2024 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 大学院情報理工学系研究科
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

クラウドや IoT の普及により、ハードウェアとソフトウェアが連携する計算基盤の安全性と柔軟性の確保が重要となっている。本研究では、隔離実行環境、インターフェイスの形式・実装検証、セキュリティアプリケーションの観点から、信頼実行基盤の構築を目指した。隔離実行環境では、クラウドの Confidential Virtual Machine（CVM）を標的とする攻撃手法「BadAML」を提案した。ホストから AML を注入し、アテステーションを回避して任意コードを実行可能にする。主要クラウド構成での実験で影響を実証し、防御策として AML 実行を制限する軽量サンドボックスを実装した。形式検証では、OS カーネルの参照モニタに対する TOCTTOU 問題を対象とし、Rust 製モックファイルシステムで並行ファイルアクセスを再現し、アクセス制御の正当性を自動検証した。実装検証では、ネストされた仮想化に特化したファジング手法「NecoFuzz」により KVM や Xen などの脆弱性を発見した。構成差に注目しバグを誘発する入力を効率的に生成した。また、C から Rust への変換を支援する「SmartC2Rust」を構築し、段階的翻訳と修正で変換精度とテスト通過率を向上させた。セキュリティアプリケーションでは、FIDO2 認証の利便性と安全性を両立する Hardware Authenticator Binding（HAB）を提案した。複数の認証器をクラウドで束ねて管理し、登録の簡略化と紛失時の復旧を可能とする。AMD SEV-SNP と仮想 TPM を用いてプライバシーを保ちつつ安全な認証処理を実現した。本年度はこれらの成果により、安全性と実用性を備えた計算基盤の構築に向けた基礎的知見を得た。

【代表的な原著論文情報】

1) Ryo Nakashima, Takahiro Shinagawa. Verifying Reference Monitors via Exhaustive Access Pattern Generation. In Proceedings of the 49th IEEE International Conference on Computers, Software, and Applications (COMPSAC 2025), Jul 2025. Accepted for publication.
2) Momoko Shiraishi, Takahiro Shinagawa. Hardware Authenticator Binding: A Secure Alternative to Passkeys. In Proceedings of the 49th IEEE International Conference on Computers, Software, and Applications (COMPSAC 2025), Jul 2025. Accepted for publication.
3) Takaaki Fukai, Manami Mori, Ryuichi Sakamoto, Takahiro Hirofuchi, and Takuya Asaka. A Thin Hypervisor Approach to Multi-Tenant SmartNICs in Edge Data Centers. 8th International Workshop on Edge Systems, Analytics and Networking (EdgeSys '25). March 2025.