Monthly Research

車載ネットワークセキュリティの現状

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 2.00.01

背景

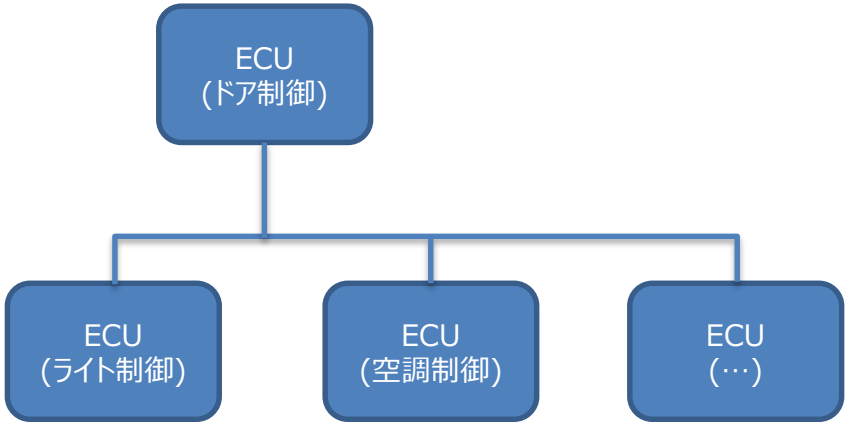
- 従来から自動車には電子デバイスが多く利用されてきた
- それらはネットワークで接続され互いに情報を交換し自動車を制御している
- 近年、自動車のネットワークへのスマートフォンやインターネットとの接続が進みつつあることで、従来にはなかった脅威が出てきている
- 今回は、自動車ネットワークのセキュリティのこれまでの動向と、今後の予測される脅威についてまとめた

車載ネットワークとは

- 現代の自動車は多くの電子部品から成り立っている
- エンジンやブレーキの制御、ドアの開閉などさまざまな部分で電子制御が行われており、それはネットワークで接続されている
  - 互いに情報をやり取りし、それぞれ適切な制御を行う
    - 速度情報の表示
    - ドアロックなど
- 代表的なものとして、CAN, LIN, FlexRayがある。

CAN (Controller Area Network)

- 車載ネットワークのデファクトスタンダード
- ECU (Electronic Controller Unit)同士を接続し、ブロードキャスト型の通信を行う。
- CANへはODB-IIポート（診断用ポート）を通してアクセスできる



車載ネットワークに関する問題の報告例1

- 2010年にUniversity of WashingtonのK. Koshcer氏らにより、「Experimental Security Analysis of a Modern Automobile」が発表された
  - 車載ネットワークのCANのセキュリティリスクについて実証
  - ODB-IIポート経由でCANにアクセス
  - ECU (Electronic Controller Unit)に対するサービス停止攻撃や、メモリ書き換えなどが可能
  - スピードメーターの改ざん、ブレーキの無効化などの危険性
  - マルウェアのECUへの感染の可能性も指摘

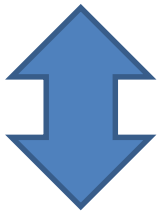
車載ネットワークに関する問題の報告例2

- 2013年のDefCon21にてCharlie Miller氏が車載ネットワークの脅威実証について発表
  - 具体的なCANパケットの取得方法、解析結果を発表
    - Ford Escape
    - Toyota Priusを具体的対象として実証
  - エンジンの停止や、ファームウェアの書き換えを実証

CANおよびECUの問題点と脅威

- CANはブロードキャスト型のプロトコルであり、盗聴が容易（暗号化なども規定されていない）
- CANの仕様そのものには認証プロセスが存在しない
  - ECUに対して任意のパケットを送信可能
  - ECU側でその真偽の確認方法がない

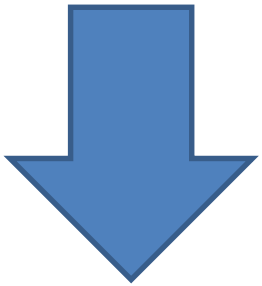
  （ただし、ECUが実装する診断用プロトコル(UDS)には認証に関する標準は存在する）
- ECUのプログラムの書き換えが可能



リアルタイム性、メンテナンス性、コストなど車載ネットワークに対する要求とのトレードオフ

新たな脅威

- 近年、車載ネットワークがスマートフォン、インターネットとの接続を持つようになってきている
- スマートフォンを経由したマルウェアによる攻撃、リモートからの攻撃も現実味を帯びる
- CANバスに接続できる、車載Android製品や無線通信用アダプタ製品も出始めている



遠隔からの車載ネットワークへのアクセスが可能になる可能性

提案されている対策

- 大きく2つの方向性
  - 従来のネットワークをよりセキュアに
    - 例：
      Cyber-Security for the Controller Area Network (CAN)Communication Protocol
      http://www.eecs.berkeley.edu/~cwlin/publications/40108_13.pdf
      CAN通信そのものをセキュアにする試み。ECU間でのパケットの認証を可能とする
  - 新たな脅威に対応する新たな技術
    - 例：
      Towards a Secure Automotive Platform
      http://www.secunet.com/fileadmin/user_upload/Download/Printmaterial/englisch/sn_Whitepaper_Secure_Automotive_Platform_E.pdf
      - ARM TrsutZoneを用いた車載ネットワークへのアクセスコントロール
      - 車載ネットワークに接続するAndroid製品などが対象（アタックベクタとして脅威）
      - Androidを動作させるCPUと、車載ネットワーク側との通信を行うOSを動作させるCPUを仮想的に切り替える
      - Android側に問題が起きても、車載ネットワーク側への影響を与えない

まとめ

- 近年、車載ネットワークのデファクトスタンダードであるCANのセキュリティ上の問題が指摘されている
- 現状ではODB-IIポートを用いた物理アクセスによるCANネットワークへの侵入の実証がされている
- 今後、車載ネットワークとスマートフォン、インターネットとの接続が加速するにしたがって、遠隔からの進入も現実のものとなる可能性がある
- ネットワークプロトコル自体のセキュア化（認証、改ざん検知）やTrustZoneを用いたネットワークへのアクセスコントロールが対策として提案されている
- 車載ネットワークへの接続デバイスの増加に伴う新たな脅威への対応を今後も続ける必要がある

参考資料

- 車載ネットワーク・システム徹底解説　(佐藤道夫 CQ出版社 2005)
- Experimental Security Analysis of a Modern Automobile
  http://www.autosec.org/pubs/cars-oakland2010.pdf
- Advectures in Automotive Networks and Control Units
  http://www.exploit-db.com/download_pdf/27404/
- 2011年度自動車情報セキュリティの動向に関する調査
  http://www.ipa.go.jp/files/000024413.pdf
- 2012年度自動車情報セキュリティの動向に関する調査
  http://www.ipa.go.jp/files/000027274.pdf
- 組み込みシステムのセキュリティ～～自動車情報セキュリティの視点から～～
  http://www.ipa.go.jp/files/000013557.pdf
- Cyber-Security for the Controller Area Network (CAN) Communication Protocol
  http://www.eecs.berkeley.edu/~cwlin/publications/40108_13.pdf
- Towards a Secure Automotive Platform
  http://www.secunet.com/fileadmin/user_upload/Download/Printmaterial/englisch/sn_Whitepaper_Secure_Automotive_Platform_E.pdf

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research