

2023 年度年次報告書
社会変革に向けた ICT 基盤強化
2022 年度採択研究代表者

穂山 空道

立命館大学 情報理工学部
准教授

アドレスの秘匿によるサイドチャネル攻撃に頑健な OS

研究成果の概要

2023 年度は (i) 本研究後の防御目標である RowHammer 攻撃とキャッシュ競合攻撃の危険性をより明らかにする研究、(ii) 過年度に提案したアドレスランダム化手法のシミュレーションの実装とランダム性・性能低下の評価、を行った。

(i) はさらに(i)-a. RowHammer 攻撃の危険性を明らかにする研究と(i)-b. キャッシュ競合攻撃の危険性を明らかにする研究に分けられる。(i)-a では既存の RowHammer 攻撃による exploit がページテーブルエントリ (PTE) のアドレス部のみを攻撃していることに着目し、PTE 内のアドレス以外の部分、すなわち各ページの属性などを表す管理フラグが狙われた場合の危険性を研究した。このような着想に基づく研究は研究代表者の知る限り他に例がない。具体的には、PTE 内の global ビットが攻撃された場合、dirty や writable ビットが攻撃された場合の二つについて危険性を明らかにした。(i)-b. では与えられたキャッシュ構造の上でキャッシュ競合攻撃が成立するか否かを強化学習で探索する既存研究を詳細に追試・分析し、既存研究での探索に無駄なエージェントのアクションがあること、その無駄を削減する方法を提案した。

(ii) では前年度に提案した物理ページのランダム割り当て手法をシミュレートし、ランダム性とランダム化による性能低下の二点を評価した。まずランダム性の評価では、ページ割り当ての要求に対して提案アルゴリズムによって割り当てられる物理ページ番号の列を 2 進数にしたものを NIST の提供するランダム性検定手法で検定した結果、ある検定法ではランダム性が十分あるが別の検定法ではランダム性が低いという結果を得た。次にランダム化による性能低下の評価では、サイクルアキュレートな CPU シミュレータである gem5 上に提案のランダム化手法を実装した。物理アドレスをランダム化するとメモリスistemから見るとアクセスの規則性がなくなるためキャッシュプリフェッチに大幅な悪影響が出ると予測していたが、実際には基本的な stride プリフェッチャでは影響はないことが分かった。

【代表的な原著論文情報】

- 1) 穂山 空道, 山田 淳二, 塩谷 亮太: DRAM の設計余裕を活用した低レイテンシ化・低消費電力化手法とその制御法の研究動向, 情報処理学会論文誌コンピューティングシステム, Vol. 16, No. 1, pp. 14 - 28, 2023.
- 2) 吉岡 恵吾, 穂山 空道: RowHammer を用いたページテーブル上の Global bit 書き換えによるプロセス間データ覗き見手法, 並列／分散／協調処理に関するサマー・ワークショップ (SWoPP2023), pp. 1 - 7, August 2023
- 3) 中西 奏人, 穂山 空道: キャッシュ構造脆弱性の強化学習による探索における無駄な操作の削減, 第 64 回 インターネットと運用技術研究会, pp. 1 - 8, March 2024.
- 4) 村田 健斗, 穂山 空道: Rowhammer 攻撃防止のためのページフレームのランダム割り当て手法, 第 161 回 システムソフトウェアとオペレーティング・システム研究会, pp. 1 - 8, September 2023.