Monthly Research

セキュリティカンファレンスから見る自動車セキュリティ

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.01

アジェンダ

- 2015年10月、11月に開催された下記のセキュリティカンファレンスのうち、自動車セキュリティに関連する発表について紹介する。
  - SyScan360 2015 (中国、北京)
  - Black Hat Europe 2015 (オランダ、アムステルダム)
  - 13th escar Europe (ドイツ、ケルン)

Car Hacking: Witness Theory to Scary and Recover From Scare

SyScan360 2015
[2015.10.21-22, 中国, 北京]

- 2014年～2015年で Tesla と BYD の脆弱性を発見した Jinhao Liu 氏らによる発表
- BYD が提供する クラウドサービスに脆弱性があり、そこからパスワードを窃取することが可能だった。
  - 窃取したパスワードを使用してサービスにログインする (成りすまし) することで、自動車のドアを開けたりエンジンを始動させたりすることが可能ということをデモを通して実証
- この問題は、 DEF CON 2015 で発表された GM のテレマティクスサービスに対する脆弱性攻撃の PoC である OwnStar に近いが、特別な装置が要らない分、より単純で危険な問題である

Remote Exploitation of an Unaltered Passenger Vehicle

SyScan360 2015
[2015.10.21-22, 中国, 北京]

- Black Hat USA 2015 で発表し、Jeep Hack として話題になった Charlie Miller 氏と Chris Valasek 氏による発表
- 内容は、 Black Hat USA 2015 と同じだが、Black Hat とは異なり使用されたスライドが公開されている (参考資料を参照)
- この発表は、業界に大きな影響を与えており、この発表後９月に開催された escar Asia 2015 でも様々な発表者がこの話題に触れていた
- 具体的な内容については、彼らが公開しているホワイトペーパーや過去の FFRI Monthly Research を参照

SELF-DRIVING AND CONNECTED CARS: FOOLING SENSORS AND TRACKING DRIVERS

Black Hat Europe 2015
[2015.11.10-13, オランダ, アムステルダム]

- Jonathan Petit 氏による、自動運転には欠かせない、カメラやレーダー (LIDAR) に対する攻撃等に関する発表

- 実験に使用した レーンディパーチャー や 後方衝突警告 、歩行者警告 などの機能を持つカメラは、 650nm の波長を (国内ではレーザーダイオードとして販売されている) 照射することで周りを認識できなくなる

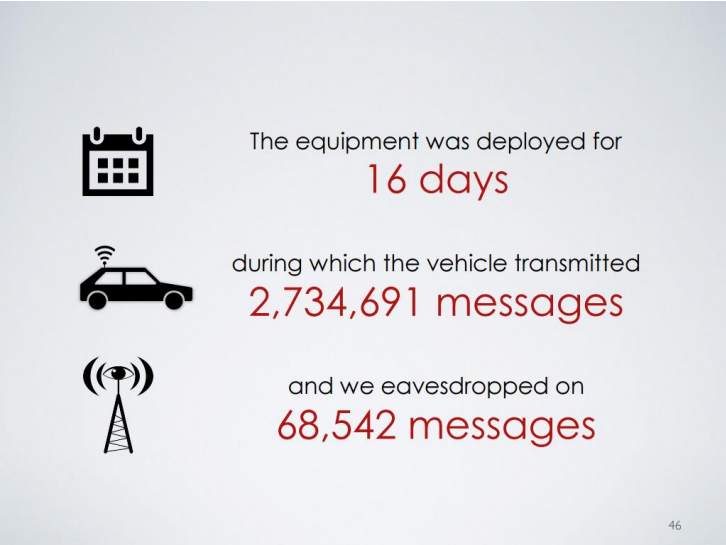
- 障害物等、周りのオブジェクトを認識するレーダー (LIDAR) については、オリジナルの信号に対して偽装した反射信号を挿入することでスプーフィングが可能な事をデモを通して実証した

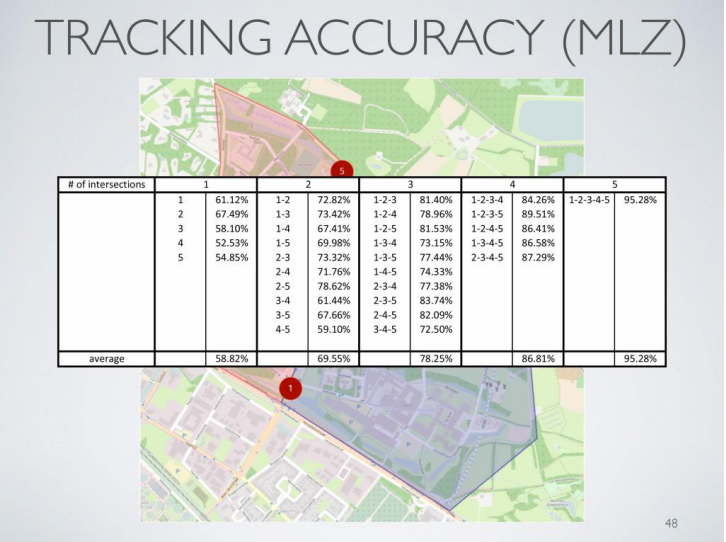
SELF-DRIVING AND CONNECTED CARS: FOOLING SENSORS AND TRACKING DRIVERS (cont.)

Black Hat Europe 2015
[2015.11.10-13, オランダ, アムステルダム]

- コネクテッド・カーの主要技術である IEEE 802.11p の盗聴による車両のトラッキングの検証結果

- 検証用の車両と、交差点に設置したステーションを使用して特定のエリアに対して検証した結果、車両から発信されたメッセージの盗聴とそれによるトラッキングが高い精度で可能であることが分かった





# of intersections	1		2		3		4		5	
	1	61.12%	1-2	72.82%	1-2-3	81.40%	1-2-3-4	84.26%	1-2-3-4-5	95.28%
	2	67.49%	1-3	73.42%	1-2-4	78.96%	1-2-3-5	89.51%		
	3	58.10%	1-4	67.41%	1-2-5	81.53%	1-2-4-5	86.41%		
	4	52.53%	1-5	69.98%	1-3-4	73.15%	1-3-4-5	86.58%		
	5	54.85%	2-3	73.32%	1-3-5	77.44%	2-3-4-5	87.29%		
			2-4	71.76%	1-4-5	74.33%				
			2-5	78.62%	2-3-4	77.38%				
			3-4	61.44%	2-3-5	83.74%				
			3-5	67.66%	2-4-5	82.09%				
			4-5	59.10%	3-4-5	72.50%				
average		58.82%		69.55%		78.25%		86.81%		95.28%

出展:https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers.pdf

Don’t Fuss about Fuzzing: Fuzzing in-Vehicular Networks

13th escar Europe
[2015.11.11-12, ドイツ, ケルン]

- Stephanie Bayer 氏らによる車両診断プロトコルの国際標準規格である UDS (Unified Diagnosis Services, ISO14229) に対するファジングのアイデアと実行結果に関する発表

- 特定のパケットを改変して送信し続けるステートレスなファジングではなく UDS のシーケンスに基づいて様々なファズパターンを送り込み、ECU からのレスポンスから判断する仕組み。

Fault Severity	Fault Kind	Reproducible	Non-Reproducible
EXPLOITABLE	Garbage Response	6	-
	Server Stopped Responding	-	2
PROBABLY_EXPLOITABLE	Response Timed Out	203	492
PROBABLY_NOT_EXPLOITABLE	Request Not Delivered	1563	-

Table 1: Triggered faults organized by severity and kind

出展:https://www.escar.info/images/Datastore/2015_escar_EU_Papers/3_escar_2015_Stephanie_Bayer.pdf

Common Security Flaws in Connected Cars Systems

13th escar Europe
[2015.11.11-12, ドイツ, ケルン]

- Yaron Galula氏による発表で、対象とした OEM (サプライヤー) や ECU などの詳細は明かされなかったが、ECU のファームウェアをリバースエンジニアリングした結果、どのような脆弱性が発見されたかを解説

- 以下の脆弱性が発見されたとのこと
  - ブートローダーの脆弱性によるRAMからのデータ読み出し
  - 使用されているオープンソースライブラリの脆弱性
  - OSにコードインジェクションの脆弱性
  - アプリケーションプロセッサからマイクロコントローラのファームウェアアップデート
  - JTAGのパスワードがアップデートファームウェアにハードコードされていた

- ECUのファームウェアアップデートにUSBやOTA経由などのユーザに依存する方法を選択する場合、通信経路やバイナリ自体の暗号化にも留意する必要がある

まとめ #1

- ITサービスとの連携
  - GM の OnStar をはじめ海外ではクラウドやモバイルデバイスと連携したテレマティクスサービスが提供されている事例がある
  - サービスの中には、モバイルアプリを通して、エンジンを始動したりドアを開けたりなどの自動車をリモートから制御する機能を提供しているものもある
  - そのため、自動車向けソフトウェアのセキュリティは車載機器だけではなくクラウドやモバイルデバイスと連携するテレマティクスサービス側でも意識する必要がある
  - 特に、 Web セキュリティや Android, iOS アプリにおけるセキュアコーディングが重要な要素である

まとめ #2

- 脆弱性の検査技術
  - 自動車に対するファジング技術のアプローチとして様々な CAN メッセージをバスに入力する方法はファジングというよりはフォルトインジェクションに近い思想であり、本来期待されるべき結果に繋がらない可能性がある（自動車がフェイルセーフモードに移行するなど）
    - そのため、 UDS のように CAN をベースとした上位プロトコルに対して行うことを検討することでより効率的に不具合を検出できる可能性がある（標準規格以外の OEM が設計する独自プロトコルに関しても同様）
  - 国外では、自動車向けのペネトレーションテストをサービスとして提供している企業もいくつかある
    - セキュリティエンジニアの育成には、ある程度のコスト・時間を要するため、社内ですぐにペネトレーションテストを実行する体制を作り上げるのは難しい
    - そのため、外部の専門企業にペネトレーションテストなどを依頼するという選択肢もある

まとめ #3

- 自動運転技術や V2X, ECU ファームウェアの OTA アップデート
  - これら技術は、近い将来民間に普及する可能性が最も高いイノベーション技術であると同時に、安全性とプライバシー保護の両面でのセキュリティ対策を考慮する必要がある
  - 3G や LTE を活用した OTA アップデートなどがインフォテイメント機器以外の ECU 等にも普及した場合、通信やファームウェアの暗号化や認証が十分に行う必要がある
    - 無線技術の普及はリモートからの攻撃領域の増加とほぼ同等である

参考情報

SyScan360 (https://www.syscan360.org/en/)

- Car Hacking: Witness Theory to Scary and Recover From Scare
  - https://www.syscan360.org/slides/2015_EN_AutomotiveCyberSecurity_JianhaoLiu_JasonYan.pdf

Black Hat Europe 2015 (https://www.blackhat.com/eu-15/)

- Remote Exploitation of an Unaltered Passenger Vehicle
  - http://illmatics.com/Remote%20Car%20Hacking.pdf
- Black Hat USA 2015サーベイレポート
  - http://www.ffri.jp/assets/files/monthly_research/MR201508_Black_Hat_USA_2015_Survey_Report_ENG.pdf
- SELF-DRIVING AND CONNECTED CARS: FOOLING SENSORS AND TRACKING DRIVERS
  - https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers.pdf
  - https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf
  - https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp2.pdf

13th escar Europe (https://www.escar.info/escar-europe.html)

- Don't Fuss about Fuzzing: In-Vehicular Networks
- Common Security Flaws in Connected Cars Systems

※スライドの閲覧にはユーザ登録 (無料) が必要

Contact Information

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