
  
 広島市立大学
   
 Hiroshima City University

## つながるクルマのセキュリティ

2016/01/31

重要生活機器連携セキュリティ協議会 (CCDS)
   
 広島市立大学大学院 情報科学研究科
   
 井上 博之

SECCON2015決勝大会併催カンファレンス

## 目次

1. DEFCON23にみるIoT/クルマのセキュリティ
  - IoT Village
  - 車載ネットワークへのハッキング事例
2. 車載LANにおけるセキュリティ分析プラットフォームの開発
3. 車載LANにおける対策
  - 機械学習を用いたセキュリティゲートウェイの開発
  - 車載LANの情報を第三者に安全に提供するサービス
4. まとめ



## DEF CON とは

- DEF CON Hacking Conference
  - 世界最大のハッキングイベント @ラスベガス Paris Hotel
    - ◆ 2015年 8/6(木)～8/9(日)の4日間、事前登録無し、US\$230
    - ◆ 今年が23回目 → DEFCON23
    - ◆ BlackHatのイベントに引き続き開催
  - 講演、CTF大会、ワークショップ、Village、デモ展示など




## CTF (Capture The Flag)

- ファイルやWebサイトに隠されているキーワード(フラグと呼ばれる)を探す
  - チーム対戦
  - 世界大会 決勝と、その場で開かれるOpenCTFの2つが開催

## 即売会 (DEFCON)

- ハッキングツール、ノベルティ、書籍などをその場で販売




USB接続のWi-Fiアナライザ、SDR解析装置、など数十ドル程度のツールを販売 → 最終日には完売

## ワークショップ (DEFCON)

- ちょっとしたハッキングツールを作ったり、ツールを使って実際にハッキングしたりというワークショップ
- 物理セキュリティ
  - ピッキング
  - シール剥がし (Tamper Evident Tapeを剥がす)
- ちょっとした電子回路の作成
  - BadUSB
- 車載LANへアクセスして目的の packets を探す、など




## Village (BoFのようなもの) 7

- 興味を持った人たちが集まって、ミニ講演会やワークショップや展示などを実施 (BoF→birds of a feather)
- Bio Hacking Village
- Car Hacking Village
- Crypto and Privacy Village
- Data Duplication Village
- Hardware Hacking Village
- ICS Village (ICS/SCADA: 産業制御システム) (昨年から)
- Internet of Things (IoT) Village
- Lockpick Village (今年から)
- Packet Hacking Village
- The Social Engineer Village
- Tamper Evident Village
- Wireless Village (SDR)



## 物理セキュリティのVillage 8

- Lockpick Village
  - ピッキングツールと錠の戦い
  - ピッキング入門?のワークショップや、ツールの即売会




- Tamper Evident Village
  - Tamper Evident テープを分らないように剥がすワークショップ






## Internet of Things (IoT) Village (1/2) 9

- 2015年に新設
  - ネットワークにつながるコンシューマー製品のセキュリティの向上を目指す
    - ◆ 広い意味でのIoT
  - 昨年にICS Villageも新設されており、組み込み機器のセキュリティへの関心が大きくなってきている
- プレゼンテーション
  - Hacking Your Fat: the FitBit Aria (→WiFi多機能体重計)
  - Hacking Satellite TV Receivers
  - Practical IoT Exploitation Workshop (MIPS/ARM)
  - Pwning IoT with Hardware Attacks

pwn: ネットスラングで「うち勝つ」「圧勝する」「ボロボロにする」等の意味

## Internet of Things (IoT) Village (2/2) 10

- ハッキングコンテスト
  - **コンシューマー製品のハッキング大会**(ワークショップ)
    - ◆ 家庭用ルータ (ASUS, Zyxel 社)
    - ◆ 防犯カメラ (Netgear, Forcam 社)
    - ◆ 赤ちゃんモニター (Samsung 社)
    - ◆ Wi-Fi対応血圧モニター (Blipcare 社)
    - ◆ Wi-Fi対応体重計 (Fitbit Araia 社)
    - ◆ タイムカード記録装置 (ZK Software 社)
    - ◆ NAS (Apple社タイムカプセル)
    - ◆ ガレージ開閉装置 (Chamberlain 社)
    - ◆ 電気錠 (LockState, Hysoon 社)
    - ◆ 冷蔵庫 (Samsung 社)
    - ◆ おもちゃ (HappyCow社)
    - ◆ カメラ付き戦車模型 (Wi-Fi接続)



## 講演 (DEFCON) 11

- 暗号解析から物理セキュリティ、ハッキングの事例など色々な発表あり
  - 1時間ずつ
  - 10:00~19:00
  - 5トラック並列
  - 139件の発表



- 以下、話題になったJeepの車載ネットワークの脆弱性に関する講演内容を紹介



## 講演紹介: Remote Exploitation of an **Unaltered** Passenger Vehicle 12

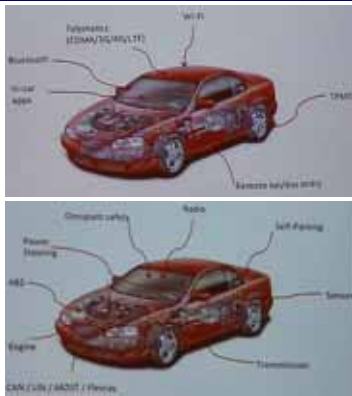
- 話題になったジープのハッキング事例の詳細



詳細なレポート (White Paper) が8/10の週に公開されている  
[http://www.ioactive.com/pdfs/IOActive\\_Remote\\_Car\\_Hacking.pdf](http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf)

## 遠隔からの攻撃対象のあれこれ

13



手順:

1. Remote compromise
2. Lateralization
3. CAN Message analysis (in advance)
  - Reprogram firmware
  - Functionality
4. CAN message injection

対象:

- Running exploit
- Self-parking
- Pre-collision system
- Adaptive cruise control

## Step.1 WiFi経由のハック

14

車内のホットスポット機能のWi-Fiで、ポートスキャン → TCP/6667が開いている



Actually its easy!

- My WPA2 password was "TYTMMPhZxp"
- This corresponds to Epoch time 0x50e22720
- This is Jan 01 2013 00:00:32 GMT
- Took 32 seconds for Wi-Fi to get started up
- Really only a few dozen passwords to try

```
Starting Nmap 6.01 (Ubuntu/Linux)
11:23 CST
Nmap scan report for 192.168.3.1
Host is up (0.002s latency).
PORT      STATE SERVICE
2011/tcp  open  esd-cc
2021/tcp  open  esd-smc
4400/tcp  open  hlsmon
4810/tcp  open  x11
5020/tcp  open  hlsmon
6667/tcp  open  AFD
8100/tcp  open  sddm
8520/tcp  open  sddm
```

## Step.2 D-Bus経由でのアクセス

15

TCP/6667番にアクセスすると、D-Busコマンドのプロンプトが... しかも、認証なしで

### D-Bus: Overview

- Interprocess communications
- Can require authentication
- Jeep did NOT
- We used Dflect to look at services
- Dbus-Python for scripts / exploits

```
telnet 192.168.3.1 6667
Trying 192.168.3.1...
Connected to 192.168.3.1.
Escape character is '^'.
AUTH ANONYMOUS
OR
4343a53752f52f92a9e4e640000
BEGIN
```

### Finding the Jeep's IP

```
# ifconfig
eth0: flags=4096<UP,LOOPBACK,RUNNING,MULTICAST> mtu 1500
    inet 127.0.0.1 netmask 0xffff0000
    flags=100<BROADCAST> mtu 1500
    up: flags=8040<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    address: 30:14:9a:0e:48:c8
    media: <unknown type> auto-select
    inet 192.168.3.1 netmask 0xffff0000 broadcast 192.168.3.255
    up: flags=4053<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1472
    inet 21.28.103.144 -> 66.28.83.83 netmask 0xffff0000
```

## Step.3 広域通信網(WAN側)のアドレスで検索

16

グローバルIPアドレス側の範囲のTCP/6667番をポートスキャンしたら簡単にアクセス可能

### Searching for Vehicles

```
$ bin/passcan 21.0.0.0/8 -p6667
$ bin/passcan 25.0.0.0 -p6667

Discovered open port 6667/tcp on 25.24.166.11
Discovered open port 6667/tcp on 25.24.166.11
Discovered open port 6667/tcp on 25.22.252.32
Discovered open port 6667/tcp on 25.17.166.228
Discovered open port 6667/tcp on 25.22.138.47
Discovered open port 6667/tcp on 25.22.67.217
Discovered open port 6667/tcp on 25.23.97.210
Discovered open port 6667/tcp on 25.22.15.114
Discovered open port 6667/tcp on 25.18.32.9
Discovered open port 6667/tcp on 25.32.29.24
```

### Gathering Vehicle Information

```
# python
import dbus
bus = dbus.BusConnection("tcp://21.24.4.11:6667")
proxy = dbus.Interface(bus.get_object("com.chrysler.remote.NBT"),
    "/com/chrysler/remote/NBT")
print proxy.get_vehicle_info()
print proxy.get_vehicle_info()
print proxy.get_vehicle_info()
```

## 車両の型番を取得

17

### Vehicles Located via Scanning

- 2013 DODGE VIPER
- 2013 RAM 1500
- 2013 RAM 2500
- 2013 RAM 3500
- 2013 RAM CHASSIS 5500
- 2014 DODGE DURANGO
- 2014 DODGE VIPER
- 2014 JEEP CHEROKEE
- 2014 JEEP GRAND CHEROKEE
- 2014 RAM 1500
- 2014 RAM 2500
- 2014 RAM 3500
- 2014 RAM CHASSIS 5500
- 2015 CHRYSLER 200
- 2015 JEEP CHEROKEE
- 2015 JEEP GRAND CHEROKEE

### Vehicle Estimates

- We found 19 duplicate VINs in a scan of 2694 vehicles
- Estimated 381,980 +/- 89,393
- We now know that the real number is 1.4 million. We obviously went with a conservative estimate

## Step.4 制御CPUのファームウェアのハック

18

通信制御のモジュールから、SPIインタフェース経由で、CANにつながるV850 CPUのファームウェア書き換えに成功



- V850 firmware is NOT signed
- No code signing mechanism present
- Updating only works if v850 in "bootrom" mode



**SPIバス経由でのCANアクセス** 19

V850 CPUのファームウェアを入れ換えて、外部からの指令を受け取り、内部のCANバスにメッセージを送信できるようにした

V850 Internals: SPI Parser

V850 Internals: Sending Arbitrary CAN Msgs

Send arbitrary CAN messages

これで任意のCANメッセージを送信できる

**Step.5 CANメッセージの調査(キャプチャ&解析)** 20

段ボールの山に衝突させて、何のデータが流れるかを分析

自動車庫入れを実行して、ビデオとデータのキャプチャ結果を分析

**そして、遠隔からCANメッセージ経由で操作可能に** 21

- そして、Jeepは携帯電話網経由で自由に操作できるようになった
  - 公開の少し前に、JeepはECUのファームウェアをリコールし、ISP (Sprint)はTCPの6667番をアクセス制限した
- Jeep問題のまとめ
  - 何も機器を追加していない車に対して、遠隔から干渉できた
    - ◆ 機器をつないでの干渉は、2011年や2013年に報告済
      - 技術的には、さほど難しい内容
    - 車内のインターネット接続サービスや、車載LAN上のECU、インターネットプロバイダなどに穴(脆弱性)があり、そこを狙われた
      - ◆ 今回の件の公開前に、自動車メーカーとプロバイダは対策済み

**車載LANにおけるセキュリティ分析プラットフォームの開発** 22

この2年ほど、広島市立大学で取り組んでいる研究

**セキュリティ分析プラットフォームの必要性** 23

- 自動車の高機能化やサービスの多様化
  - 高性能なカーナビやテレマティクス機器の導入
  - 3G/LTEの携帯電話通信網の普及(低価格化)

自動車と外部ネットワークとの常時通信が一般的に

不正アクセス、攻撃の危険性が増大  
攻撃手法や防御の仕組みを  
実際の車やネットワークで解析する

**分析プラットフォームの目的と構成** 24

- 外部ネットワークにつながる車載LANIに対する攻撃および防御手法の確立
  - 車載LANの情報セキュリティを分析および検証するための分析プラットフォームの設計、開発

## 1. メッセージ解析プラットフォーム

## 分析プラットフォームの開発

### ■ 攻撃手法の分析プラットフォームの開発と、 防御手法の確立

- 車載LANやECUへの攻撃の危険性の評価
- 攻撃内容に応じた防御手法の評価

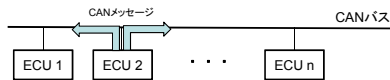
### ■ 分析プラットフォームの開発

- 攻撃のアルゴリズムやメッセージの検証
- 通信状態や流れているメッセージの解析
- 攻撃プロトタイプシステムの開発
  - ◆ インターネットに常時接続する車載器の開発
  - ◆ 攻撃者を支援するGUIの作成



## 車載LANとCAN規格

- 車載LANの規格にはいくつか規格がある
  - CAN, LIN, FlexRay, MOST, ...
  - 今回は車載LANとして、最も普及しているCANを想定



### CANの特徴

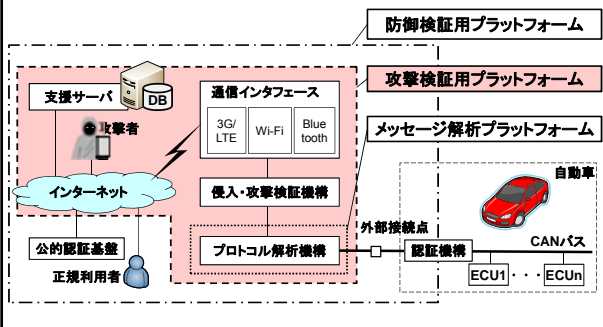
- ペイロードが小さい 最大8byte
- ソースアドレスがない 宛先アドレス(CAN ID)しかない
- 共有バスである 機器認証の仕組みもない
- 通信速度が低い 500kbps程度

CANはプロトコル上、なりすましやDoS攻撃に本質的に弱い

## 2. 攻撃検証用プラットフォーム

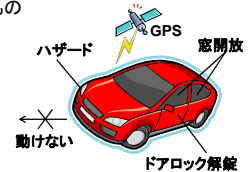
## 攻撃検証用プラットフォーム

車載LANの情報セキュリティを分析および検証するための  
分析プラットフォームの設計、開発



## 想定する攻撃シナリオの例

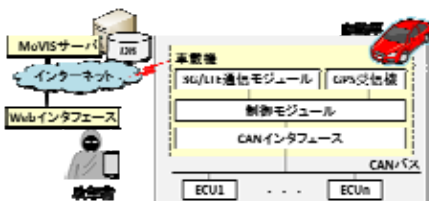
1. テレマティクス装置に模した車載器を車載LANと診断用(OBD-II)ポートへつなぐ  
車載器には攻撃プログラムが仕掛けられている
2. 車載器はGPS測位した値や自動車の状態などを定期的に支援サーバに送る
3. 攻撃者は、スマートフォンやWeb経由で、以下のような条件を指定して特定の自動車に攻撃命令を出す
  - ◆ ある範囲(緯度経度)にあるもの
  - ◆ ドアロック解錠
  - ◆ 指定した窓を開く
  - ◆ DoS攻撃を行なう



## 攻撃検証用プラットフォームの開発

31

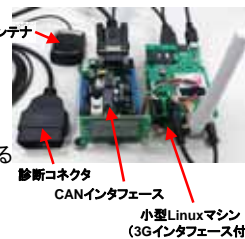
- 主要機能
  - サーバを持ち車載LANへの攻撃支援を行なう
  - 自動車の状態を監視し情報をサーバで管理する
- プロトタイプシステムであるMoVISの開発
  - インターネット常時通信を行なう車載器を想定
  - インターネット上にMoVISサーバを持つ
  - 攻撃者はWebインタフェースを経由して攻撃指令を出す



## 開発した車載器とその機能

32

- 小型Linuxマシン(Raspberry Pi)を使用して実装
  - CANバスにつながるCANインタフェース(Arduino)を搭載
- インターネットと常時通信
  - ◆ 3Gデータ通信網を使用
  - ◆ グローバルIPを持ち通信を行なう
  - ◆ 識別には車載器のMACアドレスを使用
- 自動車の情報を支援サーバに伝える
  - ◆ GPSから取得した現在地の位置情報
  - ◆ CANバスから読み取った自動車の状態
- 支援サーバからの指令を受けCANバスに送信
  - ◆ 攻撃者が指定した動作を行なうメッセージをCANバスに送信



## 判明したCANメッセージの例

33

分類	内容	備考
状態	車両速度	単位: km/h
状態	エンジン回転数	単位: rpm
状態	ハンドル舵角	単位: 度
状態	ブレーキ踏量	
状態	ギアポジション	R, N, Dのいずれか
動作	ドアロック解錠(1)	イグニッションOFFの状態有効
動作	ドアロック施錠(1)	イグニッションOFFの状態有効
動作	ドアロック解錠(2)	イグニッションONの状態有効
動作	ドアロック施錠(2)	イグニッションONの状態有効
動作	窓開け	4つの窓を個別に指定可能
動作	窓閉め	4つの窓を個別に指定可能
動作	ハザード点滅	1回または2回の指定が可能
警告	シートベルト警告	警告灯を点灯
警告	サイドブレーキ警告	警告灯を点灯
警告	エンジン油圧不足	警告灯とメッセージを表示

## 攻撃者用ユーザインタフェース

34

- 攻撃者にWebアプリのGUIを提供
  - 支援サーバから受信した車載器とIDをマップ上に表示
  - 車載器に対する動作の選択が行い、指令を送信



## 実車を使用した実験

35

- 概要
  - 2013年9月に発売されたハイブリッド自動車を使用
  - 診断(OBD-II)ポートに、開発した車載器を接続
    - ◆ カーナビやテレマティクスが乗っ取られたことを想定
  - インターネット経由で、情報取得や車載LANへのメッセージ送信を実施

- 動画によるデモ
  1. 鍵の解錠、窓開け
  2. 表示パネルの誤表示
  3. トリップメータへの干渉
  4. 大量メッセージ送信 (DoS攻撃)



## 実車ででの影響のまとめ

36

- 今回の実験で確認できた動作
  - ボディ系へのなりすまし攻撃
    - ◆ ドアロックの解錠
    - ◆ 窓を開ける
    - ◆ ハザードランプの点滅
  - インstrumentパネルへのなりすまし攻撃
    - ◆ タコメーターや速度計の数値操作  
これによりトリップメータへの干渉も確認できた
    - ◆ ギアポジション表示の変更
    - ◆ シートベルトとサイドブレーキの警告ランプの点灯
  - DoS攻撃による動作妨害
    - ◆ さまざまな異常の発生
    - ◆ パワーステアリングやブレーキへの干渉



インターネットと常時接続する車載器から車載LANへの攻撃を確認し、また、走行中に異常を起こせるなどの危険性が判明 → 守る仕組へ

## 分析プラットフォーム開発と実験のまとめ

37

- 攻撃プロトタイプシステムの動作を通じて
  - インターネットと常時接続する、テレマティクス機器を想定した車載器の開発
  - 車載器を管理する支援サーバの開発
  - 攻撃用ユーザインタフェースの開発
  - 実車を使用し、CANメッセージの意味を解析
  - 攻撃シナリオを想定し、実際の攻撃を遠隔から実施し、実車での動作を確認



インターネット経由での車載LANへ攻撃が可能であることを確認し、攻撃検証用プラットフォームの有効性を実証した → 防御の仕組みへ

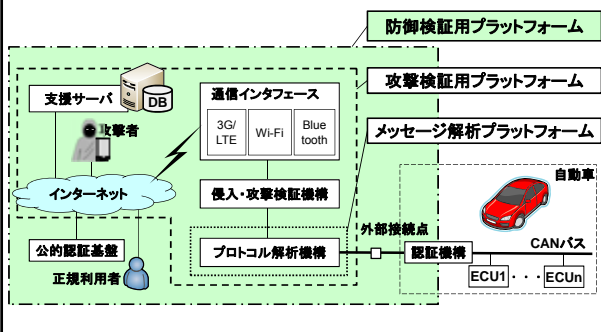
## 3. 防御検証用プラットフォーム

38

## 防御検証用プラットフォーム

39

車載LANの情報セキュリティを分析および検証するための分析プラットフォームの設計、開発



## 防御機構に関する考察 (1/2)

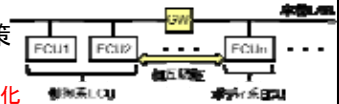
40

### 1. 物理的な対策

- 車載LANのハーネスやコネクタに利用者が容易にアクセスできないようにする
- 車載LANを機能毎に分割し、フィルタリングや認証を行うゲートウェイの設置をする
  - ◆ 1. 制御・安全系、2. ボディ系、3. 情報系

### 2. なりすまし攻撃の対策

- ECU間の相互認証
- 通信メッセージの暗号化
- トラフィックパターンによる学習機能
- 外部接続点とゲートウェイでメッセージの監査機構の導入



## 防御機構に関する考察 (2/2)

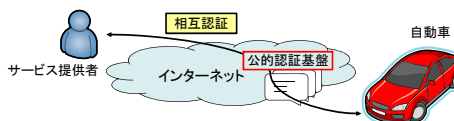
41

### 3. DoS攻撃の対策

- 制御・安全系のネットワークの二重化
- 特定の機器をネットワークから切り離す機能
- 外部接続点とゲートウェイでメッセージの監査機構導入

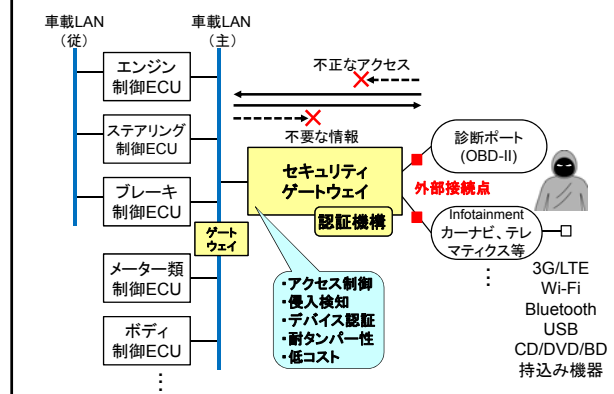
### 4. 外部サービスとの連携における対策

- 第三者による遠隔診断や故障通知のサービスの実現
- PKIのような公的認証基盤を用いた、サービス提供者と自動車との相互認証



## ゲートウェイ機構の実装例

42



43

### a) 機械学習を用いたセキュリティゲートウェイの開発

開発したプラットフォームを使った実施中の研究の1つ

44

### 車載LANトラフィックの特徴を分析

■ 実車の車載LANに流れるメッセージをキャプチャして分析

□ CANトラフィックにはCAN ID毎に3つの特徴を確認

1. 一定の周期で送信されるもの
2. 状態の変化時に追加で送信されるもの
3. 一定の周期が無く、特定動作時のみ送信されるもの

□ 特定の動作や状態によってデータ部の値が変化

- ◆ 速度情報やハンドル舵角情報などのアナログデータは連続的に変化

**CANトラフィックを機械学習することで  
動的なフィルタリングルールの生成の可能性**

45

### SGWにおける動的なルール生成機構

#### 車載セキュリティゲートウェイにおける動的なルールを機械学習によって生成

□ 機械学習によって攻撃メッセージと正常メッセージを正しく分類可能なルールを生成

□ オンライン学習を用いて動的なルールを再生成し、分類精度を向上

46

### セキュリティゲートウェイの動作

1. 導入時の初期ルールを、事前学習することで生成
  - 正常な実車トラフィックを学習
  - 分類モデルを作成
2. 分類モデルの予測分類結果をもとにフィルタリング
  - 正常、もしくは攻撃に分類
3. メッセージをオンライン学習してルールを再生成
  - メッセージと分類結果を学習し、分類モデルを更新

47

### CANトラフィックの機械学習方法

■ CANメッセージの学習による分類モデルの生成

■ 分類モデルによってCANメッセージの予測分類結果を算出

例: 入力パラメータがメッセージのデータ部の場合

CAN ID	データ部 1byte目	データ部 2byte目	データ部 3byte目	データ部 4byte目	データ部 5byte目	データ部 6byte目	データ部 7byte目	データ部 8byte目
0B4	00	31	00	02	D0	85	00	B5

予測分類結果 (スコア)

normal	attack
1.84	0.78

48

### 事前学習による初期ルールの分類精度の評価 (1)

■ 評価データ

□ 一定周期が存在する9種類のCAN ID毎に各1000メッセージ用意

- ◆ 正常メッセージ: 学習データからランダムに抽出
- ◆ 攻撃メッセージ: 実車に影響を及ぼす、なりすましメッセージを周期ランダム

CAN ID	攻撃内容
0B4	速度のなりすまし
1C4	回転数のなりすまし
394	パワーステアリング警告の誤表示
3B6	バッテリー残量の誤表示
3B7	様々な警告の誤表示
3BC	ギアランプの誤表示
620	サードブレーキとシートベルト警告の誤表示
622	ハイビーム状態の誤表示
623	ハザードのなりすまし

評価データのメッセージを初期ルールで分類  
正解率, 偽陽率を算出



事前学習による初期ルールの分類精度の評価(2) 49

- 9割以上の正解率で正しく分類可能
- 偽陽率が1割以上になるメッセージの種類が存在
  - 攻撃メッセージの誤分類が頻発

初期ルールを用いて攻撃メッセージをオンライン学習  
正常メッセージと攻撃メッセージのスコアを併用した動的ルールを生成

オンライン学習による動的ルールの分類精度の評価(1) 50

■ 動的ルールの生成

- ① なりすましメッセージを加えたトラフィックを初期ルールで分類
- ② 攻撃に分類されたメッセージを異なる分類モデルに学習
- ③ 学習したメッセージのスコアを算出し、最小スコアを**攻撃メッセージの閾値**として設定

攻撃データ		閾値の設定	
CAN ID	データ部	CAN ID	閾値
0B4	4E1FAD...	0B4	1.21
1C4	AD7E88...	1C4	2.89
.	.	.	.
.	.	.	.

オンライン学習による動的ルールの分類精度の評価(2) 51

攻撃メッセージの誤分類が減少

97%以上の正解率に向上

偽陽率が高かったメッセージが正しく分類されている  
攻撃メッセージの学習によって精度が向上

CANトラフィックに機械学習を適用したルール生成 52

実車の正常なメッセージを事前学習することで  
精度の高い初期ルールが生成可能

攻撃メッセージをオンライン学習することで  
分類精度が向上する動的ルールが生成可能

- 一定周期が存在するメッセージ
  - CAN ID毎に機械学習でルールの生成が可能
  - オンライン学習によってルールの分類精度が向上
- 一定周期が存在しないメッセージ
  - 機械学習方法、ルール生成方法の変更
    - ◆ 近いタイミングで流れているメッセージの情報など
  - 静的なルールや専用のアルゴリズムを使用

53

b) 車載LANの情報を  
第三者に安全に提供する仕組みの研究

開発したプラットフォームを使った実施中の研究の1つ

車載LANデータの活用 54

- 車載LANには、あらゆる情報が流れている
- ネット常時接続の低価格化とストレージの大容量化

→ 車載LANの情報を  
第三者に安全に提供するサービスの実現?

- ・所有者
- ・自動車メーカー
- ・ディーラー
- ・損害保険会社

## CANの生データをクラウドへ

55

データベースに格納されたCANの生データ

CANID	type	ECU名	candata	データ	受信日時
023	CAN	undefined	00 00 07 28	023#00000728	2015-11-13 17:40:02.152097
024	CAN	undefined	02 00 01 FE 41 FF 00 ED	024#020001FE41FF00ED	2015-11-13 17:40:02.174089
025	CAN	undefined	00 0A 00 02 60 00 00 00	025#000A000260000000	2015-11-13 17:40:02.105813
0A8	CAN	undefined	1A 0F 1A 0F 1A 0F 1A 0F	0A8#1A0F1A0F1A0F1A0F	2015-11-13 17:40:02.179341
0B4	CAN	undefined	00 00 00 00 00 00 00 00	0B4#0000000000000000	2015-11-13 17:40:02.131701
127	CAN	undefined	00 10 00 08 00 00 00 00	127#0010000800000000	2015-11-13 17:40:02.172389
1C4	CAN	undefined	06 00 00 00 00 00 00 00	1C4#0600000000000000	2015-11-13 17:40:02.135502
224	CAN	undefined	00 00 00 00 00 00 00 00	224#0000000000000000	2015-11-13 17:40:01.883862
230	CAN	undefined	00 00 00 01 00 00 3A	230#0000000100003A	2015-11-13 17:40:02.140242
245	CAN	undefined	00 00 00 30 7C	245#000000307C	2015-11-13 17:40:02.133986
247	CAN	undefined	06 00 FF 00 00	247#0600FF0000	2015-11-13 17:40:02.177017
260	CAN	undefined	00 00 00 00 00 00 00 00	260#0000000000000000	2015-11-13 17:40:02.133338
2A4	CAN	undefined	00 00 00 30 AB	2A4#00000030AB	2015-11-13 17:40:02.121789

## 生データの意味を解析し可視化

56

意味づけされたCANデータ



## 第三者に安全に提供する仕組みを試作

57

車載LANの情報を第三者に安全に提供するサービスの例

- 個人(所有者、家族)へ
  - 運転評価、燃費統計
  - ドライブマップ
- 自動車メーカー・ディーラーへ
  - 不具合箇所を検知して通知
  - 実車の走行時評価
- 損害保険会社へ
  - 運転リスク評価
    - ◆ 評価結果で保険料を安くなる



## まとめ

58

- DEFCON、BlackHat
  - 解析能力の向上 → 対策能力の向上
  - 便利なツールや解析ソフトウェアの入手性の向上
    - ◆ だれでもリバースエンジニアリングが可能に。よいハッカーと、悪いハッカー
    - ◆ 家電製品や身近なIoTは対象となりやすい
- IoTシステムの情報セキュリティ
  - ネットにつながる家電や自動車、産業機器にひそむ脆弱性
    - ◆ 世界レベルからのアタックに対する防御策
    - ◆ ファームウェア更新の難しさ
  - 機器単体でなく、IoTを構成するシステム全体での健全性評価の確立
- 車載LANの情報セキュリティに関する分析プラットフォームの開発およびその検証
  - 実車を使った、攻撃手法の評価
  - 機械学習を用いたセキュリティゲートウェイの研究
    - ◆ 机上での評価中、実車へ適用し評価を予定
  - 車載LANの情報まるごと上げて、第三者に安全に提供する手法の研究