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　４ 年　 ６ 月　 ６ 日現在

機関番号：１７１０２
研究種目：若手研究
研究期間：2019～2021
課題番号：１９Ｋ２０２３５

研究課題名（和文）プロセッサ内部状態のモデリングに基づく高性能志向プロセッサの高セキュリティ化

研究課題名（英文）Research for secure processors based on the microarchitectural state modeling

研究代表者
谷本　輝夫（TANIMOTO, TERUO）

九州大学・システム情報科学研究院・助教

研究者番号：６０８２６３５３

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）：アウトオブオーダプロセッサの投機実行機能を対象とした攻撃であるSpectreについてサイクル精度のプロセッサシミュレータであるgem5を用いて実行しその命令プロファイルを取得する環境を構築した。さらに，そのメカニズムのモデル化を行い、プロセッサシミュレータで実行したトレースに含まれる攻撃メカニズムの成功箇所を特定した。続けて，ソフトウェアにおける攻撃に対する対策手法を実装し、それを実装した場合の性能への影響をシミュレータ上で実行すること可視化した。これにより、ソフトウェアにおける対策のオーバヘッドが明らかになり、ハードウェアレベルでの対策とのオーバヘッド比較が可能となった。

研究成果の学術的意義や社会的意義
マイクロプロセッサにおいて投機実行はその性能を向上するために極めて重要な技術である。しかしながらマイクロアーキテクチャ攻撃によって意図しない副作用が悪用され、機密情報の漏洩などのサイドチャネル攻撃が可能である脆弱性が複数報告されている。ハードウェア起因の脆弱性はシステム運用開始後の修正が困難であることが多く、また、設計時に未知の攻撃へ対策するのは本質的に困難である。本研究の成果はこのような脆弱性を可視化し、その対策のオーバヘッドを可視化することに成功した点でコンピュータシステムの高セキュリティと高性能双方の実現に資する。

研究成果の概要（英文）：We constructed an environment to execute Spectre, an attack targeting the speculative execution function of out-of-order processors, using gem5, a cycle-accurate processor simulator, to obtain its instruction profiles. Furthermore, we modeled the mechanism and identified the successful locations of the attack mechanism in the traces executed by the processor simulator. We then implemented countermeasures against the attacks in software and visualized the impact on performance when these countermeasures were implemented by running them on the simulator. This revealed the overhead of the countermeasures in software and enabled comparison of the overhead with countermeasures at the hardware level.

研究分野：コンピュータアーキテクチャ

キーワード：コンピュータアーキテクチャ　セキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１。研究開始当初の背景

計算機システムの担う社会役割の増大に伴い、高性能や低消費電力性のみならず高セキュリティも求められる。
社会インフラの一部としてシステムの安全性担保はますます重要である。

マイクロアーキテクチャ攻撃（MA）と呼ばれる、悪意ある命令列の実行によりシステム内部の機密情報（本来知りえない情報）の取得や権限昇格を行う手法が注目されている。
中でも、高性能を目的とした投機実行の副作用を利用した攻撃が現実的な脅威であることが報告された。これらは市場に浸透した複数製品に有効なため影響範囲が広く、多くの事業者が性能低下を伴うファームウェア及び OS の修正を行った。

プロセッサを対象とした MA が成立する根本的な原因は、「アーキテクチャステート（AS)」と「マイクロアーキテクチャステート（uAS)」の違いと、本来ソフトウェアからは隠蔽されるべき uAS 情報の露見にある。AS はソフトウェアを実行するために必要なアーキテクチャレジスタや命令カウンタなどからなり、ソフトウェアにより制御・観測される。uAS は実際のプロセッサ内部の状態であり、ハードウェアレジスタやキャッシュの状態などを含む。一般に uAS は AS を包含する。前述の手法では、悪意ある命令列により AS 外の uAS を変更（これを副作用と呼ぶ）し、後続の命令実行時の AS の遷移に要する時間（つまり実行時間）の変化などを観測することで機密情報の推測を行う。

２。研究の目的

本研究課題の核心をなす学術的問いは「uAS への副作用のモデリングに基づく高性能と高セキュリティ両立の探求」にある。一般的なセキュリティの観点では、このような副作用は脆弱性の原因となるため忌避されてきた。一方で、理論的にセキュアなプロセッサはその安全性のために膨大な回路や演算を必要とする。現状、副作用を伴う高速化手法なしに今日の高性能プロセッサの性能は実現できない。したがって、性能とセキュリティのトレードオフを探索し、高性能志向プロセッサの高セキュリティ化を目指す必要がある。uAS は完全にはソフトウェア制御できず、ハードウェア状況に依存する。そのため、ソフトウェアとハードウェア双方の相互作用である副作用のモデリングによりコンピュータシステムを高セキュリティ化できる可能性がある。

３。研究の方法

本研究は uAS への副作用のモデリングに基づく高性能志向プロセッサの高セキュリティ化方法の確立を目的とし、2 つの目標を設定した。

a：機密情報の露見につながる uAS のモデリング方法の確立

既存の高性能志向プロセッサ上における命令実行の詳細解析として、アウトオブオーダプロセッサにおける動的命令のパイプラインステージごとの処理を依存グラフとして表現する手法が挙げられる。依存グラフによる命令実行の表現はプロセッサの内部状態（uAS の一部）のダイナミクスを有しており、命令実行の副作用解析にも有用であると考えられる。しかしながら、既存の取り組みは性能解析が目的であり、主な対象を AS としていたため、投機実行したが投機が不成立だった命令列の情報は破棄されていた。これまで破棄されていた情報を含むモデル化を行い、機密情報が uAS に含まれるメカニズムを特定可能にする。

B：高セキュアかつ高性能なプロセッサ構成法の確立

a のモデリングを基に機密情報が uAS から露見するのを防止する手法を確立する。uAS に含まれる機密情報は命令列の実行時間の変化として攻撃者に観測される。本研究では、実行時間が uAS に影響されないようハードウェア変更するなどして機密情報の露見を防ぐ。これにより、副作用を持つ高速化手法を適用した計算機システムのおけるセキュリティ上の問題を、最低限の性能オーバヘッドで大きく緩和またはなくすことができ、高性能と高セキュリティを両立することができる。

４。研究成果

a：機密情報の露見につながる uAS のモデリング方法の確立

アウトオブオーダプロセッサの投機実行機能を対象とした攻撃である Spectre（図１中攻撃１）についてサイクル精度のプロセッサシミュレータである gem5 を用いて実行しその命令プロファイルを取得する環境を構築した。さらに、そのメカニズムのモデル化を行い、プロセッサシミュレータで実行したトレースに含まれる攻撃メカニズムの成功箇所を特定した。続けて、ソフトウェアにおける攻撃に対する対策手法を実装し、それを実装した場合の性能への影響をシミュレータ上で実行すること可視化した（図２）。これにより、ソフトウェアにおける対策のオーバヘッドが明らかになり、ハードウェアレベルでの対策とのオーバヘッド比較が可能となった。

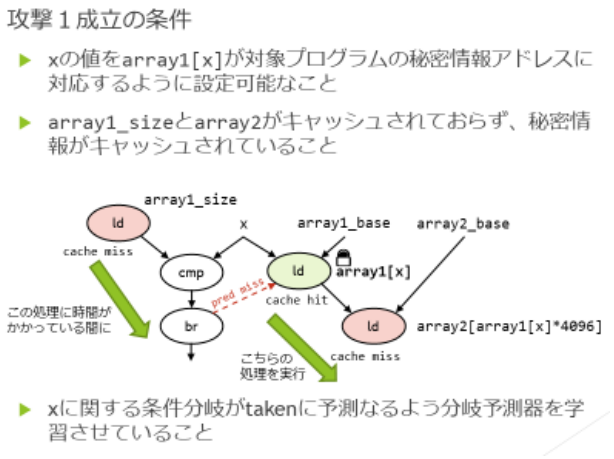

図１　Spectre 攻撃

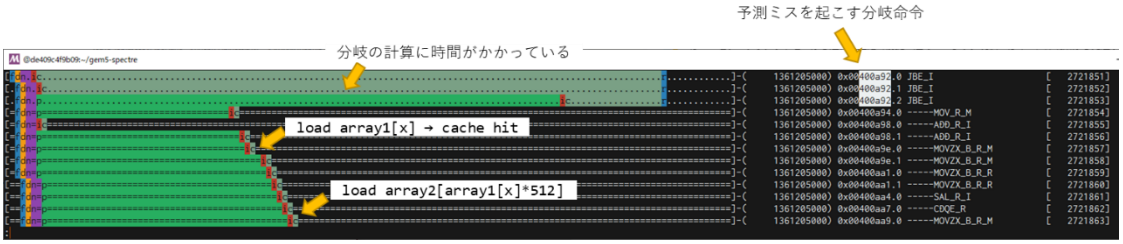

図２　Spectre 攻撃成功時の様子

マイクロプロセッサにおいて投機実行はその性能を向上するために極めて重要な技術である。しかしながらマイクロアーキテクチャ攻撃によって意図しない副作用が悪用され、機密情報の漏洩などのサイドチャネル攻撃が可能である脆弱性が複数報告されている。ハードウェア起因の脆弱性はシステム運用開始後の修正が困難であることが多く、また、設計時に未知の攻撃へ対策するのは本質的に困難である。本研究の成果はこのような脆弱性を可視化し、その対策のオーバヘッドを可視化することに成功した点でコンピュータシステムの高セキュリティと高性能双方の実現に資する。

b：特定した uAS から機密情報の露見防止方法を確立

高セキュリティと高性能を両立する手法として、本研究では２つの方法に取り組んだ。１つは、プログラム実行中にあらかじめ安全であることが分かっているプログラム以外を実行した際にハードウェアでこれを検出し実行を停止する方法である。これには機械学習を用いてプログラム実行中のハードウェアイベント（単位サイクル数当たりの命令実行数やキャッシュミス率、分岐予測ミス率など）からプログラムの特徴を予め学習して分類器を作成し、実行時にそれらのイベントを観測することで実行中のプログラムが許可されたものかを検査するものである。マイクロアーキテクチャ攻撃は攻撃者が任意プログラムを実行できるかそれに近しいことが必要となるため、このような対策が有効であると考えられる。本手法については国際学会で発表を行った。

もう１つは、プログラムを構成する主要な処理（いわゆるホットな箇所）をソフトウェア処理ではなくハードウェア処理にする方法である。マイクロアーキテクチャ攻撃はソフトウェア処理を前提とするため、より多くの処理単位をハードウェア化し実行してソフトウェア処理を減らすことができれば攻撃の余地を減らすことができる。このような方法の問題点はハードウェア処理の開発コストが高いことであるが、これを抽象度の高いドメイン特化言語からハードウェアを生成する手法を用いることで解決した。この手法は特に IoT など省コストかつ対象アプリケーションを限定可能な場合により有効である。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 山方大輔，川上哲志，谷本輝夫，井上弘士，小野貴継
２．発表標題 プロセッサへの実装に向けたORAMにおけるポジションマップ削減手法の検討
３．学会等名 暗号と情報セキュリティシンポジウム（SCIS2021）（国際学会）
４．発表年 2021年

１．発表者名 上野麟，谷本輝夫，後藤孝行，丸岡晃，川上哲志，小野貴継，飯塚拓郎，井上弘士
２．発表標題 オイラー動画像誇張処理を対象としたCPU-FPGAハイブリッドシステムの実装と評価
３．学会等名 情報処理学会研究報告，Vol.2021-ARC-244
４．発表年 2021年

１．発表者名 Teruo Tanimoto
２．発表標題 Hardware-based malware detection for IoT microprocessors
３．学会等名 The First workshop on NSF-JST SICORP Smart & Connected Communities Project（国際学会）
４．発表年 2020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