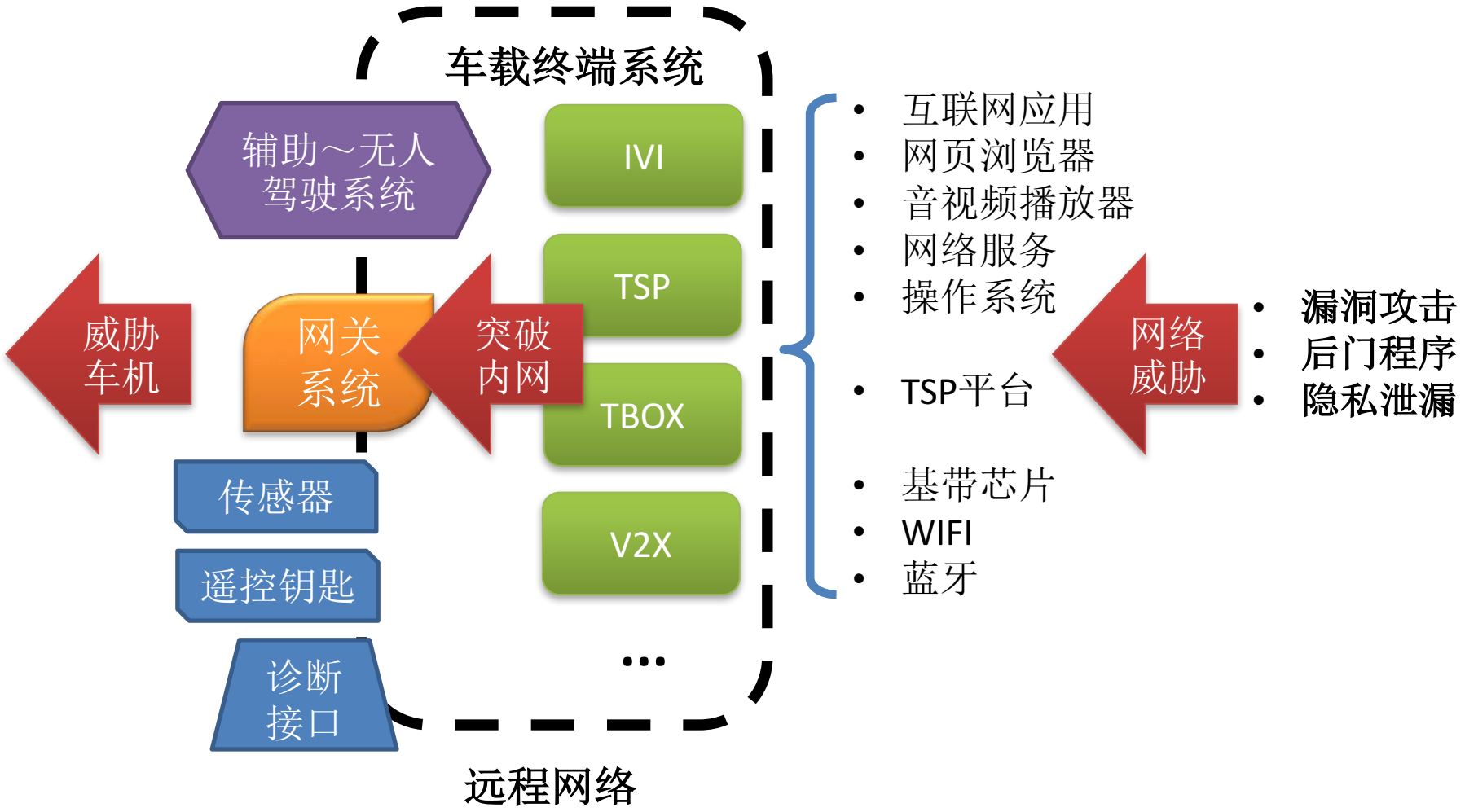
车载终端智能化演变

- 娱乐系统(IVI) → 更智能的人机交互系统(CID)
- 仪表盘 → 更智能的仪表系统(IC)
- 辅助～无人驾驶系统

从汽车网络架构看安全威胁



汽车网络威胁


车载终端系统
辅助~无人驾驶系统
IVI
TSP
TBOX
V2X
...
网关系统
突破内网
威胁车机
传感器
遥控钥匙
诊断接口
远程网络
互联网应用
网页浏览器
音视频播放器
网络服务
操作系统
TSP平台
基带芯片
WIFI
蓝牙
网络威胁
漏洞攻击
后门程序
隐私泄漏

智能网联汽车破解实例分析

科恩实验室《TESLA HACKING 2016》

- 劫持Tesla预置WIFI，实现无用户主动交互攻击
- 攻击CID内置浏览器
  - JSArray::sort 中的一个TOCTOU漏洞。CVE-2012-3748
  - CVE-2011-3928 内存信息泄露
- 攻击CID内核，提升权限
  - CVE-2013-6282 get_user/put_user任意地址读写
  - 关掉强制访问控制机制（AppArmor）
- 攻击网关及其他车内网系统，绕过完整性校验，刷写固件
- 攻击控制ECU

智能终端攻击流程

修补和改进：

- 修补漏洞，升级内核
- 增加内存漏洞利用缓解机制，增强访问控制策略
- 固件更新改用签名校验

2017年，再次被攻破

智能网联汽车终端vs智能终端

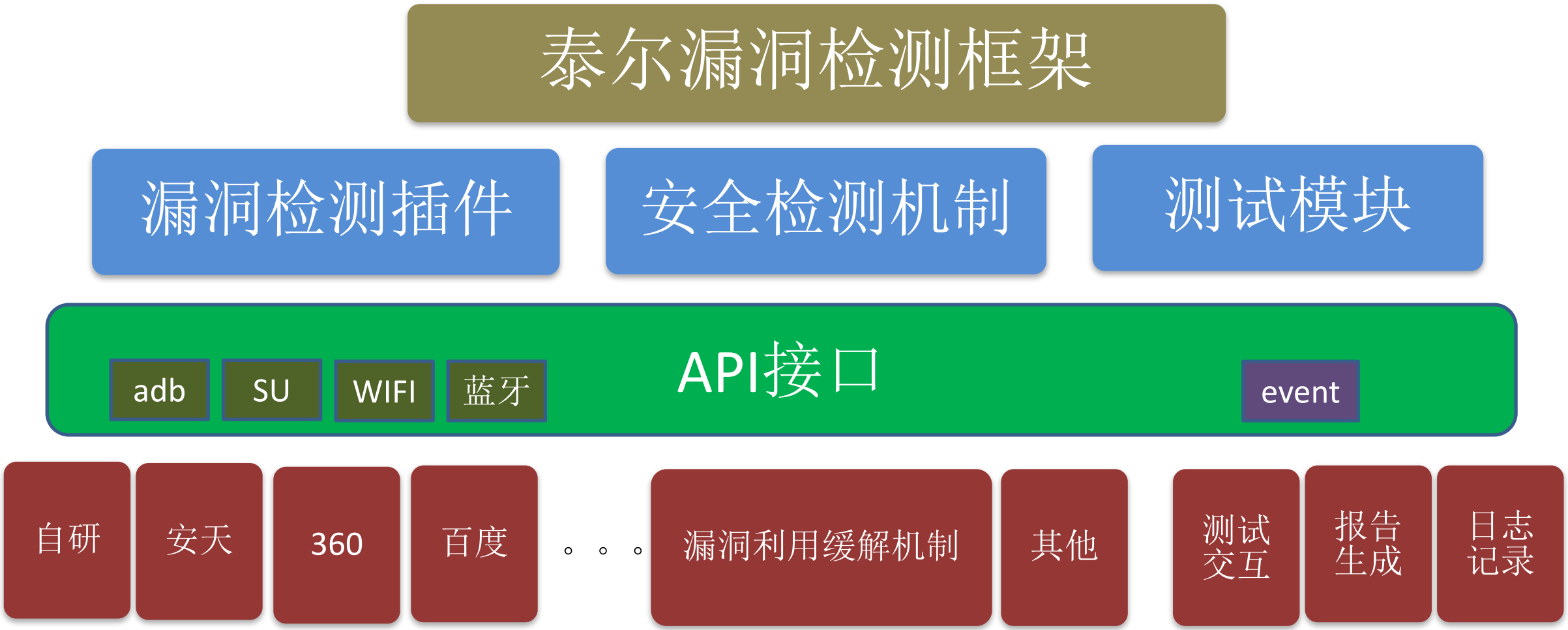
- 智能网联汽车 = 汽车 + 智能终端 + …
- 联网终端安全威胁影响车机控制系统
- 智能终端的网络和信息安全问题在智能网联汽车中同样存在，并且更严重
  - 系统碎片化和定制化引入大量没有修复的1day漏洞，而产业链上的相关厂商可能并不知道该问题
  - 保护机制、漏洞利用缓解机制没有同时期相当的智能手机完善
- 汽车行业联网、智能化刚刚起步，还存在大量问题

安全检测服务

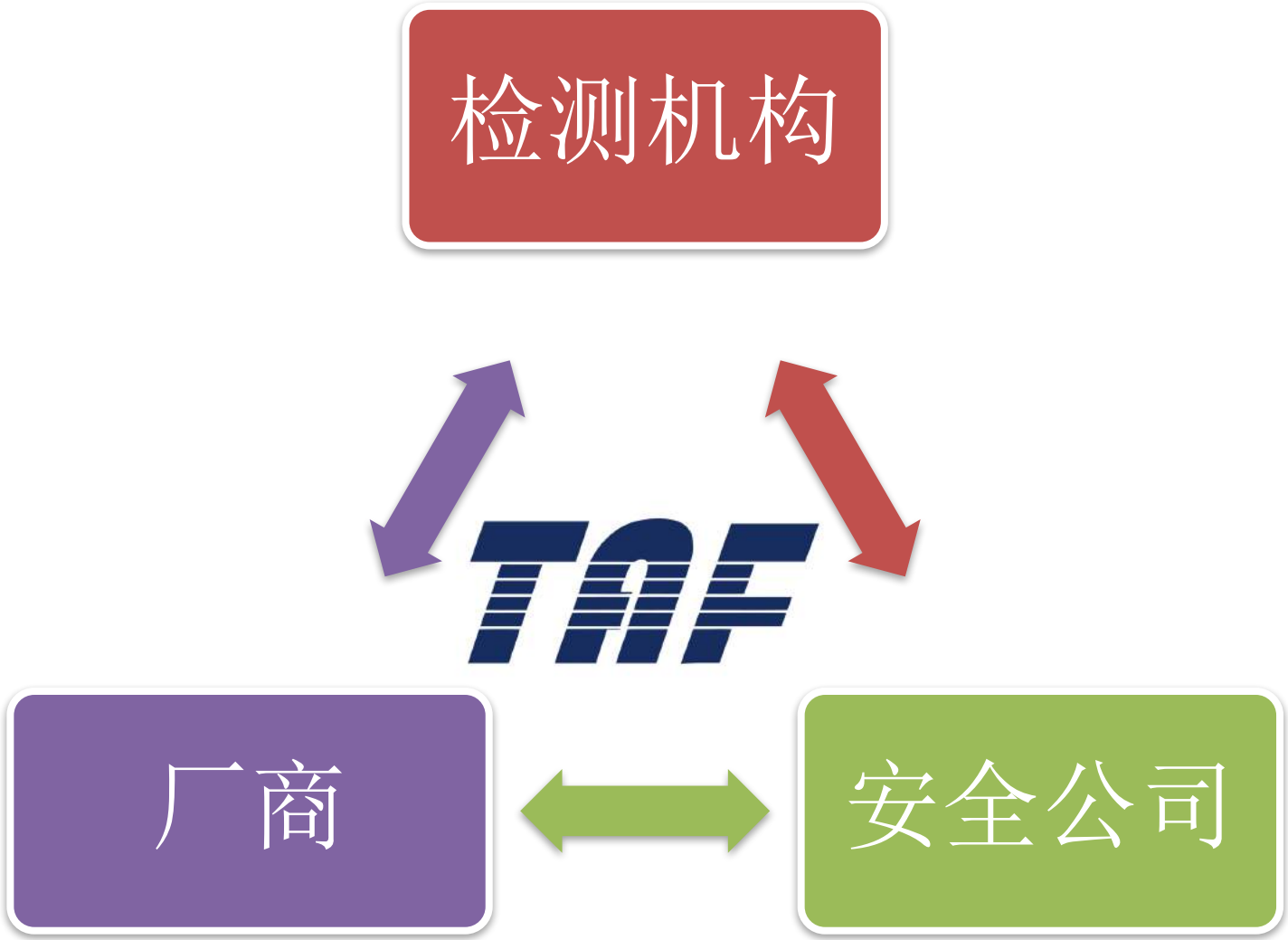
	安全性评价	安全基线校验
评价目标	对车联网系统的安全性进行黑盒检测	对车联网系统所使用的安全机制的符合性进行评估
评价方式	漏洞扫描+渗透测试，包括以下渗透接口和扫描对象： • ECUs、CAN-BUS • 云端服务器及WEB应用 • WIFI/BT/自定义协议 • 手机APP • TBOX、IVI等终端及车内通信	安全基线包括： • 安全域隔离，e.g. TEE检测认证 • 身份认证与访问控制，e.g. 定制FW • 应用安全， e.g. PKI的使用 • 数据安全，完整性保护及加密 • 监控与审计
能力要求	• 漏洞扫描 • 攻击能力 • 渗透能力	• 定义《安全基线》规范 • 检测工具配套

目录

泰尔漏洞检测框架


泰尔漏洞检测框架
漏洞检测插件
安全检测机制
测试模块
adb
SU
WIFI
蓝牙
API接口
event
自研
安天
360
百度
。。。
漏洞利用缓解机制
其他
测试交互
报告生成
日志记录

合作模式



感谢聆听
Thanks