論 文 内 容 の 要 旨

博士論文題目　秘密隠蔽のための系統的ソフトウェア保護フレームワーク

氏　名　山内 寛己

近年，ソフトウェアに含まれる秘密の漏洩を防止することの必要性が増大しており，エンドユーザによるソフトウェアシステムに対する攻撃を妨げることが急務となっている．従来，多種様々なソフトウェア保護技術が提案されてきたが，これら多くの技術をどのように使い分け，もしくは併用すべきかについての系統的な方法は，ほとんど議論がされていない．

本論文では，ソフトウェアシステムの系統的な保護を目的として，まず，エンドユーザによるソフトウェアシステムに対する攻撃モデル，攻撃方法とソフトウェア保護技術について整理し，その結果に基づいて，ソフトウェアの各開発工程において段階的にプロテクション技術を適用するためのガイドライン（段階的プロテクション）を提案した．

次に，段階的プロテクションの実施手順において重要となるソフトウェア難読化に着目し，ソフトウェア難読化手法を適材適所に適用するための枠組み（難読化フレームワーク）を提案した．提案フレームワークでは，攻撃者の攻撃におけるゴールを定義するとともに，ゴール達成に必要なサブゴールを，ゴール分解により求めていくことでゴール木を生成する．そして，得られたゴール木の全ての末端のサブゴールについて，そのゴール達成を妨げるのに必要な難読化手法を選定する．ケーススタディとして，秘密を含む典型的な Digital Rights Management (DRM) ソフトウェアの 1 つである cryptomeria cipher (C2) 暗号プログラムにおいて，復号鍵を隠蔽するためのゴール木を生成する事例を通して，多数の難読化手法を適材適所に適用できることを示した．

さらに上記の難読化フレームワークにおいて，ゴール木の各ノードを構成する攻撃者の行動に着目すると，全ての行動は，プログラム中から秘密情報，もしくは秘密情報の発見の手がかりとなる情報を探す，といった行動であり，ゴール木は事実上手がかりの連鎖を表す木となっている．そこで，プログラム中の攻撃の手がかりを網羅的に列挙し，それらを難読化によって隠蔽するため，フレームワークの拡張を行った．これにより，秘密情報とその手がかりとの関係，及び，手がかり間の関係を，アルゴリズム，ソースコード，バイナリの 3 つの抽象レベルに分けて記述し，各レベルにおいて難読化により手がかりを隠蔽することで，秘密情報の発見を困難にすることが可能となった．

氏　名	山内　寛己

（論文審査結果の要旨）

本論文では，ソフトウェアシステムの系統的な保護を目的とする 2 つのテーマに取り組んでいる．まず，(1) ソフトウェアシステムに対する攻撃モデル，および，攻撃に対するソフトウェアプロテクションの要素技術を整理し，その結果に基づいてソフトウェアの各開発工程において段階的にプロテクション技術を適用するためのガイドラインの提案している．次に，(2) 要素技術の 1 つのソフトウェア難読化に着目し，既存のソフトウェア難読化手法を適用する系統的なフレームワーク（難読化フレームワーク）を提案している．

(1) の提案では，まず，ソフトウェアに含まれる秘密を獲得しようとする攻撃を 3 つに分類し，従来系統的な防御手段が確立されていなかったエンドユーザ自身による攻撃に焦点をあて，その防御技術のサーベイを網羅的に行っている．そして，攻撃手段と保護技術の対応関係を整理し，ソフトウェアの各開発工程で適用可能なプロテクション技術を示している．近年，家電機器や携帯電話などの組み込みソフトウェアシステムにおいて，エンドユーザによる攻撃の防御の必要性が増していることから，本論文の成果はソフトウェア開発現場における高い有用性が見込まれる．

(2)については，保護対象のソフトウェアシステムに対し，想定される攻撃者の能力，および，攻撃のゴールを設定した上で，ゴール指向分析によって攻撃者の取り得る行動や攻撃対象を（サブゴールとして）網羅的に列挙する方法を提案している．この提案により，ソフトウェア難読化を適用すべき箇所や適用方法を明確にすることが可能となった．従来，難読化法は数多く提案されてきたが，本当に保護したい秘密情報の解析防止にどの程度効果があるのかが明らかでなく，やみくもに難読化が行われているのが現状であった．本論文では，難読化法ではなく攻撃に着目し，攻撃者の視点からトップダウンに（ゴール指向分析によって）攻撃方法を整理することに主眼が置かれている点が従来研究と大きく異なり，新規性は極めて高い．また，提案フレームワークに沿って難読化を施すことによって，より系統的かつ理にかなった難読化の適用を促進し，難読化の効果を最大限に高められるため，その有用性も高い．また，本論文では，暗号処理プログラムを対象とした評価実験も行っており，提案フレームワークの信頼性も確保されている．

以上のとおり，いずれの提案も，研究の位置づけが明確にされた上で，全体にわたって十分具体的に記述されており，新規性，有用性，信頼性のいずれについても問題がない．これらの研究成果は，ソフトウェア開発におけるソフトウェア保護技術の導入促進に大きな役割を果たし，ソフトウェア業界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．