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　６ 年　 ６ 月 ２１ 日現在

機関番号：３３８０３
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ１１８２１

研究課題名（和文）アルゴリズム公開型耐タンパー技術の実証的な解析と評価

研究課題名（英文）Analysis and Evaluation of Publicly Verifiable Algorithm based Tamper Resistance Technology

研究代表者
大石　和臣（Oishi, Kazuomi）

静岡理工科大学・情報学部・准教授

研究者番号：２０６３５２１３

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：1)indirect jumpとROPに基づく自己破壊的耐タンパーソフトウェアについて具体的詳細化の検討，2)既存技術のTEE等の調査が成果である．脆弱性緩和技術Intel CETとの共存可能性の検討が必要となり当初の目標より限定された成果となった．
1についてはアセンブリプログラミングの工夫によりIntel CETと共存可能な耐タンパー化を行える可能性があることを明らかにしindirect jumpの活用方法等の検討を進めた．2についてはTEEの仕様を検討しTEE外部のREEにおける耐タンパー性の欠如がTEEの欠点であることを示しその対策として耐タンパーソフトウェアを活用する方法を提案した．

研究成果の学術的意義や社会的意義
indirect jumpやReturn-Oriented Programming (ROP) を用いるアルゴリズム公開型の自己破壊的耐タンパーソフトウェアを実現する方法について具体的な仕様を検討した．脆弱性緩和技術Intel CETの登場を踏まえてROPとの共存可能性を検討して示すことができた．特別なハードウェアを利用する耐タンパー技術TEEの欠点はREE内の耐タンパー性の欠如であることと対策を示した．理論的な研究のindistinguishable ObfuscationとWhite-Box Cryptographyの最新研究動向を把握した．これらは安全・安心なプログラムの実現に貢献する．

研究成果の概要（英文）：We had two results: 1) a study on the detailed specification of indirect jumps and ROP based self-destructive tamper resistant software (SDTRS), 2) a survey of underlying technologies such as TEE. Since vulnerability mitigation technology Intel CET appeared, it was necessary to confirm that the proposed SDTRS can co-exist with Intel CET. So, the results were restricted than expected.
As to 1, we showed a possibility of the coexistence by carefully crafting assembly program of ROP-based SDTRS so that it can co-exist with Intel CET, and studied utilizations of indirect jumps, etc. As to 2, we studied TEE specification and showed that loss of tamper resistance with respect to the REE outside TEE is a disadvantage of TEE, and proposed utilization of tamper resistant software for programs in REE as a countermeasure.

研究分野：情報セキュリティ

キーワード：耐タンパーソフトウェア　indirect jump　データメモリ　Intel CET　TEE　White-Box Cryptography　iO

※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。

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1) 本研究の対象は，プログラムを一貫して安全に実行するためのアルゴリズム公開型の耐タンパー技術であり，特別なハードウェアを仮定しない耐タンパーソフトウェア(TRS)と特別なハードウェアに基づく耐タンパー技術に分類される．TRS は，実装されたデータやアルゴリズムを不正に読むことが困難である性質（秘密情報守秘性）や，改変することが困難である性質（機能改変困難性）を保つことができるソフトウェアであり，信頼できない環境で動作するソフトウェアを保護するための重要な技術である．

研究代表者は，自己書換えコードに基づく TRS 作成方法(OM 法)を提案し，科研費(研究課題/領域番号 26330165)により「組込みシステムに適用可能なアルゴリズム公開型耐タンパーソフトウェアの研究」を実施した．その結果として OM 法を PC 向けの TRS 作成ツールとして開発して実証実験を行い，正しく機能することを客観的に評価した．また，組込みシステムに適用可能な耐タンパー化技術を提案した．提案技術は，命令の自己書換えを実行できない組込みシステムに対して，OM 法の特徴である相互依存型自己インテグリティ検証の構造を保ちながら，間接ジャンプ（動的にジャンプ先を決定する）と ROP (Return-Oriented Programming) に基づくインテグリティ検証を用いる TRS 作成方法である．

間接ジャンプにより制御フローを解析困難にして，偽装された定数を動的に計算することで秘密情報守秘性を実現する．また，自己インテグリティ検証による間接ジャンプ，命令メモリおよびスタック（データメモリ）のインテグリティ検証とスタックの書換えに基づき ROP を実行する構成により機能改変困難性を実現できる．この方法は組込みシステムに適用可能であり，その手順（仕様）は示されていたが，その実装と実験は行われていなかった．

(2) 特別なハードを仮定しない他の耐タンパーソフトウェアとして，秘密情報守秘性を実現すると期待される理論的な iO (indistinguishability Obfuscation)技術，具体的な製品に搭載されているとされる White-Box Cryptography，機能改変困難性を実現する汎用的な Control Flow Integrity が活発に研究されているが，それらの前提（アルゴリズム公開型か否か）と達成できるセキュリティには違いがあり，アルゴリズム公開型の耐タンパーソフトウェアとして統一的に比較・議論することが可能か否かは明らかではなかった．

一方，特別なハードウェアに基づく耐タンパー技術として，例えば，Secure Element (SE)，Trusted Execution Environment (TEE)が知られている．これらは暗号化・復号や署名検証のような重要なプロセスを耐タンパーハードウェアの保護のもとで一貫して安全に実行する仕組みである．しかし，ハードとソフトの仕様が公開されているとは限らず，いずれかに脆弱性があると所望の性能は実現できず，耐タンパー性の前提と安全性の関係は不明確であった．

(3) 以上に示したように，1) プログラムを一貫して安全に実行するための耐タンパー技術の多様な既存技術の統一的な比較・議論が可能であるか，2) アルゴリズム公開型の耐タンパーソフトウェアについて，効率的な実行速度を持ちかつ耐タンパー性を低下させないアルゴリズムおよび実装が実現可能であるか，が本研究計画の核心をなす学術的「問い」であった．

２．研究の目的

本研究では，計画 1) indirect jump と ROP に基づく自己破壊的 TRS 作成方法の具体的詳細化および実装評価, 計画 2) 自己書換えに基づく OM 法の自己書換えルーチンの挿入位置を決定する効率的で安全なアルゴリズムの探求とその実装評価，計画 3) SE，TEE，iO (indistinguishability Obfuscation)，White-Box Cryptography，Control Flow Integrity 等の調査および比較検討を目標とする．

３．研究の方法

計画 1 と計画 2 の研究方法は，研究代表者が提案した方法に関する具体的なアルゴリズムを詳細に検討・考案して実装し，動作実験を行う．計画 3 は既存技術に関する文献，開発ボード，製品，発表聴講に基づく調査を行い，仕様，実機，動作検証，性能評価を通じた広範囲なサーベイを行う．

４．研究成果

(1) 計画 1 については，indirect jump と ROP (Return-Oriented Programming) に基づく方法の具体的詳細化を進めた．ROP を用いる自己インテグリティ検証方式として既存技術の Parallax を利用するため，その実装におけるパラメータを洗い出し，データメモリのどの領域をいつ検証するかを検討し，提案方法のセキュリティ（機能改変困難性）が従来方式の自己書換えに基づく耐タンパーソフトウェアと同等程度の強さだと思われることを明らかにした．この検討結果をコンピュータセキュリティシンポジウム 2021 で発表したところ，聴衆から Intel 社の CET (Control-flow Enforcement Technology) の存在とそれとの関係を質問された．Intel 社の CET は第 11 世代マイクロアーキテクチャ Tiger Lake (2020 年発売) の CPU に搭載されたハードウェア的な ROP 対策であり，本研究計画の提案時点には製品として存在しなかった技術である．その質問を踏まえて Intel CET の検討を行った．

Intel CET は Shadow Stack と Indirect Branch Tracking の 2 個の技術から構成される．Shadow Stack は，従来のスタック（データスタック）とは別のスタック（シャドウスタック）を設けて，リターンアドレスの書換えを CPU が検出することにより ROP を防ぐ仕組みである．call 命令が実行されるときリターンアドレスをデータスタックとシャドウスタックの両方にプッシュする．ret 命令が実行されるときデータスタックとシャドウスタックの両方からリターンアドレスをポップし，CPU はそれらを比較して一致していれば処理を継続し，不一致ならば例外を発生する．シャドウスタックへのアクセスは限定され，CPU が提供する機能を通してのみプッシュとポップが行われるため, ROP 等を利用する攻撃者が Shadow Stack の仕組みを回避することは困難だと期待される．Indirect Branch Tracking は，間接分岐命令 (indirect branch instruction) を拡張し，想定した分岐先であれば処理を継続し，想定した分岐先ではないならば例外を発生することにより JOP/COP （Jump-Oriented Programming/Call-Oriented Programming） を防ぐ仕組みである．分岐命令は jmp 命令あるいは call 命令であり，endbr 命令が新しく設けられ，想定した分岐先には endbr 命令が配置される．CPU が間接分岐を実行した直後に endbr 命令が存在しない場合は例外を発生するため，攻撃者による制御フローの変更を検出できる．また，Intel CET に対応していない CPU は endbr 命令を nop 命令とみなすため，後方互換性も確保される．

Intel CET の仕様とそれをサポートする CPU，OS，開発環境を調査して，設定による無効化が行えることを明らかにした．次に，Intel CET が有効化されている場合については，自己破壊的耐タンパーソフトウェアと共存させることが可能か否かについて検討した．その結果，Indirect Branch Tracking については間接分岐先に endbr 命令を記述することで共存できると考えられることがわかった．Shadow Stack との共存については耐タンパー化の対象がアセンブリプログラムであるため，本来の機能を持つコードと ROP による自己インテグリティ検証機能を持つコードと Shadow Stack とが互いの動作を妨げないようにアセンブリプログラムを記述することが可能であれば共存できると考えられた．そこで，ある ROP コードを選び，それを Shadow Stack が処理するときの動作と共存するようなアセンブリプログラミングについて検討を進めた結果，仕様上は共存可能であると予想できた．

以上の検討と並行して indirect jump の活用方法について検討を進めた．indirect jump の基本効果，基本ブロックのシャッフル，ダミー基本ブロックの追加，dummy indirect jump の追加について詳細を検討し，制御フローの把握をさらに困難にする効果があることを明らかにした．また，データメモリの検証について検討を進め，実行可能プログラムのデータメモリの配置とライフサイクルを詳細に検討した．グローバル変数とスタック内の変数を検証対象データ候補とすること，複数の検証関数を用意しておき一つの検証関数が別の検証関数の ROP チェインを間接定数計算の対象にする方法を考察した．

これらの理論的な詳細仕様の検討を進める一方で，ROP 対策の Intel CET との共存を考慮した耐タンパー化プログラムの実装と評価についても研究開発を進めたが，アセンブリプログラミングは高水準言語と比較して実装の難易度が高く研究代表者の他に開発リソースを確保することができなかったため実装が進まず実証評価はできなかった．

(2) 計画 2 については，目標とするアルゴリズムは見つけられていない．

(3) 計画 3 については，本研究計画はコロナ禍の直撃を受けたため当初の 3 年間の間に海外出張はできなかった．期間を 1 年延長して 2023 年度にようやく海外動向調査が行えたので ACM CCS 2023 と NDSS 2023 に参加して，耐タンパーソフトウェアおよびソフトウェア保護に関する最新研究動向を現地で確認した．海外出張ができなかった期間には論文や Web 等の文書に基づく調査と製品を入手した実機調査を行った．

TEE については仕様レベルにおける耐タンパー性について Global Platform が定める TEE の

仕様書や既存研究等を参照して調査した．TEE はハードウェアの支援により隔離実行を実現できる実行環境であり，TEE と REE (Rich Execution Environment) の実行環境を持つ．TEE 内では Trusted OS が動作しその上で Trusted Application (TA) が実行され, REE 内では Rich OS (Normal OS とも呼ぶ) が動作しその上で Normal REE Application や Client Application (CA) が実行される．Normal REE Application はユーザが使うアプリケーションであり REE 内で実行される．セキュリティに関する処理が必要な場合は CA と TA が連携し，その処理は REE から隔離され TEE 内で実行される．TEE のみがアクセスできるリソースに REE がアクセスすることはできず, そのアクセス制御は, 1) 物理的隔離, 2) ハードウェア論理に基く隔離, 3) 暗号的隔離，によって強制される．既存研究成果として偽の CA が TA を呼び出すことができるという弱点が明らかになっていることを踏まえて，REE 内の CA と REE Communication Agent が適切な耐タンパー性を有する必要があること，つまり，TEE の欠点は REE における耐タンパー性が欠如していることであることを示した．また，その対策として CA や REE Communication Agent を耐タンパーソフトウェアとして実装することを提案した.

iO (indistinguishability Obfuscation) 技術と White-Box Cryptography については，研究動向を論文や Web により調査した. 2021 年の STOC において Aayush Jain, Huijia Lin, Amit Sahai が"Indistinguishability obfuscation from well-founded assumptions"を発表した（22 February 2024 に Communications of the ACM に掲載・出版された）．この研究は従来の iO 技術の仮定を緩和した成果であり，4 個の well-founded assumptions に基づいて iO を構成する方法を提案している．2022 年の CRYPTO で Adrian Ranea, Joachim Vandersmissen, Bart Preneel が "Implicit White-Box Implementations: White-Boxing ARX Ciphers"を発表した．この研究は implicit functions に基づく新しい White-Box Cryptography 設計方法とツールを提案している．2024 年 6 月の時点でこの方法は破られていないと思われる．これらの調査結果から，iO と White-Box Cryptography はまだ発展途上の魅力的な研究テーマであることが明らかになった.

自動車の ECU (Electronic Control Unit) に使用されているマイコンについて，TOYOTA が開発した自動車向けのポータブルなセキュリティテストベッド PASTA for Education を入手して調査を行った．PASTA の ECU は Renesas の RX71M マイコンを搭載している．RX71M シリーズは RXv2 コアを採用しており，32bit CISC，ハーバードアーキテクチャである．スマートフォンの多くに採用されている ARM マイコンは RISC で, メモリアーキテクチャがハーバードである．自動車の ECU にもメモリアーキテクチャがハーバードのマイコンが採用されていることが確認できた．一方で，RX マイコンは暗号機能 (ハード暗号回路)，フラッシュメモリの保護 (Trusted Memory)，アクセス保護，外部読み出し禁止等のセキュリティ機能を備えているが，ARM TrustZone のように Trusted Execution Environment をサポートしているのではないこともわかった.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計5件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 大石 和臣
２．発表標題 Return-Oriented Programmingを用いる自己破壊的耐タンパーソフトウェアの検討
３．学会等名 情報処理学会，コンピュータセキュリティシンポジウム2021
４．発表年 2021年

１．発表者名 大石 和臣
２．発表標題 Trusted Execution Environmentの耐タンパー性に関する考察
３．学会等名 電子情報通信学会，情報通信システムセキュリティ研究会（ICSS），学技報，vol．121，no．275，ICSS2021-47，pp．7-12，2021年11月．
４．発表年 2021年

１．発表者名 大石 和臣
２．発表標題 Return-Oriented Programmingを用いる自己破壊的耐タンパーソフトウェアの検討(その2)
３．学会等名 電子情報通信学会，情報通信システムセキュリティ研究会（ICSS），信学技報，vol．121，no．410，ICSS2021-69，pp．61-65，2022年3月．
４．発表年 2022年

１．発表者名 大石 和臣
２．発表標題 自己破壊的耐タンパーソフトウェアにおけるindirect jump
３．学会等名 情報処理学会，コンピュータセキュリティシンポジウム2023
４．発表年 2023年

１．発表者名 大石 和臣
２．発表標題 Return-Oriented Programmingを用いる自己破壊的耐タンパーソフトウェアの検討(Part3)
３．学会等名 電子情報通信学会，情報通信システムセキュリティ研究会（ICSS），信学技報，vol．123，no．269，ICSS2023-55，pp．30-34，2023年11月．
４．発表年 2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

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