様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　６ 月 １８ 日現在

機関番号：１３９０１
研究種目：若手研究(B)
研究期間：2016～2018
課題番号：１６Ｋ１６０２５

研究課題名（和文）車載制御システムの脆弱性検出手法に関する研究開発

研究課題名（英文）Study on vulnerability finding methods for in-vehicle systems

研究代表者
倉地　亮（KURACHI, RYO）

名古屋大学・情報学研究科・特任准教授

研究者番号：１０５６８０５９

交付決定額（研究期間全体）：（直接経費）　　1,200,000円

研究成果の概要（和文）：本研究では，車載制御システムに対する脆弱性の検証手法の確立を目的とする．より具体的には，車載制御システムを構成するECU(Electronic Control Unit)のセキュリティ上の脆弱性を検査する手法を研究した．本研究は，(1) 車載制御ネットワーク向けの脆弱性の検査手法の研究，(2) 車載制御ネットワークに対する攻撃手法の研究の2つのサブテーマに分けて実施した．この結果，本研究で提案する攻撃手法が実車両でも有効であることを示した．また，実車両に対する攻撃手法の知見を活かして，実システムでも有効なファジング等の脆弱性評価手法についても検討した．

研究成果の学術的意義や社会的意義
現在，自動車の制御システムを乗っ取る脅威事例が多数報告されており，脆弱性を指摘された自動車が製造者責任としてリコールしなければならない自体になっている．このため，今後出荷される自動車の多くにセキュリティ評価の実施が要求されている．しかしながら一方で，自動車の制御システムに対するセキュリティ評価手法はこれまでに十分議論されておらず，既存研究が少ないことが課題である．このため，本研究では実際の車両に対する攻撃実験などを通じて，自動車の出荷前に行う評価手法を様々検討した．今後は，本研究の成果を生かして，適切な評価基準作りを目指す．

研究成果の概要（英文）：This research focuses on establishing verification methods for in-vehicle systems. Especially, we researched methods to inspect security vulnerabilities of Electronic Control Units (ECUs) where installed in in-vehicle systems. This research is divided into two sub-themes: (1) finding vulnerabilities methods for in-vehicle networks, and (2) attack and evaluation methods for in-vehicle networks. According to our experimental results, our proposed methods are effective in real automobiles. Then, we studied and proposed more effective evaluation methods for in-vehicle systems which includes fuzzing and penetration tests.

研究分野：計算機システム

キーワード：組み込みシステム　組込みセキュリティ　自動車　情報セキュリティ　評価手法

様　式　C－１９、F－１９－１、Z－１９、CK－１９（共通）

１．研究開始当初の背景

近年，自動車のセキュリティ脅威事例が多数報告されており，セキュリティ強化が必要とされている．しかしながら一方で，自動車の制御システムに対するセキュリティ評価手法はあまり議論されていない．自動車の場合，容易にソフトウェアを回収することは規制があり難しいため，出荷前に十分検査を実施することが必要である．その一方で，コンピュータセキュリティと比較し歴史が浅いことや制御システム特有の要件から，どのように脆弱性を発見して，評価するべきかが難しいことが課題となっている．

２．研究の目的

本研究では，自動車の制御システムに対するセキュリティ評価手法を包括的に検討することを目的とする．より具体的には，既知の脆弱性を分類し，他の車両でも同様の脆弱性が発生しうるかどうかを議論する．次に，未知の脆弱性を発見するための手法について検討する．

３．研究の方法

本研究では，自動車の CAN ネットワークに対する包括的なセキュリティ評価手法を検討するため，以下の 3 つのサブテーマに分割した．

(1) 車載制御ネットワークに対する攻撃手法の整理し，既存する脆弱性情報を分類した．次に，ある自動車メーカーで発生する脆弱性が設計の異なる他の自動車メーカーの車両でも発生するかを検証する手法について研究した．
(2) 車載制御ネットワークに対するプロトコルベースのファジングテスト手法の研究として，効率的なテスト実行環境に関する研究を実施した．
(3) 未知の脆弱性を発見するための手法として，既存する攻撃手法から新たな攻撃シナリオを生成する手法を研究した．

４．研究成果

前述する研究項目に従い説明する．

(1) 研究成果として，これまでに車両メーカーから提供される脆弱性情報を整理し，既存手法としてまとめた[雑誌論文 1]．この結果，自動車メーカーごとに共通する機能と共通しない機能を分類することで，共通的な機能については自動車メーカーに依存せず，同様の脆弱性が発生する可能性を指摘した．より具体的には，車両の故障時やメンテナンス時に診断機能の搭載が必須となっている．この診断機能については，車両メーカーに依存せずに同様の問題が発生する可能性がある．このため，本研究では，複数の実際に販売されている車両を対象に，ISO14229 として標準化されている診断プロトコルの認証機能が突破できるかどうか実験した．この結果，自動車メーカーごとに多少の差異があるものの，共通するアルゴリズムを用いて，同様の脆弱性が発生することを確認し指摘した．さらに，このような攻撃を防ぐためには，車両内に搭載される制御用コンピュータである Electronic Control Unit(ECU)に機器認証を搭載する必要があることを指摘した（図 1，図 2）．[学会発表 2]
この調査結果を活用し，故障した ECU をセキュアに交換する手法についても提案した [学会発表 3]

TABLE I
SECURITY ACCESS SERVICE EVALUATION RESULTS IN REAL VEHICLES

Evaluation Items		Car A	Car B	Car C
1. Number of evaluation CAN IDs		21	41	22
2. Number of evaluated session types		66	55	79
3. Total number of security access service		75(19)	26(16)	31(17)
4. Seed length	(4-1) 1 or 2 bytes	1(1)	3(2)	1(1)
	(4-2) 3 or 4 bytes	53(18)	8(5)	12(7)
5. Regular pattern in seed values	(5-1) Always same value	3(1)	3(1)	5(3)
	(5-2) Same value in multiple times	20(14)	1(1)	7(7)
	(5-3) Always difference	9(2)	8(5)	0(0)

In this table, the number indicates the number of services. Then, "()" indicates the number of CAN-IDs.

図 1．実車両 3 台の診断機能に対するセキュリティアクセス認証の診断結果

Evaluation Item	Results(times or hours)
Average attempt	28,412,000
Average time required	47.3 hours
Minimum time required	0.5 hours
Maximum time required	108.8 hours

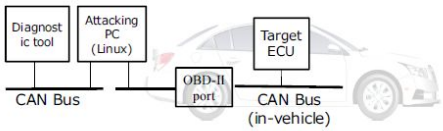
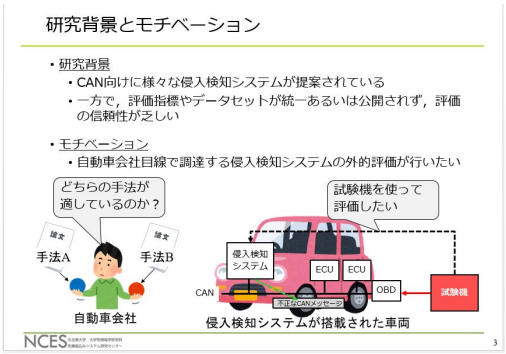


Fig. 8. Man-in-the-middle attack environment

図 2．Brute Force attack により認証を突破するのに要した時間と中間者攻撃により認証をスキップする実行環境

次に，自動車メーカー個別の機能に対する脆弱性に対する評価手法として，既存する車両から取得した CAN のデータログをベースに攻撃データセットを生成する手法を提案した [学会発表 4]．また，この攻撃データセットを生成する手法とその攻撃データセットを実機上で再生する装置の開発を実施し，その有効性を評価した(図 3，図 4)．



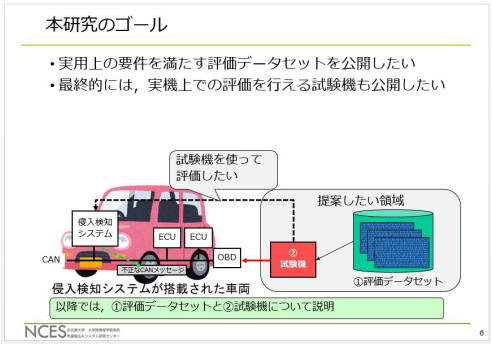
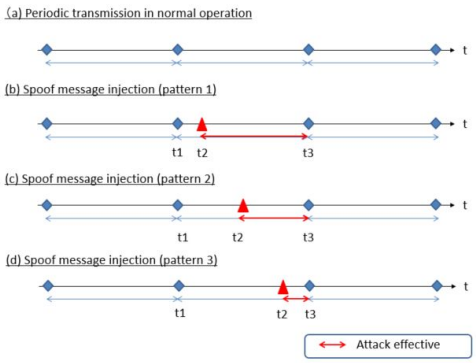


図 3．侵入検知システムの評価のモチベーション　図 4．提案する評価環境の実装

(2) 自動車の出荷前の検査において，ファジングテストの適用が検討されている．しかしながら一方で，自動車の制御システムに対するファジング手法は十分に議論されていない．このため，本研究では，まず確実にテストを実行するための環境として，Hardware In the Loop(HIL)システムを用いた評価環境を提案した．[学会発表 8]　自動車の制御システム上に配置される ECU の多くは，CAN や ECU 自身が搭載するセンサ情報を入力として制御を実行する．実行された制御結果は，アクチュエータに出力されるため，このアクチュエータへの出力結果を HILS システムで観測することにより制御結果に異常が発生していないか確認する手法である．また，仮想環境上で実行される車載制御ソフトウェアに対するファジングテストなども有効であることを示した．このような仮想環境でテストを実行する場合には，モデル検査器を用いて攻撃データを挿入するタイミングを解析した上で，攻撃が顕在化するシナリオのみを実行することができる評価フレームワークを提案した（図 5，図 6）．



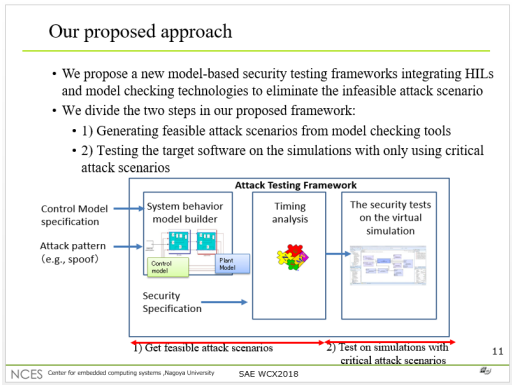


図 5．攻撃タイミングの解析方法　　図 6．提案したフレームワーク

さらに，HIL システムを用いた効率的なファジングテストを実行するため，同一の評価対象となる ECU あるいは車両を同時に同期させながら動かすことにより，攻撃環境下に置かれた ECU の制御結果と比較し，評価する手法を提案した．[学会発表 6]　この結果，第三者認証機関による外部評価を依頼する場合でも，車両内部の設計情報を渡さなくても制御結果の違いからブラックボックステストが実現できることを示した．

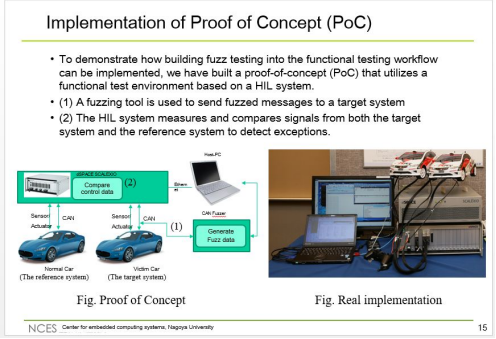


図 7．提案した HIL システムを利用したファジングテスト環境

(3) 未知の脆弱性の探索手法として，2 つのアプローチを実施した．まず，既存する脆弱性の対象を絞り込むために，既存する ECU のコーディングルールについて調査した．[学会発表 7]この結果，コンピュータセキュリティで利用されるバッファオーバーフロー脆弱性等よりも制御アプリケーション特有の脆弱性があることを指摘した．次に，未知の脆弱性に対する攻撃シナリオを導出するための手法として，モデル検査器を用いて，攻撃が成立する場合のシナリオを網羅的に導出するための手法を検討した. より具体的には, Autoencorder を用いて，既存するパケットの発生条件の特徴を分析し，攻撃パケットの生成として利用する方法を検討した[学会発表 5]．次に，実アプリケーションに対する攻撃シナリオを導出するために，自動ブレーキシステムを対象に，既存する攻撃手法がどのタイミングで発生すると攻撃が成立するかを分析し抽出する方法を提案した[学会発表 1]．本手法は，図 8 に示すような状態遷移モデルから網羅的に攻撃シナリオを抽出するための手法を実現した.

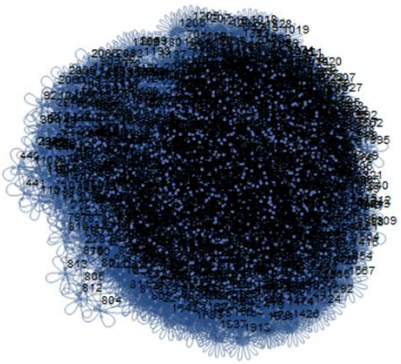


図 8. 自動ブレーキシステムに対する攻撃シナリオの導出結果(状態数は 2329，遷移数は 28665)

５．主な発表論文等

〔雑誌論文〕（計　1　件）

1. 倉地亮，制御システムに対する脅威--自動車における事例--，システム制御情報学会学会誌「システム/制御/情報」，　第 62 巻，第 4 号，pp．124-129，2018 年 4 月，査読無

〔学会発表〕（計　8　件）

1. 藤倉俊幸，倉地亮，　形式手法を用いたテストシナリオ自動生成の研究 - HILS 環境を利用したセキュリティおよび安全性試験用テストケース生成 -，　自動車技術会 2019 年春季大会学術講演会，横浜，May 2019
2. Ryo Kurachi, Kentaro Takei, Takaaki Iinuma, Yuki Sato, Manabu Nakano, Hideki Matsushima, Jun Anzai, Toshihisa Nakano, Hiroaki Takada, Evaluation of Security Access Service in Automotive Diagnostic Communication, VTC2019-spring, Kuala Lumpur, Apr 2019.
3. Ryo Kurachi, Hiroaki Takada, Naoki Adachi, Hiroshi Ueda, Yukihiro Miyashita, “Asymmetric key-based secure ECU replacement without PKI”, Workshop on Security issues in Cyber-Physical System(SecCPS), Hanzhou , Jan 2019.
4. 倉地亮，高田広章，佐々木崇光,前田学，安齋潤，松島秀樹，車載制御ネットワークの侵入検知システムに対するデータセットの提案，2019 Symposium on Cryptography and Information Security (SCIS2019)，大津，Jan 2019.
5. 藤倉俊幸，倉地亮，Autoencoder を用いた CAN メッセージの解析，2019 Symposium on Cryptography and Information Security (SCIS2019)，大津，Jan 2019.
6. Dennis Oka Kengo, Toshiyuki Fujikura, Ryo Kurachi, “Shift Left: Fuzzing Earlier in the Automotive Software Development Lifecycle using HIL Systems”, escar EU 2018, Brussel, Nov 2018.
7. Ryo Kurachi, Masato Tanabe, Jun Anzai, Kentaro Takei, Takaaki Iinuma, Manabu Maeda, Hideki Matsushima, Hiroaki Takada, “Improving secure coding rules for automotive software by using a vulnerability database”, The 20th IEEE International Conference on Vehicular Electronics and Safety (ICVES2018), Madrid, Sep 2018.
8. Ryo Kurachi, Toshiyuki Fujikura, "Proposal of HILS-based in-vehicle network security verification environment", 2018　SAE World Congress 2018(SAE WCX2018), Detroit, Apr 2018.

６．研究組織

(1)研究代表者
研究分担者氏名：倉地　亮
ローマ字氏名：RYO KURACHI
所属研究機関名：名古屋大学
部局名：大学院情報学研究科
職名：特任准教授
研究者番号（8 桁）：10568059