論 文 内 容 の 要 旨

博士論文題目

Protecting Secret Information in Software Processes and Products
（ソフトウェアプロセスおよびソフトウェアプロダクトに含まれる
秘密情報の保護）

氏　　名

Yuichiro Kanzaki　（神﨑　雄一郎）

論文内容の要旨

本論文では，秘密情報がユーザへ流出するのを防止するための方法を提案している．秘密情報とは，DRM システム(Digital Rights Management System)の暗号鍵，ソフトウェアライセンスのチェックのための条件分岐命令，商業価値の高いアルゴリズムなど，ソフトウェアシステムに含まれる情報のうちシステムの安全性に関わるもののことである．

まず，第 1 章において，研究の背景を詳しく述べ，解決すべき問題を整理している．

第 2 章においては，秘密情報を含むワークプロダクト(仕様書やソースコードなど)が，ソフトウェア開発者を通してユーザに漏えいするリスクを評価する方法を提案している．本論文では，「ある開発プロセスが実施されるとき，そのプロセスに従事した開発者の知識が互いに伝播し得る」という事実に着目し，開発者間の知識の伝達のメカニズムを定式化し，「各開発者が秘密情報を含むワークプロダクトに関する知識を持つ確率」を計算する方法を示している．得られた確率から，秘密情報を含むワークプロダクトがソフトウェア開発プロセスの外部に漏えいするリスクを見積もることが可能となる．

第 3 章においては，ユーザによるソフトウェアの解析(リバースエンジニアリング)を通した秘密情報の漏えいを防止するために，ソフトウェアの解析に要するコスト(時間や労力)を増大させる方法を提案している．提案方法では，ソフトウェア中の任意の命令(ターゲット)を異なる命令で偽装(カムフラージュ)し，自己書き換え機構を用いて，実行時のある期間においてのみ元来の命令に復元する．攻撃者がカムフラージュされたターゲットを含む範囲の解析を試みたとしても，ターゲットの書き換えを行うルーチン(書き換えルーチン)の存在に気づかない限り，ソフトウェアの元来の動作を正しく理解することは不可能となる．解析を成功させるためには，書き換えルーチンを含む範囲についても解析する必要があり，結果として，攻撃者はより広範囲にわたるソフトウェアの解析を強いられることとなる．

最後に第 4 章において，論文のまとめと，今後の展望が述べられている．

氏 名	神﨑 雄一郎

（論文審査結果の要旨）

本論文では，ソフトウェアに含まれる秘密情報がユーザへ漏えいするのを防ぐことを目的とした方法が提案されている．秘密情報がユーザに漏えいする可能性は，次の 2 つのパターンに分けられている．(1)開発者によって外部に漏えいしたソフトウェア開発プロセスのワークプロダクト（ソースコード，仕様など）を通してユーザに知られる．(2)ユーザによるソフトウェアプロダクト（リリースされたソフトウェア）の解析（リバースエンジニアリング）によってユーザに知られる．

第 2 章では，(1)を防止するのに役立つ方法として，「秘密情報を含むワークプロダクトがソフトウェア開発プロセスの開発者を通して外部に漏えいするリスク」を評価する方法が示されている．まず，「ある開発プロセスが実施されるとき，プロセスに従事した開発者の知識が，ある確率のもとで別の開発者に伝達する」という事実に注目し，開発者間における「知識の伝達」のメカニズムを定式化している．導かれた式を用いて，秘密情報を含むワークプロダクトに関する知識が信頼度の低い開発者に伝わる確率を見積もり，その確率から秘密情報が外部に漏えいするリスクを評価している．また，提案方法を応用したケーススタディとして，漏えいのリスクが低い開発者割当ての検索方法や，プロセス構造が漏えいのリスクに与える影響についての考察などが例とともに示され，提案方法の有用性が明確にされている．

第 3 章では，(2)を防止するのに役立つ方法として，ソフトウェア解析に要するコスト（時間や労力）を増大させる方法が提案されている．提案方法では，プログラム中の任意の命令を異なる命令で偽装（カムフラージュ）し，自己書き換え機構を用いて，実行時のある期間においてのみ元来の命令に復元する．攻撃者がカムフラージュされた命令を含む範囲の解析を試みたとしても，命令の書き換えを行うルーチンの存在に気づかない限りプログラムの元来の動作を正しく理解できないため，解析にかかるコストが大きくなる．提案方法の適用手順が，6 つのステップに分けて具体的に記述されており，提案方法の実用性の高さがうかがえる．また，提案方法の適用により生じる，実行時間やプログラムサイズに関するオーバーヘッドを実験的に測定したり，静的解析に要するコストの理論値を算出することで，提案方法の有効性が定量的に示されている．

以上のように，本論文は，ソフトウェアに含まれる秘密情報がユーザへ漏えいする可能性を2つのパターンに分け，各々について，漏えいを防止するのに役立つ方法を提案している．どちらの方法も，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，ケーススタディや実験により定量的評価がなされており，信頼性が高い．これらの研究成果は，ソフトウェアセキュリティの分野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．