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
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）
須崎 有康（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）
関山 太朗（情報・システム研究機構 国立情報学研究所 准教授）
松井 俊浩（東京情報デザイン専門職大学 情報デザイン学部 教授（学部長））

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。2023 年度は，PoC Phase 1 としてアルゴリズムおよびシステムソフトウェアの開発を進め，一部の統合試験を実施した.

(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の評価[1]とともに、認証ベース実行制御システムのプロトタイプ実装と評価、OP-TEE を用いた鍵管理機構[2], ソフトウェア認証機構と OTA フレームワークの開発[3]を進めた. (研究課題 2)では、提案する IoT システムモデル記述言語 Rabbit から既存の形式検証ツール Tamarin の入力言語への自動変換器を実装し、簡単な監視カメラシステムのモデルの記述・検証実験を行った[4]。(研究課題 3)では、プロトコルモニタリングのための効率的アルゴリズムの開発[5]、機械学習を使ったパケットの異常検出[8,9]、プログラムのスケーラビリティ評価技術、IoT システムの形式検証[6]や脅威分析補助[7]に関する研究を行った。(研究課題 4)では、外部から安全にセキュリティポリシーを確認するためにデバイスの真正性やソフトウェアの健全性を確認できる機能を OP-TEE に追加した。また、TEE から Linux を監視する方法がセキュアであるために OP-TEE について報告されている脆弱性を調査した。

【代表的な原著論文情報】

[1] Jie Yin, Yutaka Ishikawa, Atsuko Takefusa, A Linux Audit and MQTT based Monitoring Framework for IoT Devices and Its Evaluation, IPSJ Journal special issue of “Applications and the internet” in conjunction with the main topics of COMPSAC 2023, August 2024.

[2] 竹房 あつ子, ゼロトラスト IoT のためのシステムソフトウェア研究, システム/制御/情報「IoT とセキュリティ」特集号, vol. 68, no. 5, pp. 191-196, 2024 年 5 月.

[3] Nobuo Aoki, Atsuko Takefusa, Yutaka Ishikawa, Yasushi Ono, Eisaku Sakane, Kento Aida. ZT-OTA Update Framework for IoT Devices toward Zero Trust IoT, IEEE COMPSAC 2024 WS, NETSAP, pp. 2200-2207, Jul. 2024.

[4] 稲葉 皓信, 関山 太朗, 五十嵐 淳, 石川 裕. Rabbit: a modeling language for verifying data-flow security. 2023 年並列／分散／協調処理に関するサマー・ワークショップ(SWoPP 2023). 2023 年 8 月.

[5] Hiroya Fujinami, Ichiro Hasuo. Efficient Matching with Memoization for Regexes with Look-around and Atomic Grouping. The 33rd European Symposium on Programming (ESOP) (2) 2024: 90-118.

[6] Lélio Brun, Ichiro Hasuo, Yasushi Ono, Taro Sekiyama. Automated Security Analysis for Real-World IoT Devices. The 13th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP) 2023: 29-37.

[7] Misato. Nakabayashi, Taro Sekiyama, Ichiro Hasuo, Yutaka Ishikawa. Formal Support for Threat Modeling with Attack Decision Diagrams. The 18th IEEE International Workshop on Security,

Trust, and Privacy for Software Applications (STPSA), pp. 2459-2464, 2024.

[8] Laura Lahesoo, Uyen Do, Rodrigo Carnier, Kensuke Fukuda, SIURU: A Framework for Machine Learning Based Anomaly Detection in IOT Network Traffic. The 18th Asian Internet Engineering Conference (AINTEC), pp.87-95, 2023.

[9] Uyen Do, Laura Lahesoo, Rodrigo Carnier, Kensuke Fukuda, Evaluation of XAI Algorithms in IoT Traffic Anomaly Detection. International Conference on Artificial Intelligence in Information and Networks (ICAIIC), pp.669-674, 2024.

[10] Taichi Takemura, Ryo Yamamoto, and Kuniyasu Suzaki, TEE-PA: TEE Is a Cornerstone for Remote Provenance Auditing on Edge Devices With Semi-TCB, IEEE Access 12 26536-26549 2024/02.