博士学位論文要約（令和 4 年 3 月）

IoT デバイスへの能動的物理攻撃とその対策に関する研究

梨本　翔永
指導教員：本間 尚文

Active Physical Attacks on IoT Devices and their Countermeasure

Shoei NASHIMOTO
Supervisor: Naofumi HOMMA

Active physical attacks are emerging threats to the internet of things (IoT) devices. This paper conducts a multifaceted security evaluation based on the components of IoT devices, focusing on fault attacks on processors and signal injection attacks on sensors. Concerning fault attacks, I identified the threat of security bypass attacks based on instruction skipping. I showed that software protection with input size restrictions and trusted execution environments is vulnerable to such attacks. As a countermeasure against such attacks, I proposed a method to prevent instruction skipping by changing the control flow to depend on the instructions to be protected. About signal injection attacks, I demonstrated a deception attack on an inclination sensor with sensor fusion and a millimeter-wave frequency modulated continuous wave radar. As countermeasures, we proposed attack detection and mitigation methods with small overhead focusing on the sensor signal processing algorithm.

1. はじめに

社会基盤となりつつある IoT (Internet of Things) を安全に活用していく上では，いかにセキュリティを確保するかが重要な社会課題である．特に，IoT デバイスでは，従来の情報システムとは異なり，センサとアクチュエータにより物理世界と相互作用すること，攻撃者が対象機器に物理的にアクセスできることが想定されることから，ターゲットに異常な信号を照射・導入する能動的物理攻撃がより重要な脅威となり得る．こうした観点から能動的物理攻撃とその対策に関する研究が進められているものの，未検討の脅威はまだ多く存在している．攻撃者はターゲットの一番弱いところを狙うというセキュリティの原則から，そうした未知の脅威を明らかにし，IoT デバイスのセキュリティを底上げすることが重要である．そこで，本研究では，IoT デバイスの構成要素に基づき，プロセッサへのフォールト攻撃及びセンサへのシグナルインジェクション攻撃に着目して多面的にセキュリティ評価を行った．

2. 入力サイズ制限へのフォールト攻撃

フォールト攻撃によるセキュリティバイパスの脅威はこれまでにも指摘されていた[1]．しかし，複数回のフォールト攻撃による影響は未検討であった．本研究では，入力サイズ制限に基づく BOF (Buffer Overflow) 攻撃対策が複数回の命令スキップで無効化される可能性を指摘した．特に，ループ構造における (1) ループカウンタの更新と(2) 入力サイズ制限に基づく終了判定の 2 種類の処理が命令スキップに脆弱であることを明らかにした．多重故障によれば，こうした処理を繰り返しスキップし，BOF を引き起こすことが可能になる．AVR 及び ARM マイコンを対象に，クロックグリッチによる多重故障（図 1）で提案攻撃の有効性を実証した．図 2 に示すとおり，BOF 対

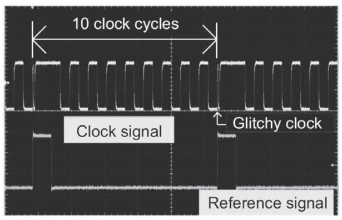


図 1　多重故障を誘発するクロックグリッチ

```
1 11 01 02 03   // msg[10]
2 04 05 06 07   // msg[10]
3 08 00 00 20   // msg[10]
4 00 04 01 40
5 27 05 00 08   // return address
```

(a) 攻撃なし

```
1 00 00 00 00   // msg[10]
2 00 00 00 00   // msg[10]
3 00 09 0a 0b   // msg[10]
4 0c 0d 0e 0f
5 55 02 00 08   // modified return address
```

(b) 攻撃あり

図 2　フォールト攻撃を利用した BOF によるメモリ書き換え

表 1　対策によるオーバーヘッド

		プログラムサイズ [byte]	クロックサイクル数 [cycle]
AVR	strncpy()	30	$10+10n\ (m=0)$ $20+10n+6m\ (m\geq 1)$
	my_strncpy()	40	$13+11n\ (m=0)$ $25+11n+7m\ (m\geq 1)$
ARM	strncpy()	38	$19+13n\ (m=0)$ $26+13n+9m\ (m\geq 1)$
	my_strncpy()	36	$14\ (n=0)$ $25+11n+9m\ (n\geq 1)$

※ n: 非 NULL 文字の数, m: NULL 文字の数

策をバイパスしリターンアドレスを攻撃コードで上書きし，任意の関数を呼び出せることを確認した．

さらに，提案攻撃への対策を考案し，(1) あらゆる命令スキップに耐性があること，(2) プログラムサイズ及びクロックサイクル数のオーバーヘッドが小さいことを検証した（表 1）．提案対策では，終了判定をデフォルトフェイル[2]で保護する．さらに，ループカウンタを保護するために，この考えを拡張した「デフォルトフェイル型保護対象依存制御フロー」を提案した．本アイデアでは，カウンタ値を利用した相対アドレス指定によるデータアクセスを利用する．これにより，カウンタ値の更新がスキップされないときのみ正しくデータコピーができるような制御フローを構築できる．したがって，本対策は提案攻撃を防ぐことができる根源的な対策である．

3. RISC-V に基づく TEE へのフォールト攻撃

TEE (Trusted Execution Environment) は信頼できる実行環境を構築し，不正なアプリケーションや脆弱性の影響を分離するセキュリティ対策である．著名な命令セットアーキテクチャ (ISA: Instruction Set Architecture) である x86 及び ARM においては，フォールト攻撃により不正なアプリケーションを TEE 上で実行する攻撃の脅威が指摘されている[3,4]．

本研究では，2011 年に発表された新たな ISA である RISC-V を対象に，TEE による隔離実行がバイパスされる可能性を検証した．本研究は既存研究とは異なるアプローチにより，フォールト攻撃を利用して TEE 上で実行しているアプリケーションのメモリに不正アクセスできることを示した．TEE を実現するメモリ管理ユニット PMP (Physical Memory Protection) によるアクセス制御自体は無効化できない．そこで，PMP が参照する隔離実行設定の変更を命令スキップで妨害する方法を考案した．本攻撃の有効性は，クロックグリッチ及び電磁パルスよるフォールト攻撃により，実機で実証した（図 3）．

さらに，「デフォルトフェイル型保護対象依存制御フロー」のアイデアを応用し，PMP 設定変更

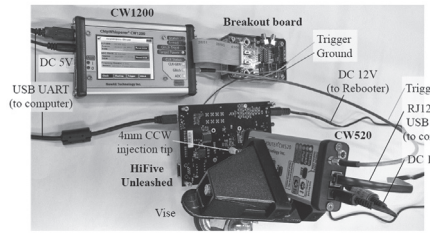


図 3　電磁パルスによるフォールト攻撃環境

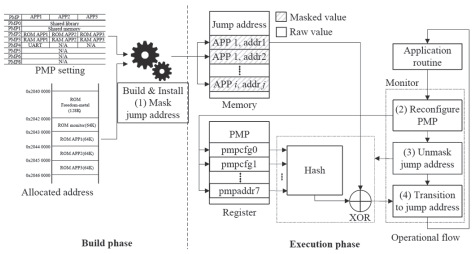


図 4　ジャンプアドレスのマスキングによる PMP 設定変更処理の保護対策

命令を命令スキップから保護する対策を提案した（図 4）．本対策では，ビルド時にアプリケーションのエントリーポイント及びリターンアドレス（ジャンプアドレス）を全て PMP 設定値との XOR (Exclusive OR) 演算によりマスキングする．アプリケーション実行時には，PMP 設定を変更した後に逆の演算でアンマスクしてジャンプする．したがって，PMP 設定値が破壊された場合には正しいアドレスに遷移できず，攻撃は成立しない．

4. AHRS へのシグナルインジェクション攻撃

MEMS (Micro Electronic Mechanical System) に基づく加速度及びジャイロセンサの出力を音響インジェクションにより操作する攻撃の脅威が指摘されていた[5]．これに対し，複数センサ出力を融合することでロバスト性を向上させるセンサフュージョンが対策になり得ると考えられていた．しかし，そのセキュリティ評価はなされていなかった．

本研究では，加速度，ジャイロ及び磁気センサから構成される姿勢方位基準装置 (AHRS: Attitude Heading Reference System) を対象に，傾きを計測するセンサフュージョンの攻撃耐性を評価した．カルマンフィルタに基づく傾き計測アルゴリズムを解析し，ノイズが極端に大きい（あるいは小さい）状況下では，あるセンサが支配的に利用されるようになることが複数センサを相補的に利用するセンサフュージョン戦略の共通の脆弱性であることを明らかにした．この考えに基づき 2 種類の方法でセンサノイズを制御するローノイズ攻撃及びノイジー攻撃を考案した．さ

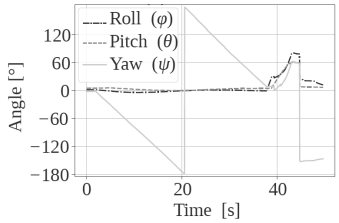
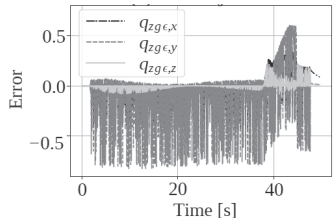
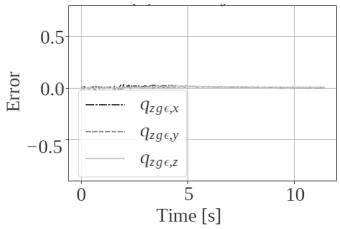


図 5　シグナルインジェクション攻撃による傾き (roll, pitch, yaw) の変化



(a)　攻撃時



(b)　正常時

図 6　重力ベクタの時間変化

らに，攻撃者がシグナルインジェクション攻撃により得られるセンサの制御性（制御可能，妨害のみ可能，影響を及ぼせない）に応じた最終的な傾きへの影響を網羅的に評価した．提案攻撃の有効性は，エミュレーション実験及び実機実験により検証した．エミュレーション実験では，センサ計測値をソフトウェア的に書き換え，原理的に 2 種類の提案攻撃が有効であることを示した．実機実験では，図 5 に示すとおり，音響及び磁気インジェクションによりノイジー攻撃で傾きを 60 度に制御できることを示した．

提案攻撃への対策として，センサフュージョンアルゴリズムの中間値である重力ベクタ及び磁気ベクタの誤差を用いた攻撃検知方法を示した．提案攻撃は強制的にセンサノイズの状況を制御しているため，正常利用では生じないようなセンサ間の不整合が生じ得る．したがって，最終的な出力である傾きは攻撃により騙されている一方で，処理途中では異常を検知できる．実機攻撃実験時及び AHRS を手動で回転させた正常時の重力及び磁気ベクタ誤差を比較した（図 6）．実験結果から，攻撃時には正常時の約 10 倍の誤差が生じていることが明らかになった．したがって，適切な閾値を設定することで，インジェクション攻撃を検知できると考える．

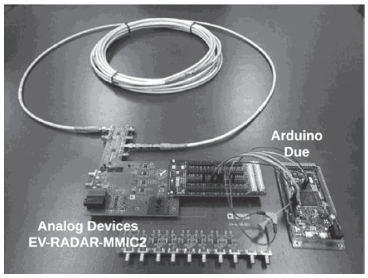


図 7　FMCW レーダ欺瞞の攻撃装置構成

5. FMCW レーダへのシグナルインジェクション攻撃

ミリ波 FMCW (Frequency Modulated Continuous Wave)レーダは，小型で安価，かつ高精度という特徴から，商用レーダとしても利用が進んできている．これまでに，FMCW 波形を模擬した SDR (Software Defined Radio) における欺瞞攻撃[6]や実車に搭載された FMCW レーダへの妨害攻撃[7]の有効性が検証されていた．本研究では，24 GHz 帯の FMCW レーダを使用した安価な攻撃装置による距離欺瞞攻撃の有効性を実証した．本攻撃装置はレーダボードと制御用マイコンから構成され，10 万円未満と安価である．しかし，安価な構成であることに起因し，(1) 同じレーダボードかつ同じ波形設定にもかかわらず，ボードの個体差による微小な時間ずれが存在すること，(2) 欺瞞に必要な ns 単位の攻撃波及び被害波の時間差を 1MS/s 未満の ADC (Analog-to-Digital Converter) で行う必要があることが欺瞞攻撃を達成するための課題であることが分かった．

本研究では，上記の課題を解決する攻撃アルゴリズムとして HCM (Half-Chirp Modulation) 及び二段階遅延挿入スキームを提案した．三角波に基づく通常の FMCW では，時間ずれの計測に GS/s の ADC が必要な一方，HCM では，時間経過とともに時間ずれが蓄積して 1MS/s の ADC でも計測できる．二段階遅延挿入スキームでは，HCM で時間ずれを計測した後，粗い遅延を挿入して攻撃波・被害波の時間差を減らす．さらに，ADC 帯域に被害波が入るように繰り返し微小な遅延を挿入する．その後，ADC 帯域に入った信号を解析して時間差を計測し，欺瞞距離に応じた精密な遅延を挿入する．

レーダボードと攻撃装置を同軸ケーブルで有線接続し，提案攻撃の有効性を実証した（図 7）．本攻撃装置によれば，図 8 に示すとおり，±10m の誤差で距離欺瞞できることが分かった．さらに，変調波形をランダム化する対策下で，距離欺瞞攻撃がどれだけ成功するかをシミュレーション実

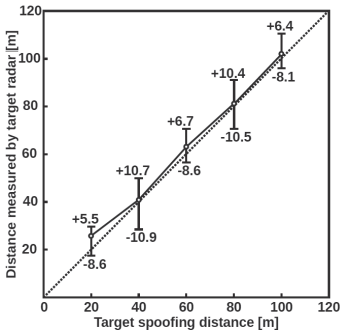


図８　目標欺瞞距離に対して計測された距離

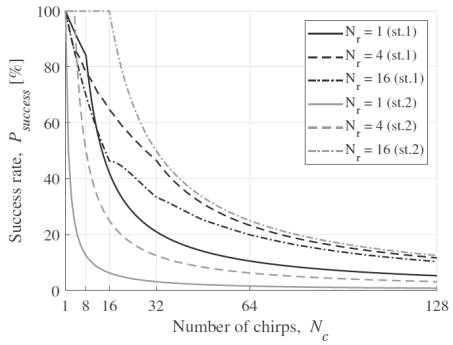


図９　二種類の攻撃戦略(st.1, st.2)における攻撃成功率と変調パターン数の関係

験により評価した. この結果, 図９に示すとおり, 変調パターンを増やしてランダム化したとしても，依然として攻撃は成功することを明らかにした．例えば，攻撃装置１台（Nr=1)、ランダムパターン 32 個　（Nc=32）の時、受信波を解析してパターンを推測する攻撃は st.1 の戦略を取ると20%以上の確率で成功する．

このような攻撃に対して，レーダ信号処理で使われているコヒーレント積分を波形のランダム化と組み合わせることで，更に攻撃成功率を低減できることを示した．また，波形のランダム化により生じた位相ずれを補正し，コヒーレント積分を適用できるようにする波形の補正方法も示した．以上の対策によれば，距離計測に悪影響を与えずに，対策効果を高めることができる．

6. まとめ

本研究では，IoT デバイスへの能動的物理攻撃として，プロセッサへのフォールト攻撃及びセンサへのシグナルインジェクション攻撃の新たな脅威を指摘し，その影響を明らかにするとともに，対策を提案した．フォールト攻撃対策としては，デフォルトフェイル型保護対象依存制御フローが攻撃を防ぐことができる根源的な対策であることを示した．シグナルインジェクション攻撃に関しては，センサフュージョンやレーダ信号処理など，センサの計測値を活用するアルゴリズムをセキュリティの観点から応用することで，コストパフォーマンスの高い対策を構築できることを示した．以上の対策はすべてソフトウェアとして実装可能である．したがって，対策にコストが掛けにくい IoT デバイスでも，ファームウェアアップデートなどの方法で適用することが可能であり，IoT デバイスと親和性の高い対策であると結論付けられる．

文献

1) Pierre-Alain Fouque, Delphine Leresteux, and Fr´ed´eric Valette, “Using faults for buffer overflow effects,” in Proceedings of the 27th Annual ACM Symposium on Applied Computing, pp. 1638–1639, ACM, 2012.
2) Sho Endo, Naofumi Homma, Yu-ichi Hayashi, Junko Takahashi, Hitoshi Fuji, and Takafumi Aoki, “A multiple-fault injection attack by adaptive timing control under black-box conditions and a countermeasure,” in Constructive Side-Channel Analysis and Secure Design, pp. 214–228, Springer, 2014.
3) Adrian Tang, Simha Sethumadhavan, and Salvatore Stolfo, “CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management,” in 26th USENIX Security Symposium (USENIX Security 17), pp. 1057–1074, 2017.
4) Pengfei Qiu, Dongsheng Wang, Yongqiang Lyu, and Gang Qu, “VoltJockey: Breaking SGX by Software-Controlled Voltage-Induced Hardware Faults,” in 2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), pp. 1–6, IEEE, 2019.
5) Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu, “ Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks,” in Security and Privacy (EuroS&P), 2017 IEEE European Symposium on, pp. 3–18, IEEE, 2017.
6) Ruchir Chauhan, “A Platform for False Data Injection in Frequency Modulated Continuous Wave Radar,” Master’s thesis, Utah State University, 2014.
7) Chen Yan, Wenyuan Xu, and Jianhao Liu, “Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle,” DEF CON, Vol. 24, 2016.