

2023 年度年次報告書

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

今年度は昨年度に引き続き、(1)階層的隔離実行環境の研究、(2)既存隔離実行環境の低遅延性研究、(3)インターフェイス実装検証の研究、(4)インターフェイス形式検証の研究、(5)セキュリティアプリの研究、の5項目について研究を実施した。

(1)階層的隔離実行環境の研究に関しては、(1-a)外部ハードウェアを活用した隔離実行環境、(1-b)CPUの新しい保護機構を活用した隔離実行環境、(1-c)ネステッド仮想化機構を活用した隔離実行環境、のそれぞれのサブテーマを実施した。(1-a)では、FPGAで実現した軽量RDMAで複数マシン間を接続して非対称マルチプロセッシングを実現するシステムの実装を進めた。(1-b)では、CHERIというCPU拡張機能を転用して軽量仮想マシンを実現するCAP-VMの技術を応用したプライバシー保護型機械学習システムを実現する研究を実施した。(1-c)では、ネステッドページング機構をパススルーする仕組みの研究や準パススルー型ハイパーバイザにおけるネステッド仮想化を最適化する研究を実施した。

(2)既存隔離実行環境の低遅延性研究に関しては、既存の隔離実行環境における処理遅延やブレを定量的に評価するために、(C.1)機密VM技術の性能評価と(C.2)SmartNICの性能評価を行った。また、既存ソフトウェア技術とハードウェアの組み合わせを評価するためのプロトタイプとして、(C.3)論理分割ハイパーバイザと機密VMの評価に向けたプロトタイプ、(C.4)SmartNIC内で論理分割ハイパーバイザを適用した場合の評価に向けたプロトタイプ、の設計と実装を行なった。

(3)インターフェイス実装検証の研究に関しては、ネステッド仮想化に関するインターフェイス実装のファジングの研究を進めた。ハイパーバイザやゲストOSを内包した入力となるVMを自動生成するためのVM生成器を導入して、有効・無効の境界状態にあるVMを多数自動的に生成することでネステッド仮想化部分のファジングを効果的に行う手法を実現し、KVMやXenにおける複数の脆弱性やバグを発見した。

(4)インターフェイス形式検証の研究に関しては、セキュリティ上重要なコンポーネントに絞って形式検証を適用するというアプローチに基づき、システムコールの参照モニタにおけるTOCTTOU問題を防止するための形式検証の研究を進めた。攻撃側も保護対象も多数のアクセスパターンがある問題に対して、攻撃が成り立ちうる双方のパターンを列挙して、それらに対して網羅的に参照モニタの安全性を検証する手法により効果的な形式検証を実現した。

(5)セキュリティアプリの研究に関しては、ディープラーニングを用いたマルウェア検知手法を新しいモデルを使って改善する手法や、TEEを利用してクレジットカード決済を安全に実現する手法、TEEを利用してFIDO2認証における認証器再登録を容易化する手法などに関する研究を進めた。

これらの研究のいくつかは国際会議でポスター発表を実施したほか、論文投稿中もしくは投稿準備を進めている。

【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%.