CAN 总线安全测试白皮书

一、行业背景与挑战

2016 年是车联网井喷式发展的一年，国内的汽车制造商纷纷和互联网公司开发下一代的联网汽车。汽车已经不再是简单的机械设备，而是近百种 ECU 通过内部车载网络进行全面的监测和控制。根据最近的估算数据，目前多数豪华轿车包含的二进制代码已经超过 100MB。尽管这种转变大大提升了效率和安全性，但也会带来一系列新的风险。攻击者几乎能潜入任何电子控制单元（ECU），控制汽车的多项功能，包括刹车和中止发动机工作等。

图 1、车联网安全

2015 年 7 月份美国克莱斯勒汽车厂商史上第一次因为安全漏洞一次召回 140 万辆汽车。鉴于不能及时保护车主的安全，7 月 26 日美国高速公路管理委员会宣布对克莱斯勒公司进 5 百万美金罚款，还不包括从车主手中买回近 20 万辆车和召回的费用。根据美国权威汽车价值评估媒体 Kelley Blue Book 最新公布的汽车黑客攻击调查报告中指出鉴于近期被广泛讨论的 Jeep 汽车被黑事件车主已经真正开始

关心车辆的网络安全问题。有 71%的参与者表示知道 Jeep 汽车被黑事件；41%的参与者表示在选购新汽车的时候会考量是否在存在被黑客攻击的新闻。

1.1 汽车总线在信息安全的缺陷

智能网联汽车已经不再是简单的机械设备，而是由近百种 ECU 通过内部车载网络进行全面的监测和控制。有些豪华轿车包含的二进制代码已经超过 100MB。尽管这种转变大大提升了效率和安全性，但也会带来一系列新的安全风险。尽管汽车产业在工程设计环节中一直非常重视 safety（安全性），但汽车制造厂商似乎并未意识到他们的在 safety 软件开发中遗漏下来的安全隐患可能会遭受信息安全攻击。例如，黑客已经证明他们能潜入电子控制单元 (ECU)来控制汽车的多项功能,包括刹车和中止发动机工作等. 更糟糕的是，随着人们将更多精细的服务和通信功能植入汽车，攻击现代汽车的通信入口也将随之迅速增多。攻击者可以借此潜入汽车内部网络，进而造成难以预知的后果。

CAN 安全防护面临的挑战有下面几点：

1. 广播特性

由于 CAN 数据包会向所有节点进行物理广播和逻辑广播，因此，网络中的恶意组件能轻松地窥探到所有通信内容，或向网络中的任何其他节点发送数据包。

2. 难以抵御 DoS 攻击

CAN 协议在拒绝服务(DoS)攻击面前显得十分脆弱。除了简单的数据包洪流攻击,还由于CAN的仲裁机制以优先级为基础,会导致某一节点能在总线上永久保持“首要”状态，从而使其他所有 CAN 节点让步。

3. 无身份验证者字段

CAN 数据包不含身份验证者字段，甚至连身份标识符字段也没有，这意味着：任何一个被入侵的组件均可用于控制相同总线上的所有其他组件（如果这些组件自身没有实施防御）。

4. 对总线的保护不足

CAN 总线缺乏必要的保护措施，无法确保完整性、保密性、有效性、消息真实性。并且对数据身份验证、数据保密性和数据实时性均缺乏必要的保护措施。

5. 对协议的不正当使用

攻击者通过不正当地使用协议中的特定机制，可以对车内网络发动攻击。某些车厂迫于上市时间的压力、线路连接成本和功能协调配合的复杂性，以及进一步完善需要付出的经济成本，没有充分贯彻协议中的标准。例如，安全标准中规定：当汽车在行驶过程中，车辆及其 ECU 不可进入编程模式。但在一

些实际情况中，即使车辆正在行驶，也可通过发出特定命令来禁用 CAN 通信，ECU 进入编程模式。

1.2 汽车攻击大事记

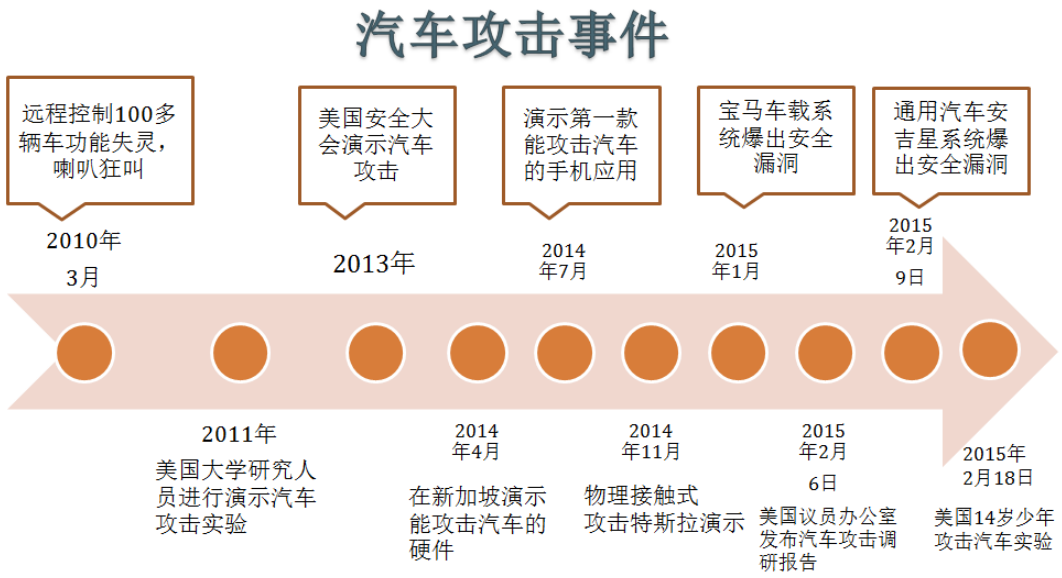

图 2、汽车攻击事件时间轴

图 2 显示了过去 5 年汽车攻击事件和发生的时间。从这张图中我们能看到 3 个特点：

1. 事件发生频率越来越密集

- 2010 年：美国德克萨斯州的一名汽车销售店的雇员因不满被解雇采用报复手段。他登入公司汽车管理账户，恶意操纵之前销售出去的 100 多辆汽车，使得这些车辆的某些功能失效，而且半夜喇叭狂叫等等。

- 2010 年到 2011 年：美国华盛顿大学及加州大学圣地亚哥分校的研究人员发表了 2 篇学术文章，演示了如何利用汽车漏洞进行远程攻击。
- 经过 2012 年的相对静默期，直到 2013 年下半年汽车安全随着移动互联网安全的延伸这个话题才又一次引起人们的注意。
- 2013 年夏季的 DEFCON 黑客大会上，美国研究人员对福特和丰田公司的汽车进行了破解演示，他们用电脑控制汽车方向盘，刹车等。并在 2014 年 4 月和 8 月分别在 SyScan 和 Blackhat 安全会议上公布了他们新的研究成果。
- 2014 年 7 月：我们团队演示了第一款对汽车进行攻击的手机安卓应用。假设此类移动应用通过传统手机病毒传播方式作为汽车病毒被下载到手机上，那么潜在攻击者则不需要对汽车技术有多深的理解，就可以进行汽车攻击，这将使得攻击技术门槛变得很低。
- 2014 年 7 月和 11 月：国内团队分别对特斯拉电动汽车进行破解，对其进行遥控控制。
- 2014 年 10 月：美国国家标准与技术研究院制定的《车联网网络攻击防护安全框架》
- 2015 年 1 月：宝马公司被爆出其车载系统 ConnectedDrive 安全漏洞。黑客可以利用这一漏洞远程攻击安装这种车载系统的 2 百万辆汽车。

- 2015 年 2 月 6 日：美国马萨诸塞州参议员 Ed Markey 办公室发布《车联网安全漏洞研究报告》，指出近 20 家汽车厂商对汽车攻击没有完整的防护方案，而且消极地面对汽车安全威胁。
- 2015 年 2 月 9 日：美国 DARPA 研究中心发现美国通用安吉星 OnStart 系统存在漏洞，导致黑客可以利用它来远程操控汽车。美国通用安吉星 OnStart 系统是最有名最老牌的汽车智能服务系统之一。
- 2015 年 2 月 18 日：在中国人欢度春节期间，大洋彼岸的一位 14 岁的美国少年却没有休息，他在 Radio Shack 电子配件店购买了 15 美元的设备，盖章后就可以遥控美国汽车厂商的汽车进行开关门动作。而且他之前对汽车没有什么技术积累，只是在请教了相关技术专家后就完成了这个演示项目。具体方法和设计的车型没有披露。

我们清楚地可以看到：2013 年之前汽车安全事件是按照年为单位，2014 年按照月为单位，但是到了 2015 年以后汽车攻击事件或者研究演示是按照天为单位了。

2. 高中低档车，传统车和电动车无一幸免

受到攻击影响的汽车涉及不同汽车厂商，即包括电动车和传统汽车，也包括高中低档的宝马，福特，丰田系列车型。我们团队研究发现，有些攻击方法甚至可以适用到多达 20 多种车型。

3. 攻击汽车是一项老少皆宜的活动（超过 14 岁就可以玩了）

汽车远远没有我们想象得那样安全，对汽车技术没有多少背景，也可以变成汽车小“黑客”。貌似钢铁侠般强壮的汽车却有着天生而来的致命安全死穴。

从以上各种事件显然可以看出，车联网系统和设备具有被入侵的可能性，这让汽车安全面对新的挑战,需要汽车厂商、安全公司等多方协同合作。

1.3 汽车信息安全攻击途径

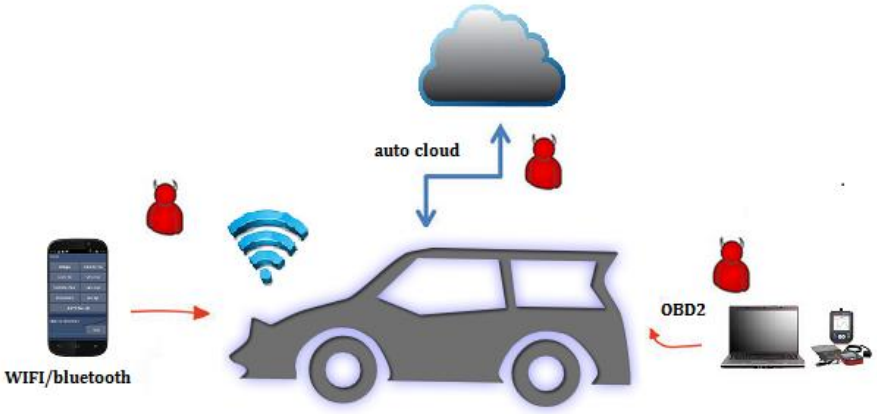

图 3、汽车网络攻击途径

“安全”在中文里有两个不同的含义：即包括“行车安全”Safe，又包括了“攻击防护安全”Security。绝大多数人们脑子里的汽车安全概念都属于行车安全，而上述汽车攻击对应的确实汽车防护安全。车厂在 Safe 方面下足了功夫，但是在 Security，尤其是汽车联网后

和外界的通信安全方面还很薄弱。

车厂在 Safe 行车安全方面积累了几十年甚至上百年经验，非常有自信。但是在 Security 汽车攻击安全防范方面却心有而力不足了。举个例子，目前绝大多数汽车内部系统是上个世纪 80 年代的技术，那时候，别说上网，连计算机和手机都没有普及，每个物件都是信息孤岛。汽车也不例外，最多和电信有个通信接口。那个年代根本都没有预测到智能化，联网化的趋势，所以基本没有黑客攻击的防护技术融于汽车设计中。

不幸的是，当前车主都希望自己的爱车变成智能汽车同自己进行交互，开启智能汽车生活。随着蓝牙，WIFI，2G/3G,甚至 4G LTE 加上移动设备和汽车进行通信，由于缺少防攻击安全手段，这些接口同时也把有潜在威胁带入到智能汽车内。这些安全隐患连同汽车内部系统先天缺失的安全防范会引发一系列的汽车攻击。

1.4 美国汽车信息安全标准和法规

2016 年由 SAE（美国汽车工程师协会）制定的 J-3061 是全球第一个汽车信息安全标准。它和之前 ISO26262 标准的侧重点不同，主要是针对汽车网络安全。2016 年 1 月发布了 128 页的“Cybersecurity guidebook for Cyber-Physical Vehicle Systems”。这里的 Vehicle Systems 不仅仅是汽车，还包括和汽车有关的系统，例如车路协同，智能交通，辅助驾驶系统以及无人驾驶系统。

此标准的目的是提供汽车网络安全的指导框架，帮助使用者发现和评估网络攻击，并帮助使用者在物理整车和汽车整体设计流程中实施网络安全防护。如果在在已经量产或者现存车辆集成安全防护，有下面的局限性：

1. 没有预留的系统资源进行安全产品集成
2. 很难实现安全功能和汽车的完整集成
3. 由于缺少汽车制造周期全面地安全测试，可能会引进新的安全漏洞

因此，汽车安全的方案不是在汽车开发完成的时候再集成的，而是要贯穿在整个汽车设计的流程。

首先，汽车厂商需要不断总结、完善汽车平台的技术安全性，这需要厂商们建立一个共同探讨的平台，而不是将其视为“商业机密”而故步自封。

其次，第三方协作的引入是必要的，如网络安全公司、白帽黑客组织等，对车载系统的安全性进行广泛评估。

第三，及时进行安全更新，但汽车拥有其特殊性，这是目前的难点之一。最后，是否应该在汽车系统中加入关键区域的隔离措施，则是需要探讨的，因为这可能会影响一部分配件的市场。

总而言之，汽车入侵和黑客行为往往是致命的，这是与传统互联网攻击最大的不同，为了避免一切隐患和悲剧发生，汽车厂商和科技公司则应该加大研发力度，保障消费者的安全。

二、Auto-X 安全测试工具介绍与用途

2.1 介绍

图 4、Auto-X 安全测试工具

Auto-X 安全测试工具采用符合车联网信息安全测试标准的安全检测流程。客户可以方便定位其车型中存在的信息安全风险，结合对应的修复建议可以有效解决安全隐患。该测试平台系统能够优化车厂内部汽车网络安全测试流程，通过消化吸收的过程延伸出自主的技术体系，促进其提升车联网安全方面的国内外市场的整体竞争力。

2.2 主要用途

使用 AUTO-X 安全测试工具,客户可以方便快捷的定位其车型中存在的安全风险，结合对应的修复建议可以有效解决安全隐患，模拟攻击库，为测试厂商生成详细的安全风险分析报告，帮助汽车企业和

其供应商实现以下价值：

1. 对联网汽车进行信息安全分析，发现安全漏洞隐患，进行详细的安全级别分类和表述。
2. 能够可视化地展示汽车的安全状态和特定问题。通过对评测结果的有效处理，弥补产品开发和车联网安全框架之间的空白。
3. 促进了车厂电子电器部门、软件开发部门和其他部门之间的沟通和协作，有助于防止未经安全测试的应用程序给企业和应用使用客户带来风险。
4. 提供了车联网自动化安全扫描以及管理界面，方便企业客户定制符合自身需要的安全测试基线。
5. 协助整车厂通过实施信息安全测试流程，使他们拥有包括汽车网络安全测试在内的全面的汽车测试中心体系，通过消化吸收的过程延伸出自主的技术体系，促进其提升车联网安全方面的国内外市场的整体竞争力。

三、Auto-X 安全测试工具的特点与技术

3.1 Auto-X 安全测试工具的特点

1. Auto-X 安全测试工具备“即插即用、随时测试、自动流程”的特色。
2. 跨汽车生产平台，不依赖于汽车品牌和私有协议。
3. 适用于汽车内部全部的 CAN 网络信息安全测试。
4. 能够为汽车厂以及其供应商，构建分阶段、多层次信息安全测试体系。
5. 帮助汽车厂以及其供应商建立先进汽车信息安全测试流程，找到安全漏洞隐患，提升车载设备安全质量，缩减安全测试周期，填补了车厂和服务供应商信息安全测试产品的市场空白。

尽管目前已经开始了一些个别车型的破解研究，但仍然局限于破解者的技术背景，无法进行通用的标准测试流程。而且，受限测试人员的水平和测试环境，无法进行多车次并行测试但对于如何用通用的、流程化的、自动化的汽车信息安全测试方法目前仍是一个空白。

而随着人们将更多精细的服务和通信功能植入汽车，汽车内部信息安全测试的缺失将使攻击者获得丰富的攻击选择，他们可以入侵某个 ECU 部件，并借此潜入汽车内部网络，进而造成难以预知的后果。目前的汽车安全测试方法都没有深入到汽车内部系统中。我们的流程

全面评估车辆内部所有重要组件的安全防护属性。

本测试框架通过研究之前发生的各种汽车黑客攻击，全面地分析-了测试车辆内部网络，建立了全面的汽车测试漏洞库。为解决车联网信息安全测试数据的问题，需要从现实世界环境记录下攻击的输入数据，这些数据将在测试环境中使用。这有助于让测试环境尽可能与黑客攻击环境一致。我们的流程用真实的攻击数据进行安全测试，完全还原真实的攻击场景。

Auto-X 安全测试工具采用先进的汽车网络安全测试标准和流程，帮助使用者发现和评估网络攻击，并帮助使用者在物理整车和汽车整体设计流程中实施网络安全防护。显而易见，针对整车厂和其供应商。标准目的是提供汽车网络安全的指导框架，并帮助使用者在物理整车和汽车整体设计流程中实施网络安全防护。

此外，测试平台提供专业的安全报告管理平台，可以专业化地进行报告汇总和风险点分析，为车厂信息化建设提供一站式安全解决方案。

3.2 Auto-X 安全测试工具硬件参数和标准接口

- 外形尺寸：40.6*33*17.4
- 工作电压：9 V ~36V

- ❖ 工作温度：-30~75℃
- ❖ 工作电流：小于 500mA
- ❖ PC 接口符合 USB3.0 全速规范，兼容 USB1.1、USB2.0
- ❖ 支持 CAN2.0A 和 CAN2.0B 帧格式， 提供标准线束插头接口
- ❖ CAN-Bus 通讯波特率在 5Kbps~1Mbps 之间任意可编程与自适应

图 5、Auto-X 安全测试工具面板

3.4 Auto-X 安全测试工具配件

- ❖ OBD 接口连接线

标准 OBD2 公母口连接线，支持车内取电支持设备在无外接电源下正常工作，降低对测试环境的要求，提供测试环境的安全性。

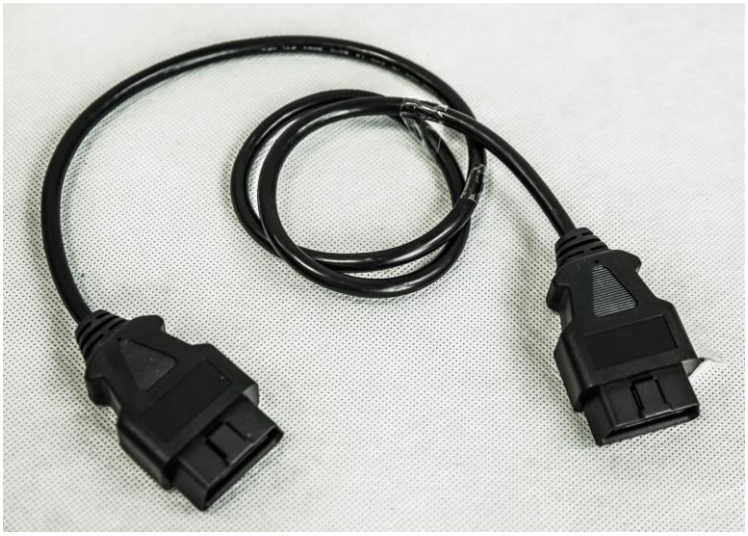

图 6、OBD 连接线

❖ USB 接口连接线

USB3.0 免驱动高速连接线，确保车内海量数据和设备的低延迟、高稳定性的数据传输和通信。

图 7、USB 连接线

❖ DIP 连接线

将标准的 OBD2 引脚串联到 CAN 高和 CAN 低的接口，无需引线和破线，即插即用，支持 125k、250k、500k、1000k 的多个

波特率普适性。

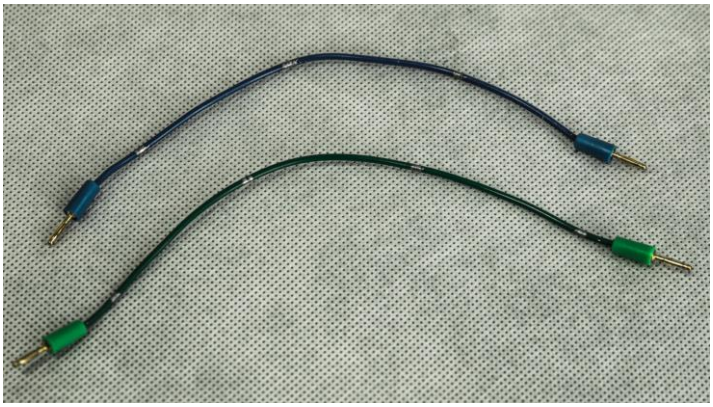

图 8、DIP 连线

❖ 电源线

支持在无汽车供电下的实验室环境测试，即插即用，也可支持多台测试设备同时对一辆汽车进行检测，提供检测的效率。

图 9、电源线

3.5 工作原理

图 10、AUTO-X 安全测试工具工作原理图

- ❖ 物理连接 Auto-X 安全测试工具到被测试设备。
- ❖ 启动测试应用服务，一键连接。
- ❖ 选择不同的测试场景进行测试。

3.6 软件的设计

3.6.1 模块化设计

整个测试环境的复杂功能和数据通讯交互设计成灵活的模块化功能，包括但不局限于以下：

- ✓ 模拟攻击库模块
- ✓ 数据收发模块
- ✓ 流量收集模块
- ✓ 日志分析模块

- ✓ 日志压缩和分布式存储
- ✓ 流量重放模块
- ✓ 报告生成和导出模块
- ✓ 第三方应用标准接口
- ✓ 文件和流量导入模块

3.6.2 标准接口调用

每个模块定制标准的 API 接口，方便内部和外部的统一格式调用，提升软件的拓展性和稳定性。

支持的语言有 Python、Java、C 等。

提供标准的第三方接口，支持多语言程序的调试和调用。

3.6.3 可视化的 Web 管理界面

应用操作界面简洁方便，只需要几次鼠标点击便可选择不同的检测场景和攻击库的调用。

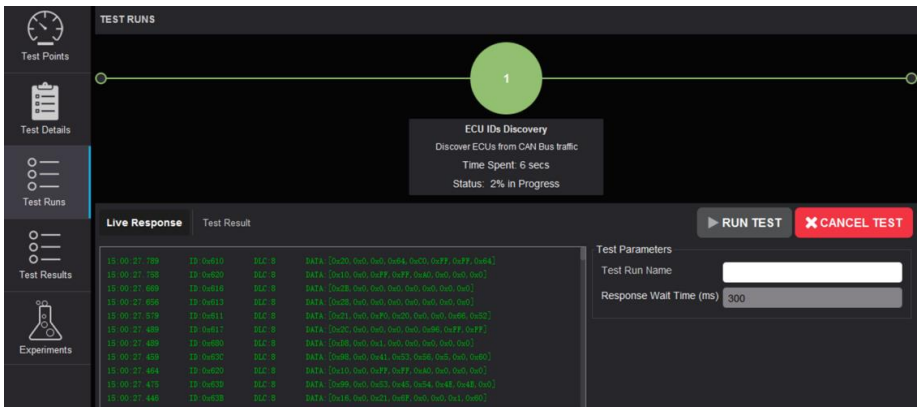

图 11、应用界面

3.6.4 数据的导入和导出

测试设备支持对数据或者文件的的批量导出和导入。

通过对外部文件的批量导入，结合标准第三方的 API 接口，可以实现对被测试设备的外部流量的批量注入测试。

四、Auto-X 安全测试工具测试功能矩阵

4.1 Auto-X 安全测试工具测试范围

Auto-X 安全测试工具车联网安全测试主要针对于五个方面的产品：

1. 整车，包括动力系统、娱乐系统、诊断系统等。
2. 汽车研发过程中的台架
3. T-BOX、网关或者 IVI 设备等车内重要 ECU 通讯节点
4. 其他 ECU 设备
5. 无人驾驶、车路协同、ADAS 和智能交通设备等

4.2 功能矩阵

4.2.1 车载终端内部网络拓扑测试

主要针对汽车内部总线设计的方法，评估其设计的安全性。汽车内部总线，拓扑结构的设计，直接影响到汽车的信息安全性。一个设计优良的网段隔离策略，能够有效的抵御黑客的入侵攻击。对于任何汽车 CAN 总线系统来说，均可根据其对输出信号的响应情况，以及全面了解整车内部电器拓扑结构。

汽车拓扑结构测试采用黑盒测试，旨在清楚地掌握正在运行的 ECU 的情况，通过车内 CAN 网络的流量采集和分析，了解到所有正在运行的 ECU 服务，并根据拓扑结构判断汽车可能存在的安全隐患。

一级测试点(可再细分)

- ✓ CAN 拓扑安全性

- ✓ 诊断包嗅探
- ✓ 软件安全标准
- ✓ ECU 测试
- ✓ CAN 总线嗅探
- ✓ 网段隔离安全性
- ✓ 安全优先级测试
- ✓ 协议逆向难度
- ✓ 拓扑结构逆向
- ✓ OBD 端口安全性

4.2.2 单点 ECU 测试

验测试车辆 CAN 网络中的单个组件，确定通过其进行通信，攻击者可能达到哪些目的。针对每一个发现 ECU，通过流量采集，并进行深入分析。通过测试矩阵，测试预先定义的各个测试点，触发各种应用场景，收集结果日志，基于日志进行整理分析统计，从而发现可能的潜在威胁。

一级测试点(可再细分)

- ✓ ECU 安全访问权限
- ✓ 拒绝服务
- ✓ ECU 保护性测试
- ✓ 模糊化测试

4.2.3 ECU 组合攻击测试

汽车的很多功能的实现都需要多个 ECU 进行复杂的配合。然而，迫于上市时间的压力、线路连接成本和功能协调配合的复杂性，以及进一步完善需要付出的经济成本，汽车制造商没有对 ECU 相互配合通信做必要的安全监测，并且有越来越多的制造厂商开始将其整合成能够访问外部网络的应用程序软件平台。ECU 组合通信的安全漏洞是危害最大的。

一级测试点(可再细分)

- ✓ ECU 数据篡改
- ✓ ECU 更新安全性
- ✓ ECU 权限提升
- ✓ ECU 欺骗
- ✓ ECU 暴力破解
- ✓ ECU 协议标准
- ✓ ECU 间通信安全
- ✓ 电池系统测试
- ✓ 协议不正当使用
- ✓ 模块更新欺骗

4.2.4 安全等级定义

1. 非常严重

车辆无法启动，ECU 之间通信失效，CAN 网络遭到严重。

破坏

2. 中等严重

车辆可以启动，但是导致部分功能失效，影响驾驶员正常驾驶，引发潜在事故。

3. 非严重

部分非关键汽车功能出现障碍。

4.3 数据分析和报告导出

工具对车载网络内部海量的实时数据进行了有效的分类和去噪，大大简化了对数据的分析效率和可视化支持。应用程序界面提供数据分析图表、检测进度条、实时的数据采集、以及最后的测试结果和报告。

日志存储和分析功能也提供和报告的导出和导入，支持 txt、vsc、word、pdf 等格式。

4.4 远程通信接口

工具内部集成了 WI-FI、蓝牙和 2G 的无线通信模块，除了通过 OBD2 和 USB 物理直连的高速数据传输，还支持远程指令的收、发功能。

工具的标准接口也支持对外部 WI-FI、蓝牙设备的连接和指令收发，具有高度的延展性。

五、Auto-X 安全测试工具的性能

对汽车进行全面网络信息安全检测是一个全面而又漫长的过程，通常需要 1-2 周的时间。目前主流车辆的 ECU 都有几十甚至上百个，每个 ECU 都是独立运行、交叉工作的行车电脑，网络内部每秒钟都会产生海量的数据，每个独立的网络甚至单个 ECU 的检测工作就需要几个小时连续不中断的过程，这就让 Auto-X 安全测试工具具备了以下性能要求：

1. 海量数量的实时处理 - 支持数据收集、压缩、分析和重放功能
2. 消息的响应率 - 丢包率几乎为 0。
3. 低延迟 - 工具和被测试设备之间的数据传输响应时间等级在 40-60 毫秒级别，实现实时的响应。
4. 高稳定性 - 单个测试点实现 24 小时以上的不中断的连续测试，满足对车在应用设备的高强度和连续性要求。
5. 高拓展性 - 标准虚拟攻击库可以随时更新，系统支持第三方的标准 API 接口，便于定制开发和其他系统的集成交互。
6. 高集成性 - 系统的高度模块化和标准 API 对其他系统做标准数据输入和导入。
7. 高安全性 - 可定制的离线单机版本可以更好的保护用户的数据隐私，系统采用 http 和 http ssl 通信安全或加密、

数据传输速率和同步通信机制。

8. 高同步性 - 一个 OBD2 标准接口和两路 CAN 可支持对汽车多个节点同时进行多个功能点的串行检测，结合软件的灵活配置功能，可以通过任务调度功能实现 5 个以上测试点的连续执行。
9. 高兼容性 - 应用于不同品牌的车辆，对车辆的生产平台、私有协议定义均不依赖，具有高度的兼容和统一性。

六、Auto-X 安全测试工具的测试部署示意图

6.1 Auto-X 安全测试工具在真车环境下的部署

Auto-X 安全测试工具自带一个标准 OBD 接口，可用于将工具与汽车 OBD 口连接，无需使用外接电源。

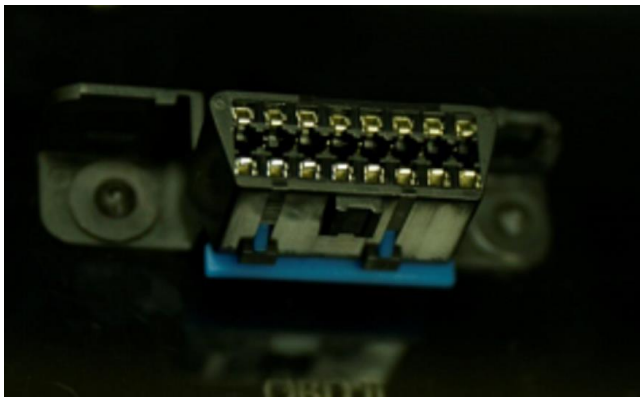

图 12、OBD2 接口

如果需要测试其他 CAN 网段，则需要将 CAN 总线引出并连接到 Auto-X 安全测试工具的 CAN 端口上进行测试。

图 13、两路 CAN 接口

图 14 是在真实汽车内使用 Auto-X 安全测试工具搭建的真实测试环境，操作便捷，充分利用车内现有 CAN 总线标准接口，搭配 Auto-X

安全测试工具人性化设计的丰富标准接口，即插即用。

图 14、真车上搭建 Auto-X 安全测试工具测试环境

OBD 双向连接线，一端连接 Auto-X 安全测试工具，另外一端和汽车的 OBD 端口相连。

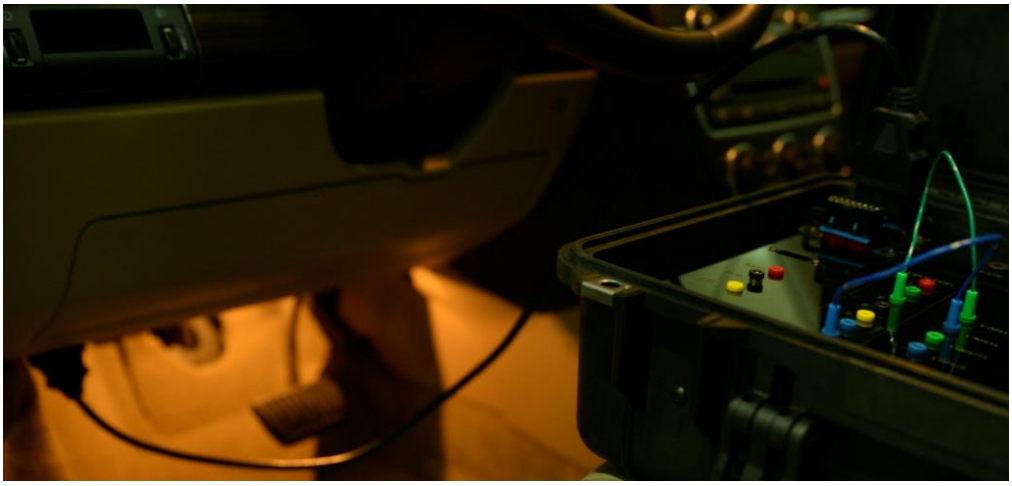

图 15、工具与汽车连接

USB 双向线连接计算机和 Auto-X 安全测试工具。

图 16、工具与计算机连接

图 17、正在车内工作的 Auto-X 安全测试工具

6.2 实验室环境部署

如图 18 所示，左边是一个 CAN 总线模拟设备，连接时只需要将各自的 OBD 接口相互连接即可。

图 18、Auto-X 安全测试工具连接 CAN 总线模拟节点

CAN 节点之间互连，用户根据自己的需要进行 HS CAN 和 MS CAN 的连接。

Auto-X 安全测试工具可同时支持两路 CAN。

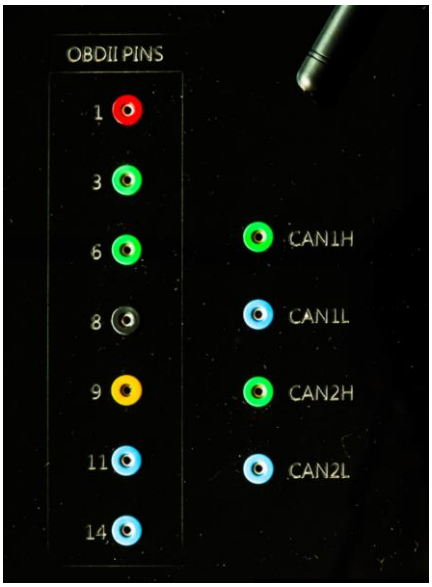

图 19、Auto-X 安全测试工具的 OBD 引脚和 CAN 端口

通过两根 DIP 连接线连接 引脚，将汽车的 CAN 网络与 Auto-X 安全测试工具进行连接。

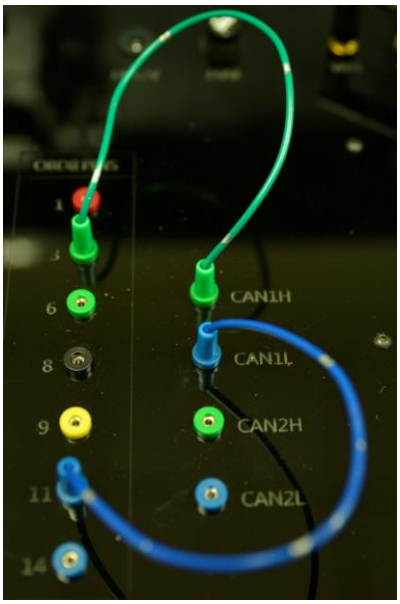

图 20、DIP 连线 CAN 连接图

图 21、通过 USB 接口连接 Auto-X 安全测试工具