

令和 3 年 6 月 9 日現在

機関番号：12612

研究種目：若手研究

研究期間：2018～2020

課題番号：18K18047

研究課題名（和文）レーザを用いてセンサに誤情報を挿入する攻撃とその対策に関する研究

研究課題名（英文）A study on laser-based signal injection attack and its countermeasure

研究代表者

菅原 健（Sugawara, Takeshi）

電気通信大学・大学院情報理工学研究科・准教授

研究者番号：60785236

交付決定額（研究期間全体）：（直接経費） 3,200,000円

研究成果の概要（和文）：スマートフォンやスマートスピーカーで使われる小型マイクにレーザーを照射することで、実際には無音であるにも関わらず、あたかも音声を受信したかのような電気信号を発生させることができる現象を発見した。また、この現象が音声アシスタントに及ぼす脅威を明らかにした。市販されている機器に対して安全性評価を行い、レーザーポインター程度のパワーで、100メートル以上先から攻撃ができることを明らかにした。本研究成果により、セキュリティ分野のトップカンファレンスである USENIX Security に採録を受けた。本脆弱性について責任ある脆弱性開示を行い、対策構築に協力した。

研究成果の学術的意義や社会的意義

センサに誤情報を挿入する攻撃は活発に研究されているが、提案法は、物理量変換（光から振動）を伴う初めて攻撃である点に大きな学術的意義がある。また、スマートスピーカーのマイクを対象とする攻撃研究の流れとしては、従来法の数倍に攻撃可能距離を延伸した点に意義がある。また、成果への社会的関心も高く、脆弱性開示のタイミングでは、CNN を始めとする一流メディアで報道された。また、スマートスピーカーのメーカーなどの関係各所に対して脆弱性開示するとともに、攻撃の理解と対策について協力を行った。

研究成果の概要（英文）：We discovered a new attack that injects arbitrary audio signals to a target microphone by aiming an amplitude-modulated light at the microphone's aperture, and proposed a command injection attack on voice-controllable systems such as smartphones and smart speakers. We evaluated several products showing that we can achieve a successful injection from more than 100 meters using laser power similar to ordinary laser pointers. The paper is accepted at USENIX Security 2020, which is one of the most prestigious conference in the computer-security research field. We made responsible disclosure and collaborated with the vendors for mitigating the vulnerability.

研究分野：セキュリティ

キーワード：ハードウェアセキュリティ センサのセキュリティ 音声アシスタント レーザー 光音響効果

科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

1. 研究開始当初の背景

情報システムと自動車・ロボット・工場などが連携することで、社会を自動・自律化することへの期待が高まっている（図1）。そのような情報システムと物理世界の結合の強化は世界的な潮流であり、Internet of Things (IoT) やサイバーフィジカルシステムとして技術開発が進められている。情報システムと物理世界をつなぐインターフェースであるセンサが信頼できることは、そのような技術開発を押し進めるための大前提である。

それに対し、妨害信号の照射によりセンサへ誤情報を挿入するシグナルインジェクション攻撃の脅威が指摘されている。ジャイロセンサに超音波を照射してセンシングを妨害することでドローンを墜落させる攻撃や、車載測距センサに妨害電波を照射することで、無いはずの物体をあるように誤認させて自動運転を妨害するような攻撃が知られている。

センサへの攻撃は、未だデータになっていないアナログ領域での攻撃であり、従来の情報セキュリティ技術では対策ができない。そのため、アナログ情報を守るための新しいセキュリティ技術が必要である。

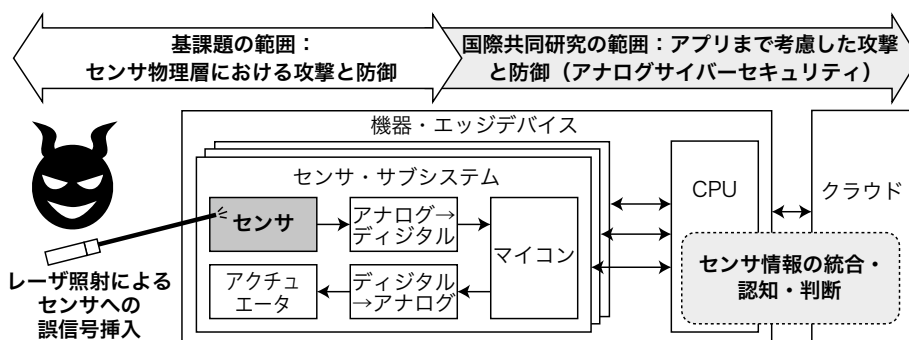


図1 センサを備えた情報システムに対する、レーザー照射によるセンサへの誤信号の挿入

2. 研究の目的

レーザーには、大きなエネルギーを遠隔に届けることができる点と、振動や熱などのセンシング対象の物理量への変換が容易であるという優れた性質があり、計測器や加工機に应用されている。レーザーがセンサへの攻撃手段として利用された場合、深刻な脅威になりうるとの着想を得た。特に、変調したレーザーを照射することで、ジャミングだけでなく、シグナルインジェクション攻撃ができる可能性がある。

以上の着想に基づき、「レーザー照射によるセンサへの誤信号挿入」の実現可能性とその脅威をオフenseセキュリティの立場から研究する。そうすることにより、センサへのシグナルインジェクション攻撃に関する脆弱性を事前に発見することを目的とする。究極的には、(i) その脆弱性が悪用される前に事前に対策を行うこと、(ii) 攻撃技術をオープンに議論することで、社会全体としてセキュリティ技術を高めていくことを目的とする。

3. 研究の方法

まず、どのようなセンサが影響を受け、どのような影響があり得るのかを分析するところから研究に着手する。その分析の結果を元に、危険性が高いと思われる対象について実証実験を行い、その結果を元に対策法を構築するという計画で研究を行った。より詳細には以下の通りである。

(I) 脅威の明確化。 レーザとセンサには大きな多様性がある。その中で、どのような組み合わせで攻撃が有りうるかを、系統的な脅威分析により明らかにする。もし攻撃が原理的に可能であることが分かった場合、そのセンサの応用例に照らし、攻撃によって生じうる被害（攻撃シナリオ）を明らかにする。以上の結果として、対象のセンサ、レーザーの利用法、および攻撃シナリオをまとめた脅威リストを得る。

(II) 脅威の実証と攻撃者のモデル化。 (I) で作成した脅威リストのうち、深刻度の高いケースについて、まず妨害信号の挿入ができるかどうかの実証実験を行なう。もし単純な攻撃ができることが分かった場合、攻撃者がどれだけ精密に妨害信号を制御できるかを追求する（図2・ステップ1）。それにより、センサなりすまし攻撃は実行できるのか、またできるならばどの程度の精密さなのかを明らかにできる。以上により、対策の前提となる、攻撃者に想定される能力（攻撃者モデル）を決定することができる。

(III) 対策技術の構築. (II)で得た攻撃者モデルに基づき、対策のための信号処理技術を構築する。より具体的には、攻撃がされていることに気づくための攻撃検知法と、妨害信号があった場合でも動作し続けられるような、攻撃無効化法を構築する(図2・ステップ2)。また、それらの有効性を実験により実証する。加えて、上記対策法を、(II)で検討したレーザーの吸収・遮蔽と組み合わせることで、対策効果と、ハードウェア・ソフトウェアコストの関係を明らかにする。

アナログサイバーセキュリティ研究への発展 上記(I)および(II)の進捗の結果、レーザー照射によって対象物体に振動を発生させることが、マイクに誤信号を挿入する強力な手段になりうる事が明らかになった。基課題は、センサの物理層を範囲としており、アプリケーションへの影響は机上検討に留めていた。しかし、予想を上回る進捗を得たことで、センサだけではなく、スマートスピーカーや自動運転車などのアプリケーションのセキュリティ(アナログサイバーセキュリティ)に研究を拡張する道筋を得た。

研究の遂行には、アプリケーションのセキュリティに関する豊富な研究経験と、ケーススタディのための実験設備が不可欠である。そこで、その両者を兼ね備えた共同研究者との国際共同研究を立案するに至った。そこで、本課題を基課題として、科研費・国際共同研究強化(A)へ応募し、「レーザーを用いてセンサに誤情報を挿入する攻撃のアナログサイバーセキュリティ(18KK0312)」として採択を受けた。その結果、2019年4~11月の期間で米国ミシガン大学へ滞在し、国際共同研究を行った。

4. 研究成果

脅威分析を行ったところ、レーザー照射によって対象物体に振動を生じさせることができれば、従来の超音波によるシグナルインジェクション攻撃と同様の脅威があるとのアイデアを得た。また、基礎実験により、実際に生じることを確認した。これは、予想を上回る発見であり、それにより、センサ単体だけではなく、スマートスピーカーや自動運転車などのアプリケーションのセキュリティ(アナログサイバーセキュリティ)に研究を拡張する道筋を得た。

以上を元に、レーザーによる振動の励振が、アプリケーションのレベルでどのような意味を持つかという方向に研究を進めた。「レーザー照射によるセンサへの誤信号挿入」では、対象のセンサにレーザーを照射しなくてはならないことが、攻撃者にとっての大きな制約事項となる。特に、多くの製品ではシャーシが光を遮蔽するため、センサに光を届けるのは容易ではない。以上の制約条件の基で検討を重ねたところ、マイクが重要なユースケースであるとの結論に至った。音波を取り入れなくてはならないという性質上、マイクは開口部を介して外界に対して露出しており、そこから光が侵入するためである。中でも特に、スマートスピーカーに代表される音声アシスタントへの攻撃が、セキュリティ上の被害を引き起こす可能性に至った。

以上より、レーザー照射を元に、遠隔から無音で音声コマンドを挿入する **LightCommands** の着想に至った。**LightCommands** の実現可能性と、その深刻さを定量的に評価するために、以下の小課題に分解し、それぞれを解決するというアプローチで研究を行った。

- レーザー照射によってマイクに生じる電気信号の特性の評価
- 攻撃可能な距離・状況の定量的評価
- 音声コマンドの挿入により生じる被害の調査
- 対策法の検討

レーザー照射によってマイクに生じる電気信号の特性の評価 スマートスピーカーなどで一般的なMEMSマイクを対象に基礎実験を行い、レーザー照射実験を行った。その結果、強度を振幅変調したレーザー光を照射すると、ほぼ線形な変調信号がマイク出力に現れることを明らかにした。これはすなわち、任意の音声信号を対象のマイクに挿入できることを意味している。また、これが、多くのMEMSマイクで生じる一般的な現象であること、レーザーポインタ程度の弱い光でも十分に生じることを明らかにした。

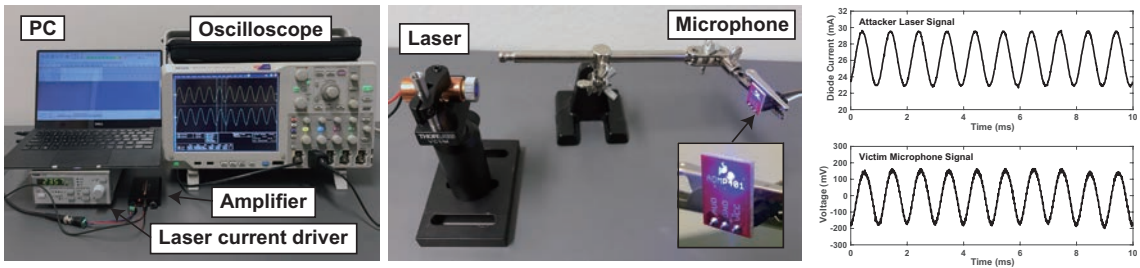


図2 MEMS マイクを搭載した評価基板を用いた基礎実験. (左) 評価装置の全体. (中央) レーザーダイオードから照射した光をマイクの開口部に照射する様子. (右) 強度変調したレーザーの振幅に対応する信号が、マイクより出力された様子

攻撃可能な距離・状況の定量的評価

複数の音声アシスタント (Amazon Alexa, Apple Siri, Facebook Portal, そして Google Assistant) に対応する機器 (スマートフォンとスマートスピーカーを含む合計 18 機種) を評価し、その全てでレーザー照射による音声コマンド挿入が行えることを明らかにした。また、以下の写真に示すようなセットアップで実験を行い、攻撃可能な距離を定量的に評価した。その結果、特に感度が高い機器では、レーザーポインタ程度の弱い光でも 110 メートル以上の遠方から攻撃できることを示した。

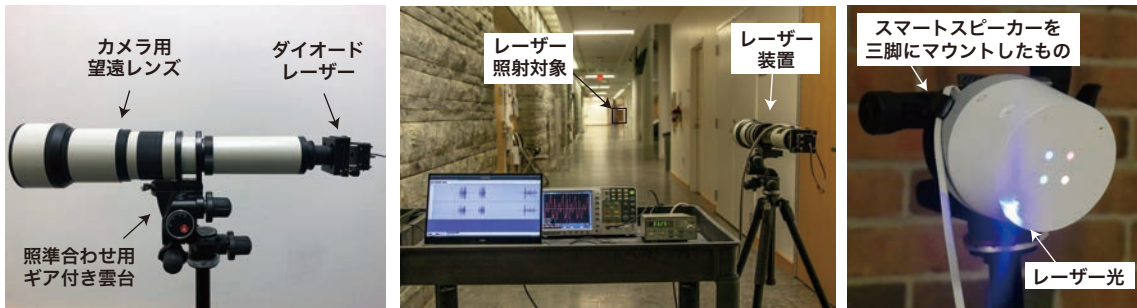


図3. 攻撃可能な距離を調べる実験の様子: (左) レーザーを望遠レンズにマウントした装置, (中) 110 メートル遠方にあるスマートスピーカーに照準合わせをしている様子, (右) 対象にレーザーが当たっている様子

また、制御されていないより現実的な状況でも攻撃が可能であることを示すために、図4に示すように、70 メートル離れた建物から、隣の建物の一室に対して窓ガラスを貫通してレーザー照射を行い、その場合でも攻撃が可能であることを実証した。



図4 70 メートル離れた隣の建物から、窓ガラス越しにレーザーを照射することで音声コマンドを挿入する実証実験の様子

音声コマンドの挿入により生じる被害の調査 LightCommands により、攻撃者は、正規所有者に気づかれることなく、遠隔から音声コマンドを挿入することができる。そのことが、どのような脅威を引き起こしうるのかを研究した。音声アシスタントは、さまざまな周辺機器と連携して動作するため、脅威は、それらの周辺機器の提供する機能に対応する。そこで、セキュリティ上の意義が大きいと思われる周辺機器をリスト化し、安全性評価を行った。

研究の結果、音声アシスタントにはセキュリティの認証が全く無い場合や、もしあったとしても不適切な実装がされている（例：PIN を総当りできる）場合があることを明らかにした。その結果、(i) スマートロックの解錠、(ii) ガレージドアの開放、(iii) E コマースサイトによる買い物、および (iv) VCS に接続された特定車種（Tesla および Ford）の位置特定、解錠、およびエンジン始動が行えることを示した。

対策法 以上の評価実験における知見を元に、いくつかの対策法を提案した。（ハードウェア再設計を伴わない）ソフトウェアによる対策法としては、認証の層を追加することで攻撃を緩和できることを示した。また、ユーザと機器の間で簡単なインタラクションをすることや、複数マイクを用いて異常検知を行うことでも攻撃の難易度を上げることができることを示した。ハードウェアによる対策としては、機器をカバーなどで覆うことで、攻撃者からマイクまでの視線を遮ることことが対策になることを示した。

産業界への還元 責任ある脆弱性開示（Responsible Disclosure）の実践に従い、関連企業・機関に対して事前に脆弱性開示を行い、合意した情報解禁日（2019 年 11 月 4 日）に公知化した。また、関連企業・機関の技術者と連携して、発見した攻撃の理解と緩和法構築に協力した。事前に連絡を行った企業・機関は以下の通りである：Google, Amazon, Apple, August（スマートロック製造者）、Ford, Tesla, Analog Devices（MEMS マイクの製造者）、ICS-CERT（産業機器に関する脆弱性を取り扱うコーディネーター）、およびアメリカ食品医薬品局（FDA）。

出版物 セキュリティ分野のトップカンファレンスである USENIX Security Symposium 2020（採録率 16.1%、T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, “Light Commands: Laser-Based Audio Injection on Voice-Controllable Systems,” USENIX Security Symposium 2020, 2020）に採録を受けたのが主たる研究成果である。この成果を国内に周知することを目的に、国内学会（コンピュータセキュリティシンポジウム 2020）において日本語でも発表した。また、複数の学会・学会研究会において招待講演を行った：

- SPQR Laboratory Embedded Security Workshop
- 暗号と情報セキュリティワークショップ 2020
- 第 5 回 IoT セキュリティフォーラム
- FIT2021 トップカンファレンスセッション（発表予定）

また、上記発表に関連して、電子情報通信学会・情報セキュリティ研究会・研究会活動貢献感謝状の授与を受けた。

以上と並行して、レーザー照射によるセンサへの誤信号挿入に関する研究成果を、レーザー照射によるレーザー学会「レーザー研究」誌、Institution of Engineering and Technology (IET) 「Electronics Letters」誌、Elsevier 「Microelectronics Journal」誌などで発表した。

アウトリーチ活動 本研究のインパクトは大きく、一般メディア（New York Times, CNN, Washington Post ほか）および技術メディア（Wired, Ars Technica）で報道がされた。著者によるデモ動画は YouTube において、累計 30 万回以上再生された。また、技術メディアによる研究紹介の動画は、執筆次点で 430 万回以上再生された。

研究の発展 LightCommands の研究の過程で、レーザー照射による音声信号の挿入は、光電効果と光音響効果が混ざった複雑なメカニズムによって生じていることが明らかになった。脆弱性の根本的な解決には、レーザー照射により音声信号が挿入できる物理メカニズムの解明が必要であるとの知見に至り、メカニズム解明のための実験と研究テーマ立案を行った。本項目については、2021 年度より、基盤 (C) の枠組みで研究を継続する。その基盤 (C) も、ミシガン大学と共同で実施する。

5. 主な発表論文等

〔雑誌論文〕 計4件（うち査読付論文 3件/うち国際共著 1件/うちオープンアクセス 3件）

1. 著者名 T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu	4. 巻 2020
2. 論文標題 Light Commands: Laser-Based Audio Injection on Voice-Controllable Systems	5. 発行年 2020年
3. 雑誌名 USENIX Security Symposium 2020	6. 最初と最後の頁 2631--2648
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する
1. 著者名 菅原 健, 崎山 一男	4. 巻 47
2. 論文標題 組込機器のセキュリティを脅かすレーザーフォールト攻撃	5. 発行年 2019年
3. 雑誌名 レーザー研究「新しい光セキュリティの研究開発動向」特集号	6. 最初と最後の頁 305-309
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -
1. 著者名 Takeshi Sugawara, Yang Li, and Kazuo Sakiyama	4. 巻 55
2. 論文標題 Probing attack of share-serial threshold implementation of advanced encryption standard	5. 発行年 2019年
3. 雑誌名 Electronics Letters	6. 最初と最後の頁 517~519
掲載論文のDOI（デジタルオブジェクト識別子） 10.1049/el.2018.7518	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 -
1. 著者名 Takeshi Sugawara, Natsu Shoji, Kazuo Sakiyama, Kohei Matsuda, Noriyuki Miura, Makoto Nagata	4. 巻 90
2. 論文標題 Side-channel leakage from sensor-based countermeasures against fault injection attack	5. 発行年 2019年
3. 雑誌名 Microelectronics Journal	6. 最初と最後の頁 63~71
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.mejo.2019.05.017	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 -

〔学会発表〕 計5件（うち招待講演 3件 / うち国際学会 1件）

1. 発表者名 菅原 健, シア ベンジャミン, ランパッジ サラ, ゲンキン ダニエル, フー ケビン
2. 発表標題 ライトコマンド: レーザーを用いて音声コマンドを挿入する攻撃
3. 学会等名 コンピュータセキュリティシンポジウム2020
4. 発表年 2020年

1. 発表者名 菅原健
2. 発表標題 ライトコマンド: レーザー照射により音声コマンド を挿入する攻撃
3. 学会等名 第5回 IoT セキュリティフォーラム (招待講演)
4. 発表年 2020年

1. 発表者名 T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu
2. 発表標題 Light Commands: レーザーを用いて音声コマンドを挿入する攻撃
3. 学会等名 暗号と情報セキュリティワークショップ2020 (招待講演)
4. 発表年 2020年

1. 発表者名 T. Sugawara
2. 発表標題 Laser Injection Attacks on Integrated Circuits and Sensors
3. 学会等名 SPQR Laboratory Embedded Security Workshop (招待講演) (国際学会)
4. 発表年 2020年

1. 発表者名 西山優太, 李陽, 崎山一男, 菅原健
2. 発表標題 様々な実験条件におけるジャイロセンサのセンサなりすまし攻撃に関する基礎的検討
3. 学会等名 電子情報通信学会2018年ソサイエティ大会
4. 発表年 2018年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

Laser-Based Audio Injection on VCS https://lightcommands.com レーザーを用いて音声コマンドを挿入する攻撃 https://lightcommands.com/index_jp.html 研究成果のWebページ https://www.youtube.com/channel/UC2y3z169n9xXxPEBtxcAYjA

6. 研究組織			
	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関		
米国	ミシガン大学		