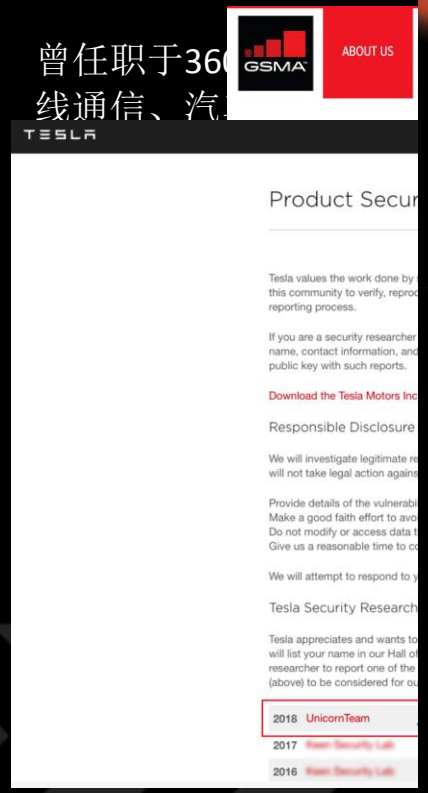
网络安全创新大会
Cyber Security Innovation Summit

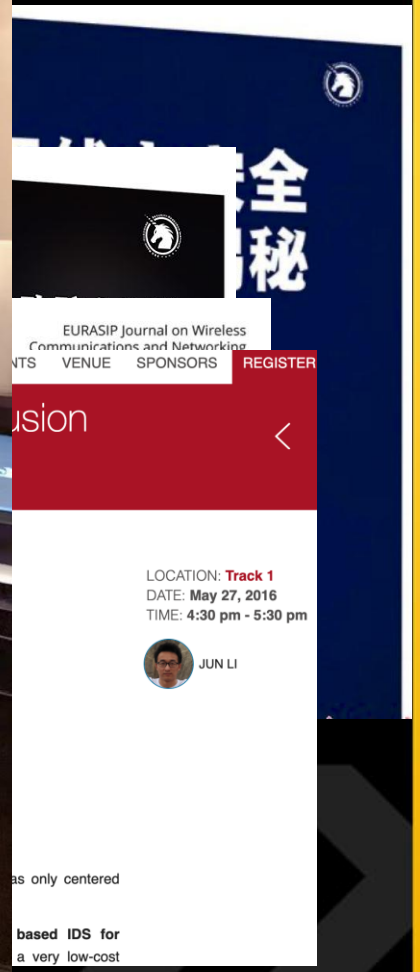
汽车网络安全守方之殇

姓名 李均 GoGoByte创始人

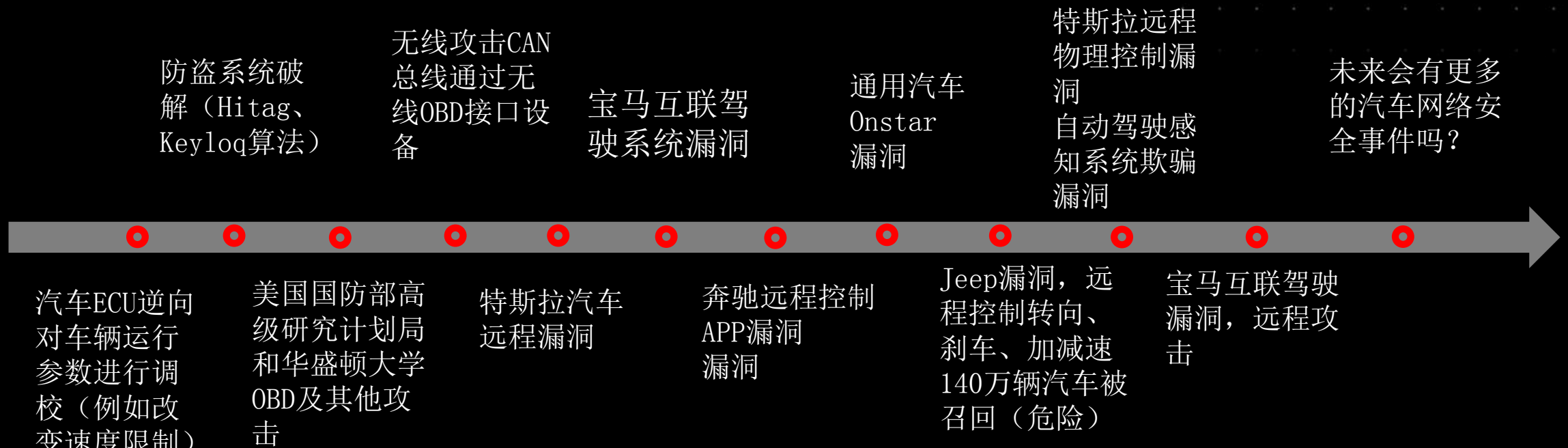
自我介绍

曾任职于360
线通信、汽



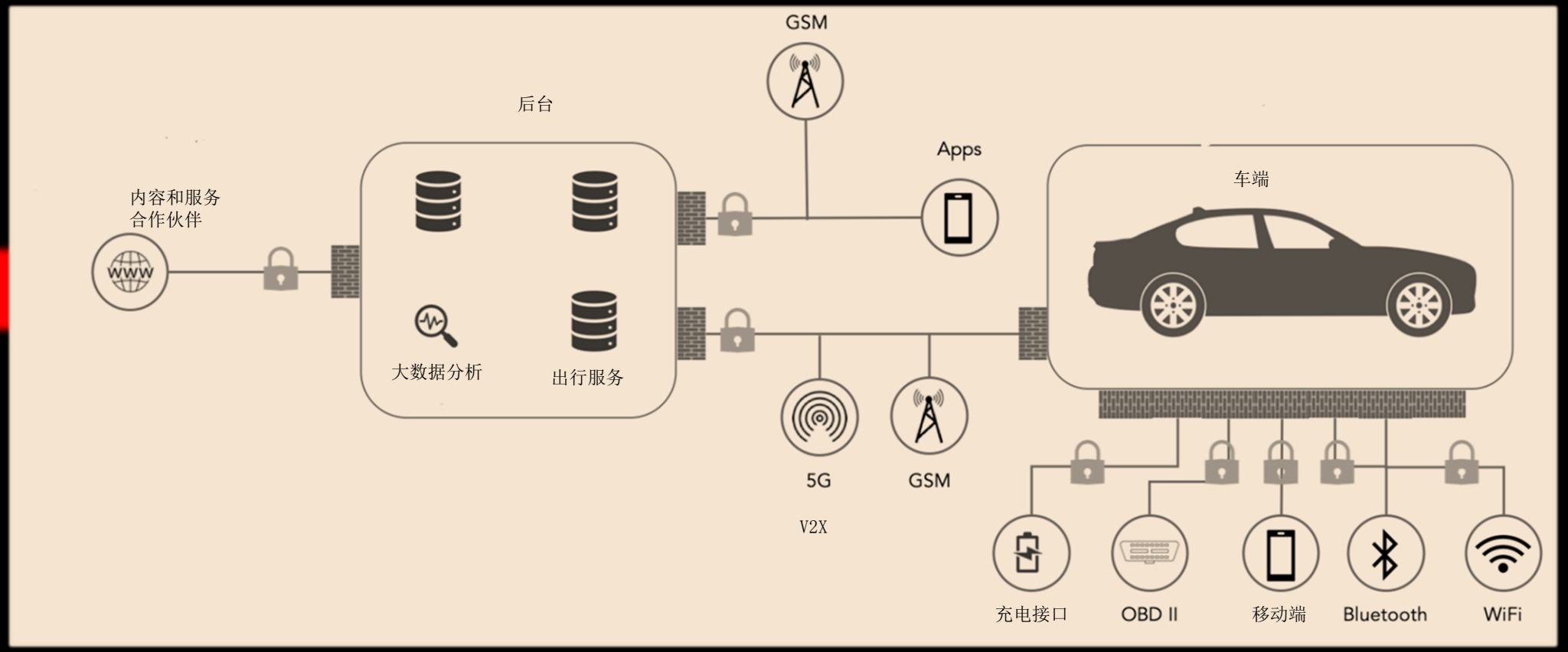


汽车攻击的发展

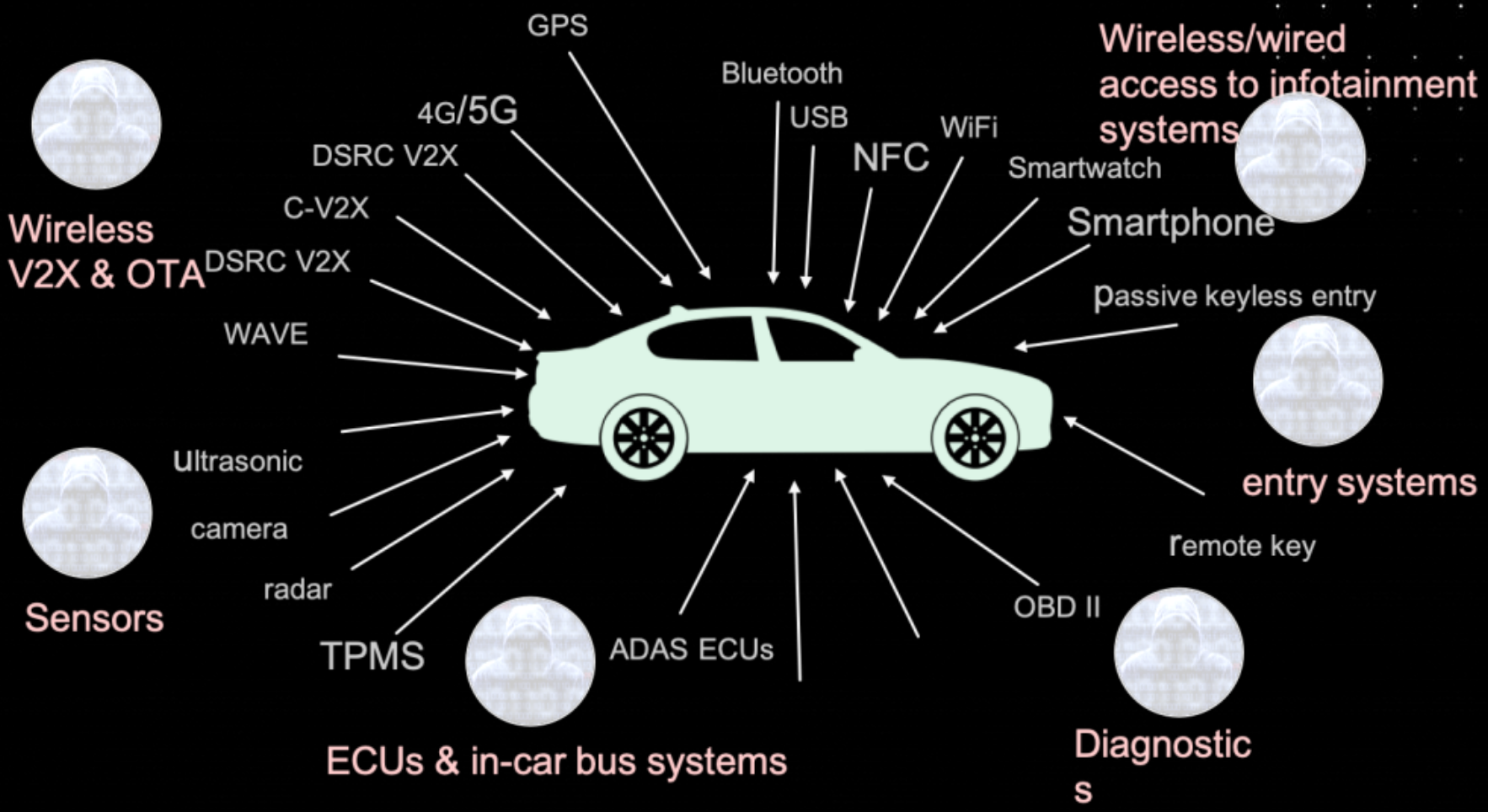

汽车ECU逆向对车辆运行参数进行调校（例如改变速度限制）
美国国防部高级研究计划局和华盛顿大学OBD及其他攻击
防盗系统破解（Hitag、Keyloq算法）
特斯拉汽车远程漏洞
无线攻击CAN总线通过无线OBD接口设备
奔驰远程控制APP漏洞
漏洞
宝马互联驾驶系统漏洞
Jeep漏洞，远程控制转向、刹车、加减速
140万辆汽车被召回（危险）
通用汽车Onstar漏洞
宝马互联驾驶漏洞，远程攻击
特斯拉远程物理控制漏洞
自动驾驶感知系统欺骗漏洞
未来会有更多的汽车网络安全事件吗？

汽车行业如火如荼变革

连接



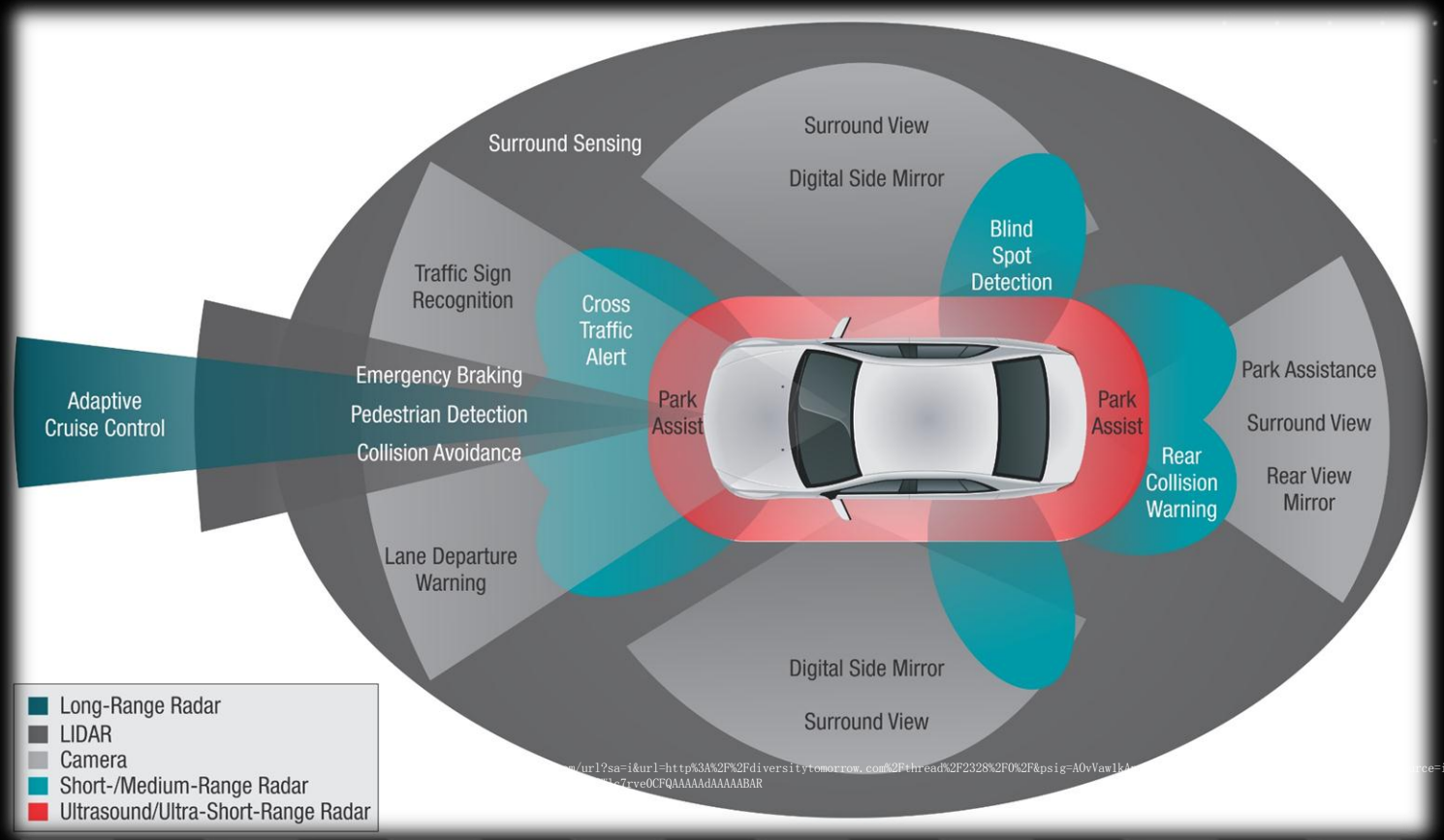
汽车行业如火如荼变革



Source:https://dekra-cyber-security.com/cyber-security-a-holistic-view/

汽车行业如火如荼变革

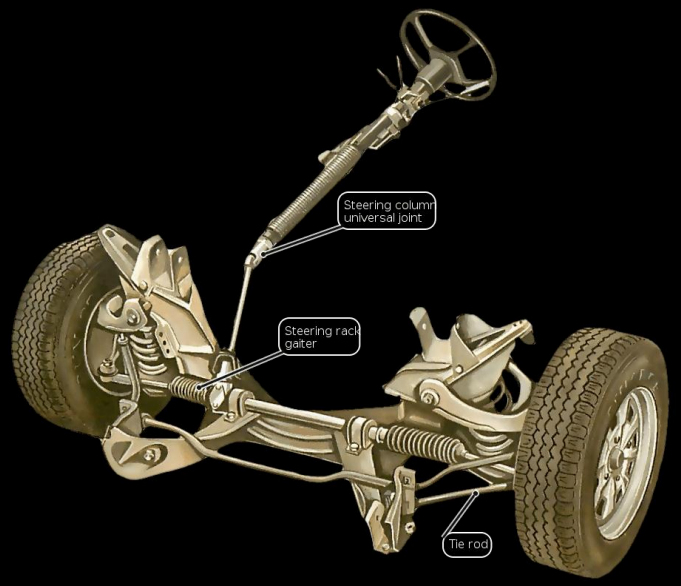
自动化
智能化



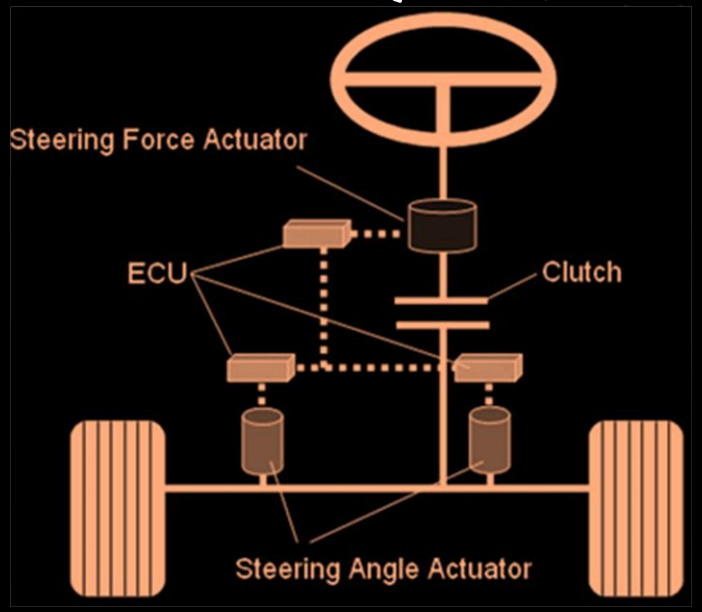
新的功能引入新的威胁

X-By-Wire
线控

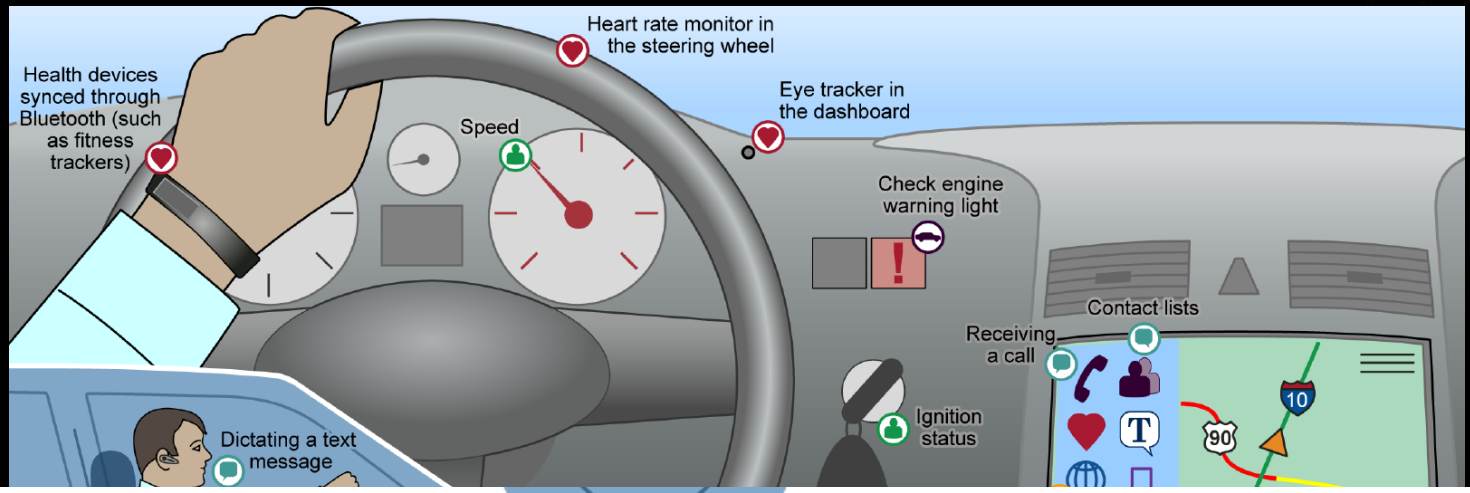
传统转向系统



电子控制转向系统



汽车对攻击者来说越来越具吸引力



Infotainment
Data generated by the infotainment system (such as music selections or mobile applications used).

Personal Communications
Data generated by individuals in the vehicle and sent or received via a vehicle's infotainment system, often through a synced smartphone.

Location
Data about a vehicle's location at any given time.

Driver behavior
Data on how and when a driver operates the vehicle.

Biometrics and health
Data on vehicle occupants gathered by biometric or health monitoring devices in or linked to the vehicle.

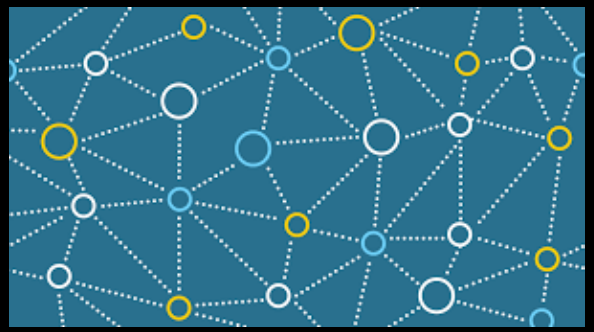
Vehicle health
Data generated by a vehicle's internal systems on the performance of vehicle components.

ources: British Columbia Freedom of Information and Privacy Association, and GAO. | GAO-17-656

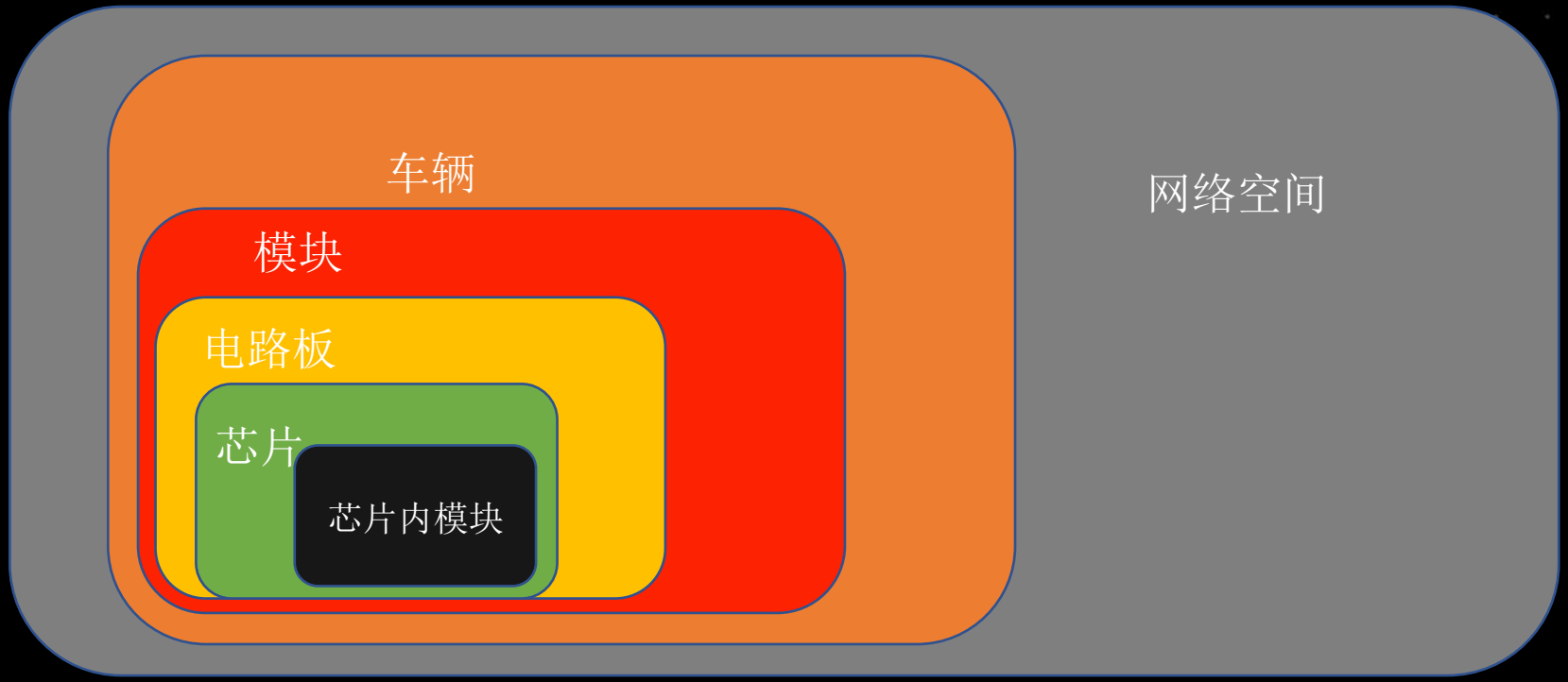
Note: This figure summarizes connected vehicle data categories and data elements presented in P. Lawson, B. McPhail, and E. Lawson, *The Connected Car: Who is in the Driver's Seat? A Study on Privacy and Onboard Vehicle Telematics Technology* (Vancouver, British Columbia: British Columbia Freedom of Information and Privacy Association, 2015), https://fipa.bc.ca/wordpress/wp-content/uploads/2015/05/CC_report_lite-1v2.pdf.

守方之殇---要操心的事儿

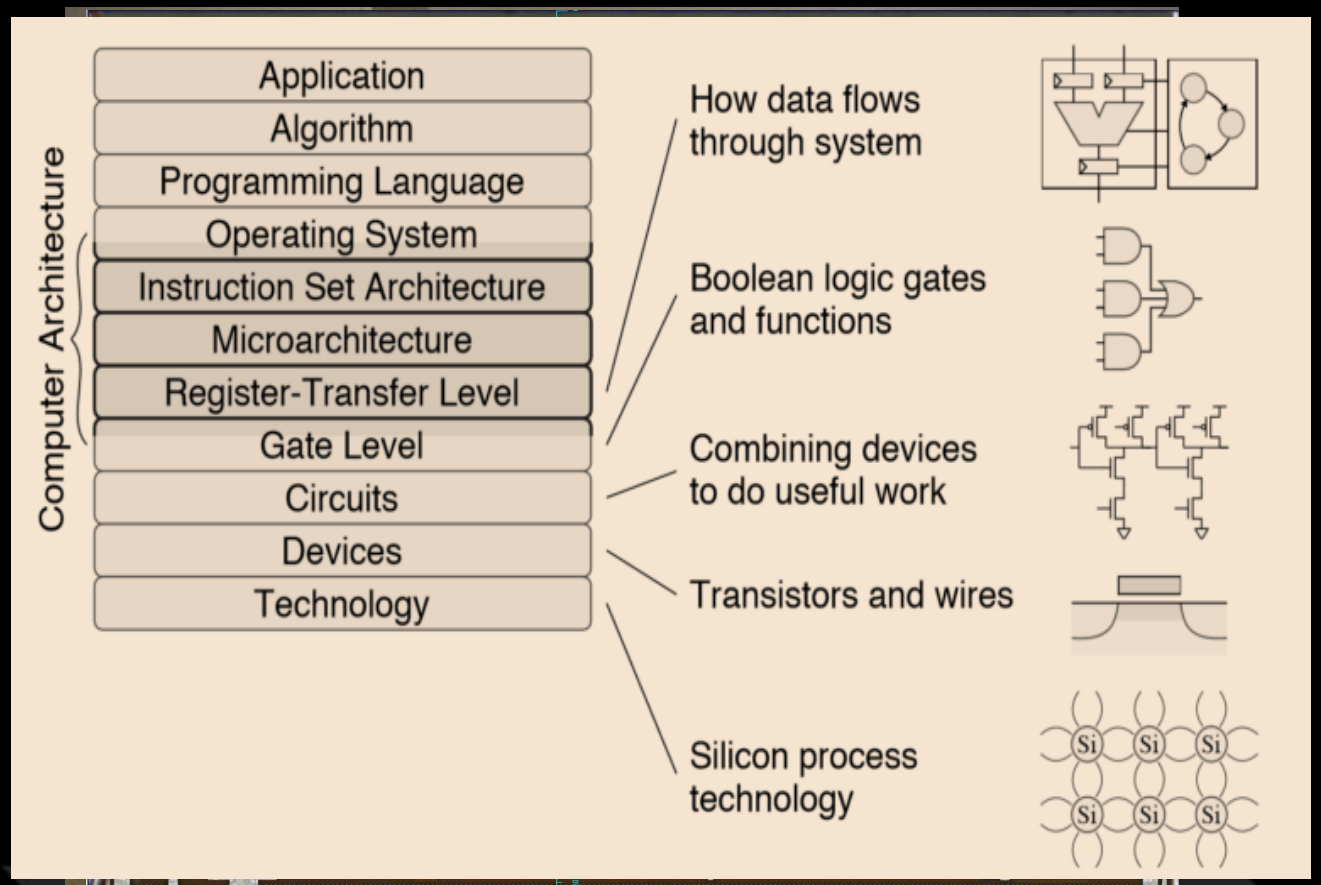
- 芯片安全
- 模组安全
- 通信管道安全
- 应用安全
- 云端后台安全
- 感知系统的安全
- 生产环境安全
- 售后流程安全
- 安全开发
- …



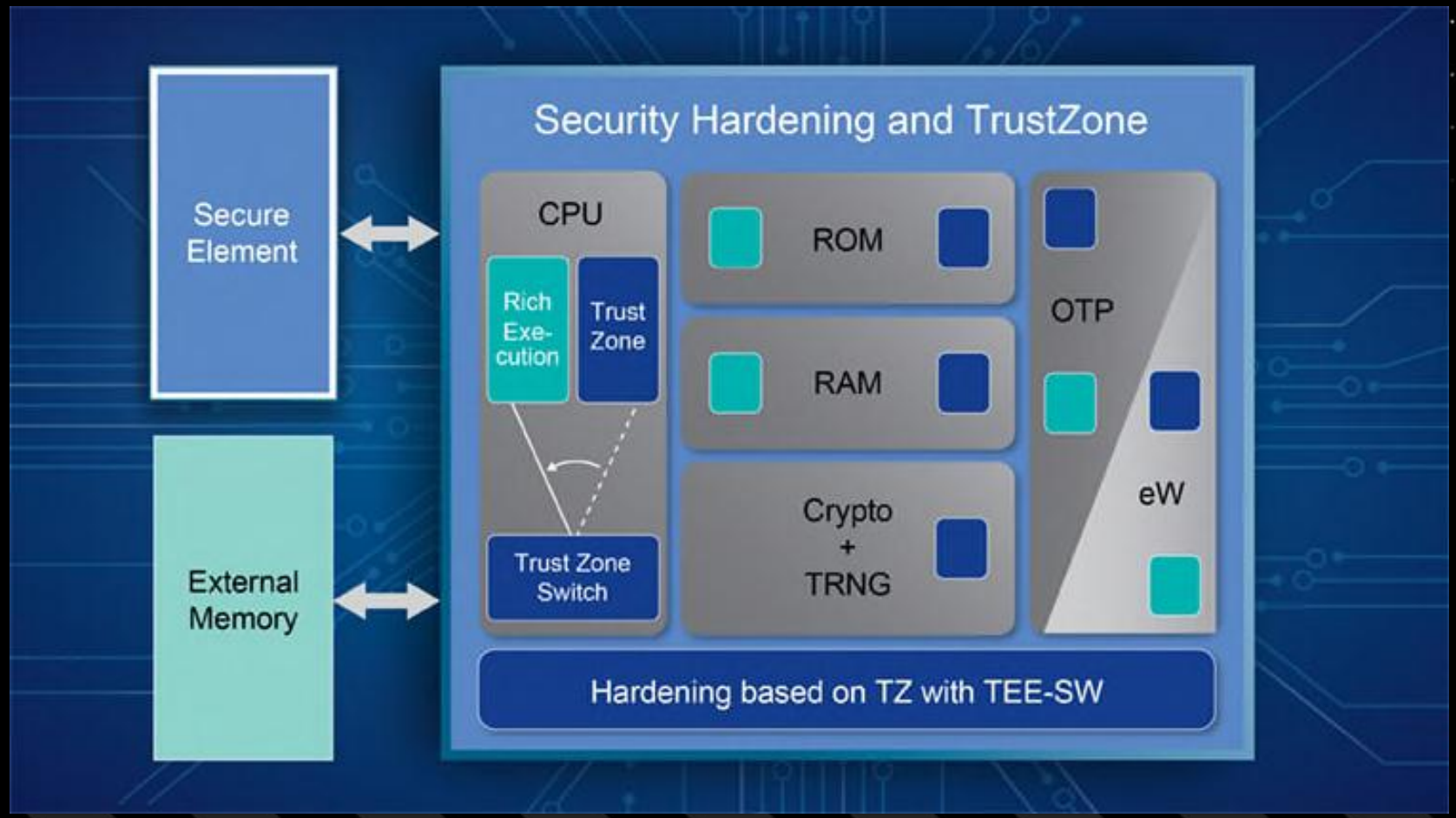
守方之殇---宏观来看

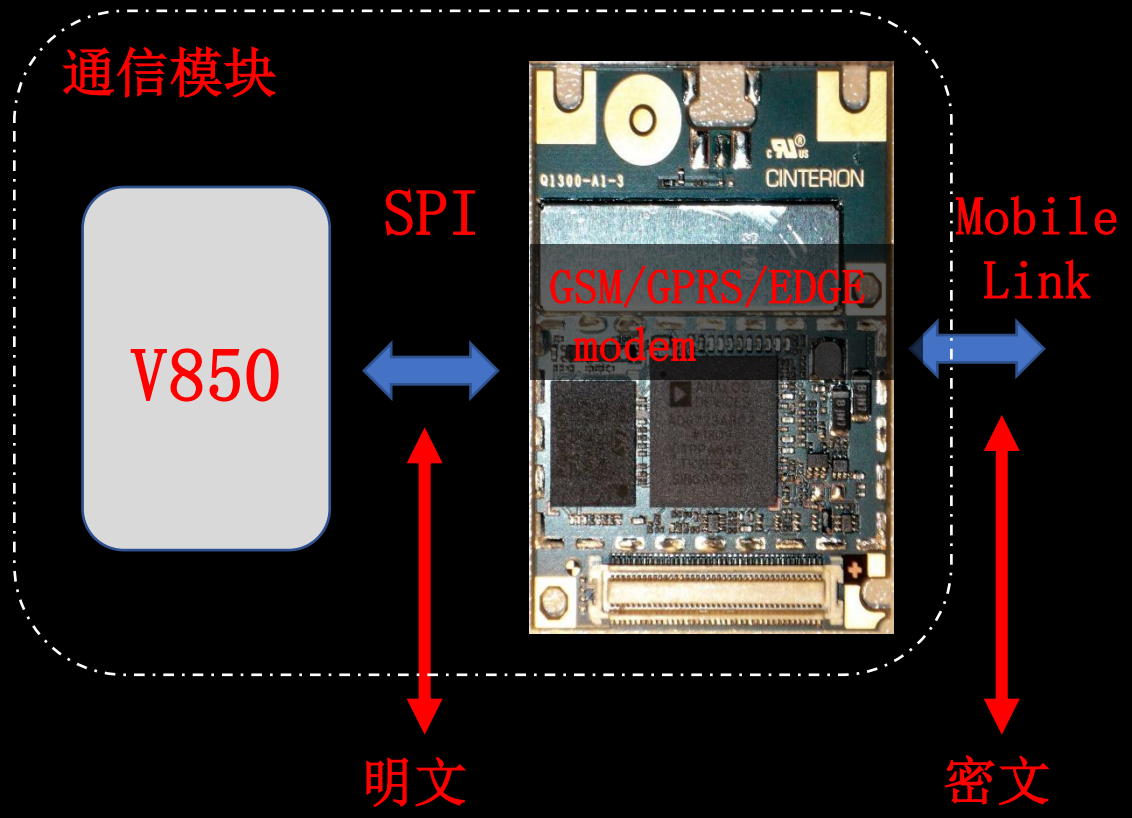


逆向分析为例

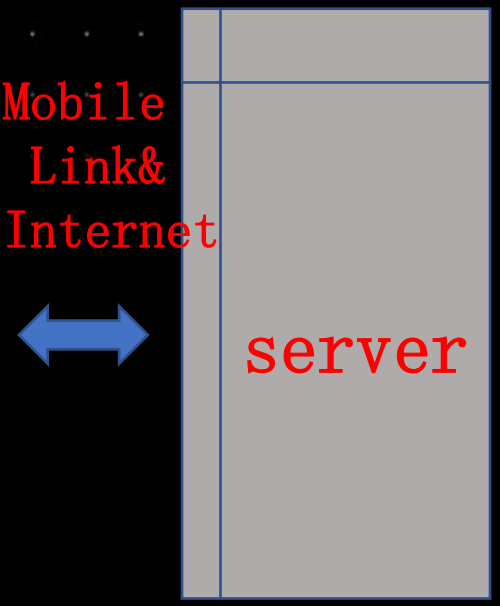

Application
Algorithm
Programming Language
Operating System
Instruction Set Architecture
Microarchitecture
Register-Transfer Level
Gate Level
Circuits
Devices
Technology
Computer Architecture
How data flows through system
Boolean logic gates and functions
Combining devices to do useful work
Transistors and wires
Silicon process technology
Si

守方之殇---知道不一定能做对




通信模块
V850
SPI
明文
CINTERION
GSM/GPRS/EDGE
modem
Mobile
Link
密文


SysmoBTS
nanoBTS


Mobile
Link&
Internet
server

守方之殇---攻击者的

守方之殇---需要全面防御

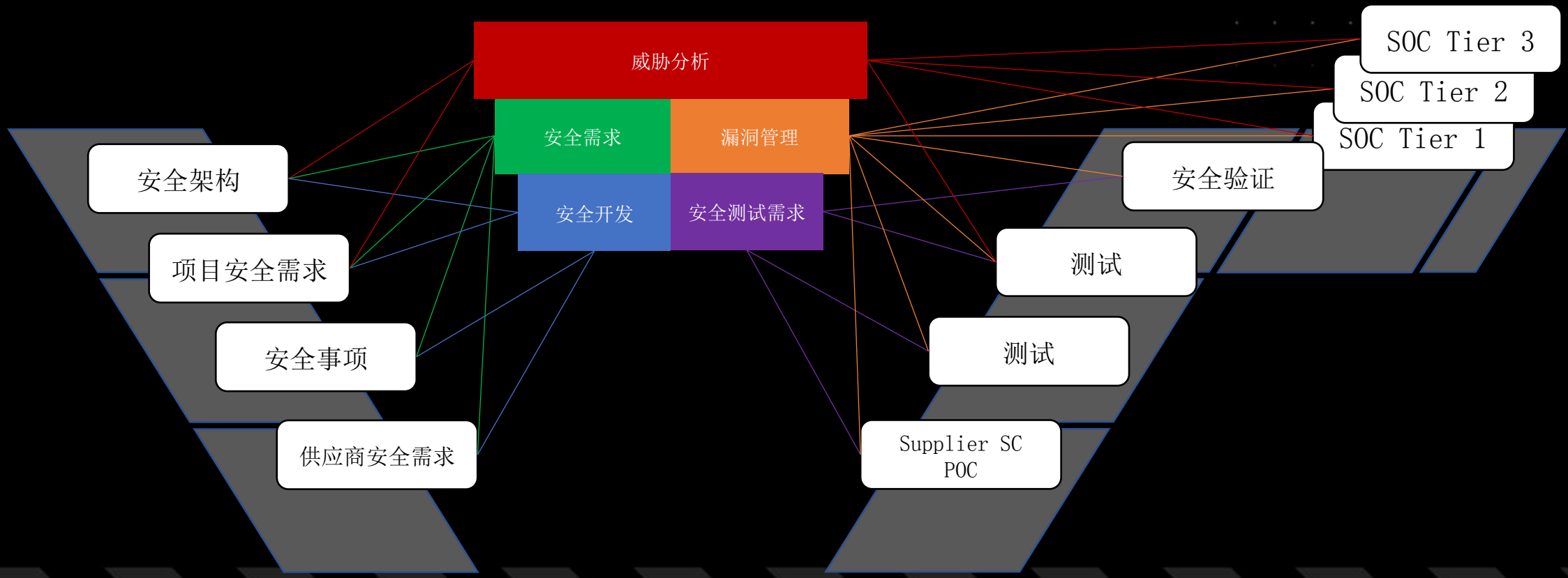
攻击主要是技术问题
防守不只是技术问题

守方之殇---安全研究人员的不理解

报告了漏洞根本没人理！
厂家漏洞响非常慢！
漏洞根本无法远程修复！
这么简单的安全问题都搞不定？
.....

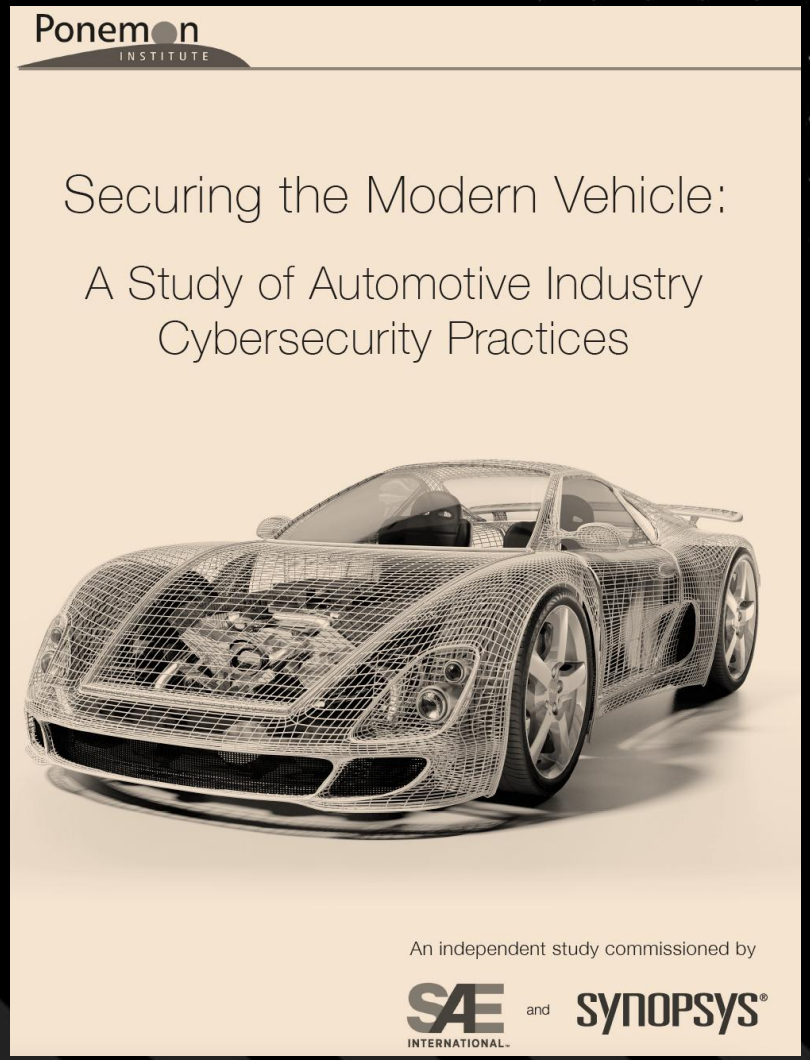
守方之殇---全面防御

网络安全创新大会
Cyber Security Innovation Summit



汽车行守方之殇---守方的武器库

产品或服务
安全管理咨询
合规咨询
21434 Work Product management
安全测试
OTA
VSOC
IDPS
安全 SDK （cypher, communication lib, CA）
HSM
防火墙，安全网关
V2X，CA
资产管理、漏洞管理
终端（linux，rtos） 安全
移动安全
安全开发
安全培训
安全测试工具



Conclusions

- The Building Security In Maturity Model (BSIMM) and the Synopsys Automotive Security resource page can help organizations develop a security initiative and meet security, safety, reliability, and compliance requirements for automotive software.

These solutions advocate developing and utilizing a risk-based, process-driven approach that binds cybersecurity to the entire product development life cycle and the secure software development life cycle.

Cybersecurity training is also a critical investment that not only targets one pain point respondents shared in the survey but also pays dividends far into the future, helping to build a culture of security throughout an enterprise.

The automotive industry also has resources to enhance knowledge of emerging security issues and trends, develop professional networks, and contribute to industry-wide security.

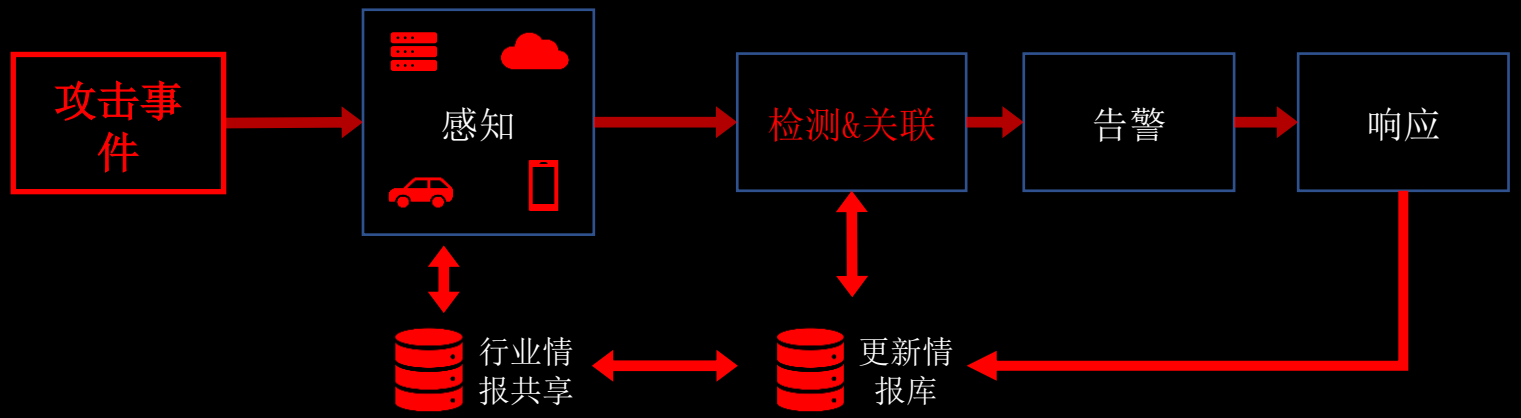
- The Automotive Information Sharing and Analysis Center (Auto-ISAC) is a valuable forum for security professionals to share and analyze intelligence about emerging cybersecurity risks to the vehicle, and to collectively enhance automotive industry cybersecurity.
- SAE International has several cybersecurity groups developing standards, guidelines, and best practices, provides professional development training, and hosts conferences and events to keep the industry abreast of the state of the practice.

The concerns about supply chain risks noted in this report can be addressed or even mitigated by paying close attention to the requirements phase of the development life cycle. This may involve working closely with suppliers to identify weaknesses in the design or architecture of relevant components. Additional assurances can be achieved by conducting periodic reviews of suppliers' cybersecurity processes or imposing cybersecurity assurance requirements on supplier agreements.

Cybersecurity shouldn't be viewed as a cost center and tacked on at the end of production, but instead should be programmed into every step of the systems engineering process that guides the entire product development life cycle—notably, the secure software development life cycle (SSDLC). Automotive companies can enjoy a wide range of solutions through guidance, best practices, and standards that have already been developed in other industries.

This rigorous approach to cybersecurity is vital to achieve enhanced safety while ensuring security, quality, and rapid time to market.

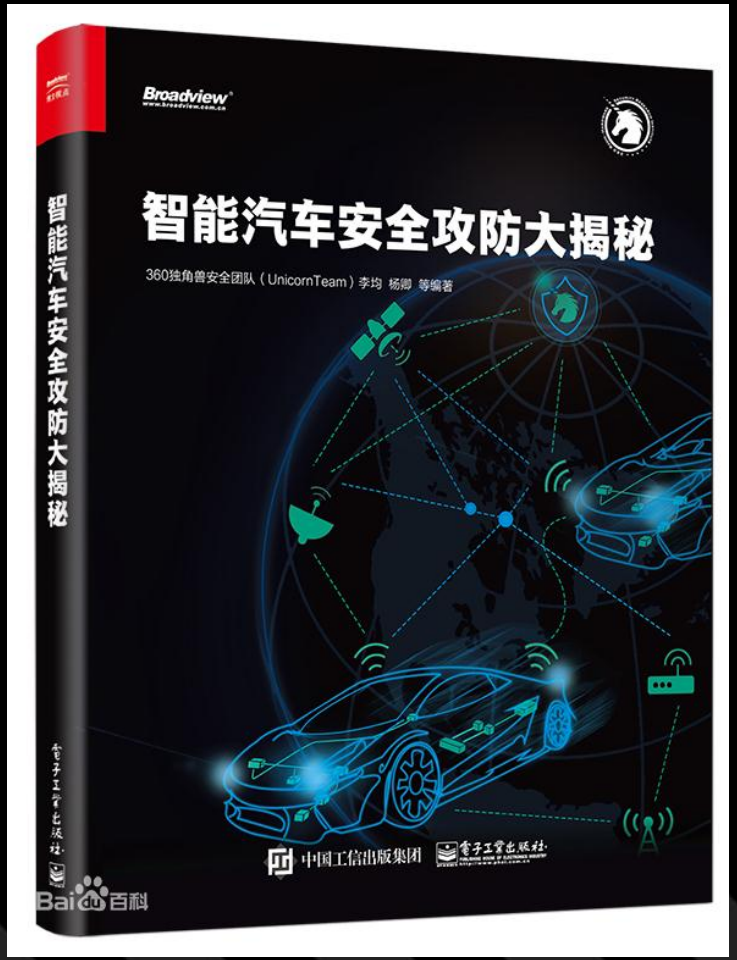
情报驱动的安全检测与响应

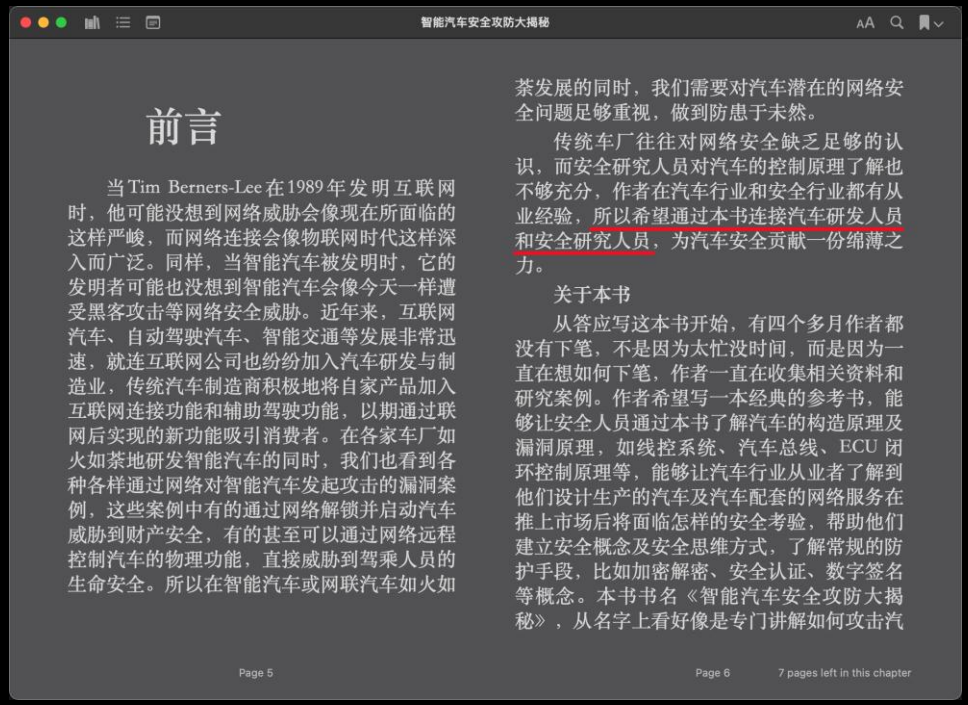


Advantages of Integrating Security into Product Development

1. Integrating security concepts into product design achieves higher security than applying security controls post production.
2. Risks and vulnerabilities are identified early, and appropriate security controls can be applied.
3. This is a vastly more efficient way to apply limited cybersecurity resources and normalizes cybersecurity costs as a critical piece of the product development discipline.

守方之殇---管理篇


Broadview
智能汽车安全攻防大揭秘
360独角兽安全团队（UnicornTeam）李均 杨卿 等编著
智能汽车安全攻防大揭秘
中国工信出版集团
电子工业出版社
Baidu百科


智能汽车安全攻防大揭秘
前言
当Tim Berners-Lee在1989年发明互联网时，他可能没想到网络威胁会像现在所面临的这样严峻，而网络连接会像物联网时代这样深入而广泛。同样，当智能汽车被发明时，它的发明者可能也没想到智能汽车会像今天一样遭受黑客攻击等网络安全威胁。近年来，互联网汽车、自动驾驶汽车、智能交通等发展非常迅速，就连互联网公司也纷纷加入汽车研发与制造业，传统汽车制造商积极地将自家产品加入互联网连接功能和辅助驾驶功能，以期通过联网后实现的新功能吸引消费者。在各家车厂如火如荼地研发智能汽车的同时，我们也看到各种各样通过网络对智能汽车发起攻击的漏洞案例，这些案例中有的通过网络解锁并启动汽车威胁到财产安全，有的甚至可以通过网络远程控制汽车的物理功能，直接威胁到驾乘人员的生命安全。所以在智能汽车或网联汽车如火如荼发展的同时，我们需要对汽车潜在的网络安全问题足够重视，做到防患于未然。
传统车厂往往对网络安全缺乏足够的认识，而安全研究人员对汽车的控制原理了解也不够充分，作者在汽车行业和安全行业都有从业经验，所以希望通过本书连接汽车研发人员和安全研究人员，为汽车安全贡献一份绵薄之力。
关于本书
从答应写这本书开始，有四个多月作者都没有下笔，不是因为太忙没时间，而是因为一直在想如何下笔，作者一直在收集相关资料和研究案例。作者希望写一本经典的参考书，能够让安全人员通过本书了解汽车的构造原理及漏洞原理，如线控系统、汽车总线、ECU闭环控制原理等，能够让汽车行业从业者了解到他们设计生产的汽车及汽车配套的网络服务在推上市场后将面临怎样的安全考验，帮助他们建立安全概念及安全思维方式，了解常规的防护手段，比如加密解密、安全认证、数字签名等概念。本书书名《智能汽车安全攻防大揭秘》，从名字上看好像是专门讲解如何攻击汽
Page 5
Page 6
7 pages left in this chapter

基于风险评估的安全需求

纵深防御
每个攻击点都要最高的防护级别难度太大
让安全能力发挥到最需要的地方去才是王道

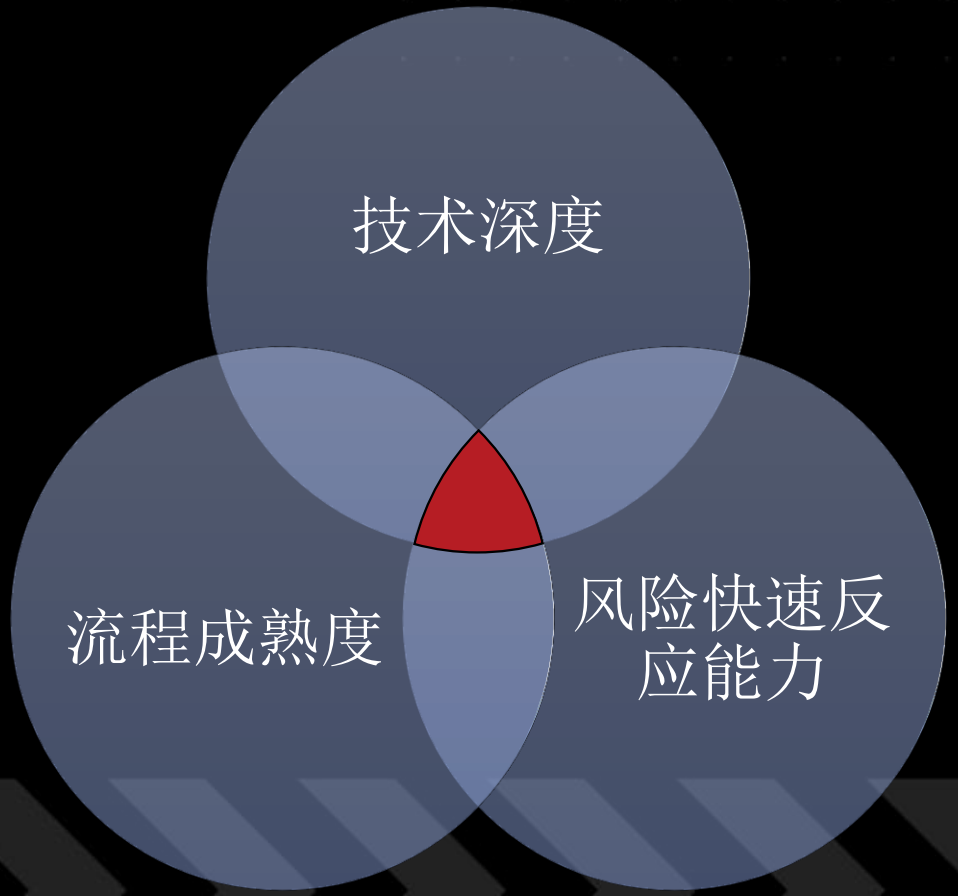
哪里是最需要安全的地方？需要什么样的安全级别？
功能安全&网络安全
TARA

汽车网络安全的主要问题—— 漫长的产业链反应时间

- 冗长的产业链反应时间造成对网络威胁的响应迟缓
- 传统汽车工程流程与互联网技术团队的鸿沟
  - 网络安全技术等信息技术和传统汽车成熟的工业流程之间的不匹配
  - 目前的网络安全供应商往往专注于渗透测试没有深入到产品生命周期中去
  - 特斯拉之类的一些新兴汽车厂商注重网络安全，所以有较成熟的安全能力，但是也在汽车制造工艺上面较弱。
- 详细的网络安全技术要求往往来的太迟
  - 漏洞的存在和发现是必然的，在互联网领域当出现新的漏洞时可以非常方便快捷的进行修复升级，而汽车行业冗长的供应链和对互联网技术的理解决定了漏洞信息的传递时间、理解时间、反应时间、测试时间都非常长，导致漏洞迟迟得不到修复，使得漏洞影响的驾乘人员面临安全威胁。

全面融入的网络安全

- 成功的网络安全成果要求结合多方面的能力 ：
  - 对网络安全漏洞和修复及缓解措施的深入理解
  - 用成熟的流程来保证网络安全在产品生命周期中对每个环节都得到充分的考量
  - 能够良好的将网络安全风险集成到其他需求的能力



United Nations ECE/TRANS/WP.29/2020/79 REVISED

Economic and Social Council

Distr.: General
23 June 2020

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

Submitted by the Working Party on Automated/autonomous and Connected Vehicles *

安全建设之路

网络安全管理

WP.29, ISO/SAE 21434 差距分析

网络安全管理系统

成熟度模型

架构设计和咨询

威胁建模和风险分析

TARA 验证

集成需求工程

专家安全测试

渗透测试

安全验证

代码审计

培训与能力建设

ISO/SAE 21434 网络安全管理系统

威胁和风险评估培训

安全开发

安全运营中心建设

安全实验室建设

测试台架设计&集成

设备验证采购

测试流程设计

团队部分成员介绍

李均 安全技术专家，曾在奇虎360任高级安全研究专家专注于无线、硬件等，360独角兽团队核心成员，《智能汽车安全攻防大揭秘》、《无线电安全攻防大揭秘》、《Inside Radio—An Attack&Defense Guide》等多本安全书籍的作者，并拥有IDPS、无线距离绑定认证协议等多项汽车安全相关专利。他的安全研究得到了恩智浦、特斯拉、 3GPP, 阿里巴巴、通用汽车的致谢，参加美国MITRE公司物联网安全挑战赛获得全球第六名

Peter Wesley Rivendell安全咨询公司创始人、首席咨询师，Hacklabs首席技术官。曾在华为任安全研究专家、拜腾汽车任南京安全实验室负责人、澳电讯公司(Telstra)任云安全架构师、 澳大利亚国民银行任应用安全架构师和安全技术专家，他在多个技术领域拥有丰富经验，包括安全策略和治理、安全架构和风险评估、威胁情报和安全漏洞研究， 30余年的国际化企业技术和管理经验使他对全球安全行业的技术发展方向和需求有着敏锐的洞察力。

Patrick Laird （英国）在全球汽车厂商和一级供应商领域拥有超过20年的经验，曾供职于阿斯顿马丁任系统集成项目工程师、NISSAN欧洲技术中心任电气设计和测试工程师 、麦格纳斯太尔（MAGNA STEYR）公司任电子/电气设计负责人 、拜腾汽车任动力及电源项目技术经理兼整车EE和功能安全经理 、本田任电气测试与设计部门经理。他在车身、底盘、信息娱乐和高压动力总成以及功能安全要求的应用方面拥有丰富经验。

安全应该像基因一样充满汽车行业的每个环节

GoGoByte

网络安全创新大会
Cyber Security Innovation Summit

THANKS

selfighter

Afghanistan

Scan the QR code to add me on WeChat