OWASP
Open Web Application Security Project

智能网联汽车的安全测试

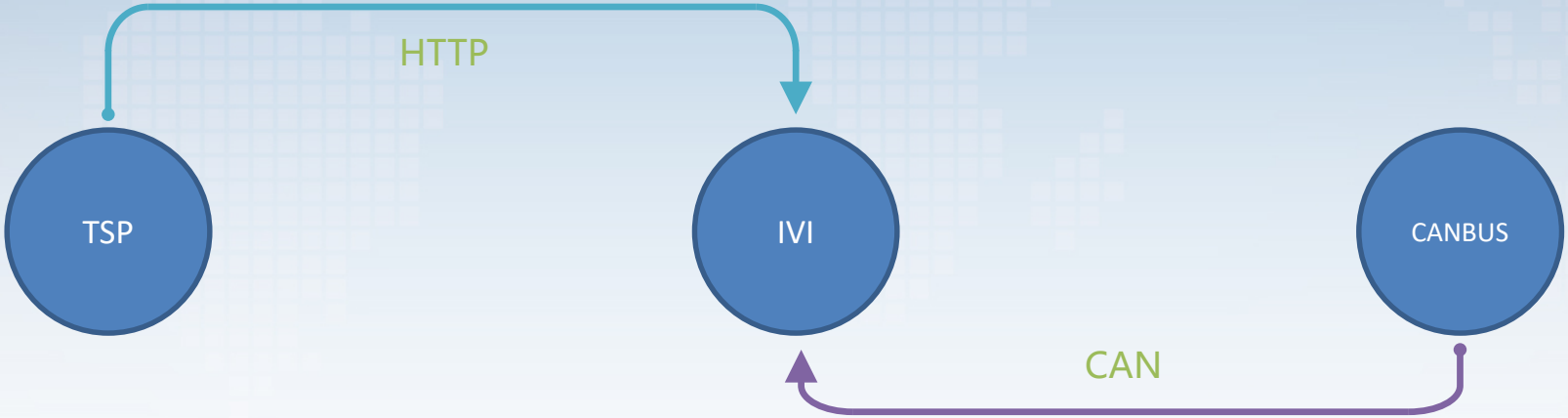
赵成宇
奇安信科技集团

目录

智能网联汽车进化史
智能网联汽车攻击面分析
智能网联汽车测试工具与案例

智能网联汽车进化史

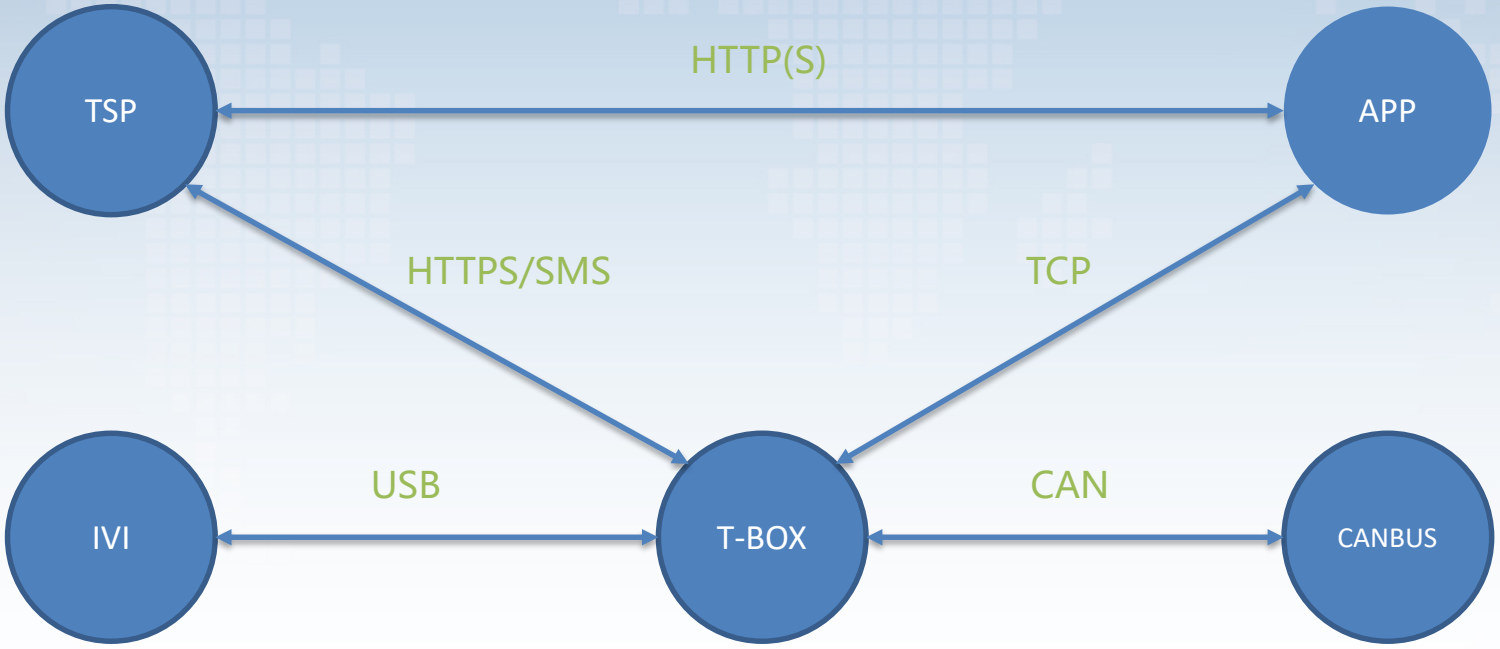
第一代(过去)



TSP (Telematics Service Provider)
IVI (In-Vehicle Infotainment)
CANBus (ControLLer Area Net-work Bus)

智能网联汽车进化史

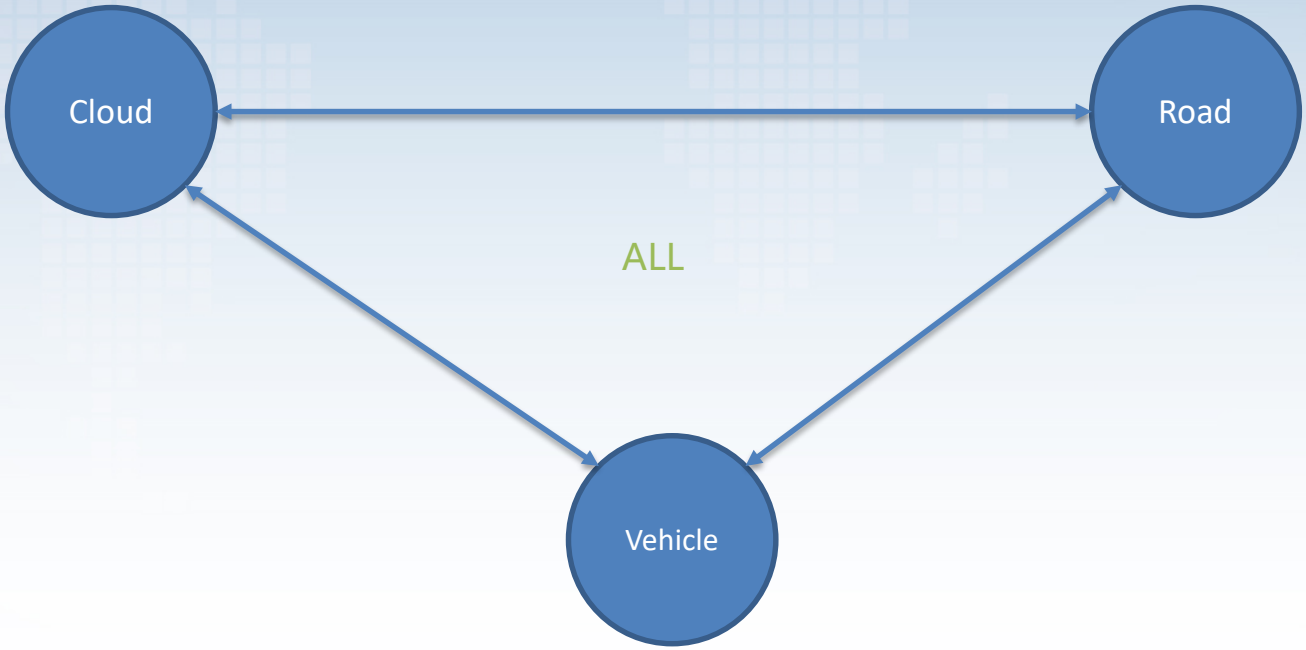
第二代(现在)



TBox(Telematics BOX)

智能网联汽车进化史

第三代(将来)



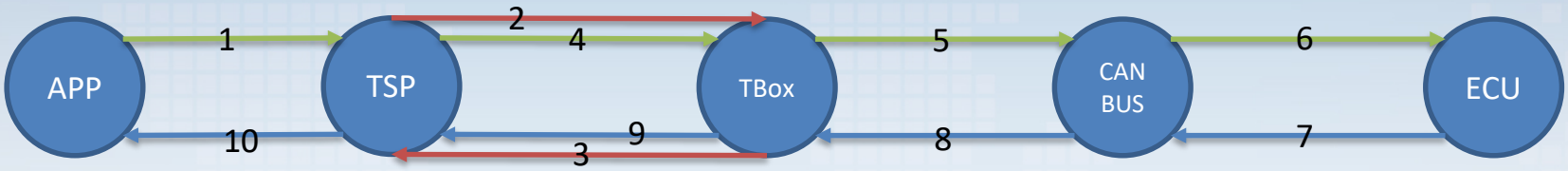
V2X(vehicle to everything)

智能网联汽车攻击面分析

- **TSP** (Telematics Service Provider)
  - OWASP TOP 10
- **APP** (Telematics Service Provider)
  - 应用层攻击
  - 逆向分析
  - 证书获取
  - 流量解密
- **TBox** (Telematics BOX)
  - 固件逆向
  - FOTA劫持
  - 功能越权
  - 近场通讯劫持
- CANBUS(ControLLer Area Net-work Bus)
  - 自有协议分析
  - Gateway Fuzzing
  - DOS攻击

智能网联汽车测试案例

•远程打开汽车空调



1. 请求打开空调(Https)
2. 激活Tbox(SMS)
3. 激活成功(Https)
4. 请求打开空调(Https)
5. 发送打开空调消息集(CAN)
6. 转发消息集到ECU
7. ECU返回结果消息集(CAN)
8. 转发结果消息集(CAN)
9. 返回操作结果(Https)
10. 回复APP操作结果

智能网联汽车测试工具

OWASP
Open Web Application Security Project

致谢