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

2021 年度採択研究代表者

竹房 あつ子

情報・システム研究機構 国立情報学研究所
教授

形式検証とシステムソフトウェアの協働によるゼロトラスト IoT

主たる共同研究者：

五十嵐 淳（京都大学 大学院情報学研究科 教授）
関山 太朗（情報・システム研究機構 国立情報学研究所 助教）
松井 俊浩（情報セキュリティ大学院大学 情報セキュリティ研究科 教授）

研究成果の概要

形式検証とシステムソフトウェアの融合により、ゼロトラストの概念を踏襲した安全な IoT システム(ZT-IoT)の実現を目指し、(研究課題 1)ZT-IoT システムのためのシステムソフトウェア、(研究課題 2)ZT-IoT システムのためのセキュリティポリシエンジン、(研究課題 3) ZT-IoT システムを支える監視・介入技術、(研究課題 4) ZT-IoT サービス連携のためのセキュア・オブジェクトの研究を進めている。2022 年度は、2023 年度の統合試験に向けてアルゴリズムまたはシステムの詳細設計、開発を行った。

(研究課題 1)では、実時間挙動トラッキング機構のプロトタイプ実装を進める[1]とともに、認証ベース実行制御システムの設計、OP-TEE を用いた鍵管理を行うデータ完全性保証通信機構の実装、ソフトウェア認証機構の詳細設計を進めた. (研究課題 2)では、IoT システムモデル記述言語 Rabbit の基本設計を行い、Rabbit から形式検証ツール Tamarin の入力言語への変換アルゴリズムの開発と、アルゴリズムに従い手動変換したシステム記述に対して簡単な性質が検証できることを確認した。また、完全準同型暗号を用いた秘匿モニタリング技法の研究を行った[2]。(研究課題 3)では、オートマトンを用いた IoT システムの監視手法を検討し，記述用ドメイン特化言語を Ruby で実装した。また、メッセージブローカでパケット異常検出を行うパイプライン機構の初期設計と実装、IoT システムの耐負荷性評価のための検証手法の研究[3]と、実 IoT 機器の Tamarin でのモデル化とセキュリティ要件の検証を行った。(研究課題 4)では、悪意のあるデバイスドライバやカーネルコードの侵入検出可能な LKRG 自体の改ざんを防ぐ手法の設計と、TEE で実行するモニタである OP-TEE の脆弱性について調査した。

【代表的な原著論文情報】

[1] A Linux Audit and MQTT- based Security Monitoring Framework. Jie Yin, Yutaka Ishikawa, Atsuko Takefusa. Proc. IEEE COMPSAC 2023, 2023 年 6 月 (to appear).

[2] Ryotaro Banno, Kotaro Matsuoka, Naoki Matsumoto, Song Bian, Masaki Waga, Kohei Suenaga: Oblivious Online Monitoring for Safety LTL Specification via Fully Homomorphic Encryption. CAV (1) 2022: 447-468

[3] Temporal Verification with Answer-Effect Modification: Dependent Temporal Type- and-Effect System with Delimited Continuations. Taro Sekiyama, Unno Hiroshi. Proceedings of the ACM on Programming Languages (POPL), 7, POPL, pp. 2079-2110, 2023 年 4 月.