ICS 43.020
CCS T 40

中华人民共和国国家标准

GB/T 40857—2021

汽车网关信息安全技术要求及试验方法

Technical requirements and test methods for cybersecurity of vehicle gateway

2021-10-11 发布　　2022-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会(SAC/TC 114)归口。

本文件起草单位：广州汽车集团股份有限公司、中国汽车技术研究中心有限公司、泛亚汽车技术中心有限公司、上海汽车集团股份有限公司技术中心、北京汽车研究总院有限公司、戴姆勒大中华区投资有限公司、吉利汽车研究院(宁波)有限公司、东软集团股份有限公司、重庆长安汽车股份有限公司、东风汽车集团股份有限公司技术中心、交通运输部公路科学研究院。

本文件主要起草人：尚进、孙航、顾吉杰、李宝田、冯海涛、费枭、陈新、吕明、杨成浩、陈静相、贺可勋、何文、程周、刘智超。

汽车网关信息安全技术要求及试验方法

1 范围

本文件规定了汽车网关产品硬件、通信、固件、数据的信息安全技术要求及试验方法。

本文件适用于汽车网关产品信息安全的设计与实现，也可用于产品测试、评估和管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069 信息安全技术 术语

GB/T 37935—2019 信息安全技术 可信计算规范 可信软件基

GB/T 40861 汽车信息安全通用技术要求

3 术语和定义

GB/T 25069、GB/T 37935—2019、GB/T 40861 界定的以及下列术语和定义适用于本文件。

3.1

汽车网关 vehicle gateway

主要功能为安全可靠地在车辆内的多个网络间进行数据转发和传输的电子控制单元。

注 1：汽车网关通过不同网络间的隔离和不同通信协议间的转换，可以在各个共享通信数据的功能域之间进行信息交互。

注 2：汽车网关也称中央网关。

3.2

后门 backdoor

能够绕过系统认证等安全机制的管控而进入信息系统的通道。

[来源：GB/T 40861—2021，3.12]

3.3

可信根实体 entity of root of trust

用于支撑可信计算平台信任链建立和传递的可对外提供完整性度量、安全存储、密码计算等服务的功能模块。

注：可信根实体包括 TPCM、TCM、TPM 等。

[来源：GB/T 37935—2019，3.12]

4 缩略语

下列缩略语适用于本文件。

ACL 访问控制列表(Access Control Lists)

ARP 地址解析协议(Address Resolution Protocol)

CAN	控制器局域网络(Controller Area Network)
CAN-FD	灵活数据速率的控制器局域网络(CAN with Flexible Data-rate)
DLC	数据长度码(Data Length Code)
DoS	拒绝服务(Denial of Service)
ECU	电子控制单元(Electronic Control Unit)
ICMP	网际控制报文协议(Internet Control Message Protocol)
ID	标识符(Identifier)
IP	网际互连协议(Internet Protocol)
JTAG	联合测试工作组(Joint Test Action Group)
LIN	局域互联网络(Local Interconnect Network)
MAC	媒体访问控制(Media Access Control)
MOST	面向媒体的串列传输(Media Oriented System Transport)
OBD	车载诊断 (On-Board Diagnostics)
PCB	印制电路板(Printed Circuit Board)
SPI	串行外设接口(Serial Peripheral Interface)
SYN	同步序列编号(Synchronize Sequence Numbers)
TCP	传输控制协议(Transmission Control Protocol)
TCM	可信密码模块(Trusted Cryptography Module)
TPCM	可信平台控制模块(Trusted Platform Control Module)
TPM	可信平台模块(Trusted Platform Module)
UART	通用异步收发器(Universal Asynchronous Receiver/Transmitter)
UDP	用户数据报协议(User Datagram Protocol)
UDS	统一诊断服务(Unified Diagnostic Services)
USB	通用串行总线(Universal Serial Bus)
VLAN	虚拟局域网(Virtual Local Area Network)

5 汽车网关网络拓扑结构

5.1 CAN 网关

基于 CAN 和/或 CAN-FD 总线的车内网络结构中,大多数的 ECU、域控制器之间都会通过 CAN 和/或 CAN-FD 总线进行通信。

这类结构中的汽车网关主要有 CAN 和/或 CAN-FD 总线接口,可称为 CAN 网关。

典型的 CAN 网关拓扑结构见附录 A 中图 A.1。

5.2 以太网网关

基于以太网的车内网络结构中,大多数的 ECU、域控制器之间会通过以太网进行通信。

这类结构中的汽车网关主要有以太网接口,可称为以太网网关。

典型的以太网网关拓扑结构见图 A.2。

5.3 混合网关

部分新一代车内网络结构中,一部分 ECU、域控制器之间通过以太网通信,而另一部分 ECU、域控制器之间仍通过传统通信协议(例如:CAN、CAN-FD、LIN、MOST 等)通信。

这类结构中的汽车网关既有以太网接口,还有传统通信协议接口,可称为混合网关。

典型的混合网关拓扑结构见图 A.3。

附录 B 中举例列出了针对汽车网关和车内网络通信的部分典型攻击。

6 技术要求

6.1 硬件信息安全要求

6.1.1 按照 7.1 a)进行试验,网关不应存在后门或隐蔽接口。

6.1.2 按照 7.1 b)进行试验,网关的调试接口应禁用或设置安全访问控制。

6.2 通信信息安全要求

6.2.1 CAN 网关通信信息安全要求

6.2.1.1 访问控制

网关应在各路 CAN 网络间建立通信矩阵,并建立基于 CAN 数据帧标识符(CAN ID)的访问控制策略,按照 7.2.1 a)进行试验后,应在列表指定的目的端口检测接收到源端口发送的数据帧;按照 7.2.1 b)进行试验后,应对不符合定义的数据帧进行丢弃或者记录日志。

6.2.1.2 拒绝服务攻击检测

网关应对车辆对外通信接口的 CAN 通道(例如:连接 OBD-II 端口的通道和连接车载信息交互系统的通道)进行 CAN 总线 DoS 攻击检测。

网关应具备基于 CAN 总线接口负载的 DoS 攻击检测功能,宜具备基于某个或多个 CAN ID 数据帧周期的 DoS 攻击检测功能。

按照 7.2.1 c)、d)进行试验,当网关检测到某一路或多路 CAN 通道存在 DoS 攻击时,应满足以下要求:

a) 网关未受攻击的 CAN 通道的通信功能和预先设定的性能不应受影响;

b) 网关对检测到的攻击数据帧进行丢弃或者记录日志。

6.2.1.3 数据帧健康检测

网关宜根据通信矩阵中的信号定义,对数据帧进行检查,检查内容包括 DLC 字段、信号值有效性等,按照 7.2.1 e)、f)进行试验,对不符合通信矩阵定义的数据帧进行丢弃或者记录日志。

6.2.1.4 数据帧异常检测

网关宜具有数据帧异常检测功能,即检查和记录数据帧之间发送与接收关系的机制,按照 7.2.1 g)进行试验,对检测到异常的数据帧进行丢弃或者记录日志。

示例:

网关检测到一定时间内数据帧的发送频率与预定义的频率差距较大,或相邻时间同一数据帧的信号值内容冲突或者不正常跳跃时,对数据帧进行丢弃或者记录日志。

6.2.1.5 UDS 会话检测

网关应检查 UDS 会话发起的 CAN 通道是否正常,按照 7.2.1 h)进行试验,对非正常通道发起的会话进行拦截或者记录日志。

注: 正常通道通常包括连接 OBD-II 端口的通道和连接车载信息交互系统的通道。

6.2.2 以太网网关通信信息安全要求

6.2.2.1 网络分域

网关应支持网络分域，按照 7.2.2 a)进行试验，对不符合网络分域的数据包进行丢弃。

示例：用 VLAN 分隔车载网络内的不同域。

6.2.2.2 访问控制

网关应配置访问控制列表（ACL），访问控制列表中的访问控制要素主要应包括源 IP 地址、目的 IP 地址、协议类型（例如 TCP、UDP、ICMP 等）、协议源端口、协议目的端口，也可包括物理端口、通信方向（输入或输出）、源 MAC 地址、目的 MAC 地址等。

访问控制列表应遵循默认拒绝原则，即丢弃所有不符合条件的数据包。

访问控制列表应遵循最小化授权原则，即只授予必要的权限。

按照 7.2.2 b)、c)进行试验，对不符合访问控制列表的数据包进行丢弃或者记录日志。

6.2.2.3 拒绝服务攻击检测

网关应对车辆对外通信的以太网通道进行以太网 DoS 攻击检测。支持 ICMP 协议、TCP 协议和 UDP 协议的网关，检测的 DoS 攻击类型，应分别至少包括 ICMP 泛洪攻击、TCP 泛洪攻击和 UDP 泛洪攻击。

按照 7.2.2 d)进行试验，当网关检测到以太网 DoS 攻击时，应确保自身正常的功能和预先设定的性能不受影响，并对检测到的攻击数据包进行丢弃或者记录日志。

6.2.2.4 协议状态检测

网关宜具有对部分或全部的 TCP/IP 会话流进行状态检查的功能。检查项包括 TCP 握手状态、数据包长度、包序列和 TCP 会话关闭状态等，按照 7.2.2 e)进行试验，对检测到的攻击数据包进行丢弃或者记录日志。

6.2.3 混合网关通信信息安全要求

对于混合网关，CAN 通信和以太网通信的信息安全要求应分别符合 6.2.1 和 6.2.2 的规定。

6.3 固件信息安全要求

6.3.1 安全启动

网关应具备安全启动的功能，可通过可信根实体对安全启动所使用的可信根进行保护。按照 7.3 a)、b)、c)进行试验，网关的可信根、Bootloader 程序及系统固件不应被篡改，或被篡改后网关无法正常启动。

6.3.2 安全日志

如网关具有安全日志功能，则满足如下要求：

a) 按照 7.3 d)、e)、f)进行试验，当网关探测到不符合 6.2 要求的通信、网关发生软件配置变更、网关软件完整性校验失败等各类事件时，应对相关信息进行记录；

b) 按照 7.3 g)进行试验，网关的安全日志中，应至少包括触发日志的事件发生时间（绝对时间或相对时间）、事件类型和车辆唯一标识码；

c) 按照 7.3 h)进行试验，网关应对安全日志进行安全存储，防止非物理破坏攻击情况下日志记录

的损毁，同时防止未授权的添加、访问、修改和删除，安全日志记录存储的位置可在网关内、其他 ECU 内或云端服务器内；

d) 按照 7.3 i)进行试验，网关的安全日志中，不应包含任何形式的个人信息。

6.3.3 安全漏洞

按照 7.3 j)进行试验，网关不应存在权威漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞。

注：处置包括消除漏洞、制定减缓措施等方式。

6.4 数据信息安全要求

网关中的安全重要参数应以安全的方式存储和处理，防止未经授权的访问、修改、删除和检索。按照 7.4 进行试验，网关内的安全区域或安全模块不被未经授权的破解、读取和写入。可通过使用提供适当授权程序的安全区域、安全模块或等效安全技术来实现。

7 试验方法

7.1 硬件信息安全试验

网关硬件信息安全试验按照下列流程及要求依次进行：

a) 拆解被测样件设备外壳，取出 PCB 板，检查 PCB 板硬件是否存在后门或隐蔽接口；

b) 检查是否有存在暴露在 PCB 板上的 JTAG、USB、UART、SPI 等调试接口，如存在则使用试验工具尝试获取调试权限。

7.2 通信信息安全试验

7.2.1 CAN 网关通信信息安全试验

CAN 网关通信信息安全试验按照下列流程及要求依次进行。

a) 设置 6.2.1.1 所规定的访问控制策略(若被测样件的访问控制策略无法通过软件配置修改，则由送样方提供已预置的访问控制策略列表)，检测设备向列表指定的源端口发送符合策略规定的数据帧，并在列表指定的目的端口检测接收数据帧。

b) 设置 6.2.1.1 所规定的访问控制策略(若被测样件的访问控制策略无法通过软件配置修改，则由送样方提供已预置的访问控制策略列表)，检测设备向列表指定的源端口发送不符合策略规定的数据帧，在列表指定的目的端口检测接收到的数据帧，并收集样件日志。

c) 由送样方确认网关连接车辆对外通信接口的 CAN 通道，检测设备对此通道以大于 80％总线负载率发送符合通信矩阵的泛洪攻击数据帧，在指定的目的端口检测接收到的数据帧，并收集样件日志。如果有多个此类通道，则依次分别试验。

d) 由送样方确认网关连接车辆对外通信接口的 CAN 通道，检测设备对此通道以 1 ms 为周期，发送符合通信矩阵的某个 CAN ID 数据帧，在指定的目的端口检测接收到的数据帧，并收集样件日志。如果有多个此类通道，则依次分别试验。

e) 检测设备对网关发送一个或多个 DCL 字段值不符合通信矩阵定义的数据帧，在指定的目的端口检测接收到的数据帧，并收集样件日志。

f) 检测设备对网关发送一个或多个信号值不符合通信矩阵定义的数据帧，在指定的目的端口检测接收到的数据帧，并收集样件日志。

g) 检测设备对网关连续发送一个或多个周期不符合通信矩阵定义(与定义周期偏差±50％)的周

期型数据帧，在指定的目的端口检测接收到的数据帧，并收集样件日志。如果有多个此类通道，则依次分别试验。

h) 由送样方确认网关连接 OBD-II 端口的通道和连接车载信息交互系统的通道，检测设备对除此类通道以外的通道，发送 UDS 诊断数据帧，在指定的目的端口检测接收到的数据帧，并收集样件日志。如果有多个此类通道，则依次分别试验。

7.2.2 以太网网关通信信息安全试验

以太网网关通信信息安全试验按照下列流程及要求依次进行：

a) 对被测样件设置不同网络分域(如 VLAN 1 与 VLAN 2)(若被测样件的网络分域策略无法通过软件配置修改，则由送样方提供已预置的网络分域策略列表)，在选定区域(如 VLAN 1)发送符合网络分域策略和访问控制策略的广播数据包，检查不同区域(VLAN 2)是否可以收到数据包；

b) 设置 6.2.2.2 所规定的访问控制策略(若被测样件的访问控制策略无法通过软件配置修改，则由送样方提供已预置的访问控制策略列表)，检测设备向列表指定的源端口发送符合策略规定的数据包，在列表指定的目的端口检测接收数据包；

c) 设置 6.2.2.2 所规定的访问控制策略(若被测样件的访问控制策略无法通过软件配置修改，则由送样方提供已预置的访问控制策略列表)，检测设备向列表指定的源端口发送不符合策略规定的数据包，在列表指定的目的端口检测接收数据包，并收集样件日志；

d) 检测设备对网关发送符合网络分域策略和访问控制策略的泛洪攻击数据包，攻击类型可选择 ICMP 泛洪攻击和 UDP 泛洪攻击，在目的端口检测接收数据包，并收集样件日志；

e) 基于 TCP 协议，构造多个不符合协议标准的数据包或数据包序列，组成试验集，检测设备对网关发送该试验集，在目的端口检测接收数据包，并收集样件日志。

7.2.3 混合网关通信信息安全试验

对于混合网关，CAN 通信和以太网通信的信息安全试验分别按 7.2.1 和 7.2.2 执行。

7.3 固件信息安全试验

网关系统信息安全试验按照下列流程及要求依次进行。

a) 网关安全启动可信根防篡改试验：
   1) 获取网关安全启动可信根存储区域的访问方法和地址；
   2) 试验人员使用软件调试工具写入数据，重复多次验证是否可将数据写入该存储区域。

b) 网关安全启动 Bootloader 程序校验试验：
   1) 提取网关正常运行的 Bootloader 程序；
   2) 使用软件调试工具修改该 Bootloader 程序的签名信息；
   3) 将修改后的 Bootloader 程序写入到网关内的指定区域；
   4) 监测网关是否正常加载 Bootloader 及系统固件。

c) 网关安全启动系统固件校验试验：
   1) 获取网关正常运行的系统固件；
   2) 使用软件调试工具修改系统固件程序的签名信息；
   3) 将破坏后的系统固件写入到网关内的指定区域；
   4) 监测网关是否正常工作。

d) 如果被测网关有安全日志记录功能，检查被测样件依次执行 7.2 所产生的日志。

e) 如果被测网关有安全日志记录功能，尝试对被测样件改变信息安全设置(如修改访问控制列

表),检查产生的日志。

f) 如果被测网关有安全日志记录功能,尝试对被测样件改变系统关键配置(如路由表等),检查产生的日志。

g) 如果被测网关有安全日志记录功能,检查日志中是否包含触发日志的事件发生时间、事件类型和车辆唯一标识码。

h) 如果被测网关有安全日志记录功能,通过试验工具尝试访问、修改或删除已记录的安全日志。

i) 如果被测网关有安全日志记录功能,检查日志中是否包含个人信息。

j) 使用漏洞扫描工具对网关进行漏洞检测,检测是否存在权威漏洞平台发布6个月及以上的高危安全漏洞;若存在高危漏洞,则检查该高危漏洞处置方案的技术文件。

7.4 数据信息安全试验

网关数据信息安全试验按照下列流程及要求依次进行:

a) 试验人员尝试对网关安全区域或安全模块的授权访问控制进行破解(例如:使用暴力破解或字典破解方式,尝试破解安全区域或安全模块的访问口令);

b) 被测样件送样方提供网关内部安全存储区域的地址范围或安全模块的访问方式,试验人员使用送样方授权的软件工具,尝试对安全区域或安全模块进行读取访问;

c) 试验人员使用非送样方授权的软件工具或访问方式,尝试对安全区域或安全模块进行读取和写入。

附 录 A
（资料性）
汽车网关拓扑结构示例

图 A.1～图 A.3 给出了汽车网关相关拓扑结构的示例。

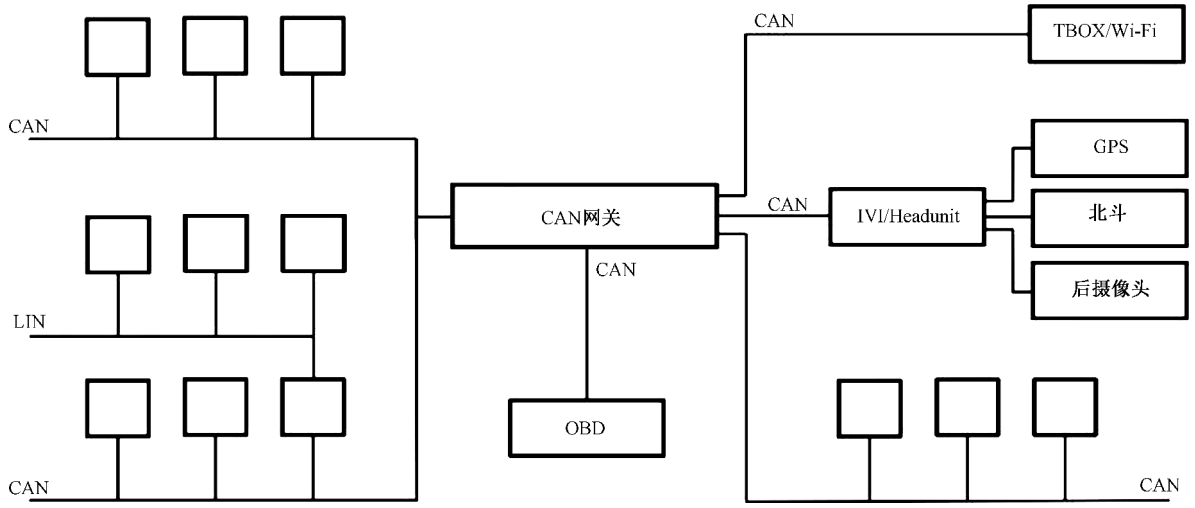

图 A.1 汽车 CAN 网关拓扑结构示例

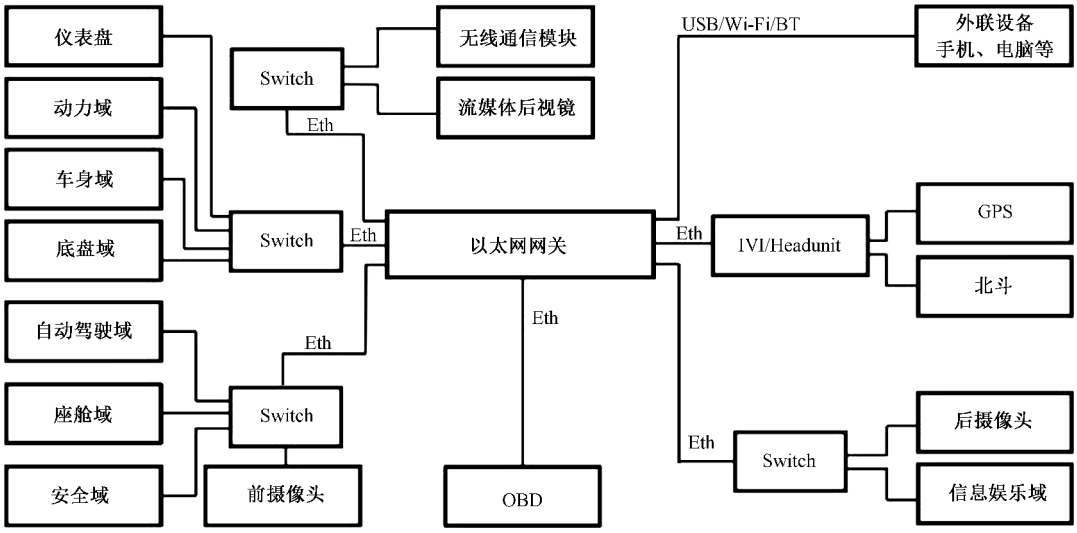

图 A.2 汽车以太网网关拓扑结构示例

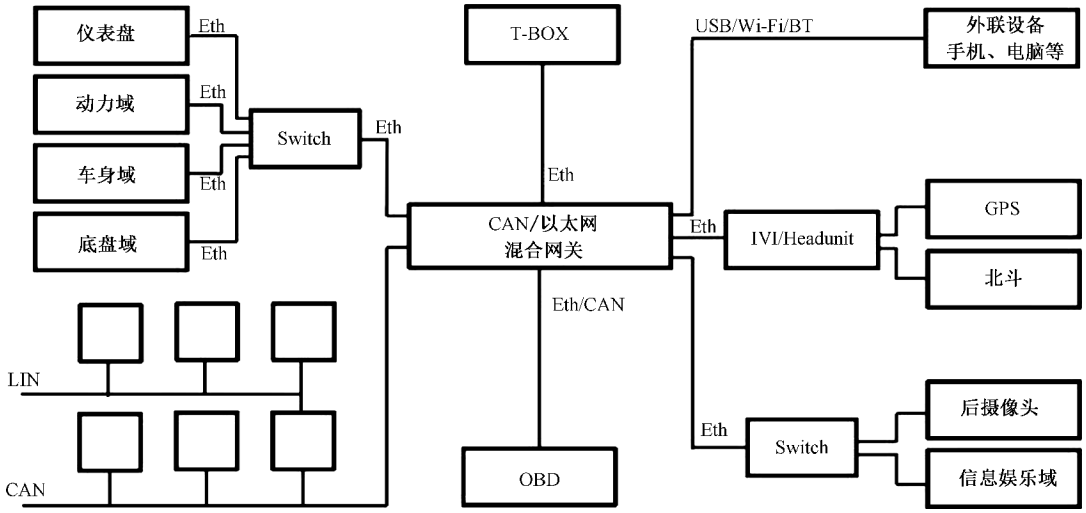

图 A.3　汽车混合网关拓扑结构示例

附 录 B
（资料性）
典型攻击举例

B.1 死亡之 Ping(Ping of death)

一种通过向计算机发送格式错误或其他恶意的 ping 协议数据包的攻击，也称死亡之 ping。例如由攻击者故意发送大于 65536 比特的 IP 数据包给被攻击者，导致被攻击者无法处理甚至系统崩溃。

B.2 ICMP 泛洪攻击

一种简单的拒绝服务攻击，也称作 ping 泛洪攻击，攻击者用 ICMP“回应请求”(ping)数据包淹没被攻击者。

B.3 UDP 泛洪攻击

使用 UDP 协议(一种无会话、无连接的传输层协议)进行的拒绝服务攻击。

B.4 TCP SYN 攻击

一种拒绝服务攻击形式，攻击者向目标系统发送一连串 SYN 请求，试图消耗足够的服务器资源，使系统对合法流量无响应。

B.5 Teardrop 攻击

在 IP 数据包的包头中，其中有一个字段是片位移，该字段指示了该分片数据包在原始未分片数据包中的起始位置或偏移量。

Teardrop 攻击是指利用恶意修改了 IP 分片偏移值的 IP 数据包进行攻击，从而使被攻击者无法正常进行 IP 数据包重组，甚至导致系统崩溃。

B.6 ARP 欺骗攻击

这种欺骗攻击是攻击者将欺骗性的地址解析协议(ARP)数据包发送到本地网络上。目的是将攻击者的 MAC 地址与另一个主机或网络设备的 IP 地址相关联，从而导致网络上其他节点将该 IP 地址的任何流量发送给攻击者。

B.7 IP 欺骗攻击

IP 地址欺骗，指攻击者假冒某个合法主机的 IP 地址发送数据包，从而达到获取被攻击者信任或者隐藏攻击者真实 IP 地址的目的。

B.8 ICMP Smurf 攻击

这种攻击方法结合使用了 IP 欺骗攻击和 ICMP 泛洪攻击。攻击者伪造 ICMP 数据包的源地址，并将数据包目的地址设置为网络的广播地址。如果网络设备没有过滤此流量，则该 ICMP 数据包将被广播到网络中的所有计算机，而网络中所有计算机将向被伪造的源地址发送应答请求包，从而淹没这个被

伪造源地址的计算机，并可能使整个网络拥塞而降低可用率。此攻击以最初发动这种攻击的恶意程序“Smurf”来命名。

B.9 IP 地址扫描

IP 地址扫描是一种基本的网络扫描技术，用于确定地址范围内的哪些地址具有活动的计算机主机。典型的地址扫描是向某个地址范围中的每个地址发送 ping 请求以尝试获得应答。

B.10 端口扫描(Port scan)

端口扫描，指攻击者尝试与目标主机上的每个端口建立通信会话。如果在某个端口的会话连接成功，则说明目标主机在该端口有开放的服务。

B.11 恶意软件

恶意软件是指在计算机系统中安装执行恶意任务的勒索软件、病毒、蠕虫、特洛伊木马、广告软件、间谍软件等程序。

B.12 CAN 数据帧泛洪攻击

CAN 总线网络通信协议规定 ECU 间传输数据帧的优先级由 CAN 数据帧的 ID 决定，ID 越小则数据帧优先级越高。因此，入侵者如果在一个 CAN 总线上以很高的频率发送一个高优先级的 CAN 数据帧，将很可能会阻塞其他数据帧的发送，从而实现 DoS 攻击。

B.13 CAN ID 伪造

由于 CAN 总线网络通信是广播通信，入侵者可以很容易获取在一条 CAN 总线上发送的所有数据帧。通常 CAN 数据帧是明文传输的，入侵者可以通过猜解、遍历或其他手段解析数据帧格式和内容，对车辆关键控制信号进行逆向破解，进一步在该 CAN 总线上以这些 ID 的名义发送非法的数据帧，从而干扰或阻塞 ECU 间的正常通信，乃至实际控制关键系统(如动力系统)的某一个或者多个 ECU。

B.14 CAN 数据帧重放攻击

由于 CAN 总线网络通信是广播通信，入侵者可以很容易按时序捕获某个特定 CAN ID 的所有数据帧，然后在 CAN 总线网络上重新注入这些数据帧，达到干扰和非法控制某一个或多个 ECU 的目的。

B.15 CAN 网络扫描

攻击者可以通过结合网络管理数据帧和功能寻址的诊断服务，对每条 CAN 总线上 ECU 的数量信息进行探测，也可以利用通过遍历物理寻址的方式进行探测。这些信息可以被攻击者进一步利用，从而发现潜在的 ECU 安全漏洞，更准确地对特定 ECU 进行攻击。

B.16 ECU 认证破解

攻击者可以通过遍历的方式暴力破解 ECU 安全访问的密钥。

另外若某个 ECU 的认证算法存在漏洞，则攻击者可以利用漏洞绕过安全验证，进而实现对该 ECU 的非法控制。

B.17 UDS 服务攻击

UDS 协议(ISO 14229-1 和 ISO 27145-3 所约定的协议)主要用于通过 CAN 网络读取 ECU 的信息和向 ECU 写入信息。UDS 定义了若干应用层服务,入侵者如果能探测到 ECU 开启了哪些服务,并且通过暴力破解或其他方式获取了这些服务的身份认证信息,就可以利用这些服务进行攻击,例如向 ECU 注入非法固件、读取或修改敏感数据、不断地重启 ECU 等。

参 考 文 献

[1] GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范

[2] GB/T 37027—2018 信息安全技术 网络攻击定义及描述规范

[3] ISO 14229-1 Road vehicles—Unified diagnostic services (UDS)—Part 1:Application layer

[4] ISO 27145-3 Road vehicles—Implementation of World-Wide Harmonized On-Board Diagnostics (WWH-OBD)communication requirements—Part 3:Common message dictionary