情报驱动的智能网联车攻击面管理解决方案

万会来　沈传宝　郝　伟　张晶晶　刘仟丰
(北京华云安信息技术有限公司　北京　100094)
(wanhl@huaun.com)

摘　要　以华云安攻击面管理产品为支撑,结合汽车漏洞情报处理能力,构建情报驱动的智能网联车攻击面管理解决方案.云端由华云安汽车漏洞情报中心推送高价值汽车情报数据,落地车企本地端部署的智能汽车漏洞与攻击面管理中心,实现车辆部件资产、漏洞一体化管理,同时还提供智能汽车漏洞与攻击面检测的安全工具与服务,涵盖智能网联车攻击面管理的攻击面检测、攻击面分析、攻击面验证、漏洞情报预警、漏洞修复、漏洞态势感知6大维度.

关键词　智能网联车;攻击面管理;漏洞情报;资产部件管理;匹配关联

中图法分类号　TP393.08

1　方案背景

随着新四化的快速发展,车内功能大幅增加,软件代码急剧增长,存在大量安全漏洞隐患[1].另一方面,汽车与外界连接逐渐增多,攻击面随之增长,在智能化背景下,全球主机厂无一幸免,奔驰、宝马、奥迪等国际一线品牌,均遭受了不同程度的安全攻击.汽车网络攻击可能直接造成人员伤亡,因此比传统网络安全更加敏感和重要[2-3].

情报驱动的智能网联车攻击面管理解决方案以华云安汽车漏洞情报中心为核心能力支撑,向车企实时推送汽车漏洞情报,车企通过本地端智能汽车漏洞与攻击面管理中心接收汽车漏洞情报.同时,方案能够通过资产部件录入、Bom文件导入等多种方式对智能汽车整车及零部件包括T-BOX、IVI、OBD、CAN总线、ECU等资产部件进行管理,将漏洞情报和资产部件自动化分析,实现当前漏洞受影响资产部件匹配关联,以及实时告警信息提示等功能.

2　解决方案介绍

2.1　方案意义

华云安创新地将汽车漏洞挖掘能力和攻击面检测能力通过情报方式赋能主机厂、零部件厂商、VSOC厂商等,重点解决以下6大痛点:

1)汽车部件资产众多、统计不全.

汽车涉及的控制系统、娱乐系统、电子钥匙系统、无线通信系统、蓝牙系统等,与传统IT资产有明显差别,对这些相关资产梳理不足无法全面掌握.

2)漏洞数据少、漏洞情报获取难.

汽车行业网络安全人才不足,漏洞数据极为欠缺,分析深度有限,无法从公开渠道获取车端有价值的数据,漏洞情报获取渠道较少,信息收集不健全,导致对安全事件的后知后觉.

3)漏洞验证时间长、成本高.

汽车资产部件结构复杂,形式多样,在漏洞验证过程中使成本大幅提高,并且验证周期普遍较长,加大了漏洞带来的损失.

收稿日期:2022-08-15
引用格式:万会来,沈传宝,郝伟,等.情报驱动的智能网联车攻击面管理解决方案[J].信息安全研究,2022,8(增刊):56-59

4）漏洞难定位、无法判断漏洞影响.

当某个攻击事件发生时，往往伴随着多个攻击向量，涉及到汽车的多种部件，由于关系的复杂性，漏洞往往无法与汽车资产直接相关联，难以确定漏洞的影响范围.

5）无法预判潜在威胁.

媒体往往会爆出各种各样关于智能网联车的攻击事件，这类信息往往是为了吸引眼球而夸大其词不够具体，导致车厂/主机厂、用户都无法判断自己是否会受到威胁.

6）漏洞修复机制匮乏.

当检测到重大漏洞时，无论是主机厂、还是整车厂，都没有完整的漏洞修复流程，修复也难以跟踪和 2 次验证，流程未实现闭环.

2.2 主要目标

通过构建强大的汽车漏洞情报中心，帮助车厂/主机厂解决漏洞情报获取不全的问题；具备部件管理功能，帮助车厂/主机厂梳理核心资产，发现自身弱点，建立覆盖全车型的数字资产信息库；以攻击者视角对汽车各部件和模块进行合规性检测和定向的漏洞挖掘，检测完整的攻击面；结合车厂和主机厂本地部署的智能汽车漏洞与攻击面管理中心与公司云端的汽车漏洞情报中心进行数据交互，通过指纹将情报自动匹配到汽车资产，形成资产的告警信息；分析告警信息在攻击路径中的位置、威胁程度、影响等指标，评定告警处置的优先级；最后建立完整和开放式的流转体系，将技术和流程打通，从而完成对告警的验证和漏洞修复.

实现情报、平台、服务一体化，将情报的价值赋能到攻击面管理的过程中，充分有效地利用情报快速响应，防患于未然.

3 解决方案

3.1 架构原理图

方案主体架构以华云安汽车漏洞情报中心为核心能力支撑，通过基于自然语言处理、大数据、人工智能[4-5]等分析技术，针对大数据监控的车辆系统特征，向车企实时推送汽车漏洞情报，并对重要敏感信息发出预警.

方案架构原理如图 1 所示：

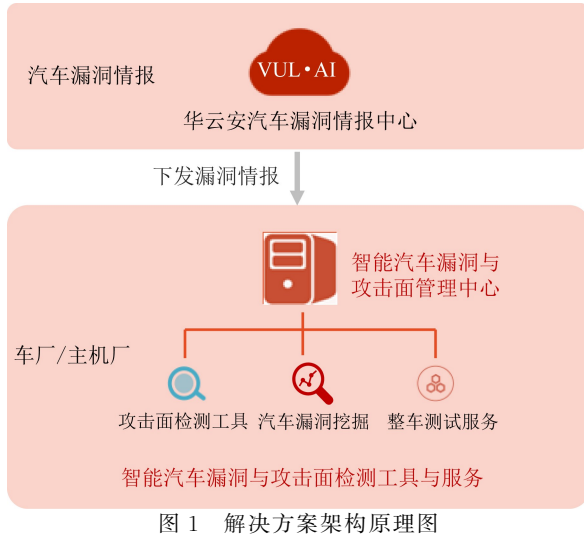

图 1 解决方案架构原理图

车厂/主机厂通过建立智能汽车与漏洞攻击面管理中心，实现与华云安云端汽车漏洞情报中心进行数据交互，同时华云安为车企提供攻击面检测、汽车车载系统漏洞挖掘和整车测试服务，通过对资产部件进行自动化分析，以及漏洞受影响资产部件的自动化匹配与关联，实现重要汽车信息的实时告警提示功能.

方案能够实现智能网联车攻击面闭环管理功能，覆盖攻击面检测、攻击面分析、攻击面验证、漏洞情报预警、漏洞修复、漏洞态势感知 6 大维度.

3.2 详细设计

3.2.1 资产部件管理

智能汽车漏洞与攻击面管理中心通过资产部件录入、Bom 文件导入等多种方式，实现对智能网联车资产部件进行管理.如在无钥匙进入系统中主要包括对以下内容的管理.

蓝牙：协议版本、固件更新的方式、固件混淆、调试口和 flash.

NFC：钥匙卡的密码算法、随机数产生方式、认证中的时间机制.

RF：信号是否相同、信道抗干扰.

3.2.2 攻击面检测

以漏洞挖掘、安全检测、整车测试等多种技术方式，最大化发现智能网联车存在的攻击面.

漏洞挖掘：根据具体网联车整车和主机厂商的需求，华云安网联车团队进行定向的漏洞挖掘和安全分析服务，并以情报的方式赋能管理平台.

安全检测：对智能汽车各部件和模块进行漏洞攻击面检测，包括单次检测、周期性检测及漏洞情报检测.

整车测试：根据具体网联车整车和主机厂商的需求，华云安网联车团队进行整车安全测试和分析服务.

3.2.3 攻击面分析

对于智能网联车漏洞，以汽车行业漏洞分级方法为参照，更加关注车辆漏洞被利用后遭受的危害程度，分析维度包括场景参数、威胁参数、影响参数 3 大维度.

3.2.4 攻击面验证

针对接收到的漏洞情报，华云安能够提供漏洞真实性验证，对于云端的云平台服务器、APP 方面的漏洞提供自动化验证工具以及匹配的 PoC 验证插件更新；对于车端的 IVI、T-BOX、无钥匙进入系统、OBD 诊断系统等漏洞提供验证脚本、说明文档，辅助主机厂人员人工验证.

3.2.5 汽车漏洞情报

华云安汽车漏洞情报中心的漏洞来源包括外部和内部 2 种途径，外部漏洞数据源通过自动化采集国家级漏洞库、在野漏洞、汽车安全会议论坛、汽车黑客及移动安全黑客博客相关漏洞；内部漏洞主要通过华云安智能网联车研究团队定向挖掘、整车测试以及汽车行业漏洞库进行数据整合.

汽车漏洞情报中心核心功能是将通用漏洞转化为车联网漏洞，将通用漏洞描述，依靠自然语言处理技术，提取出关键词，结合对智能汽车安全研究能力及汽车部件资产经验积累，实现对通用漏洞的过滤与转化.

3.2.6 漏洞态势感知

结合大数据 AI 技术、数据关联分析技术、可视化展示技术等，可以全场景展示资产态势、漏洞态势、安全态势等.

资产态势：收集展示不同厂商、不同类型设备、不同协议标准的海量各类被监控系统或设备信息.

漏洞态势：漏洞的级别统计、分类统计、地理区域漏洞发生和处理情况、资产漏洞发生和处理情况等.

安全态势：地理区域内资产统计、漏洞统计、已处置及未外置漏洞统计、整体安全态势等.

4 创新先进性技术

4.1 基于 NLP 的汽车漏洞实时分析技术

通过多种消息渠道对已公开的车辆相关的漏洞情报信息的进行收集汇总，并针对车载系统、应用软件、漏洞、补丁、厂商等相关信息，使用公司自研的基于 NLP 的语义分析与提取技术，实现高效的漏洞核心信息过滤与转换能力，形成精准有效的汽车漏洞情报，并在第一时间向车企和主机厂下发，从而实现用户对最新汽车漏洞情报的快速精准地掌握和利用的能力.

4.2 自动化汽车漏洞情报与资产部件分析技术

依托公司自研的知识图谱关联分析技术，利用 NLP 提取和分析的主体及关系，实现汽车漏洞情报与汽车资产部件关系的自动化建立，并通过关联信息分析，实现对漏洞影响的汽车资产部件的报警.同时在此基础上，通过图谱化的数据分析技术，对数据进行深度分析与挖掘，预测可能存在的漏洞问题，并将预测结果实时地向智能汽车漏洞与攻击面管理中心报告.

4.3 智能化汽车漏洞危害评价方法

构建了一套基于强化学习的多项加权漏洞危险性评估方法.通过本方法，能够根据用户人群评价进行动态迭代改进，并通过平台＋服务＋反馈的方式，在向用户提供一体化漏洞评价服务的同时，结合用户主动提交的漏洞危险性评价，实现随时间动态更新的漏洞危险性指数，并根据指数提供有针对性的专业漏洞修复服务.同时，能够对监测中发现的汽车安全漏洞进行整改修复，从而能够有效降低受到各类攻击的可能性.

5 应用场景

5.1 全车型信息化部件的资产台账管理

以车型为单元对车型下具体汽车整车及零部件组成的相关信息化资产进行管理，包括 T-BOX、IVI、OBD、CAN 总线、ECU、网关、域控制器等资产部件进行识别，构建资产台账.全面的资产清点并识别完整的资产暴露面，才能从暴露的资产中找到可能被攻击者利用的攻击面，防患于未然.

5.2 高价值汽车漏洞情报推送

解决当前汽车行业漏洞情报匮乏，无法从漏

洞管理中得到有价值的数据的难题，通过丰富的采集渠道，深入的行业研究，对通用漏洞进行过滤与转化，为车企输出高价值汽车漏洞情报数据，使其具备先于攻击者发现弱点和威胁的能力，并采取针对性的主动防御措施，极大缩短车企自身风险暴露时间，先于攻击者修复漏洞，预防入侵事件的发生.

5.3 汽车部件漏洞及时发现

结合汽车情报推送服务及本地化部署的智能汽车漏洞与攻击面管理中心中全系车型信息化部件台账信息，自动化匹配关联，通过图谱化的数据深度分析，对可能存在的漏洞问题进行预测，提供受影响部件告警信息，为快速响应处置提供决策支撑.

6 总　　结

本文主要以攻击者视角对智能网联车的安全进行全面分析，创新地将智能网联车的漏洞挖掘能力、攻击面检测能力通过情报方式赋能车厂、智能网联车安全方案供应商，是针对智能网联车当前安全形势下最具落地和实践推广的攻击面管理解决方案.

参　考　文　献

[1] 薛世豪，宁玉桥，于明明，等. 智能网联汽车漏洞管理实践探索[J]. 汽车实用技术，2022，3(1)：34-37

[2] 郭文佳，周千荷，李立雪. 汽车网络安全路在何方[J]. 智能网联汽车，2022，2(1)：49-51

[3] 赵文博. 软件不能成为智能网联汽车“软肋”[J]. 智能网联汽车，2022，1(1)：22-23

[4] 张建国，袁建华. 汽车人工智能技术的发展现状及展望[J]. 道路交通科学技术，2018，5(1)：3-5

[5] 赵新勇，李珊珊，夏晓敬. 大数据时代新技术在智能交通中的应用[J]. 交通运输研究，2017，5(1)：1-7

万会来

工程师.主要研究方向为攻击面管理相关技术及车联网场景安全防护体系.

wanhl@huaun.com

沈传宝

硕士，国家漏洞库特聘专家.主要研究方向为国家级漏洞资源管控及共享标准、体系、机制.

shencb@huaun.com

郝　伟

博士，副研究员.主要研究方向为人工智能技术在网络安全中的应用.

haowei@huaun.com

张晶晶

安全研究员.主要研究方向为车联网硬件安全和通信安全.

zhangjj@huaun.com

刘仟丰

安全研究员.主要研究方向为车联网无线安全、Web 安全.

liuqf@huaun.com