論 文 内 容 の 要 旨

博士論文題目　バースマークと動的名前解決によるソフトウェアプロテクション

氏　名　　玉田 春昭

論文内容の要旨

本論文では，ソフトウェアの盗用(他人の作成したソフトウェアを許可なく自分のソフトウェアに組み込む行為)，および，ソフトウェアクラック(ソフトウェア内部に含まれる秘密情報の解析・改ざんなどの行為)をそれぞれ抑止するための2つの方法を提案する．

まず盗用の抑止を目的として，ソフトウェアバースマークという概念を提案する．バースマークとは，各ソフトウェア固有の特徴を表す値の集合であり，ソフトウェアが改ざんされてもほとんど変化しないという``保存性''と，異なるソフトウェアからは全く異なるバースマークが抽出される``弁別性''の2つの性質を持ことが望まれる．本論文では，Java 言語を対象に変数初期値バースマーク，メソッド呼び出し系列バースマーク，継承関係バースマーク，使用クラスバースマークの4種類のバースマークを提案し，保存性，弁別性の評価を行った．

まず保存性の評価では，Apache Ant に4種類の難読化ツールを適用し，難読化前後のクラスファイルからバースマークを抽出し，比較した．その結果，バースマークの類似度の平均は0.940であり保存性があることを示した．また，弁別性評価では，Java バイトコードを扱う3つのライブラリ BCEL, javassist, bloat に含まれるクラスファイルから4種類のバースマークを抽出した結果，0.962の割合で異なるクラスファイルを弁別できることを確認した．

次に，クラックの抑止を目的として，動的名前解決を利用して，ソフトウェアの名前難読化を行う方法を提案する．名前難読化とはプログラム中に現れる名前(識別子)を別のものに付け替える難読化である．しかし，従来法ではユーザが定義した名前しか隠すことができず，標準ライブラリのようなシステムが提供するライブラリに含まれるメソッドやクラス名を隠すことはできない．提案方法は，メタプログラミングに用いられる動的名前解決機構を難読化に導入することで，ユーザライブラリの呼び出しのみならず，従来隠すことのできなかった標準ライブラリの呼び出し（クラス参照やメソッド呼び出し，フィールドの参照・代入のことを言う）を隠すことが可能となる．これにより，秘密にすべき呼び出し（例えば認証処理）を隠すことができ，ソフトウェアをクラックから守ることができる．実用規模のライブラリである Jakarta Commons Digester に提案手法を適用した結果，2,359のフィールド参照，673のフィールドへの代入，197のオブジェクト生成，7,351のメソッド呼び出しの全てのクラス名，メソッド名，フィールド名を隠蔽することができた．

氏 名	玉田 春昭

（論文審査結果の要旨）

本論文では，開発の局面におけるソフトウェアの不正利用であるソフトウェアの盗用（他人の作成したソフトウェアを許可なく自分のソフトウェアに組み込む行為）と，利用の局面におけるソフトウェアの不正利用であるソフトウェアクラック（ソフトウェア内部に含まれる秘密情報の解析・改ざんなどの行為）を防止するための手法を提案している．本論文において，提案されたソフトウェア保護方法は以下の 2 点であった．

1. ソフトウェアバースマーク
2. 動的名前解決を用いたソフトウェア難読化手法

まず，1. ソフトウェアバースマークでは，ソフトウェアの盗用を効果的に発見するための概念として，バースマークを定義し，バースマークが満たすべき 2 つの性質である保存性と弁別性とを明らかにしている．ソフトウェアの盗用という従来定義が困難であった問題を，バースマークという概念により明確に定義したことは画期的であり，多くの実務者や研究者にとって有用である．さらに，Java 言語を対象として，提案したバースマークの定義に従う 4 種類の具体的なバースマークを提案し，実用規模のソフトウェアを対象に定量的な評価を行っており，提案手法の有用性・信頼性を明確に示している．

2. 動的名前解決を用いたソフトウェア難読化手法では，ソフトウェアに対するクラックを防止するための手法を提案している．提案手法はプログラム中に使われる名前を理解しづらいものに変換し，プログラム理解にかかるコストを増大させる名前難読化の一手法である．メタプログラミングに用いられる動的名前解決機構を難読化に導入することで，従来隠すことのできなかったシステム定義の名前を隠すことができ，高い新規性と有用性が認められる．さらに，提案難読化手法を自動化する具体的手順も示されており，実際にアプリケーションとして実現されている．そして，実用規模のアプリケーションを対象に提案手法を適用した評価結果が示されており，提案手法の信頼性は高いといえる．

以上のとおり，本論文は，開発の局面と利用の局面におけるソフトウェアの不正利用を防ぐためのソフトウェア保護手法を提案している．それぞれの提案内容は，実用規模のアプリケーションに対して適用可能であることが示されており，また，提案手法の有用性・信頼性が評価実験により定量的に示されている．これらの研究成果は，ソフトウェアプロテクション技術の発展に大きく貢献するものであり，本論文は博士（工学）論文として価値あるものと認める．