様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１２　日現在

機関番号：　８２６２６
研究種目：　研究活動スタート支援
研究期間：　2015～2016
課題番号：　１５Ｈ０６８８６

研究課題名（和文）サイバーフィジカルシステムからの情報漏洩の定量的解析

研究課題名（英文）Quantitative Analysis of Information Leakage in Cyber-Physical Systems

研究代表者

川本　裕輔（Kawamoto, Yusuke）

国立研究開発法人産業技術総合研究所・情報技術研究部門・研究員

研究者番号：６０７６０００６

交付決定額（研究期間全体）：（直接経費）　　2,000,000円

研究成果の概要（和文）：本研究では、サイバーフィジカルシステムからの情報漏洩の定量的解析技術を改良することを目指し、大規模な確率的システムからの秘密情報の漏洩量を効率的かつ自動的に推定する新たな手法を開発した。具体的には、定量的情報流解析の理論研究を発展させるとともに、記号的手法と統計的手法を組み合わせることによって、従来手法よりも高い品質で、より効率的な定量的情報流解析手法を提案した。さらに、このハイブリッド手法を用いて、定量的情報流解析ツールHyLeakを開発した。また、スケジューリングと観測が情報漏洩にどのような影響を与えるのかについても研究を行った。

研究成果の概要（英文）：In this project we developed a new analysis method for automatically estimating the amount of information leakage in larger probabilistic systems in order to improve the techniques for quantitatively analyzing information leakage in cyber-physical systems. More specifically, we developed theories in quantitative information flow, and proposed a new hybrid approach that combines the formal approach with the statistical approach to obtain faster analysis with better accuracy. Then we developed a new analysis tool HyLeak for estimating leakage amount using this hybrid approach. In addition we also investigated how scheduling and observation influence information leakage properties.

研究分野：　プログラム検証

キーワード：　情報セキュリティ　プログラム検証　形式手法　情報理論　定量的情報流解析

１．研究開始当初の背景

サイバーフィジカルシステムが日常生活に普及し、様々なデバイスから大量のデータを収集するようになると、健康状態、位置情報、行動内容などの秘密情報が意図せず漏洩してしまう危険性が高まる。このようなプライバシ情報は、他の情報と組み合わせることで漏洩することもあり、いかなる部分情報も漏洩せずに現実的なシステムを実現することは、たいてい不可能である。したがって、現実的なシステムでは、ある程度の情報漏洩を許容することが求められる。

そのため、大規模システム全体から漏洩する秘密情報の度合いが深刻かどうかを定量的に確かめることが重要であり、システムの出力から漏洩する秘密情報の量を計算するための技術（定量的情報流解析, quantitative information flow analysis）が、最近十数年にわたって盛んに研究されてきた。定量的情報流解析では、システムの出力に漏洩する秘密情報の度合いを定量化するために、（秘密情報と出力の間の）相互情報量などの情報理論の概念を用いる。

２．研究の目的

本研究は、大規模な確率的システムからの秘密情報の漏洩量の推定を効率化・自動化するための定量的情報流解析技術の開発を目的とした。より具体的には、研究の目的を以下の 2 点とした。

(1) 大規模なシステムはしばしば複数の部分システムを合成して得られるが、複数の部分システムの実行のスケジューリングが秘密情報の漏洩にどのように影響を及ぼすのかについて理論的に明らかにすること。
(2) 定量的情報流解析において、従来よりも高速かつ高品質に情報漏洩量（秘密情報と出力の間の相互情報量）を推定する技術を開発すること。

３．研究の方法

前述の研究目的に対応して、以下の方法により研究を進めた。

(1) スケジューリングと情報漏洩の関係
スケジューリングが情報漏洩に及ぼす影響を明らかにするために、スケジューラと攻撃者の振る舞いを定式化し、定量的情報流解析の枠組みを用いて情報漏洩をモデル化し、スケジューラの性質や構成方法に関する理論を検討した。

(2)定量的情報流解析の高速化・高品質化
定量的情報流解析を高速化・高品質化するために、従来用いられてきた「記号的解析手法」と「統計的解析手法」を融合させることにより、新たな定量的情報流解析技術を開発し、これをツールとして実装した。

４．研究成果

本研究の成果は、(1)スケジューリングと情報漏洩の関係についての理論的成果、(2)定量的情報流解析の高速化・高品質化についての理論的成果と(3)そのツール実装、そして(4)その他の解説論文からなる。

(1) スケジューリングと情報漏洩の関係についての研究成果
複数の部分システムの実行のスケジューリングが秘密情報の漏洩にどのように影響を及ぼすのかについて理論研究を行った。具体的には、スケジューラの振る舞いと攻撃者の観測能力が情報漏洩の度合いにどのように影響を及ぼすかについて、定量的情報流解析の枠組みを用いて定式化した。特に、スケジューラに依存するシステムが漏洩する情報量の上限を示した。また、min-entropy ベースの情報漏洩量を最小化するスケジューラの構成方法を示した。
これらの研究成果をまとめ、査読付国際ワークショップ QAPL 2015 （ The 13th International Workshop on Quantitative Aspects of Programming Languages and Systems）で発表した。なお、この成果は、研究協力者 Thomas Given-Wilson との共同研究に基づくものである。

(2) 定量的情報流解析の高速化・高品質化についての研究成果
定量的情報流解析には、前述のとおり、「記号的解析手法」と「統計的解析手法」がある。記号的解析手法はソースコードの情報を用いてシステムを抽象化して記号的に解析するのに対し、統計的解析手法はシステムをブラックボックスとして繰り返し実行して得られたトレースの集合に対して、統計手法を用いて解析する。前者はトレース数が大きなシステムの解析に不向きで、後者は秘密情報と公開情報の間の関係を表す同時確率分布行列のサイズが大きなシステムの解析に不向きである。
このように二つの手法の長所と短所が異なる点に着目し、本研究では、両手法を組み合わせることにより、解析の品質と効率を両立させた新たな定量的情報流解析手法を開発した。具体的には、解析対象の確率的プログラムをコンポーネントに分解し、各コンポーネントの性質を評価することにより、統計的手法に適した部分に対しては統計的手法

を用い、記号的手法に適した部分に対しては記号的手法を用いる手法を提案した。この推定では、情報漏洩量（相互情報量）の推定値の信頼区間を計算し、解析結果の品質を評価できるようにした。また、記号的手法に基づいてソースコードを解析することにより、解析の品質を保ちつつも、統計的手法におけるシミュレーションの実行回数を削減する手法を考案した。

これらの研究成果をまとめ、形式手法に関する査読付国際会議 FM 2016（The 21st International Symposium on Formal Methods）で発表した。なお、この成果は、研究協力者 Fabrizio Biondi らとの共同研究に基づくものである。

(3) 定量的情報流解析の新たなツールの実装についての研究成果

(2)で述べた定量的情報流解析の新手法において、確率的プログラムの各部分に対して、記号的手法と統計的手法のどちらを用いて解析するとより効率的なのかを判定するヒューリスティクスを改良し完成させた。

このヒューリスティクスを前述の解析技術と組み合わせることにより、確率的システムからの情報漏洩の度合いを、従来よりも高速かつ高品質に推定する解析技術を開発した。さらに、(2)で実装したプロトタイプを改良し、定量的情報流解析ツール HyLeak を開発した。このツールは後述のウェブサイトからダウンロードして利用することができる。なお、この成果は、研究協力者 Fabrizio Biondi、Louis-Marie Traonouez らとの共同研究に基づくものである。

(4) その他の解説論文

これらのほかに、確率的システムの安全性の検証に関して、定理証明支援系ベースの検証手法・検証ツールについて調査を行い、確率的システムの中でも暗号システムに焦点を当てて、安全性の形式検証の入門から計算機上での証明までを紹介する解説論文を執筆し、コンピュータソフトウェア誌で発表した。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 3 件）

1. 川本 裕輔. 暗号系の安全性検証 – 入門から計算機による証明まで. コンピュータソフトウェア, Vol.33 No.4, pp.67-83, November 2016, 査読有. DOI: 10.11309/jssst.33.4_67

2. Yusuke Kawamoto, Fabrizio Biondi and Axel Legay. Hybrid Statistical Estimation of Mutual Information for Quantifying Information Flow. In Proc. of 21st International Symposium on Formal Methods (FM 2016), Lecture Notes in Computer Science, Vol.9995, pp.406-425, November 2016, 査読有. DOI: 10.1007/978-3-319-48989-6_25

3. Yusuke Kawamoto and Thomas Given-Wilson. Quantitative Information Flow for Scheduler-Dependent Systems. In Proc. of 13th International Workshop on Quantitative Aspects of Programming Languages and Systems (QAPL 2015), Electronic Proceedings in Theoretical Computer Science, Vol.194, pp.48-62, September 2015, 査読有. DOI: 10.4204/EPTCS.194.4

〔学会発表〕（計 5 件）

1. Yusuke Kawamoto, Fabrizio Biondi and Axel Legay. プログラム解析と統計手法の融合による定量的情報流解析. 第 19 回プログラミングおよびプログラミング言語ワークショップ（PPL2017）, 日本ソフトウェア科学会 プログラミング論研究会, 華やぎの章 慶山（山梨県笛吹市）, 2017 年 3 月.

2. Yusuke Kawamoto, Fabrizio Biondi and Axel Legay. Hybrid Statistical Estimation of Mutual Information for Quantifying Information Flow. In the 21st International Symposium on Formal Methods (FM 2016), St. Raphael Resort, Limassol (Cyprus), November 2016.

3. Yusuke Kawamoto. Combining Static and Statistical Approaches to Quantitative Information Flow. In NII Shonan Meeting Seminar 069, 湘南国際村センター（神奈川県葉山町）, October 2015.

4. Yusuke Kawamoto. Formal and Statistical Approach to Quantitative Information Flow of Programs. In the workshop on Formalization of Applied Mathematical Systems, University of Hawaii, Manoa (USA), October 2015.

5. Tom Chothia, Yusuke Kawamoto and Chris Novakovic. 統計的手法によるプログラムの定量的情報流解析. 日本応用数理学会 2015 年度年会, 金沢大学（石川県金沢市）, 2015 年 9 月.

〔その他〕

定量的情報流解析ツール HyLeak のウェブ

サイト：
https://project.inria.fr/hyleak/

６．研究組織

(1)研究代表者
川本裕輔（Yusuke Kawamoto）
国立研究開発法人 産業技術総合研究所・
情報技術研究部門・研究員
研究者番号：60760006

(4)研究協力者
Fabrizio Biondi
Chair of Threat Analysis,
CentraleSupélec & Inria/IRISA Rennes,
France.

Thomas Given-Wilson
Post-doctoral Researcher,
Inria/IRISA Rennes, France.

Louis-Marie Traonouez
Post-doctoral Researcher,
Inria/IRISA Rennes, France.