車載ネットワークセキュリティ演習プログラムの報告

相馬 大輔[1]　森 彰[1]　山本 秀樹[2]　畑 洋一[2]

概要：近年、自動車、プラント・工場など、様々なモノがネットワークに接続される Internet of Things の普及が進み、それらの分野でセキュリティについての検討が不可欠となっている。実際、自動車分野においては実際の車両に対しリモートでのハッキングが報告され、大規模なリコールが発生している。しかし、これまでセキュリティについて考慮する必要性が大きくなかった分野であり、実践的なセキュリティ人材が不足している。例えば、自動車分野において実践的にセキュリティを検討するためには暗号化、認証など従来から検討されているセキュリティ知識に加え、自動車に特有の背景に関する知識も必要となる。我々は、自動車分野の実践的なセキュリティを考慮可能となる人材を育成するために、車載ネットワークの基礎について学び、それへの攻撃実験を行う演習プログラムを作成した。本論文では作成した演習プログラムについて紹介する。また、演習プログラムを用いて JCSSE 2018 Bangkok で実施した car hacking workshop の様子も合わせて報告する。

キーワード：情報セキュリティ, 人材育成, 自動車, Control Area Network (CAN)

Report on In-vehicle network security exercise program

Daisuke Souma[1]　Akira Mori[1]　Hideki Yamamoto[2]　Yoichi Hata[2]

Abstract: Recently we have to mentioned about security of systems since various systems (automotive, plant, factory, etc.) are connected to the network (Internet of Things). In fact, researchers reported remote hacking of the actual automoitive and it caused a large-scale recall. Before now, it was no need for considering security in such domains. Thus there are few personnel to consider practical security. To consider practical security in automotive domain, we need the both knowledge about general IT security (encryption, authentication, etc.) and specific background of automoitive systems. In order to develop human resources capable of taking paractical secuirty in the automotive domain, we develop a exercise program to learn in-vehicle network security. The exercise program inculde from the basics of the invehicle network to the advanced attack experiments. In this paper we introduce the exercise program of in-vehicle network security and report 'Car Hahcking Workshop in JCSSSE 2018 Bangkok' using the exercise program.

Keywords: Information Security, Education, Automotive, Control Area Network (CAN)

1. はじめに

近年、自動車、プラント・工場などをはじめ様々なモノがネットワークに接続される IoT の普及が進む事で、サイバー攻撃の可能性が高まっている。しかし、それらのシステムには、これまでネットワークとは切り離されて運用されていたため、サイバーセキュリティに関しての検討が不要であった分野も多い。そのため、サイバーセキュリティへの対策が十分に行えていない可能性がある。実際、自動車分野においては 2015 年にリモートでの攻撃が報告され [7]140 万台に及ぶリコールが行われた。また、2014 年のドイツの製鉄所での不正操作 [1]、2015 年のウクライナの大規模停電 [9] などインフラなどにもサイバー攻撃による被害が及んでいる。それらのシステムのサイバーセキュリ

[1] 国立研究開発法人 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
[2] 住友電気工業株式会社
Sumitomo Electric Industries, Ltd.

ティを検討する場合、従来の情報システムのセキュリティに関する知識だけでなく、各分野に特有の知識が必須となることが多い。我々は、これまで自動車、プラント・工場をはじめとする IoT システムのセキュリティに関して研究を実施してきた。特に自動車セキュリティに関する研究成果を元に、従来の情報システムセキュリティの知識ではカバーできない車載ネットワークキュリティに関する演習教材を開発した。実車により演習を行うことは困難であるため、車載ネットワークのシミュレータを作成し、これに対して攻撃演習を行なっている。

本論文では、開発した教材について紹介し、教材を用いて実施したワークショップの様子を報告する。ワークショップは 2018 年 7 月にタイ Mahidol 大学で開催された JCSSE 2018, ICT-ISPC 2018 で Car Hacking Workshop として実施した。

2. 車載ネットワークセキュリティ演習

自動車の車載ネットワークには様々な通信が使用されているが、その中で制御に関わる情報のやり取りの多くを行なっているのが Controlled Area Network (CAN) である。CAN に関しては、すでに様々な攻撃が報告されており [2], [3], [5], [7]、攻撃への対策も検討されている [8]。これらの報告および我々の研究成果の一部を基に、車載ネットワーク CAN に焦点を当てたセキュリティ教材を開発した。

本節ではこの車載ネットワークセキュリティ演習のために作成した演習教材とカリキュラムについて説明する。

2.1 演習教材

演習では、図 1 に示す機材を用いた。図 1 左の PC および機材はオシロスコープである。これを用いて、送信タイミングや攻撃時の通信の様子を観測する。図 1 右側の PC およびインターフェイスは CAN メッセージの送受信を行うためのものである。インターフェイスを通じて CAN バスへ接続し、can-utils や Python などを使用して通信の分析、攻撃をする。図 1 中央および図 2 はラズベリーパイを用いた CAN シミュレータである。ラズベリーパイとチップが接続されたボードが、ECU (Electronic Control Unit)1 つに相当する (以後、これをノードと呼ぶ)。3 つのノードによりメッセージをやり取りし、実車シミュレーションを行う。各ノードのスイッチや LED は、ブレーキ、アクセル、ステアリングやライトといった自動車の機能の代わりである。また、スイッチのみのボードは CAN シミュレータの電源やモード切替を行うためのシミュレータ操作スイッチである。モードの詳細については 2.1.1 で説明する。

2.1.1 CAN シミュレータ

攻撃演習には実車の CAN 通信を元に作成した CAN シミュレータを開発した。CAN 通信が可能なものとして [10], [12] などで報告されているテストベットがある。

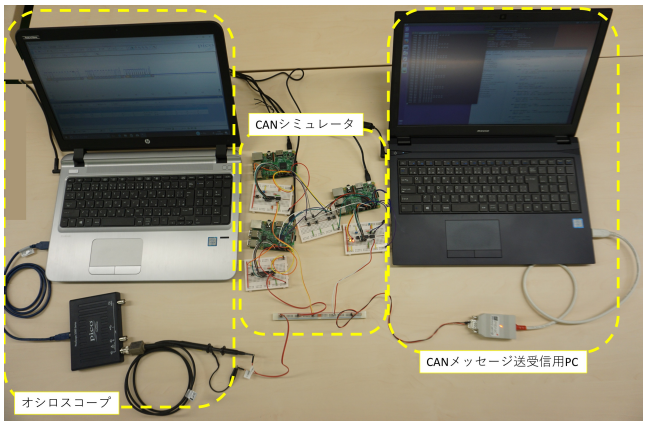

図 1 演習機材

作成した CAN シミュレータは操作スイッチ、CAN バス、3 つのノードで構成されている (図 2)。ノードは制御メッセージ受信ノードと送信ノードの 2 種類がある。

スイッチがついている 2 つのノードが送信ノードである。これらは LED を制御するメッセージを送信する。スイッチの on/off により送信するメッセージのデータを変える。

LED がついているノードが受信ノードである。受信ノードは制御メッセージを受信し、そのデータにより LED の明滅を制御する。つまり、送信ノードはブレーキペダル、アクセルペダル、ステアリングや各種スイッチの ECU に相当し、受信ノードはブレーキ、エンジン、タイヤや各種機能を制御する ECU に相当する。

CAN シミュレータによって行われる通信は、simple モードと complex モードの二つのモードがある。各モードの目的と通信の概要について以下で説明する。

simple モード

simple モードは CAN 通信の観測や攻撃の練習をするために、 [3] を参考に作成したモードである。各ノードの振る舞いは以下の通りである。

- 送信ノード 1
  1 秒周期で ID x と ID y のメッセージを続けて送信する ($x < y$)。
- 送信ノード 2
  ID x のメッセージを受信した場合、ID z のメッセージを送信する ($y < z$)。送信するメッセージのデータはスイッチ on の時は D_1、スイッチ off の時は D_2。
- 受信ノード
  ID z、データ D_1 のメッセージを受信した場合、赤と黄の両方の LED を点灯する。ID z、データ D_2 のメッセージを受信した場合、赤と黄の両方の LED を消灯する。

complex モード

complex モードは実車で行われている CAN 通信を基に、実車に対しての攻撃を体験できるよう作成したモードであ

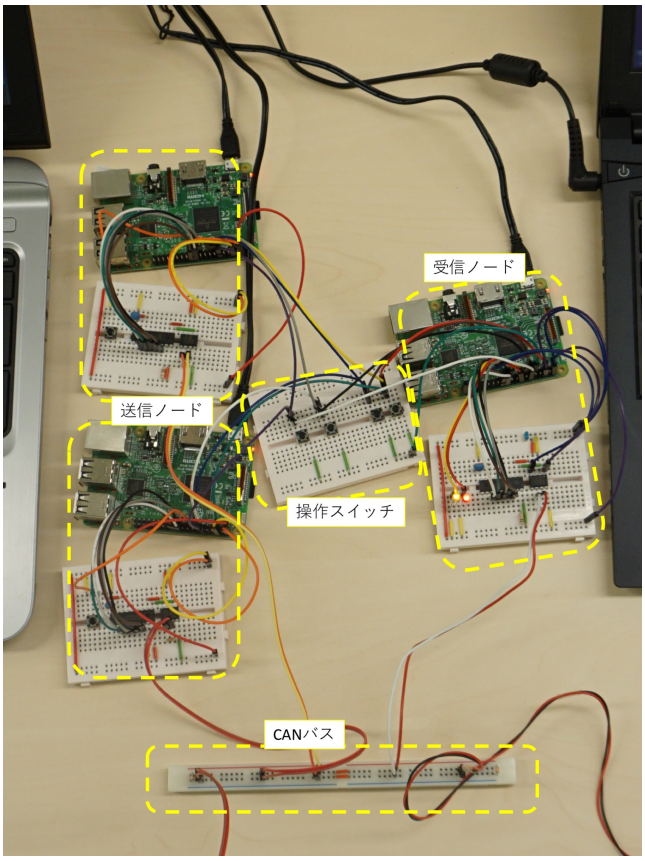

図 2 CAN シミュレータの構成

る。各ノードの振る舞いは以下の通りである。

- 送信ノード 1
  ある ID x_1 のメッセージを受信した場合、ID y のメッセージを送信する ($x_1 < y$)。送信するメッセージのデータはスイッチ on の時は Y_1、スイッチ off の時は Y_2。
- 送信ノード 2
  ある ID x_2 のメッセージを受信した場合、ID r のメッセージを送信する ($x_2 < r$)。送信するメッセージのデータはスイッチ on の時は R_1、スイッチ off の時は R_2。
- 受信ノード
  ID x_1、x_2 を含む 10 種類の ID のメッセージを送信する。ID x_1、x_2 は、周期的に送信する。その他のメッセージは周期的またはランダムに送信を行う。
  ID y、データ Y_1 のメッセージを受信した場合、黄の LED を点灯する。ID y、データ Y_2 のメッセージを受信した場合、黄の LED を消灯する。
  ID r、データ R_1 のメッセージを受信した場合、黄の LED を点灯する。ID r、データ R_2 のメッセージを受信した場合、黄の LED を消灯する。

また、各メッセージのデータにはメッセージカウンターやチェックサムなどの仕組みも付与している [6]。

2.2 演習カリキュラム

車載ネットワーク演習は 1 日の集中プログラムとして開発をした。対象者に車載ネットワークの予備知識を仮定せず、CAN の基礎から高度な攻撃まで理解することを目標としている。まず、IoT セキュリティの現状、車載ネットワークの概要と攻撃手法に関する座学を行う。この座学の理解を深めるために、単純な車載通信のシミュレーションを用いた通信実験や攻撃練習を行う。最後に、複雑な実車シミュレーションへ攻撃をおこなう。表 1 に演習スケジュールを示す。

2.2.1 IoT セキュリティの現状、車載ネットワークの概要と攻撃手段

まず自動車を含む IoT システムのセキュリティに関する状況、特に本演習で取り上げる自動車の内部ネットワークのセキュリティへの検討状況について把握することを目的とし、IoT セキュリティの概要および攻撃事例について詳細な説明を行う。特に自動車分野についての事例などを多く取り上げるが、工場・プラント、航空機、医療機器などについても触れる。

次に、本演習で対象としている車載ネットワーク CAN について、その特性および通信の基礎的な仕組みの説明を行う。本プログラムは 1 日のコースを想定しているため、CAN の仕様全てに触れることは難しい。そのため、詳細な説明は CAN を特徴付ける部分と本プログラムに関連する部分に絞っている。特に本プログラムでは、メッセージ送信権獲得メカニズム (アービトレーションを含む) とエラー処理メカニズムの部分が重要である。

最後に CAN 通信によって制御されている機能の操作および、機能を不能にする攻撃手法について説明を行う。ここでは CAN の仕様を悪用したメッセージインジェクションによる機器操作と、bus-off 攻撃を説明する。bus-off 攻撃にはいくつかの方法が報告されているが [3], [5], [8]、本プログラムでは CAN の仕様に従ったメッセージを攻撃に用いる bus-off 攻撃 [3] を対象として取り上げている。最終的に実車シミュレーションに対し、これらの攻撃手法を再現することが目標である。

2.2.2 攻撃練習と実車シミュレーションでの攻撃再現

CAN 通信の特徴や攻撃手法に関する理解を深めるために、CAN シミュレータの simple モードに対して攻撃練習を行う。攻撃練習の目標は「メッセージインジェクションによる LED 操作」、「bus-off 攻撃による LED 点灯不能」の二つである。

まず、攻撃対象のメッセージを特定するために、can-utils やオシロスコープなどのツールを利用したメッセージ受信・観測・分析を行う。simple モードでは高々 3 種類しかメッセージがないため容易に特定可能であるが、実車 (本プログラムでは実車シミュレーション) で実施できるよう、様々なツールの使い方を試す。次に特定したメッセージか

表 1　カリキュラム

	実施項目	学習目標
座学	• IoT、自動車セキュリティの現状について • 車載ネットワーク CAN の仕組みについて • CAN に対する攻撃 (メッセージインジェクション、bus-off 攻撃)	• IoT、特に自動車分野におけるセキュリティの現状を理解する。 • アービトレーションやエラー処理など CAN 通信の特徴と、CAN への攻撃手法を理解する。
演習	• 使用機材およびソフトウェアツールの説明と通信実験 • CAN 通信への攻撃練習 • 実車シミュレーションでの攻撃再現	• CAN 通信の仕組みを実際の通信を通して確認する。 • CAN メッセージを解析できるようになる。 • CAN 通信への攻撃を再現し、対策について検討できるようになる。

ら攻撃メッセージを作成、送信し LED の操作を行う。意図した通りに LED の操作を行うために満たすべき条件 (送信頻度やタイミングなど) を考えることが目的である。ここでは攻撃メッセージの送信に can-utils や Python などを使用する。最後に特定したメッセーに対し bus-off 攻撃を行う。bus-off 攻撃の成功には攻撃メッセージが以下の 3 つの条件を満たす必要がある。
[条件 1]攻撃対象メッセージと同じ ID をもつ。
[条件 2]攻撃対象メッセージと異なる、適切なデータをもつ。
[条件 3]攻撃対象メッセージと同じタイミングで送信する。

攻撃練習ではある条件に従って攻撃メッセージを送信すると、[条件 3] は自動的に成立するよう設定した。その条件についても事前に説明し、[条件 1]、[条件 2] の検討に集中できるようにした。[条件 3] が自動的に成立する仕組みは解説だけにとどめている。

最後に、モードを complex モードに変更し実車シミュレーションに対し攻撃を行う。実車シミュレーションでの目標は黄 LED と赤 LED それぞれの操作と点灯不能である。黄 LED の攻撃難易度は、受信ノードからのメッセージ送信により特定が困難になっている以外、simple モードでのものと大きく変わらない。赤 LED の攻撃難易度は、受信ノードからのメッセージ送信に加え、赤 LED 制御メッセージ自身にもメッセージカウンタなどを付与し特定を困難にしている。さらに、bus-off 攻撃については、攻撃練習での解説を基にタイミングを合わせる工夫が必要となるように設定している。

3. JCSSE 2018 Car Hacking Workshop

本節では演習プログラムを用いて 2018 年 7 月 11 日にタイ Mahidol 大学で行った Car Hacking Workshop について報告する。参加者は情報科学の大学院生や研究者など (詳細なバックグラウンドは不明)14 名。演習教材毎に 2-3 名の 6 グループに別れ、以下に示すスケジュールで実施した。

- 09:00 - 10:30
  Overview: IoT Secuirty and Recent Automotive Security Incidents
- 10:30 - 10:50
  Break
- 10:50 - 12:00
  CAN BUs Basics and Attack Methods (group work)
- 12:00 - 13:00
  Lunch
- 13:00 - 16:00
  CAN Bus Attack Exercises

攻撃練習、実車シミュレーション共に通信の分析および攻撃対象となるメッセージの同定はほぼ全てのグループが達成できていた。一部のグループが達成できなかったのは、他の課題を優先し同定を行っていなかったためであった。また、メッセージインジェクションによる LED 操作についても同様の結果であった。対象メッセージの同定方法はスライドによる説明のみであったため、試行錯誤を繰り返すグループが多く見られた。メッセージ同定のデモを交えて解説することで、より理解しやすいものになるのではないかと考える。

bus-off 攻撃の再現は一部のグループが達成できなかった。攻撃練習での bus-off 攻撃で再現できなかったのは 2 グループで、攻撃メッセージの送信条件の理解ができていなかった。本設定による bus-off 攻撃の原理をわかりやすく解説する方法が必要と考えられる。また、実車シミュレーションでは、攻撃メッセージの送信条件の同定まで必要とした。半分のグループがこの同定をできず、達成できなかった。さらに、赤 LED はメッセージ送信タイミングを合わせるための工夫ができなかった。全ての課題を達成できたのは 1 グループのみであった。

攻撃練習および実車シミュレーションでの攻撃再現における課題達成状況を表 2 に示す。

表 2　課題達成状況

課題	達成率 (達成グループ数/全グループ数)
攻撃練習 対象メッセージ同定	6/6
攻撃練習 LED 操作	6/6
攻撃練習 bus-off 攻撃	5/6
実車シミュレーション 黄 LED メッセージ同定	6/6
実車シミュレーション 黄 LED 操作	6/6
実車シミュレーション 黄 LED の bus-off 攻撃	3/6
実車シミュレーション 赤 LED メッセージ同定	5/6
実車シミュレーション 赤 LED 操作	5/6
実車シミュレーション 赤 LED の bus-off 攻撃	1/6

4. 考察と今後

本論文では、IoT システム、特に自動車のセキュリティを実践的なレベルで扱える人材育成を行うことを目的とし作成した車載ネットワークセキュリティ演習の教材について紹介した。また、演習教材を用い、タイ Mahidol 大学で実施した Car Hacking Workshop の様子について報告をした。自動車の車載ネットワークにおいて重要な位置を占める CAN に関する理解、実車への攻撃方法・通信分析方法の取得に関して、本教材を用いて十分な効果が確認できたと考えられる。一方で高度な攻撃である bus-off 攻撃に関しては、多くの参加者が理解できていたと思われるが、その確認となる攻撃再現が達成率が良いものではなかった。攻撃の理解をより容易にする工夫を行うことで、この点の改善ができると考えられる。また、IoT の普及はプラント・工場、医療機器、鉄道、航空機など様々な分野へ広がっていくと考えられる。そのため自動車だけでなく、それらの分野の演習も今後必要になる。そのために、すでに複数の攻撃・被害が報告されている工場・プラントの演習を作成することを考えている。

今後、本教材を学生向けに提供し各 IoT セキュリティの普及を目指すとともに、早急に実践的なセキュリティ人材を必要とする企業への教材提供も行う予定である。

謝辞

今回、車載ネットワークセキュリティ演習プログラムを実施する機会をいただいた Mahidol 大学 ICT (Faculty of Information and Communication Technology) の Vasaka Visoottiviseth 助教授に感謝いたします。

参考文献

[1] BSI, The State of IT Security in Germany 2014, 2014.
[2] C. Smith, The Car Hacker's Handbook: A Guide for the Penetration Tester, No Starch Press, 2016.
[3] K. Cho, and K. G. Shin. "Error handling of in-vehicle networks makes them vulnerable," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016.
[4] ISO 11898, Road vehicles – Controller area network (CAN), 2015.
[5] R. Kameoka, T. Kubota, M. Shiozaki, M. Shirahata, R. Kurachi and T. Fujino, "Bus-Off Attack against CAN ECU using Stuff Error injection from Raspberry Pi," Proceedigs of Symposium on Cryptography and Information Secuirty (SCIS), Japan, 2017 (in Japaneses).
[6] C. Miller and C. Valasek, Adventures in Automotive Networks and Control Units, DEFCON 21, 2013.
[7] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, 2015.
[8] A. Palanca, E. Evenchick, F. Maggi and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against automotive networks," International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, Cham, 2017.
[9] R. M. Lee, M. J. Assante and T. Conway. Analysis of the cyber attack on the Ukrainian power grid, SANS Industrial Control Systems, 2016.
[10] 遠山 毅, 小熊 寿 and 松本 勉, ポータブルな自動車向けセキュリティテストベッド, 電子情報通信学会 ハードウェアセキュリティ研究会, 弘前, 2017.
[11] Vector, The Virual VectorAcademy, https://elearning.vector.com/vl_index_en.html
[12] X. Zheng, L. Pan, H. Chen, R. Di Pietro, and L. Batten, "A testbed for security analysis of modern vehicle systems", Trustcom/BigDataSE/ICESS, IEEE, 2017.