汽车总线防火墙

（MCU平台） 文档

V1.0

第1章　汽车防火墙 SDK 介绍

1.1　简要介绍

VT_SCAN MCU Engine 是针对汽车信息安全性提供的车载防火墙解决方案接口函数。此方案通过嵌入 VT_SCAN 安全防护层和配置防火墙特征来监控 CAN 总线，并发现总线流量异常。VT_SCAN 通过模块化的设计，强调软件的易移植性和通用性。 以达到对目标设备资源占用的最小化和方便移植，帮助客户实现在目标设备的移植，完成对 CAN 总线的安全防护与监控。

1.2　开发运行环境和平台支持

- 平台支持
  MCU和LINUX两种环境
- 支持两种检测方式
  - 实时阻断
    实时检测并阻断恶意指令，上报云端
  - 非实时阻断，仅向云端报警
    检测后并不阻断，仅向云端报警

1.3　组成说明

VT_SCAN分为用户API调用库和engine，特征库。 VT_SCAN core 核心库包括两个部分：

a. VT_SCAN 防火墙匹配引擎 Matching Engine
b. VT_SCAN 特征库 Signature
c. APIs

1.4 资源需求

MCU平台：256kb memory, one core, 2-CAN

LINUX平台： 2MB memory

第2章　模块构成

2.1　模块构成说明

VT_SCAN 主要由防火墙引擎模块、接口模块和特征库模块三部分组成，具体产品结构如下图所示：

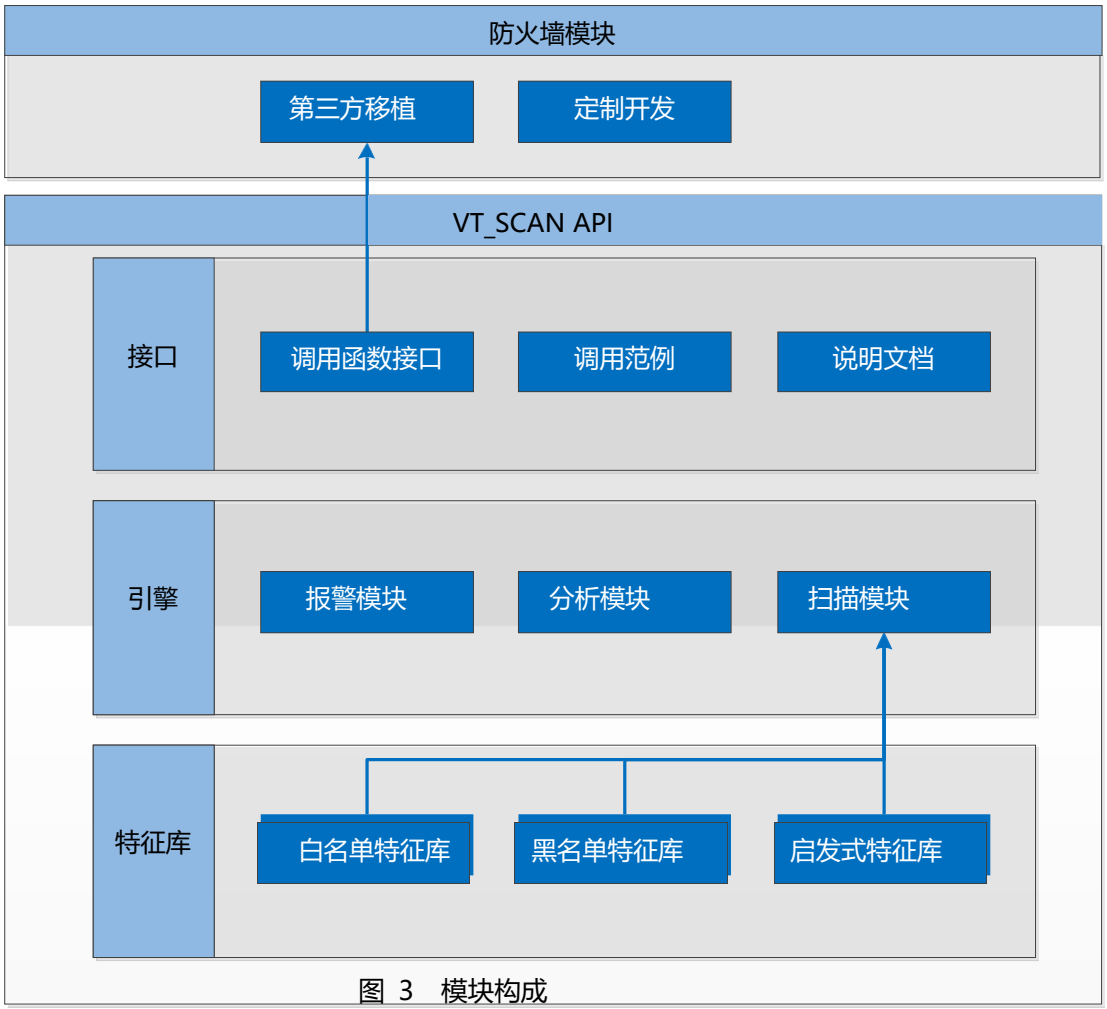


图 3　模块构成

引擎	防火墙引擎，分析数据流量，扫描匹配并返回检测结果。
接口	提供函数调用接口，编写例子代码调用引擎，将分析结果传递给调用接口。因此开发者可以按照使用手册， 通过函数调用为产品扩展汽车总线防火墙防御模块。
特征库	多种特征库检测异常，攻击，故障等场景。

2.2 VT_SCAN安全方案移植集成步骤

本节介绍将VT_SCAN移植到目标设备的基本流程和步骤。 VT_SCAN安全防护方案的移植需要客户提供：

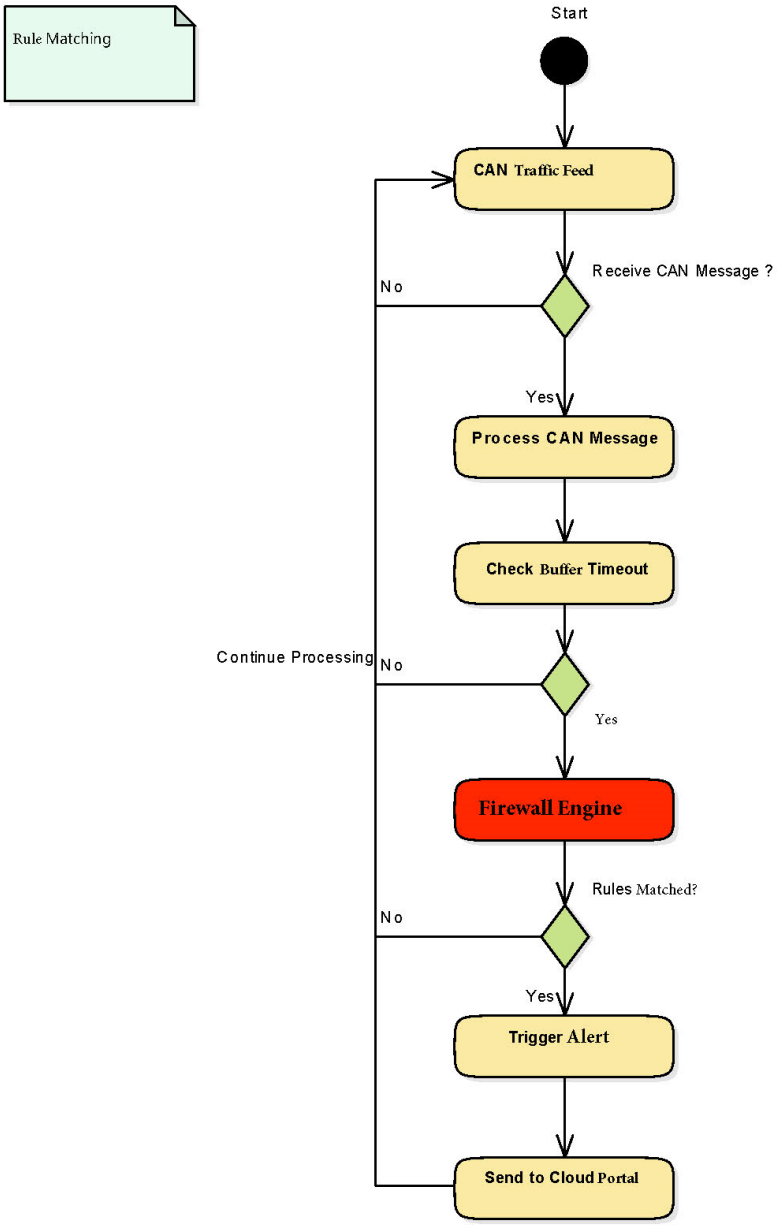
a. 汽车网关或者 TBOX 设备和相关 CAN 设备驱动用户手册，以及集成环境的资源限制，如内存等。
b. 目标平台的编译环境，以生成适合目标设备的 VT_SCAN 类库
c. 网络通讯接口函数。VT_SCAN 将通过网络通讯接口上传报警日志和相关数据到云端汽车防火墙实时监控平台。

移植集成步骤：

a. 根据目标设备的 CAN 通信驱动接口，修改、调整 VT_SCAN 相应的驱动 。
b. 使用目标平台的编译环境和相应的目标平台系统类库，重新编译生成 VT_SCAN 类库 。
c. 修改 VT_SCAN 例子代码，在目标平台运行启动引擎，进行测试调试。
d. 在目标平台上完成 VT_SCAN 安全防护层集成。

第3章　引擎扫描开关

引擎检测方式分为在线inline和离线offline方式。在线方式可以集成在网关自身CAN包转发模块里，用来阻断对汽车攻击的指令片段。离线方式用于并行处理，不影响网关正常工作。发现异常后进行报警。



引擎可以设置不同的扫描开关，满足不同场景需求：

Engine model	扫描开关	应用场景
FW ALL	Default normal 缺省（全部开关打开） 黑名单扫描开关 攻击扫描开关 启发式扫描开关 特征扫描开关	以高检测率，低误报率为第一优先，扫描速度和内存CPU资源占用其次 分析扫描统计结果
FW Quick	快速扫描 特征扫描开关	以扫描速度和资源占用小为优先，扫描开销小
FW Quick + Heuristic	启发式扫描开关 特征扫描开关 通过启发式判断再次确认	以速度+低误报率优先，牺牲部分速度和内存CPU，提高扫描检测性能

三种扫描开关，分别是快速扫描，启发式扫描和深度完全扫描。具体特点见上表。

第4章　攻击检测点说明

4.1　车型白名单扫描

目的:
车辆正常情况 下的监控。
指标:
误报率
测试方法
测试车型不同状态下的流量，特征库判断是否属于正常情况，并返回结果。
结果
是否异常

4.2　其他车型白名单扫描

目的:
误报测试一部分内容，防火墙对每款车型定制，测试其他车辆正常流量，可以提高误报率指标。
指标:
2不同车型的误报率指标。
测试方法
测试不同车型不同状态下的流量，特征库判断是否属于正常情况，并返回结果。
结果
是否异常

4.3　攻击流量扫描

目的:
模拟多种左右不同场景的总线攻击，例如扫描，暴力破解，DoS, Spoof等，检测攻击。
指标:
能够检测到每一种攻击。
测试方法
重放攻击流量文件，特征库引擎扫描并返回结果。
结果

是否异常

4.4 精确攻击流量

目的:
针对该车型的的漏洞隐患而生成对应的精确攻击，这些攻击危害更大。
指标:
能够检测并实时阻断
测试方法
重放相关流量或指令，特征库引擎扫描并返回结果。
结果
是否异常

检测的攻击点包括:

扫描结果以文本方式输出。以后可以通过网口传到云端在监控平台显示。防火墙匹配某条特征时会触发一个报警事件，这个报警事件包括该特征的代号和事件描述。当报警事件送到云端时，云端会在云端报警数据库中查询该代号对应的信息，显示在云端监控界面，这样云端事件管理界面的内容就很丰富。

云端安全监控模块的 功能包括：

- 持续监控分析
- 攻击预测
- 检测
- 响应： 攻击回溯， 调查取证， 策略调整，攻击隔离