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　５ 年　 ６ 月 １２ 日現在

機関番号：１２６０８
研究種目：研究活動スタート支援
研究期間：2020～2022
課題番号：２０Ｋ２３３１９

研究課題名（和文）Spectre攻撃に対して堅牢なプロセッサアーキテクチャの研究

研究課題名（英文）Exploring Foundations for Spectre Defenses

研究代表者
佐々木　広（SASAKI, Hiroshi）

東京工業大学・工学院・准教授

研究者番号：２０５３４６０５

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：2018年に報告されたSpectreというプロセッサのハードウェア実装に関する脆弱性は、最悪の場合攻撃者がメモリ内の任意のアドレスのデータを読み出せるため非常に深刻である。本脆弱性を利用したSpectre攻撃は現実的な対策技術が提案されておらず、その対策は重要な課題となっている。本研究を通して、プログラムを実行する際にプロセッサに意図的に誤った分岐方向の実行を（投機的に）させること（およびファジングと呼ばれるソフトウェアのテスト手法）を利用した、Spectreガジェット（Spectre攻撃に用いることが可能な命令列）の検出機構を構想するに至った。

研究成果の学術的意義や社会的意義
Spectre攻撃はプロセッサのハードウェア実装に起因するものであり、ソフトウェアでの対策は大きな性能オーバーヘッドを伴う。一方でハードウェアによる対策は現実的なものが提案されておらず、実現の可否については不透明である。本研究を通して得られた構想は実行ソフトウェア内からSpectre攻撃に利用され得るSpectreガジェットを検出するものであり、効果的な対策への足がかりとなる可能性を有している。

研究成果の概要（英文）：The vulnerability related to the hardware implementation of a processor called Spectre, which was reported in 2018, is highly critical as it allows attackers to potentially read data from any address in the memory. Spectre attacks exploiting this vulnerability have no practical countermeasures proposed yet, making mitigation a significant challenge. Through this research, we have conceived a detection mechanism for Spectre gadgets (instruction sequences that can be used in Spectre attacks) by deliberately inducing (speculative) execution of incorrect branch directions in the processor during program execution, utilizing a software testing technique called fuzzing.

研究分野：コンピュータアーキテクチャ、コンピュータセキュリティ、コンピュータシステム

キーワード：Spectre　ハードウェアセキュリティ　分岐予測　投機実行

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

2018 年に報告された Spectre というプロセッサのハードウェア実装に関する脆弱性は、最悪の場合攻撃者がメモリ内の任意のアドレスのデータを読み出せてしまうため非常に深刻である。本脆弱性を利用した Spectre 攻撃として様々な亜種が報告されているが現状では未だに現実的な対策技術が提案されておらず（本脆弱性は今日のプロセッサの根幹となる性能向上技術に本質的に内在するものであり、その対策には非常に大掛かりな変更が必要となると考えられている）、Spectre への対策はコンピュータセキュリティ研究において最も重要な課題の一つとなっている。

２．研究の目的

本研究は Spectre 攻撃の解析、およびそれに基づいた研究（例えばハードウェアへの変更および性能オーバーヘッドを極力抑えた Spectre 対策技術）を提案・開発する足がかりを作ることを目的としている。Spectre 攻撃はプロセッサの高性能化手法である投機実行（例えば分岐方向が確定する前に分岐方向を予測することで実行を継続する）によりプロセッサが誤った命令列を実行した際に、本来アクセスできないデータにアクセスし得ることを利用する。具体的には、攻撃者は分岐命令における分岐予測器の予測ミスを誘発することで Spectre 攻撃を実行する。アクセスされた秘匿データが、秘匿データに基づいたアドレスへとさらに書き込まれた場合、後に（前述の例の場合はキャッシュ）サイドチャネル攻撃を用いることで読み出すことが可能となる。

本研究ではまず Spectre 攻撃を受けている分岐命令実行の際のプロセッサの挙動を解析する。また、Spectre 攻撃を受けている分岐命令と他の分岐命令との振る舞いの差異を明らかにする。上記の解析を基に、ハードウェアで Spectre 攻撃を受けている分岐命令を検知可能であることを示す。また、該当命令を動的にハードウェアで検出し投機実行を抑制する機構や、該当命令列をプログラム内からソフトウェアまたはハードウェアで発見する手法などを提案することを目指す。

３．研究の方法

まず Spectre 攻撃を受けている分岐命令の振る舞いを詳細に解析するために、プロセッサの挙動を詳細にシミュレーションする環境の構築を行なう。具体的にはプロセッサの挙動をサイクルレベルでシミュレートする、プロセッサアーキテクチャ研究におけるデファクトシミュレータである gem5 を用いる。

キャッシュサイドチャネル攻撃を用いる Spectre 攻撃が成功するためには、投機的に実行する誤った命令列の中に（ともするとアクセスが許されない）データにアクセスするロード命令、およびその読み出したデータに基づいたアドレスへのストア命令、が含まれている必要がある。逆に言うと、このパターンが出現しない限りは投機実行を止める必要がない。そのため次に、上記シミュレーション環境を用いて、このパターンが（そうでないパターンと比較して）どの程度出現するかの調査を行なう。例えば、もしもこのパターンが通常のプログラムにおいてほとんど出現しないことが分かればその事実を用いることで効率的な対策手法を考案することが考えられる。

これらの調査を通して Spectre 攻撃についての理解を深め、既存の研究についても広くサーベイすることで、新しい研究の方向性を考案する。

４．研究成果

まずシミュレータへの Spectre 攻撃の実装により、プロセッサパイプライン内の様々な構成要素で攻撃の検知に役立つ特異的な振る舞いが観測されないかを詳しく調べるための準備ができた。

次いで、Spectre 攻撃を上記シミュレータで調査した結果、多くのプログラムにおいてこのパターンは無視できない頻度で出現することが分かった。このことからプログラム実行時にハードウェアで該当命令列を効率的に検出できたとして、非常に多くの偽陽性が生じるという問題が生じることが明らかになった。

偽陽性を取り除くためには、詳細なプログラムのコンテキストやメモリアクセスの具体的なアドレスなどを考慮する必要がある。そこで、実行時に Spectre を検出し防ぐという方向性ではなく、実行するプログラム内から Spectre ガジェット（Spectre 攻撃に用いることが可能な命令列）を実行時に検出する機構を構想するに至った。この目的のためには、プログラムを実行する際にプロセッサに意図的に誤った分岐方向の実行を（投機的に）させること（およびファジングと呼ばれるソフトウェアのテスト手法）が利用できると考えられる。ハードウェア的な工夫を加えることで小さいオーバーヘッドで Spectre ガジェットの検出を可能とする研究を今後行なっていく予定である。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 Keisuke Nishimura, Takahiro Ishikawa, Hiroshi Sasaki, Shinpei Kato
２．発表標題 RAPLET: Demystifying Publish/Subscribe Latency for ROS Applications
３．学会等名 27th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), 2021（国際学会）
４．発表年 2021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