博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　マルウェアの自動解析システムと視覚化に関する研究
申請者　：　堀合啓一
審査委員会　：　主査　教授　田中英彦
副査　教授　辻井重男
副査　教授　板倉征男
副査　教授　内田勝也
副査　教授　佐藤直

Ⅰ．論文内容の要旨

本論文は、「マルウエアの自動解析システムと視覚化に関する研究」と題し、7 章と付録などからなる。近年、情報ネットワークで流通するマルウエアは多くの種類が出現し、それに用いられている技術も多様化しており、その対策は単純でない。この研究は、そのような環境の変化に鑑み、定点観測によってマルウエアを捕獲して、その状況を組織の管理者が利用しやすい形で表示するとともに、市販のマルウエア対策製品では検出が困難なものについてもその挙動を自動的に解析し、管理者が必要とする情報を抽出することで、マルウエアによる被害の局限と対策の効率化に寄与することのできるシステムについて考察したものである。

第1章は「序論」で、本研究の背景と目的、及び論文の構成についてまとめたものである。

第 2 章は「マルウエア自動解析システムの現状」で、マルウエアの自動解析システムを実現する上で必要となる、マルウエア検体の収集手法、マルウエアの解析手法、マルウエアの自動分類手法について、世の中の現状をまとめ、それらの機能とその問題点を分析している。その結果、解析手法については、近年のマルウエアが備える難読化、暗号化、ポリモーフィック機能などの耐解析機能によって、自動化が困難になっていること、分類手法として動的挙動に基づいた個別の分類研究はあるが、既存のマルウエアとの関係が不明で、管理者が使いにくいこと、収集手法については単なる観測に留まらずマルウエアそのものの挙動を解析し感染 PC 内部の挙動を把握することが必要で、また、解析環境が仮想マシンに留まらず実マシン上での挙動を解析できることも必要であると述べている。

第 3 章は「マルウエア自動解析システムの要件と全体構成」で、マルウエアの動的挙動を自動的に解析するために必要な要件を明らかにするとともに、その具体的な実現法について述べたものである。すなわち、自動解析に必要な要素として、マルウエア、実行 OS と応用の環境、マルウエア実行のネットワーク環境、挙動の観測・記録、記録の解析と特徴抽出、感染 PC を感染前へ復旧させる仕組み、システム全体の制御機構などを挙げ、それらの要件について詳しく述べるとともに、提案するシステムの全体構成を与えている。

第 4 章は「マルウエアの自動解析システム」で、マルウエアの挙動の解析環境の実装、挙動として取得するデータの種類、挙動の数値化と類似性の判定手法について述べている。解析環境として、ネットワーク環境には Liunx のカーネルパケットフィルタの機能を利用し、模擬サーバには、感染 PC、制御 PC、解析結果を閲覧する利用者 PC、更に、模擬 DNS、IRC、SMTP、HTTP などが実装されている。マルウエアを実行する感染 PC は、OS に Windows XP（SP0、SP2）や Windows 2000 を使っているが、仮想マシンを利用する場合と実マシンを利用する場合の双方を用意している。各マルウエアの解析には挙動観察に 90 秒、解析に 3 分程度、合計数分かけており、マルウエアを実行する前の状態と後の状態をログとして記録し、その差分をマルウエアの挙動を示す情報として抽出している。それには、レジストリ

の変化、関連ファイルの変化など7種類の情報があるが、更に、幾つかの既存対策製品によるスキャン結果を挙動を示す取得情報として収集している。次に、この情報を数値化し、各マルウエアの挙動を数値化したベクトル間のハミング距離を類似性の判定基準として用いる手法について述べ、幾つかの具体的なマルウエアについての解析例を示している。

第 5 章は「定点観測とマルウエアの収集」で、マルウエアの収集機能を持った定点観測システムの構成とその機能に付いて述べたものであり、離れた複数個のセンサーから集めたログを正規化して集約し、様々な表示形態を工夫して管理者が容易に状況把握できるようにしたものである。この章では、そのような定点観測システムの全体構成と使用例について述べ、視覚化の有効性を示すとともに、捕獲した約 8000 個のマルウエアの観測結果について分析をした結果を示している。

第 6 章は「実験と結果の考察」で、この手法の類似性判定に関する分類精度を、同種を同種と判定した割合と、異種を同種と判定した割合を両軸に取り、過去の幾つかの手法と提案手法とを ROC 曲線によって比較し、提案手法の優れていることを示している。また、マルウエアのファミリー名や亜種名までの分類一致率を求め、従来の手法より優れていることを示している。

第 7 章は「結論」である。

Ⅱ. 論文審査結果の要旨

これを要するに本論文は、巧妙化するマルウエアに対する対策を組織の管理者が容易に行えることを目的に、ハニーポットを利用した定点観測によってマルウエアを捕獲し、それを実行させて挙動解析を自動化するとともに、各マルウエアと名前の与えられた既存マルウエアとの類似性を明示することのできるシステムを提案し、その有効性を示したもので、情報学に貢献するところ少なくない。

よって、本論文は、博士（情報学）の学位請求論文として合格と認められる。

Ⅲ. 審査経過

本審査委員会は、2009 年 2 月 5 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。