平成30年度 情報工学コース卒業研究報告要旨

関 研究室	氏　　名	三 輪 竜 矢
卒業研究題目	動的情報漏洩量の解析および適応的制御入力最適化に関する研究	

プログラムのセキュリティ強度を表すための尺度として，量的情報流（QIF）が注目されている．QIF は，プログラムの機密入力 S と出力 O に対して，O の値の観測前後で S の曖昧さがどれだけ減少したか，すなわち，S と O の相互情報量と定義される．しかしこれはすべての実行に対する漏洩量の期待値を表している．個々の実行ごとの出力値から動的に漏洩量を計算できることが望ましい．著者らの研究グループでは動的情報漏洩量の定義を提案しているが，その計算方法についてはあまり検討されていなかった．

本研究ではまず，上記の動的漏洩量の近似値を求めるための解析法を提案した．次にプログラムの入力の一部を観測者が選択できる場合，動的漏洩量の期待値が最大となるような制御入力値を適応的に求める手法を提案した．

1 つめの課題の解析法は，Besson らの QIF の監視法を参考に提案した．Besson らの監視法では，各プログラム変数に対する知識を「環境に値を割当てる写像」として定義している．しかし，この定義は煩雑であるため，本研究ではこれを，プログラムが扱うデータ値を背景理論として用いる否定を含まない命題論理式の形で表す．具体的には，抽象解釈法を用いて与えられたプログラムの状態空間を有限で近似し，それによって得られたプログラムにおける機密入力と観測出力の間の制約条件を表す論理式 φ を構成する．実行時に観測出力値が得られたらこれを φ に代入し，機密入力値の候補集合を求める．論文では，上の制約条件を表す論理式の構成法の正当性を証明した．さらに，この解析法から機密入力の候補を絞り込めるか否か，すなわちプログラムが安全か否かを判定する近似解析問題が PSPACE 完全であることも証明した．

2 つめの課題については，制御入力付きのプログラムに対して，実際に制御入力値 l を与えたときの漏洩量の期待値を最大化する問題を定式化し，そのような制御入力値を計算する方法を示した．最適入力値およびそのときの漏洩量の計算はプログラム側でも行えるため，漏洩量が閾値を超える場合，実行を中断するなどの対策を動的に取ることができるようになるであろう．具体的なモデルは次のようになる．攻撃者は，確率的なプログラムを解析して，そのプログラムを制御できるような入力値を自由に送信できる．送信後，プログラムが実行され 1 つの値が出力される．攻撃者は，その出力値を観測することでプログラム側の機密入力についての情報を得られる．この出力値と前回送信した制御入力値から，再びプログラムを制御する入力値を計算する．これを何回でも繰り返すことで，機密入力を特定できるようになる．本研究では，送信する制御入力は機密情報に関する漏洩量の期待値を最大にするように選ぶものと定義し，その具体的なアルゴリズムを示した．さらに，プログラムが決定性で機密入力が一様分布に従う場合は，この問題は集合の要素数の数え上げ問題として考えられることを示した．

論文ではそれぞれの課題に対する提案手法を説明する例をいくつか挙げている．1 つ目の課題の例では，解析結果から機密入力と観測出力の対応を求め，個々の出力の漏洩量の上界と下界を計算することで，実際の漏洩量の近似値になっていることを確認した．2 つ目の課題の例では，確率的なプログラムの AOCIP を考え，攻撃者は提案したアルゴリズムによって機密入力の特定ができることを確認した．また，制御入力を提案アルゴリズムによって求めたときとランダムに選んだときにおける，事後エントロピーと動的 QIF を定量的に比較した．事後エントロピーは提案アルゴリズムの方が小さくなり期待通りとなるが，動的 QIF はランダムに選択したときにも大きくなりうることを確認した．