論文審査の要旨および学識確認結果

報告番号	甲　第　　号	氏　名	糟谷 正樹

論文審査担当者：				
	主査	慶應義塾大学准教授	博士(理学)	河野 健二
	副査	慶應義塾大学教授	博士(工学)	重野 寛
		慶應義塾大学准教授	博士(工学)	高田 眞吾
		慶應義塾大学准教授	博士(工学)	西 宏章

(論文審査の要旨)

学士 (工学), 修士 (工学) 糟谷正樹君提出の学位請求論文は,「マルウェアの特徴的振る舞いの誘発によるマルウェア対策手法に関する研究」と題し, 全 6 章から構成されている.

マルウェア対策はコンピュータセキュリティ上の重要な課題である. マルウェアは悪意あるソフトウェアの総称であり, マルウェアを利用した個人情報の流出や詐欺行為などの犯罪が増加している. マルウェア作成技術は向上し続けており, 洗練されたマルウェアに対処するためには, 同様に対策技術を向上する必要がある. しかし, 現在のマルウェア対策はステルス性が高いマルウェアに十分に対処できていない. ステルス性の高いマルウェアは 1) 頻繁な動作を避ける, 2) 害のない振る舞いを模倣することにより, 既存のマルウェア対策を回避する. 本論文では, マルウェアの特徴的な振る舞いを誘発するアプローチによりステルス性の高いマルウェアに対処する 2 つの手法を提案し, 現在においても猛威を振るっているアドウェア, スパイウェア及び偽アンチウイルスソフトに対して提案手法を適用している.

第 1 章は本論文の序論である. 本研究の背景, 目的, 及び論文の構成について述べている.

第 2 章の関連研究では, 既存のマルウェア対策手法について述べている. 本論文では既存のマルウェア対策手法をシグネチャマッチング, 静的解析を利用する方法, 動的解析を利用する方法の 3 つに分類して, 各手法が対処できる有効範囲を明らかにするとともに, それぞれ単体ではステルス性の高いマルウェアに対処できないことに言及している.

第 3 章は本論文の核となる考え方である, マルウェアの特徴的な振る舞いを誘発するアプローチについて述べている. ステルス性の高いマルウェアに対処するために, 本アプローチはマルウェアが実行せざるを得ない作為的な環境を用意して意図的にマルウェアの振る舞いを誘発している.

第 4 章はアドウェア, スパイウェアの解析を行うシステムである Blayzard を提案している. 頻繁な動作を避けるステルス性の高いアドウェア, スパイウェアの解析を行うために Blayzard は特徴的な振る舞いを誘発させる大量のイベントを注入している. 実験の結果, Blayzard は実在する 32 個のアドウェアとスパイウェアの振る舞いを正しく解析している. また, 大量のイベントを注入することによりステルス性の高い振る舞いを活性化させることができている.

第 5 章は偽アンチウイルスソフトを判別する方法を提案している. 偽アンチウイルスソフトは正規のアンチウイルスソフトの振る舞いを模倣するステルス性の高いマルウェアであり, 偽アンチウイルスソフトはマルウェアの検出を行わない. 本論文はこの点に着目して, マルウェアのあり, なしにより得られる振る舞いの違いを比較することにより正規のアンチウイルスソフトと偽アンチウイルスソフトの判別を行う. 本論文では, 検査対象のアンチウイルスソフトをマルウェアのあり, なしの環境で動作させ, 両環境から得られるメモリ使用量に違いが出るかどうかを統計的に判別することにより, 正規のアンチウイルスソフトか偽アンチウイルスソフトかの判別を行っている. 実験では, 提案手法により実在する 39 個の偽アンチウイルスソフトを偽物と判別し, 8 個の正規のアンチウイルスソフトを本物として判別している.

第 6 章は本論文の結論であり, 論文を総括すると共に今後の展望について述べている.

以上, 本論文は, マルウェアの特徴的な振る舞いを誘発するアプローチにより, 実在するステルス性の高いマルウェアに対処できることを示しており, その貢献は工学上寄与することが少なくない. よって, 本論文の著者は博士(工学)の学位を受ける資格があるものと認める.

学識確認結果	学位請求論文を中心にして関連学術について上記審査会委員で試問を行い, 当該学術に関し広く深い学識を有することを確認した. また, 語学（英語）についても十分な学力を有することを確認した.