基礎理論とシステム基盤技術の融合による Society 5.0 のための基盤ソフトウェアの創出　　2022 年度年次報告書

2022 年度採択研究代表者

品川 高廣

東京大学 情報基盤センター
准教授

隔離実行と形式検証による総合的セキュリティ基盤システム

主たる共同研究者:

住井 英二郎（東北大学 大学院情報科学研究科 教授）
広渕 崇宏（産業技術総合研究所 デジタルアーキテクチャ研究センター 研究チーム長）

研究成果の概要

今年度は、主に(1)仮想マシンレベルの隔離実行、(2)ハードウェアレベルの隔離実行、(3)インターフェイス検証、(4)エッジにおける隔離実行の 4 種類の研究を実施した。

(1)仮想マシンレベルの隔離実行では、まず隔離実行のメモリ利用効率を向上させるために、CHERI という新しい CPU に基づく軽量仮想マシンである CAP-VM をベースに、オブジェクトレベルでメモリ共有して効果的に重複排除する仕組みを研究した[1]。また、仮想化環境におけるメモリアクセス性能を効率化させるために、ハイパーバイザによるページングをパススルーしつつハードウェアによるタグ付け機構で保護をおこなう変換パススルーという仕組みを研究した[2]。

(2)ハードウェアレベルの隔離実行では、外部コプロセッサから DMA によるメモリ監視をおこなう環境において、IOMMU を悪用してメモリ監視を妨害する攻撃を防ぐために、軽量ハイパーバイザと連携して最小限のアクセス制御をおこなう仕組みを研究した。また、Spectre のようなハードウェアレベルの脆弱性に対処するために、マシンレベルでプロセスとカーネルを隔離して RDMA でシステムコールをおこなう仕組みを研究した。

(3)インターフェイス検証では、ネステッド仮想化部分の脆弱性を発見するために、専用命令を実行する小型ハーネスや仮想マシンの有効状態判定器などを用いて効果的にファジングをおこなう仕組みを研究し、KVM の脆弱性 CVE-2023-30456 を発見した[3]。また、システムコールレベルの参照モニタにおいて TOCTTOU 問題が生じない参照モニタのモデル化を研究した。

(4)エッジにおける隔離実行では、隔離実行が遅延などにあたえる影響を探るために、AMD-SEV を有効にした環境での性能を分析する実験をおこなって、各種暗号化機能によって生じるオーバーヘッドを研究した。

【代表的な原著論文情報】

1) Vasily A. Sartakov, Lluís Vilanova, Munir Geden, David Eyers, Takahiro Shinagawa, Peter Pietzuch. ORC: Increasing Cloud Memory Density via Object Reuse with Capabilities. In Proceedings of the 17th USENIX Symposium on Operating Systems Design and Implementation (OSDI 2023), Jul 2023. Acceptance Ratio: 19.6%

2) Shai Bergman, Mark Silberstein, Takahiro Shinagawa, Peter Pietzuch, Lluís Vilanova. Translation Pass-Through for Near-Native Paging Performance in VMs. In Proceedings of the 2023 USENIX Annual Technical Conference (USENIX ATC 2023), Jul 2023. Acceptance Ratio: 18.4%.

3) 石井 玲真, 深井 貴明, 品川 高廣. ネステッド仮想化のファジングにおけるカバレッジ向上に向けて. 第 159 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, 沖縄, 2023 年 5 月. 情報処理学会研究報告, 第 2023-OS-159(12)巻, 2023 年 5 月. 優秀若手発表賞受賞