2024 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

稚山 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

2024 年度は (i) RowHammer 攻撃の新たな応用に対する防御手法の提案、(ii) 過年度に提案したキャッシュタイミング攻撃に対する脆弱性探索手法の高速化についての網羅的評価を行った。(i) はさらに (i)-a. VM 間 RowHammer 攻撃の防御手法の様々な環境での定量的評価を可能にする研究と (i)-b. 偽装 shadow stack 攻撃に対する防御策の研究の二つに分けられる。

(i)-a. では RowHammer 攻撃の応用である VM 間 RowHammer 攻撃について、既存の防御手法の評価の不十分性を解決した。評価とは防御手法が様々な環境において攻撃を低オーバーヘッドで防ぐことを確認する行為で、その結果はマシンの DRAM アドレスマッピング（データのアドレスから当該データのメモリチップ内の物理的な格納位置を決める対応）ごとに変わる。この対応は CPU の世代やマシン構成によって変わるため、網羅的な評価には未だ存在しないものも含め様々なマシンを用意する必要がある。そこで我々はこの対応をソフトウェアで定義可能なシミュレータの上に評価系を全て載せることでより網羅的な評価を可能にした。

(i)-b. では、過年度に発見した偽装 Shadow stack 攻撃に対するソフトウェアレベルでの防御策を考案した。本攻撃は、RowHammer 攻撃によってページテーブルの dirty bit または writable bit を書き変え、アプリケーションの利用する通常のメモリページを Shadow stack 用のページに見せかけることで書き込みエラーによる DoS を引き起こす攻撃である。これに対し、偽装 Shadow stack 攻撃を受け書き込みエラーが起こった際には OS が自身の管理するメタデータとページテーブル上の管理ビットを比較し、書き込みが起こったメモリページが偽物の Shadow stack であることを検知可能であることを発見した。

(ii) では過年度に提案したキャッシュタイミング攻撃への脆弱性の自動検知を高速化する手法を様々なキャッシュ構造に対して網羅的に評価した。評価の結果、既存研究で扱われているほとんどのケースで提案手法が自動検知の効率化を達成すること、逆に効率化を達成ケースにおいてその原因が明らかになった。

【代表的な原著論文情報】

1) Keigo Yoshioka, Soramichi Akiyama: “GbHammer: Malicious Inter-process Page Sharing by Hammering Global Bits in Page Table Entries”, Fourth Workshop on DRAM Security (DRAMSec), pp. 1 - 7, June 2024.
2) 川﨑 秀昌, 西村 俊和, 穐山 空道: VM 間 Rowhammer 類似攻撃に対する多重 Canary を用いた検出・隔離手法の提案, 第 163 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 - 9, May 2024.
3) 谷口 智哉, 穐山 空道: Rowhammer による Shadowstack への偽装に対するプログラムごとの危険度判定の提案, 第 163 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 - 9, May 2024.