科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ５ 月 １１ 日現在

機関番号：１３９０１
研究種目：若手研究(B)
研究期間：2011～2013
課題番号：２３７０００２６

研究課題名（和文）量的情報流の正確な検証

研究課題名（英文）Verification of Quantitative Information Flow

研究代表者
寺内　多智弘（Terauchi, Tachio）

名古屋大学・情報科学研究科・准教授

研究者番号：７０４４７１５０

交付決定額（研究期間全体）：（直接経費）　　3,200,000円、（間接経費）　　960,000円

研究成果の概要（和文）：量的情報流の困難性に関する研究を行い、beliefやmin entropy channel capacityなど様々な情報理論的尺度に基づく量的情報流に関する検証・推論問題の困難性を解明した。計算量理論的困難性のみならず、「hyperproperty」と呼ばれるプログラム検証問題の分類を用いての困難性も考察した。また、ソフトウェアモデル検査技術と#SATソルバ等カウンティングアルゴリズムを応用した高精度な量的情報流上限検証・推論アルゴリズムを提案した。また、検証アルゴリズムの基礎となるソフトウェアモデル検査技術の改良に関する研究を行った。

研究成果の概要（英文）：We solved open problems concerning the complexity of various quantitative information flow verification problems. We considered quantitative information flow definitions based on various information theoretic notions such as belief and min entropy channel capacity, and studied the problems both from the computational complexity theoretic aspect and the program verification property classification aspect formalized by the notion of "hyperproperties." We also proposed algorithms for precisely inferring and verifying the quantitative information flow bounds that utilize software model checking and counting algorithms. We also proposed new approaches to software model checking.

研究分野：情報科学

科研費の分科・細目：情報学・ソフトウェア

キーワード：セキュリティ　プログラミング言語　プログラム検証　量的情報流

１．研究開始当初の背景

近年、ネットワーク環境の普及に伴い、コンピュータソフトウェアのセキュリティの重要性が高まっている。RSA など個々の暗号系の安全性は計算量理論の手法により手動で証明されるが、ソフトウェアシステム全体の安全性（いわゆる、end-to-end セキュリティ）を手動で検証するのは困難であるため、プログラム検証の技術を用いた自動検証の手法が注目されてきた。従来の end-to-end セキュリティには非干渉性(Non-interference, NI)という概念が用いられてきた。NI は（暗号系などの安全性を仮定した上で）、プログラムが外部（「攻撃者」と呼ばれる）に機密情報を全く漏らさない、という定義である。これは場合により非常に厳しい条件であり、NI を緩和する目的で量的情報流(Quantitative Information Flow, QIF)という漏洩する情報量を安全性の尺度とするプログラムの安全性の定義が提案された。例として次のプログラムを考える。ただし、password_hash = hash(password)、つまり、password のハッシュ値とする。

```
if password_hash = hash(guess)
 then output(“access granted”)
 else output(“access denied”)
```

機密情報 password はハッシュ関数により隠蔽されているため直接漏洩することはないが、攻撃者はプログラムを実行することにより「password が入力 guess と一致しているか」という情報を得ることができる。ゆえに、このプログラムの情報流はゼロではなく NI を満たさない。しかし、（password が十分に広い範囲から無作為に選ばれると仮定した場合）1 回の実行で得られる情報は少ないため、安全であるといえる。例のように、正当に情報を漏洩するプログラムの安全性を正確に表現するのが QIF である。password が 64bit の値で一様に分布されていると仮定し、例のプログラムの QIF を実際に求めると約 3.47x10-18 ビットとなる。QIF の数値は攻撃者が機密情報を推論できる確率に関係し、QIF から安全性の推測が可能となる。

QIF の研究は、英国クイーンメリー大学の Malacaria 博士による論文「Assessing security threats of looping constructs」が 2007 年にプログラミング言語研究分野で最高峰の会議 POPL に採録され、2009 年にはドイツ ザールランド大学の Backes 教授らによる論文「Automatic Discovery and Quantification of Information Leaks」が情報セキュリティの分野で最高峰の会議 Symposium on Security and Privacy に採録されるなど、世界的に注目を集めている。しかし、QIF の検証は NI のそれと比べまだ未発達であり、大規模ソフトウェアの QIF を自動的に検証する手法は確立されていない。本課題の応募者は、2011 年、いくつかの定義において QIF 検証の検証理論的および計算量理論的困難性を解明する研究を行い、これらを明らかにした。これは QIF 検証の困難性を解明した世界初の結果である。

２．研究の目的

本課題では上記の QIF 検証の理論的困難性の研究をさらに発展すると共に、より現実的なプログラムに対する QIF 検証の応用を目指す。具体的には以下のテーマに重点をおいて研究を推進する。

I. Belief などの概念に基づいた QIF 定義に対する検証困難性の解明
II. 困難性の研究で得られた知見をもとにした、大規模プログラムに効果的な QIF 検証手法の開発

QIF には情報理論に基づいた様々な定義が存在し、応募者は、これまで、Shannon entropy, Min entropy など様々な概念に基づいた QIF の定義での検証理論的および計算量理論的な検証困難性について研究し、定義の相違が困難性の相違に反映されることを明らかにした。これは様々な QIF 定義の現実的有効性を比較する上で非常に役立つ結果である。故に、Belief-based(*2)など近年提案された他の QIF の定義についても困難性を検証する。そして、困難性の研究で得られた知見をもとに、self composition、型システムやモデル検査などプログラム検証の技術を用い、より現実的なプログラムに対する QIF 検証の研究を行う。(QIF,NI を含めプログラム検証は一般には決定不可能であるが、近年、モデル検査などプログラム検証技術の発展により、多くの現実的なプログラムに対する検証が可能となり、Microsoft 社の Static Driver Verifier など、実用的なツールも開発されている。)

３．研究の方法

Belief の概念に基づいた定義、min entropy channel capacity, guessing entropy channel capacity 等の QIF 定義につき、QIF 比較問題と QIF 上限問題の困難性を求める。困難性の尺度には k-safety property の性質およびブーリアンプログラムなどに限定されたプログラムでの計算量を用いる。

また、より現実的なプログラムに対する QIF 検証の手法を開発する。これまでの QIF 検証の研究には、正確に検証する手法は少なく、不完全および不健全な（つまり、場合として間違った答えを返す）手法が多い。また、既存の正確に検証する手法はごく小さい toy program しか扱うことができない。

４．研究成果

量的情報流の困難性に関する研究を行い、belief や min entropy channel capacity など様々な情報理論的尺度に基づく量的情報流に関する検証・推論問題の困難性を解明した。計算量理論的困難性のみならず、「hyperproperty」と呼ばれるプログラム検証問題の分類を用いての困難性も考察した。また、ソフトウェアモデル検査技術と#SAT ソルバ等カウンティングアルゴリズムを応用した高精度な量的情報流上限検証・推論アルゴリズムを提案した。また、検証・推論アルゴリズムの基礎となるソフトウェアモデル検査技術の改良に関する研究も行った。

これらの研究は Journal of Computer Security, ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)など、トップレベルの国際論文誌および国際会議に採録された。また、Dagstuhl セミナーなど国際セミナーに招待され講演も行った。

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 4 件）

1. Hiroshi Unno, Tachio Terauchi, and Naoki Kobayashi. Automating Relatively Complete Verification of Higher-Order Functional Programs. In Proceedings of the 40th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2013), ACM SIGPLAN Notices 48 (1), pp. 75-86. ACM, 2013.
2. 岩塚卓也, 寺内多智弘, 結縁祥治. 無限小定数と限量子除去法によるハイブリッドシステムの検証に向けて. 情報処理学会論文誌：プログラミング(PRO) 6(3):2013.
3. Hirotoshi Yasuoka and Tachio Terauchi. Quantitative Information Flow as Safety and Liveness Hyperproperties. In Proceedings of the 10th Workshop on Quantitative Aspects of Programming Languages and Systems (QAPL 2012), Electronic Proceedings in Theoretical Computer Science 85, pp. 77-91. 2012.
4. Hirotoshi Yasuoka and Tachio Terauchi. On Bounding Problems of Quantitative Information Flow. Journal of Computer Security 19.6 (2011): 1029-1082.

〔学会発表〕（計 6 件）

1. Takuya Kuwahara, Tachio Terauchi, Hiroshi Unno, and Naoki Kobayashi. Automatic Termination Verification for Higher-Order Functional Programs. ソフトウェア科学会 第 16 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 (PPL 2014). 2014.
2. Hiroshi Unno, Tachio Terauchi, and Naoki Kobayashi. Automating Relatively Complete Verification of Higher-Order Functional Programs. ソフトウェア科学会 第 15 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 (PPL 2013). 2013.
3. 岩塚卓也,寺内多智弘,結縁祥治. 無限小定数と限量子除去法によるハイブリッドシステムの検証. 情報処理学会 第 93 回プログラミング研究会. 2013.
4. Tachio Terauchi. On Complexity of Verifying Quantitative Information Flow. Dagstuhl Seminar 12481: Quantitative Security Analysis. 2012.
5. Tachio Terauchi. Automated Verification of Higher-Order Functional Programs. In Proceedings of the 11th International Symposium on Functional and Logic Programming (FLOPS 2012), Lecture Notes in Computer Science 7294, pp.2. Springer, 2012. (招待講演)
6. Tachio Terauchi. Relatively Complete Refinement Types from Counterexamples. NII Shonan Meeting Seminar 005: Automated Techniques for Higher-Order Program Verification. 2011.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者

寺内 多智弘（TERAUCHI TACHIO）
名古屋大学・大学院情報科学研究科
准教授
研究者番号：70447150

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：