ICS 43.040
T

中华人民共和国国家标准

GB/T XXXXX—XXXX

汽车网关信息安全技术要求

Technical requirements for cybersecurity of vehicle gateway

（征求意见稿）

（本稿完成日期：202004）

－XX－XX 发布　　XXXX－XX－XX 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

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国汽车标准化技术委员会（SAC/TC114）归口。

本标准起草单位：

本标准主要起草人：

汽车网关信息安全技术要求

1 范围

本标准规定了汽车网关产品硬件、通信、软件、数据的信息安全技术要求与测试方法。

本标准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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 可信计算基

GB/T XXX 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 XXX界定的以及下列术语和定义适用于本文件。

汽车网关 vehicle gateway

用于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，也称中央网关。

注：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。

4 缩略语

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）
DoS	拒绝服务攻击（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）
LIN	局域互联网络（local interconnect network）
MOST	面向媒体的串列传输（media oriented system transport）
OBD	车载诊断系统（on-board diagnostics system）
TCP	传输控制协议（transmission control protocol）
UDP	用户数据报协议（user datagram protocol）
UDS	统一诊断服务（unified diagnostic services）
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和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网关拓扑结构参考附录A中图A.1所示。

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 和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参考附录 A 中图 A.2 所示。

5.3 混合网关

部分新一代车内网络结构中，一部分 ECU 和域控制器之间通过以太网通信，而另一部分 ECU 和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参考附录 A 中图 A.3 所示。

6 技术要求

6.1 硬件信息安全要求

6.1.1 按照 7.1 a)进行测试,网关不应存在后门或隐蔽接口。

6.1.2 按照 7.1 b)进行测试,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)进行测试后，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)进行测试后，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 CAN ID 的 DoS 攻击检测功能。

按照 7.2.1 c)、d)进行测试,当网关检测到 DoS 攻击时，应满足以下要求：

a) 网关全部功能和性能不应受影响；

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，对数据帧中的信号值进行检查，检查内容包括信号值长度、信号值有效性等，按照 7.2.1 e)、f）进行测试,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)进行测试,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。

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)进行测试,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（如T-Box）的通道。

6.2.2 以太网网关通信信息安全要求

6.2.2.1 安全区域划分

网关应支持网络分域,按照 7.2.2 a)进行测试,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 (ACLs)，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，另外也可包括物理端口、通信方向（输入或输出）、源 MAC 地址、目的 MAC 地址等要素。

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)进行测试,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

网关应具备以太网 DoS 攻击检测功能。支持 ICMP 协议和 UDP 协议的网关，检测的 DoS 攻击类型，应至少包括 ICMP 泛洪攻击和 UDP 泛洪攻击。

按照 7.2.2 d)进行测试,当网关检测到以太网 DoS 攻击时,应确保自身正常的功能和性能不受影响，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)进行测试,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 软件信息安全要求

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)进行测试,网关的可信根、BootLoader 程序、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，则应满足如下要求：

a) 按照7.3 d)、e)、f)进行测试,当网关探测到不安全通信、网关发生软件配置变更、网关安全启动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)进行测试,网关的安全日志中，应至少包括触发日志的事件发生时间、事件类型等内容；
c) 按照7.3 h)进行测试,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)进行测试,网关安全日志在车载端应至少存储100条记录；
e) 按照7.3 j)进行测试,在非车载端（比如后台服务器）存储的安全日志，应至少保存7天；
f) 按照7.3 k)进行测试,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 l)进行测试,网关不应存在由权威漏洞平台公开发布6个月及以上且未经处置的高危安全漏洞。

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 进行测试,网关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 测试方法

7.1 硬件信息安全测试

网关硬件信息安全测试应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，通过5倍率以上的光学放大镜，观察网关PCB板，检查PCB板硬件是否存在后门；
b) 检查是否有存在暴露在PCB板上的JTAG接口、USB接口、UART接口、SPI接口等调试接口，如存在则使用测试工具尝试获取调试权限。

7.2 通信信息安全测试

7.2.1 CAN 网关通信信息安全测试

CAN网关通信信息安全测试应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，则依次分别测试；

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毫秒为周期，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，则依次分别测试；
e) 检测设备对网关发送一个或多个信号长度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（实际周期相比定义周期偏差大于±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，则依次分别测试；
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（如T-Box）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，则依次分别测试。

7.2.2 以太网网关通信信息安全测试

以太网网关通信信息安全测试应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VLAN1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IP、TCP和UDP协议，构造多个不符合协议标准的数据包或数据包序列，组成测试集，检测设备对网关发送该测试集，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测试

对于混合网关，CAN通信和以太网通信的信息安全测试应分别按7.3.1和7.3.2的执行。

7.3 软件信息安全测试

网关系统信息安全测试应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测试：
   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) 测试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程序校验测试：
   1) 提取网关正常运行的Bootloader程序；
   2) 使用软件调试工具对该Bootloader程序进行篡改；
   3) 将修改后的Bootloader程序写入到车载终端内的指定区域；
   4) 监测网关是否正常加载Bootloader及下一阶段系统固件。

c） 网关安全启动系统固件校验测试：
   1） 获取网关正常运行的系统固件；
   2） 使用软件调试工具对系统固件进行篡改；
   3） 将破坏后的系统固件写入到车载终端内的指定区域；
   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7.3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；
h） 如果被测网关有安全日志记录功能，通过测试工具尝试访问、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且安全日志存储在车载端，则检查能够存储日志的最大数量；
j） 如果被测网关有安全日志记录功能且安全日志存储在非车载端，则检查能够存储日志的最长时间范围；
k） 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；
l） 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 数据信息安全测试

网关数据信息安全测试应按照下列流程及要求依次进行：

a） 测试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，测试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） 测试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
（资料性附录）
汽车网关拓扑结构举例

图A.1至图A.3给出了汽车网关相关拓扑结构的举例。

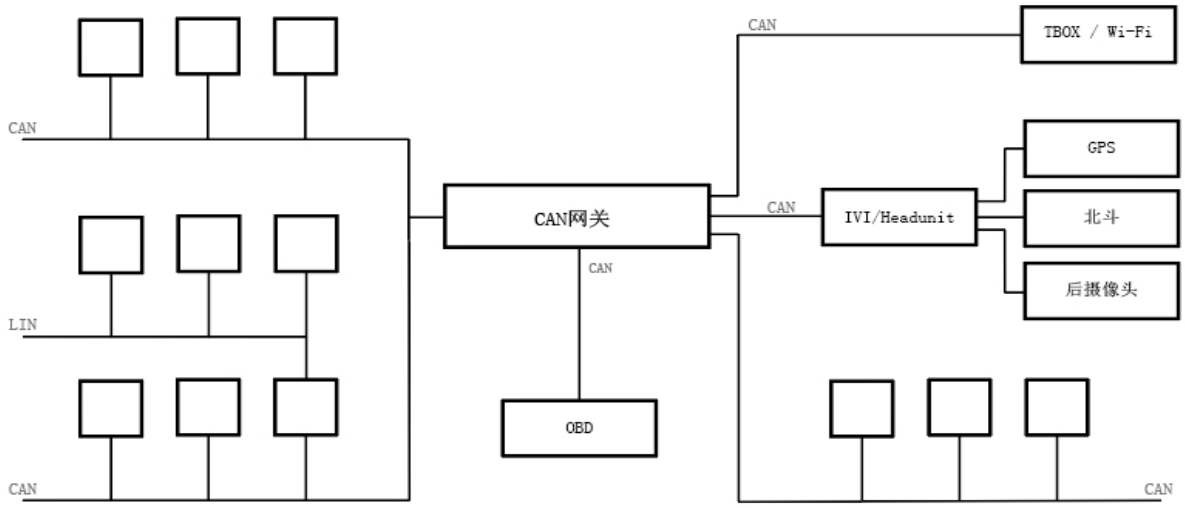

图 A.1 汽车 CAN 网关拓扑结构示例

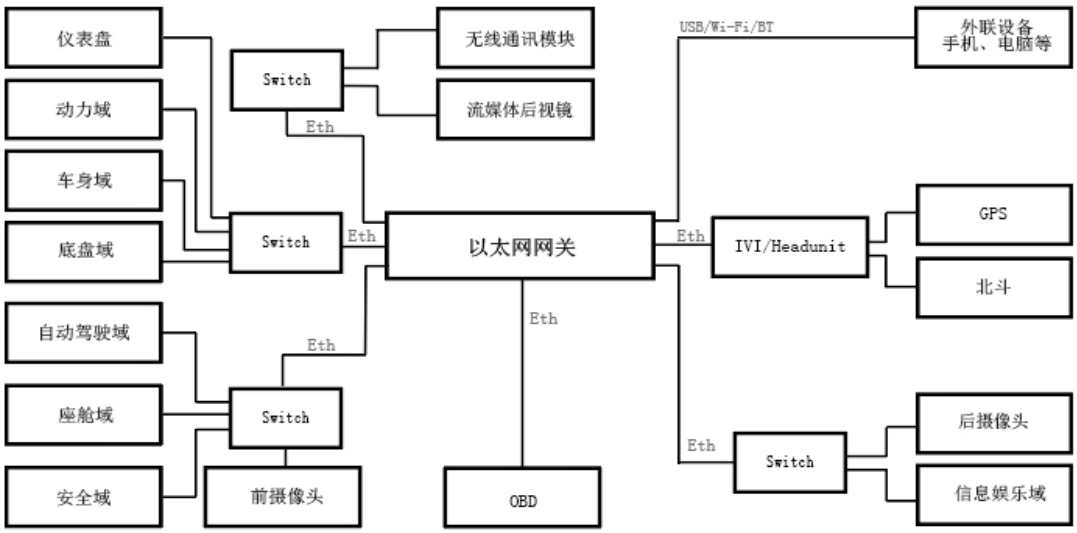

图 A.2 汽车以太网网关拓扑结构示例

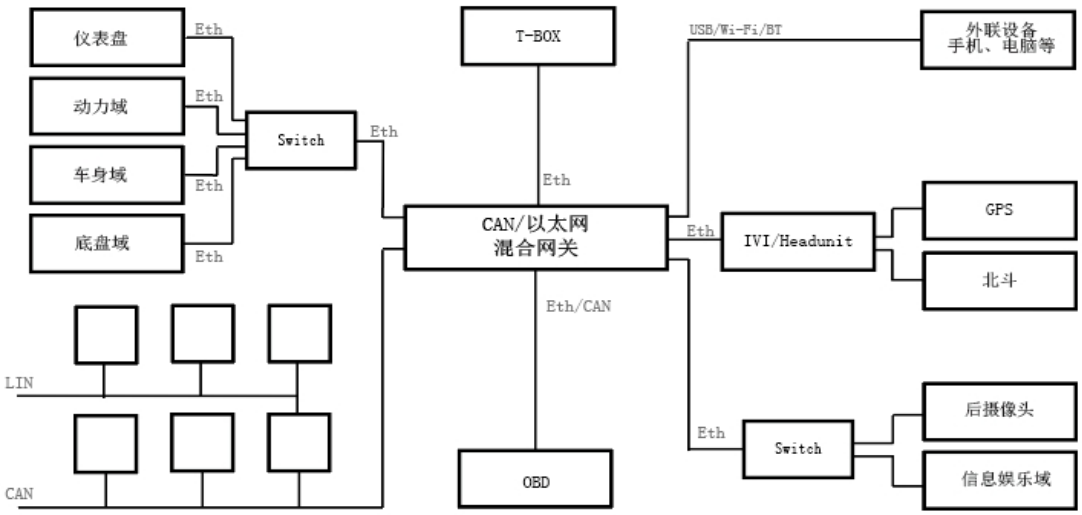

图 A.3 汽车混合网关拓扑结构示例

附 录 B
（资料性附录）
典型攻击举例

B.1 Ping of death

是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

是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

UDP泛洪攻击是使用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

TCP SYN 攻击是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。如果网络设备不过滤此流量，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 XSS跨站攻击（Cross-site scripting）

攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上对其他用户造成影响的HTML代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行恶意软件注入。

B.12 SQL 注入攻击（SQL injection注入）

SQL注入是指攻击者把SQL语句插入到Web表单提交，或输入域名、页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL语句的目的。

B.13 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.14 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.15 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.16 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.17 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.18 ECU 密钥暴力破解

攻击者可以通过遍历的方式暴力破解ECU安全访问的密钥。

例如某个ECU的认证算法存在漏洞，则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.19 UDS 服务攻击

UDS协议（ISO 14229-1和ISO 27145-3标准所约定的协议）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、不断重启ECU等。

参 考 文 献

[1] GB/T 28458-2012 信息安全技术 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