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

平成　３０　年　　５　月　２５　日現在

機関番号：　１１３０１
研究種目：　挑戦的萌芽研究
研究期間：　2016～2017
課題番号：　１６Ｋ１２４３６

研究課題名（和文）組込みシステムへのサイバー・フィジカル協調型攻撃を防ぐ命令シーケンス構成法の開拓

研究課題名（英文）Development of constitution method for instruction sequence against cyber-physical cooperative attacks on embedded systems

研究代表者

本間　尚文（Homma, Naofumi）

東北大学・電気通信研究所・教授

研究者番号：００３４３０６２

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：本研究では，組込みシステムに対するサイバー・フィジカル協調型攻撃の脅威を明らかにするとともに，同攻撃への効果的な対策技術を開拓した．具体的には，まず，一般的なサイバー攻撃対策を施した組込みシステムに対しても脅威となり得るサイバー・フィジカル協調型攻撃を系統的に分類・整理するとともに，特にサイバー攻撃としてバッファオーバーフロー（BOF）攻撃，フィジカル攻撃（物理攻撃）として故障注入攻撃を想定した場合の協調型攻撃に対する効率的なソフトウェア対策手法を開発した．その上で，典型的なサイバー・フィジカル協調型攻撃を再現可能な評価・解析システムを構築し，開発した対策手法の安全性および効率性を実証した．

研究成果の概要（英文）：This research clarified the threat of cyber-physical cooperative attacks on embedded systems and developed effective countermeasure techniques for this kind of attack. We first survey and classify cyber-physical cooperative attacks that can pose a threat to embedded systems equipped with general cyber attack countermeasures in a systematic manner. In particular, we focused on buffer overflow (BOF) attack and fault injection attack as a cyber attack and a physical attack, respectively. We have developed an efficient software countermeasure method against their cooperative attacks. In addition, we built an evaluation / analysis system that can reproduce typical cyber-physical cooperative attacks and demonstrated the security and efficiency of the developed countermeasure method.

研究分野：　計算機科学

キーワード：　計算機システム　組込みセキュリティ

１．研究開始当初の背景

近年，暗号組込みシステム（暗号処理を実行するLSIシステム）に物理的にアクセスして秘密情報を奪う物理攻撃の脅威が指摘されている．とりわけシステムの非正規入出力を観測・操作して得られる情報を用いて秘密情報を奪うサイドチャネル攻撃や故障注入攻撃は，その非侵襲性や攻撃コストの低さから現実的な脅威と言われている．IoT（Internet of Things）時代の到来に伴って秘密情報を扱う組込みシステムが身近に存在することで，こうした攻撃の脅威は益々高まると予想されている．特に近年，物理攻撃を従来のサイバー攻撃と組み合わせることにより，サイバー攻撃対策を施した一般的な組込みシステムであっても攻撃に成功し得ることが報告されており，現在こうしたサイバー・フィジカル協調型攻撃への対策技術の確立が急務となっている．

本研究者は，これまでサイドチャネル攻撃標準評価ボード（SASEBO）やISO/IEC国際標準暗号ハードウェアIPを開発・公開するなど，組込みシステムに対する物理攻撃とその防御に関する研究を開拓してきた．上記の協調型攻撃に対する効果的な対策は現時点では報告されていないが，本研究者らは，これまで培ってきたサイドチャネル攻撃に対するソフトウェア対策技術を応用することで，同協調型攻撃に対しても高効率かつ安全性の証明された対策技術を開発できるとの着想に至った．

２．研究の目的

本研究では，組込みシステムに対するサイバー・フィジカル協調型攻撃の脅威を明らかにするとともに，同攻撃への効果的な対策技術を開拓することを目的とした．具体的には，まず，一般的なサイバー攻撃対策を施した組込みシステムに対しても脅威となり得るサイバー・フィジカル協調型攻撃を系統的に分類・整理するとともに，特にサイバー攻撃としてバッファオーバーフロー（BOF）攻撃，フィジカル攻撃（物理攻撃）として故障注入攻撃を想定した場合の協調型攻撃の振る舞いをモデル化し，その完全かつ効率的なソフトウェア対策手法を開発する．その上で，典型的なサイバー・フィジカル協調型攻撃を再現可能な評価・解析システムを構築し，開発した対策手法の安全性および効率性を実証することを目的とした．

３．研究の方法

本研究では，上記の研究目的を2年間で達成することを目指した．平成28年度は，サイバー・フィジカル協調型攻撃として想定される攻撃の組合せを精査し，可能性の高い攻撃シナリオに関してその脅威の分類と推定を行った．また，それと並行して，現時点で最も現実的な脅威と考えられるバッファオーバーフロー（BOF）攻撃と故障注入攻撃を組み合わせた協調型攻撃へのソフトウェアによる対策手法を開発し，その形式的検証を実施した．平成29年度は，前年度に分類・推定したサイバー・フィジカル協調型攻撃実験を可能とする評価・解析システムを構築した．特に，組込みソフトウェアの安全性評価のため，最も攻撃対象となり得るICカードを搭載可能な基板をシステムに使用した．その上で，同システムを用いて前年度に開発したソフトウェア対策の有効性を実証した．

４．研究成果

平成28年度は，下記2項目の研究成果が得られた．

(a) サイバー・フィジカル協調型攻撃の調査および攻撃モデルの構築

サイバー・フィジカル協調型攻撃をモデル化し，その脅威を分類・整理するとともに将来的に起こり得る攻撃を推定した．サイバー・フィジカル協調型攻撃では，サイバー攻撃のタイミングに合わせて物理攻撃を実施し，一時的にサイバー攻撃対策を無効化することで，結果としてサイバー攻撃を成功させる．本研究では，同協調型攻撃に利用される代表的なサイバー攻撃として，BOF攻撃を想定した．代表的な物理攻撃としては，対象機器を破壊しない故障注入攻撃を想定した．典型的な協調型攻撃のシナリオとして，故障注入攻撃によるサイバー攻撃対策の無効化を行った上で，サイバー攻撃が実行される状況を考えた．このとき，どのような協調型攻撃が可能かは実装形態や応用・運用に依存するため，いくつかの実装形態・応用に対して攻撃をモデル化し，その実現可能性を精査した．一方，サイバー攻撃への対策手法としては，CPU，OS，コンパイラ，プログラムの各レベルを想定した．特に省リソースの機器でも適用可能なプログラムレベルの対策として，典型的な冗長化と検算の対策を想定し，そのときに可能となる攻撃とその影響を明らかにした．

(b) BOF攻撃と故障注入攻撃を組合せたサイバー・フィジカル協調型攻撃への対策手法の開発

上記のサイバー・フィジカル協調型攻撃のうち，すでに現実的な脅威として報告されているBOF攻撃と故障注入攻撃の協調型攻撃への効率的なソフトウェア対策を開発した．これまでに報告された協調型攻撃では，BOF攻撃対策に入力サイズ制限（ISL: Input Size Limitation）を行った組込みソフトウェアに対して，その対策で用いる条件分岐命令を故障注入攻撃により無効化した上でBOF攻撃の入力を送り込むことで，同攻撃を成立させている．そこで，この攻撃を一般化し，任意の命令が無効化（物理攻撃により命令スキップが起こることが示されている）されたとしてもBOF攻撃が不成立となる命令シーケンスの構成法を開発した．具体的には，まず，組込みプロセッサとしてAtmelおよびARMの命令セットを対象として，対策に直接関わる一分

岐命令スキップおよび関連する算術演算命令スキップに対して BOF 攻撃が不成立となるような命令シーケンスを与え，時相論理を用いてそのアセンブラが BOF 攻撃の成立する状態に移行しないことを検証した．その上で，上記対策済み命令シーケンスに新たに追加された複数の分岐命令に対しても命令スキップが起こり得るという想定に拡張し，同様に安全性の検証を与えた．

平成 29 年度は，下記 2 項目の研究成果が得られた．

(a) サイバー・フィジカル協調型攻撃評価・解析システムの開発

前年度に分類・整理したサイバー・フィジカル協調型攻撃を評価・解析するための実験システムを構築した．同システムは， PC，ディジタルオシロスコープ，組込みソフトウェアを搭載するテストベンチ（評価ボード）で構成した．PC は，オシロスコープと評価ボードの動作を制御し，適切なタイミングでサイバー攻撃と物理攻撃を連携させた．また，得られた結果の収集・解析も担った．それらの制御用コード開発には，これまで組込みシステムの制御で本研究者が用いてきた Python コードを利用した．オシロスコープ制御用コードはすでに開発したものを用いた．一方，組込みソフトウェアを実装する評価ボードは，本研究者らの研究グループが AIST と共同で開発したサイドチャネル攻撃標準評価ボード（SASEBO-W）を用いて開発した．SASEBO-W は，組込みソフトウェアを実装する IC カード用のソケットとその制御用の FPGA を搭載しており，IC カード（Atmel プロセッサ）に実装されたソフトウェアへの物理攻撃（故障注入攻撃）に対する安全性評価システムを構築した． 物理攻撃用コードはすでに同評価ボードに対して開発済みのものを一部再利用した．

(b) 開発したソフトウェア対策の有効性評価の実施

前年度に開発した BOF 攻撃と故障注入攻撃の協調型攻撃対策の有効性を，上記の評価・解析システムを用いて実験的に評価した．ここでは，特に同協調型攻撃の故障注入攻撃のため，上記評価ボードの FPGA 上にグリッチ入りクロック信号発生器を設計・実装した．同信号発生器は，位相の異なるクロック信号を任意のクロックタイミングで切り替え可能とすることにより，様々な故障注入攻撃を再現できる．同協調型攻撃のためには，適切なタイミングで定期的に故障を注入し，さらに，その結果をモニタリングする必要があったため，そうした機能を新たに設計・実装した．また，同 FPGA に BOF 攻撃を実施するための解析用 PC とのインタフェースも合わせて実装することにより，再現性の高い実験環境を実現した．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

1. Kazuhide Fukushima, Rui Xu, Shinsaku Kiyomoto, and Naofumi Homma, “Fault Injection Attack on Salsa20 and ChaCha and a Lightweight Countermeasure,” 2017 IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1032–1037, August 1, 2017.査読有
2. Wataru Kawai, Rei Ueno, Naofumi Homma, Takafumi Aoki, Kazuhide Fukushima, Shinsaku Kiyomoto, “Practical Power Analysis on KCipher-2 Software on Low-End Microcontrollers,” 2017 IEEE European Symposium on Security and Privacy, pp. 113-121, Paris, April 30, 2017.査読有
3. Shoei Nashimoto, Naofumi Homma, Yu-ichi Hayashi, Junko Takahashi, Hitoshi Fuji, Takafumi Aoki, “Buffer overflow attack with multiple fault injection and a proven counter-measure,” Journal of Cryptographic Engineering, Vol. 7, Issue 1, pp. 35-46, April 2017.査読有
4. Wataru Kawai, Rei Ueno, Naofumi Homma, Takafumi Aoki, Kazuhide Fukushima, and Shinsaku Kiyomoto, “Side channel Security Evaluation for KCipher－2 Software on Smart Cards, ” 25th International Workshop on Post-Binary ULSI Systems, pp.9-12, May 17, 2016.査読有

〔学会発表〕（計 7 件）

1. 伊東燦, 上野嶺, 本間尚文, 青木孝文“ハードウェアトロイ挿入が困難な公開鍵暗号データパスに関する検討,” ハードウェアセキュリティフォーラム 2017, ポスターNo.9, 東京都, December 2017.
2. 本間尚文, “IoT セキュリティを支える暗号技術の最新動向,”IEEE SSCS Kansai Chapter 技術セミナー, 大阪, Octrober 6, 2017（招待講演）
3. 遠藤空, ヴィッレウリマウル, 本間尚文, 青木孝文 “剰余演算に基づく秘匿計算向け暗号の高効率実装,”第 40 回多値論理フォーラム, Vol.40, No.17, 飛鳥村, 奈良県, September 2017.
4. 伊東燦, 上野嶺, 本間尚文, 青木孝文“算術演算ハードウェアアルゴリズムの改変検知に関する検討,” 第 40 回多値論理フォーラム, Vol.40, No.16, 飛鳥村, 奈良県, September 2017.
5. 遠藤空, ヴィッレ ウリマウル, 本間尚文, 青木孝文 “数論変換に基づく秘匿

計算向け暗号の高効率実装，” 平成 29 年度 電気関係学会東北支部連合大会，弘前，No. 1F15，p. 1，August 24，2017

6. 伊東燦，上野嶺，本間尚文，青木孝文“乗算アルゴリズムに対するハードウェアトロイ挿入可能性の評価，”平成 29 年度電気関係学会東北支部連合大会，弘前，No. 1E05，p. 1，August 24，2017
7. 福島和英，許 瑞，清本晋作，本間尚文“Salsa20/ChaCha に対する故障利用攻撃とその対策，” 2017 年暗号と情報セキュリティシンポジウム，那覇，Vol. 2A3-1，pp.1--5，January 25，2017.

〔図書〕（計 1 件）

1. Naofumi Homma (Ed)，“Special Section on PROOFS 2016，” Journal of Cryptographic Engineering，Springer，Vol. 7，Issue 4，pp. 297-351，November，2017.

〔その他〕
ホームページ等
東北大学電気通信研究所環境調和型セキュア情報システム研究分野
http://www.ecsis.riec.tohoku.ac.jp/

６．研究組織
(1)研究代表者
本間　尚文（HOMMA，Naofumi）
東北大学・電気通信研究所・教授
研究者番号：00343062