永続メモリプログラムの情報漏洩のGPU超並列検出

Massively Parallel Analysis of Precise Information Flow in Persistent Memory Systems

荒堀喜貴
防衛大学校（申請時: 東京科学大学）

１．研究目的

・背景: 永続メモリ情報漏洩の二系統と既存検知技術の限界

永続メモリは計算機システムのメモリ大容量化、レイテンシ削減、および障害耐性の向上を同時に実現できるため、大規模AIモデルの実現やビッグデータ処理を支える基盤技術の一つとして有望視されている。その一方で近年、永続メモリシステムのに固有のバグや脆弱性が報告されており、情報漏洩の原因となる脆弱性が存在する。 NVLeak [USENIX Security 2023] に代表される脆弱性は、永続メモリハードウェアの動作特性（読み書きレイテンシ等）を悪用してOSや仮想マシンによるセキュリティ保護境界を破り機密情報を盗み取ることを可能にする。この脆弱性はSide Channel起因の永続メモリ情報漏洩として分類できる。これに対し、永続メモリ上で秘匿情報を格納するオブジェクトに対するDangling Pointerの永続化に起因して起きる情報漏洩もあり、本研究ではこの脆弱性をPersistent UAF（Persistent Use-After-Free）と分類する。後者は、揮発メモリ上の通常のUse-After-Freeと異なり、永続メモリ上の秘匿データを指すポインタが電源断や再起動・クラッシュをまたいで残存し得る点を特徴とする。

いずれの系統の情報漏洩も、その発現機序は複雑であり、高精度な攻撃検知には永続メモリハードウェアの動作特性に加え、攻撃準備パスと攻撃パスという複数の実行パスを同時に扱う高負荷なコード解析技術が必要となる。既存の情報漏洩検知法は揮発メモリの情報流を汎用CPU上で逐次的に解析する手法が主であり、永続メモリ情報漏洩に対しては検知精度が低い、または、解析可能なコード規模が小さいという問題を抱える。

本研究の目的は、永続メモリシステム固有の秘匿情報漏洩の脆弱性を対象とする、高精度かつ高効率な検知技術を確立することであり、この目的達成のためのアプローチとして永続メモリシステムに固有の情報流解析をGPUで超並列実行する基盤システムの実現を目指す。

２．研究成果の内容

・申請当初の研究目的: 永続メモリ情報漏洩を高精度に検知する超並列情報流解析

本研究の申請当初の目的は、上記の永続メモリ情報漏洩のうち、特にSide Channel起因の永続メモリ情報漏洩（NVLeak類似系）を主な対象として、大規模コードに対する高精度かつ高速な検知を実現する超並列情報流解析を開発することであった。具体的には、永続

メモリハードウェアの動作特性を正確にモデル化したマルチパス情報流解析を、高性能GPU上で超並列実行するアルゴリズムおよび最適化技法を開発する計画であった。

・本年度の研究対象の見直し: Persistent UAF起因の永続メモリ情報漏洩へのフォーカス

2025年度の研究遂行に際して、関連研究の精査および攻撃シナリオの検討を行った結果、上記の二系統のうちPersistent UAF起因の永続メモリ情報漏洩について、この脆弱性を主な検知対象として設定した研究がほぼ未開拓であるという、現状技術の重大な限界を確認した。具体的には、永続メモリ上の時間的メモリ安全性（temporal memory safety）に関しては SafePM [EuroSys 2022] や TENET [FAST 2023] で研究され、永続メモリプログラミングにおける Dangling Pointer の静的抑制に関しては Corundum [ASPLOS 2021] で研究され、並行実行下の永続化整合性違反に関しては HawkSet [EuroSys 2025], PMRace [ASPLOS 2022], Yashme [ASPLOS 2022] 等で活発に研究されている一方で、「Persistent UAF脆弱性を悪用して秘匿情報の漏洩させる攻撃の実現可能性」にまで踏み込んだ解析技術は十分に研究されていない、という調査結果を得た。

この調査結果を踏まえ、2025年度の研究では、申請当初の研究計画において主対象としていた脆弱性を、Side Channel起因の永続メモリ情報漏洩から、Persistent UAF起因の永続メモリ情報漏洩へ変更し、Persistent UAF起因の情報漏洩を主な検知対象とする基盤技術の検討および試作を進めた。ここで、情報流解析を高性能GPU上で超並列実行するという全体方式自体は申請当初の研究構想を踏襲しており、2025年度の研究遂行において見直したのは解析対象とする脆弱性の根本原因である。Side Channel起因の永続メモリ情報漏洩は、Persistent UAF対応の超並列情報流解析を確立した後の拡張技術の適用対象とする。

・本年度の研究成果:

本年度は、上記の研究目的および既存技術の有効範囲と限界の精査を踏まえ、Persistent UAF起因の永続メモリ情報漏洩を主な検知対象とする技術について、以下の4項目を実施した。

(1) Persistent UAF脆弱性および攻撃シナリオの具体化

本研究で扱うPersistent UAFとは、永続メモリ上で秘匿情報を格納したオブジェクトを指すDangling Pointerが、当該オブジェクトの解放後も永続メモリ上に残存し、（例えばクラッシュ回復処理等の）後続実行において当該Dangling Pointerが参照解決されることで秘匿情報の漏洩を引き起こす脆弱性を指す。揮発メモリ上の通常のUAFと異なり、Persistent UAFは以下の2点を特徴とする。第一に、永続メモリの永続性および再起動・クラッシュ後の状態保存特性により、Dangling Pointerおよび解放済みオブジェクトの内容（秘匿情報を含む）がクラッシュ前後の長期にわたり永続メモリ上に残存し得る。第二に、PMDK等の永続メモリ向けプログラミングフレームワークでは、永続オブジェクトへの参照は仮想アドレスではなく永続オブジェクトID（PMEMoid 等）として表現され、プロセス再起動やクラッシュ回復後にも参照解決可能であるため、永続メモリ上のDangling Pointerはクラッシュをまたいで有効な参照として（攻撃者により）復元され得る。

本年度は、既存の関連技術では正確に捕捉できないPersistent UAFを介した情報漏洩が成立する具体的な攻撃シナリオを以下の複数条件のもとで検討した: (i) 秘匿情報を含む永続メモリオブジェクトが存在する、(ii) 当該オブジェクトを指す永続参照、または回復後に再構成可能な永続参照が永続メモリ上の到達可能グラフに残存する、(iii) 解放処理・トランザクション・回復処理の不整合により当該参照が無効化されない、(iv) 永続メモリアロケータが解放時に秘匿情報の永続的消去（ゼロクリア）を行わないか、または再利用前に内容が残存する、(v) 型検査/generation tag/capability/epoch 再利用制御等が不十分であり、クラッシュ回復処理後のコード実行が古い永続オブジェクトIDを別型として解釈し得る。これらの条件が組み合わさることで、攻撃者がDangling Pointer経由で秘匿情報を読み出すPersistent UAF攻撃が成立することを確認した。

(2) Persistent UAFを含む小規模ネットワークプログラムの試作と攻撃の実証

永続メモリシステム（エミュレータ）を活用し、Persistent UAF脆弱性を含んだ小規模ネットワークプログラムを試作した。このプログラムは、永続メモリ上に秘匿情報を保持するオブジェクトを格納し、ネットワーク経由のクライアントリクエストに応じて当該オブジェクトを参照する。このプログラムを永続メモリエミュレータ上で実行し、(1)で整理した攻撃シナリオに沿ってPersistent UAF脆弱性を突く攻撃を加えた結果、本来は保護されるべき秘匿情報が情報漏洩として観測されることを確認した。

(3) 情報流解析に基づくPersistent UAF起因情報漏洩の逐次解析の設計

Persistent UAFに起因する情報漏洩を情報流解析に基づき逐次的に検知する技術を設計した。永続メモリシステム上のUAFを含む時間的メモリ安全性違反を検知する従来技術が「永続メモリオブジェクトを指すDangling Pointerがデリファレンスされた」事実までしか検知できないのに対し、本研究で設計した手法は、Persistent UAFの検知に加え情報流解析により「秘匿情報が攻撃者の観測可能点ないし制御可能点まで実際に到達したか」を追跡する。具体的な設計方針として、永続メモリ上のメモリ操作（永続メモリオブジェクトの割り当てや解放、読み書きを担当するマクロ/関数呼び出し）に対し、情報の秘匿性を起点とする情報流の生成/伝播/観測に対応する意味論を定義し、永続オブジェクトの解放後にも残存するDangling Pointer経由の秘匿情報伝播を追跡できるようにした。ここで、攻撃準備パスがクラッシュ前かつ攻撃パスがクラッシュ回復処理後であるケースを想定し、両パスを横断して秘匿ラベルを伝播させるために、秘匿ラベルの管理そのものを永続メモリ上で実現する情報流解析メタデータ管理機構も同時に設計した。更に、設計したPersistent UAF起因情報漏洩の逐次解析のプロトタイプ実装を行い、(2)で試作したPersistent UAFを含む小規模ネットワークプログラムに適用し、実際にPersisten UAF起因情報漏洩を検知できることを確認した（永続メモリシステムのエミュレータ上での確認）。

(4) Persistent UAF逐次解析の並列化方式の検討

(3)で設計した逐次解析を、当初の研究目的であるGPU超並列情報流解析へ発展させる

ための並列化方式を検討した。具体的には、攻撃準備パスと攻撃パスの組合せにより生じる解析候補（情報漏洩候補）の追跡、永続メモリシステムの動作特性や永続メモリオブジェクト操作ライブラリの動作特性に基づく情報漏洩実現可能性判定、解析器スナップショットの管理について、GPUアーキテクチャ上での情報流解析の超並列実行に向けた解析用メタデータ構造および処理分割の方針を整理した。本検討結果は、次年度に行うGPU並列解析の設計指針として活用する。

３．学際共同利用プログラムが果たした役割と意義

本研究は、申請当初の計画として、永続メモリ（Intel Optane Persistent Memory）および高性能GPU（NVIDIA H100 Tensor Core GPU）を搭載した実機環境上で、提案する超並列情報流解析の試作および評価を行うことを予定していた。この予定に対し、本年度は、前節で述べたとおり主対象とする情報漏洩脆弱性の根本原因を永続メモリ固有のSide ChannelからPersistent UAFに設定し直した上で、永続メモリ上のネットワークサーバに対しPersistent UAF起因の情報漏洩を発現させる攻撃シナリオの具体化、情報流解析ベースの脆弱性検知技術の設計および逐次解析器のプロトタイプ実装の試作に注力した結果、スパコン実機上での提案技術の実装および定量的評価には到達しなかった。本年度の実施内容は、いずれも永続メモリエミュレータ上での試作および動作確認に留まる。このため、当初予定していた永続メモリ情報漏洩のGPU並列解析の実現および評価は、次年度の継続研究へと持ち越すこととなった。

一方で、本年度の研究遂行において、学際共同利用プログラムが提供するスパコン実機の構成情報、特に永続メモリおよびGPUまわりの仕様/構成情報等は、本年度実施の永続メモリエミュレータ上の研究開発の実施に対して一定の役割を果たし（次年度まで含む）本研究の基盤整備に寄与した。

４．今後の展望

本年度に試作したPersistent UAF起因情報漏洩の逐次解析のプロトタイプおよび並列化方式の検討結果を基盤として、次年度の継続研究では、申請当初の研究目的である永続メモリ情報漏洩のGPU超並列解析を、Persistent UAF起因の永続メモリ情報漏洩を対象とするGPU並列解析として実装および評価する予定である。具体的には、上述の2節(3)で試作した情報流解析の逐次プロトタイプを、(4)で検討した並列化方式に基づきGPUアーキテクチャ向けに設計および実装する。更に、学際共同利用プログラムが提供する永続メモリ実機およびGPU実機を用いて、より大規模な永続メモリプログラムに適用し提案技術の有効性と限界を確認する実験を行う。また、既存の永続メモリバグ検知技術との比較を含め、永続メモリ情報漏洩の検知精度と検知効率を定量評価する。これらにより、Persistent UAFを根本原因とする永続メモリ情報漏洩を高精度かつ大規模コードに対しても効率的に検知するGPU超並列解析の確立を目指す。

５．成果発表

(1) 学術論文: なし（2026年度に予定）

(2) 学会発表: なし（2026年度に予定）

(3) その他

使用計算機	使用計算機に○	当初配分	移行※	追加配分
Pegasus	○	4040		
Miyabi-G				
Miyabi-C				

※ 配分リソースについてはノード時間積を記入。

※ バジェット移行を行った場合、「+2000」「-1000」のように記入。