論 文 内 容 の 要 旨

博士論文題目

Verification Methods for Security against Inference Attacks on XML and Relational Databases

（XML および関係データベースにおける推論攻撃に対する安全性検証法）

氏　　名　Chittaphone Phonharath

（論文内容の要旨）アクセス制御はデータベース管理において不正なユーザからのアクセスを防ぐための最も重要な機能の１つである。アクセス制御を実現する典型的な方法は、許可された問合せの集合と許可されない問合せの集合を切り分け、ユーザはデータベースインスタンスに対する許可問合せの結果しか得られないようにすることである。一見するとこのアクセス制御ポリシーで十分に思われるが、不正なユーザは許可問合せの結果や問合せのコード（意味）、その他に利用可能な外部情報を巧妙に利用することで、許可されてない問合せの結果（すなわち、機密情報）を得ることが可能である場合がある。このような攻撃を推論攻撃と呼ぶ。本論文では、XMLおよび関係データベースにおける推論攻撃に対する安全性を検証する手法についての2つの研究成果が与えられている。

第3章では、k-安全性というXMLデータベースにおける推論攻撃に対する安全性の尺度についての静的解析問題に関する成果が与えられている。直観的に、k-安全性は、許可問合せとそれらの結果などの利用可能な情報を用いて、データベースインスタンス中の機密情報、すなわち、インスタンスに対する許可されない問合せの結果の候補の数がk-1個以下に絞り込まれることがないことを意味する。本研究では、次のように定義されるスキーマk-安全性の決定可能性について考察されている：XMLデータベーススキーマと許可問合せ、不許可問合せが与えられたときに、そのスキーマに従うすべてのデータベースインスタンスがk-安全である。成果として、問合せが線形決定性トップダウン木変換器（LDTT）のシンプルなサブクラスで表現される場合でも、任意の有限の値k>1についてスキーマk-安全性問題が決定不能であることが示されている。一方で、LDTTのクラスに対するスキーマ∞-安全問題が決定性指数時間完全であることが示されている。さらに、LDTTと同様に、正規先読み付きのLDTTに対してもスキーマ∞-安全問題が決定可能であることが示されている。

第4章では、関係データベースにおけるl-多様性を問合せのアクセス制御を考慮した場合に拡張して、推論攻撃に対するインスタンスレベルの安全性の概念が与えられている。具体的には、問合せに基づくl-多様性と呼ばれるプライバシーの概念が提案されている。データベースインスタンスTが許可問合せに関してl-多様性をもつとは、攻撃者がインスタンスTに対する許可問合せ結果とその問合せの意味からでは、機密情報の値の候補をlよりも少ない数までは絞り込むことができないことをいう。本論文では、この性質を判定する2つの方法が与えられている。1つ目の方法は、関係データベース管理システム、たとえばSQLを用いて、入力に対して直接的に判定を行うものである。2つ目の方法は、入力を論理式に変換し、#SATソルバを用いてモデル計数を行うことによって判定を行うものである。これらの2つの方法の有効性とスケーラビリティについて実験結果に基づいて議論されている。

氏　名	Chittaphone Phonharath

（論文審査結果の要旨）

セキュリティやプライバシーに関する適切な定量的尺度を導入し、それらの尺度に基づきシステムが安全であるかどうかを自動検証する技術の開発が望まれる。特にデータベースセキュリティにおいては、どのようなデータモデルに基づいているか、インスタンス／スキーマのいずれに着目するか等、問題設定も多様である。このような背景のもと、本論文では、データベースにおける推論攻撃に対する安全性の定量的尺度の提案およびそれらの尺度に基づく安全性の検証手法について以下の成果を得ている。

本論文前半では、XMLデータベースにおけるスキーマレベルの k-安全性問題について論じている。k-安全性は橋本らによって導入された概念であり、XML スキーマ，スキーマに従うインスタンス D，許可問合せ，禁止問合せが与えられたとき、攻撃者が閲覧や実行を許可されたデータに基づいてどのような推論を行っても、禁止問合せの結果の候補を k 個未満に絞り込めないならば、D は k-安全性を満たす（有限個に絞り込めないとき∞-安全性を満たす）という。本論文ではまず、スキーマの k-安全性を導入している。スキーマ A が k-安全性を満たすとは、A に従うすべてのインスタンスが k-安全性を満たすことをいう。次に、与えられたスキーマが k-安全性を満たすかどうかを判定する問題に着目し、問合せが決定性線形ボトムアップ木変換器(LDTT)によって与えられるとき、本問題は有限の k（$\geqq 2$）に対して判定不能、$k=\infty$ に対して判定可能であることを示している。また後者については計算量の上下界を精密に分析している。

本論文後半では、関係データベースにおけるインスタンスレベルの l-多様性問題について論じている。l-多様性は Machanavajjhala らによって導入された概念であり、準識別子の値によってインスタンスを同値類に分割したとき、どの同値類も秘匿属性の異なる値を l 個以上含むことをいう。しかしこの定義においては許可問合せが複数存在しそれらに対して推論攻撃が行われることが想定されていない。本論文ではまず、問合せに基づく l-多様性という尺度を定義している（以降、単に l-多様性とよぶ）。次に、l-多様性を判定する２つの手法を提案し評価実験によりその有効性について論じている。１つ目の手法は秘匿属性値の種類を直接計数する手法であり、高速であるが問合せとして射影演算しか取り扱えない。２つ目の手法は命題論理式のモデル計数問題に帰着して判定する方法であり、実行時間が大きくなるものの、自己結合と否定以外の任意の関係演算を用いた問合せを取り扱えるため適用範囲が広いことが示されている。

以上の通り、本論文で提案された手法と得られた結果は、セキュリティやプライバシー保護における形式的手法、とりわけ定量的尺度に基づくデータベースセキュリティの検証技術に重要な知見を与えており、博士（工学）の学位論文として価値あるものと認める。