Monthly Research

自動車の脆弱性事例とCVSS v3による評価

株式会社FFRI
http://www.ffri.jp

Background

- 自動車セキュリティに関する研究は数年で急速に進んでいる
- Black Hat USA 2015 や DEF CON 23 では立て続けにインパクトのある発表が行われたが、それ以外のカンファレンスでも自動車セキュリティ領域はホットトピックである
- 自動車のサイバーセキュリティ対策はもはや必須であり、早急に検討すべきである
- 上記の背景に基づいて、本ドキュメントについては以下のトピックについて紹介、解説する
  - Black Hat/DEF CON 以外のカンファレンスでの発表
  - CVSS v3 による自動車のリスク評価手法の紹介

Agenda

- 24th USENIX Security Simposium Survey
- escar Asia 2015 Survey
- CVSS v3 概要
- CVSS v3 による脆弱性評価例
- まとめ

24th USENIX Security Symposium

Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer

- 発表内容としては自動車のイモビライザーに使用されているMegamos暗号システムが脆弱であり、攻撃によって解読されてしまう恐れがあるというもの

- 発表者は2つの問題点（攻撃手法）を挙げている
  - Partial Key-update Attack
    - ロックビットが設定されておらず、Writableな状態
    - デフォルトのPINでアンロックが可能
    - 上記に加えて、ブロック毎に秘密鍵が書き込まれることを利用し、ブロック毎にキービットを検証し暗号解読を行う攻撃手法
  - Weak key attack
    - ある車両では十分なエントロピーが確保されていない脆弱な秘密鍵によって数秒で解読できてしまうことが分かった

Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer (cont.)

- この発表は、元々は22nd USENIX Security Symposium で発表されるはずだった内容だが、英国の裁判所によって差し止め命令が出た関係で当時は発表することができず、今回の USENIX で発表されたという経緯がある

- 考察
  - リサーチャーが発表した脆弱性のうち、「Partial Key-update Attack」についてはユーザでも対策可能とのことだが、「Weak key attack」については、ディーラーなどによる対策が必要なものである

  - サイバー攻撃対策をする上で、暗号通信をすればよいというものではなく、暗号に必要な情報（秘密鍵など）をどのように生成、管理するか検討することも重要な対策といえる

Fast and Vulnerable: A Story of Telematic Failures

- OBD-II ポートを使用して自動車のモニタリングを行うデバイスの脆弱性に関する報告
- 報告では、複数の脆弱性が指摘されていて CVE 番号も割り当てられている（CVE-2015-2906, CVE-2015-2907, CVE-2015-2908）
- デバイスには、USBポートから Web UI や Telnet サービスが利用可能であり、認証が無かった
- SSH サービスに関しては、 NAND フラッシュからダンプした /etc/shadow を調べたところ脆弱なパスワードが使用されていることが分かった
- これらの脆弱性を利用することで、任意の CAN メッセージを送信可能

Fast and Vulnerable: A Story of Telematic Failures（cont.）

- 前述のサービスはすべてのネットワークインタフェースにバインドされていた（Web UI, Telnet, SSH）
- そのため、ローカルネットワークで可能ないくつかの攻撃は条件を満たすことでインターネット越しに行うことが可能
- デバイスは、 SMS (ショートメッセージサービス) コマンドに対応していて、デバイスのステータスやGPSによる位置情報、リセット、リモートアップデートができる
- アップデートは暗号化や認証無しで行われており、その結果アップデートの仕組みを悪用することで任意のコマンドを実行させることが可能

Fast and Vulnerable: A Story of Telematic Failures（cont.）

- 考察
  - 後述する escar Asia 2015 で発表された「車載診断機能 OBD-II を狙った攻撃と防御」で指摘されている脅威が現実のものとなっている事例といえる
  - 報告の中で研究者は、脆弱性があるデバイスを SHODAN を使用して検索しており、悪意のある攻撃者側もこのようにして問題のあるデバイスを探す可能性が高い
  - 自動車に対するサイバーセキュリティ対策はOEMやサプライヤーだけではなく、 OBD-II などの自動車のインタフェースを活用するベンダー側でも考えなければいけない

escar Asia 2015

車載診断機能「OBD-II」を狙った攻撃と防御

- OBD-II を介して、保険会社のサーバーに車両情報（車速や走行時間、ブレーキ回数など）を送信し、その情報に基づいて保険料率を割引するサービスに使われたOBD-II Dongle の脆弱性に関する講演

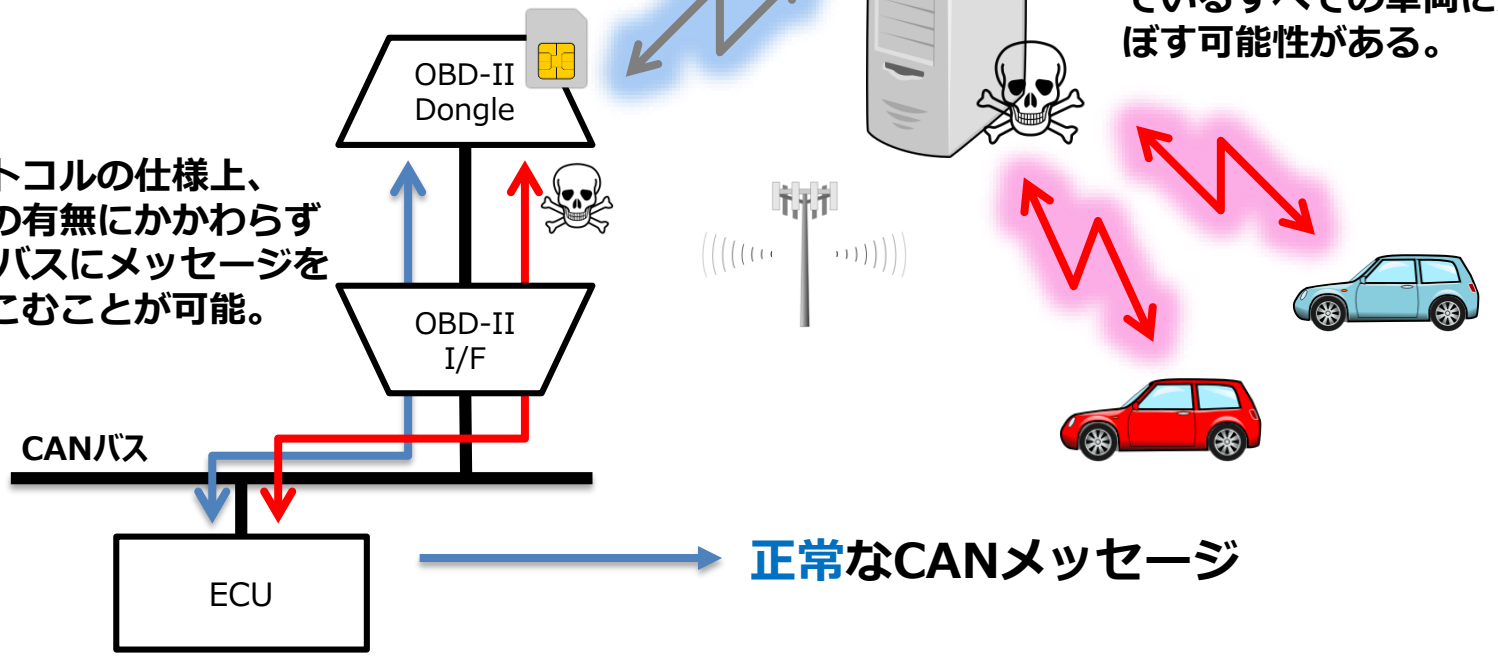
- 講演では以下の問題点が指摘された
  - 送信されるデータは暗号化が行われていなかった
  - ソフトウェアアップデート機能を持っていないため、脆弱性に対して対策することが不可能
  - OBD-II は CAN バスに簡単にアクセス可能なため、攻撃によって任意の CAN メッセージが送信されるリスクがある
  - 今回のケースのように外部サーバーとの通信を行うような仕組みの場合、サーバーが攻撃されると様々な車両に影響を与える可能性がある

車載診断機能「OBD-II」を狙った攻撃と防御（cont.）

OBD-IIを活用したアダプタは、市販のものを含めると、3G以外にもBluetoothやWi-Fiなど、様々なものがある。

バックエンド（サーバー）が攻撃された場合、サービスを受けているすべての車両に影響を及ぼす可能性がある。

プロトコルの仕様上、悪意の有無にかかわらずCANバスにメッセージを送りこむことが可能。



正常なCANメッセージ

不正なCANメッセージ

車載診断機能「OBD-II」を狙った攻撃と防御（cont.）

- 考察
  - 近年、 OBD-II を活用したデバイスが多く出回っているが、これらの利用は任意の CAN メッセージが挿入されてしまう可能性があるという リスク を認識すべき
  - 不正な CAN メッセージを挿入されないよう、モニタリング目的の場合は、特定のメッセージ以外送信出来ないような仕組みにするなどの対策に加え、クラウド連携する場合は通信の暗号化やバックエンド（サーバ）側でのセキュリティ対策も十分に行う必要がある

CVSS v3

概要

- 従来の CVSS v2 は、脆弱性によって影響を受けるシステムに対する深刻度を評価基準をしてきたが、 CVSS v3 では脆弱性のあるコンポーネント単位で評価する手法に変化している
  - 具体的な変化内容は、 IPA が公開している「共通脆弱性評価システム CVSS v3 概説」を参照

- 上記変化に伴い、攻撃による影響評価と攻撃の難易度評価が分離され、更に影響評価には影響の広がり（スコープ）が加味される

- この変化は、自動車業界においても情報セキュリティ分析とその対策の検討材料として有効と考えられる

- そこで、今回紹介した事例のうちUSENIXで発表された脆弱性について、CVSS v3 で基本値の算出例をしめす

CVSS v3による脆弱性評価例

(1) Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer

(2) Fast and Vulnerable: A Story of Telematic Failures
（CVE-2015-2906, 2907, 2908共に同じ）

評価項目	(1)		(2)	
	CVSS v3	CVSS v2	**CVSS v3**	CVSS v2
AV：攻撃元区分	**隣接**	隣接	**ネットワーク**	ネットワーク
AC：攻撃の複雑さ	**高**	高	**低**	低
Au：攻撃前の認証要否	**ー**	不要	**ー**	単一
PR：攻撃に必要な権限レベル	**不要**	ー	**低**	ー
UI：ユーザ関与レベル	**要**	ー	**不要**	ー
S：スコープ	**変更なし**	ー	**変更なし**	ー
C：機密性への影響	**高**	全面的	**高**	全面的
I：完全性への影響	**なし**	影響なし	**高**	全面的
A：可用性への影響	**高**	全面的	**高**	全面的
基本値	**6.4**	**6.2**	**8.8**	**9.0**

まとめ

- OBD-IIなどの CAN ネットワークに直接接続が可能なインタフェースを利用する側もセキュリティを意識すべきである
- 無線に関するセキュリティは近年急速に研究が進んでいる領域となるため、有線同様に盗聴のリスクを考慮すべきである
- 通信の暗号化を行う場合、秘密鍵の生成や管理方法は窃取の可能性を考慮して十分に検討すべきである
- CVSS v3 はコンポーネント単位で評価が出来ることから、自動車の情報セキュリティ分析および対策の検討段階でより効果的に利用できる可能性がある

References

- Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer
  - https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/verdult
- Fast and Vulnerable: A Story of Telematics Failures
  - https://www.usenix.org/conference/woot15/workshop-program/presentation/foster
- Vulnerability Note VU#209512
  Mobile Devices C4 OBD2 dongle contains multiple vulnerabilities
  - https://www.kb.cert.org/vuls/id/209512
- escar Asia 2015 クルマのハッキング対策 世界の最前線
  - http://techon.nikkeibp.co.jp/escar/
- 共通脆弱性評価システムCVSS v3概説
  - https://www.ipa.go.jp/security/vuln/CVSSv3.html
- CVSS 計算ソフトウェア多国語版
  - http://jvndb.jvn.jp/cvss/index.html
- CVSS v3 計算ソフトウェア多国語版
  - http://jvndb.jvn.jp/cvss/v3/index.html