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　：　セキュアなクライアント端末の構成法の提案
申請者　：　宮本久仁男
審査委員会　：　主査　教授　田中英彦
副査　教授　小柳和子
副査　教授　佐藤直
副査　教授　松尾和人
副査　客員准教授　辻秀典

Ⅰ．論文内容の要旨

本論文は、「セキュアクライアント端末の構成法の提案」と題し、8章からなる。近年、PC の紛失やウイルス感染などによる情報漏洩問題が深刻化しており、それを軽減するためにシンクライアントと呼ばれる端末が商用化されている。しかしながら、商用のシンクライアントは必ずしも万能ではなく、よく分析すると問題点も多い。特に、仮想マシンが広く用いられ始めた現在、それを用いた攻撃の脅威は端末も例外ではない。この研究は、そのような状況に鑑み、シンクライアントに残存する脆弱性を分析し、それらに対策を施すことによりセキュアな端末を構成する手法を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、及び本論文成果の特徴についてまとめたものである。

第2章は「研究の背景」で、端末の紛失や盗難による情報漏洩対策としてどのような対策が用いられているかを述べ、また、典型的な端末構成からその漏洩原因を分析し、現状技術として、セキュア OS、検疫システム、シンクライアントを挙げている。更に、シンクライアント技術をより詳細に取り上げ分析することにより、残存するオフラインの脅威として、物理媒体を経由した漏洩、端末そのものの紛失略取、意図しない仮想マシン構成による端末ソフトウエアの起動および利用、の3種があり、またオンラインの残存脅威として、通信内容の解析、中間者攻撃による通信内容改ざん/なりすまし、マルウエアの感染、ネットワークを経由した第三者の侵入・乗っ取りの 4 種を挙げている。

第3章は「セキュアクライアント端末の構成」で、セキュア端末が備えるべき基本要件を、ベースとなる端末機能の保有と残存する脅威への対応の二つに分類し、後者への対応方針を5つにまとめている。すなわち、端末そのものの紛失/略取、通信内容の解析・改ざん・なりすまし、意図しない仮想マシン構成による端末ソフトウエアの起動および利用、マルウエアの感染、及び、ネットワークを経由した第三者の侵入乗っ取りである。更に、この章では、それらの方針を実現するための端末構成を考察している。すなわち、仮想マシンモニタの上に二つの仮想マシンを置き、それぞれに表示機能と、サーバとの交信を担当する端末機能を割り当て、後者の仮想マシンのユーザ層に TCP/IP スタックを配置し、前者の仮想マシンのコアからはそのプロトコルスタックを除いた構成である。

第4章は「セキュアクライアント端末を構成するために必要となる技術要素」で、上記構成を実現するための要素技術について述べている。まず、端末の機能を上述の二つに分けたことの妥当性を示し、次いで通常のシンクライアントでは残されているが、端末としては余分な機能を除去する方法を検討し、カーネル機能、その上位層機能、更にネットワークの機能に分けて、何を残し何を除くかを詳細に考察している。更に、分割した構成が正しい VM モニタの上で動いていることを保証するための VM 検知手法を技術要素として挙げ、端末を安全に起動するために、それを使うことを提案している。

第５章は「端末に適用されるVM検出技術」で、４章で述べたVM検出技術の詳細を議論している。まず、VM検出をユーザレベルで行う手法として一般化し、VM の上でプログラムを動かすときと、実マシンの上で動かす場合の差異を考察し、後者の経過時間は通常一定であるが、前者は大きくばらつくことを測定データによって具体的に示し、その差を利用した検出方式を与えている。それは、TSC 命令を2回発行し、それぞれの測定値の差異を用いるもので、その値が変化するか否かを複数回に分けてチェックする。論文では、この手法が割り込みによって誤る可能性があり、その誤り確率を任意の設定値よりも少なくするための方式設計を行うとともに、更にこの誤検知を減らすための測定法などの詳細をも与えている。

第６章は「VM 検出技術のブートプロセスへの適用」で、５章で提案した方式を端末の起動時に適用して、安全なシステム起動を行うための手法の詳細と実装を述べたものである。

第７章は「セキュアクライアント端末構成のための技術適用とその結果」で、前章までに提案してきた端末構成の実装について述べたものである。ベースとなるOSを Debian Gnu/Linux とし、仮想マシンモニタ Xen3.2、リモートデスクトッププロトコルによる通信プログラム rdesktop、表示機能 VNC Viewer、ブートローダ GNU Grub どからなる実装について詳細に述べるとともに、その実装結果を吟味して、３章で抽出した脅威が十分除かれていることを示している。

第８章は「結論と課題」であり、結論として、画面転送型クライアント端末に対しては十分脅威を除去することができたが、ネットワークブート型シンクライアントに対する詳細な検討は今後の課題であり、また、サーバ側の対策と、実際に端末を使うユーザの認証方式が課題として残されていると結んでいる。

Ⅱ. 論文審査結果の要旨

これを要するに本論文は、企業活動の大きな問題である情報漏洩を軽減させるシンクライアント方式の詳細な分析により未だ幾つかの脅威が残されていることを示し、今後増大する可能性の高いそれらの脅威を減らすための端末構成方式について提案・実装することで、具体的にそれが可能であることを示したもので、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、平成 22 年 3 月 3 日に論文内容について口述試問を行い、その後、平成 23 年 3 月 8 日これに関連する事項の最終試験審査を実施して、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。