学 位 論 文 の 要 旨

Advancing Intrusion Detection and Prevention Systems through the Use of Computer Virtualization
（計算機仮想化を用いた先進的な侵入検知及び防止システム）

氏 名　Ahmad Bazzi　印

The aim of this dissertation is to research the different approaches that help improve current security solutions, in particular Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Chapter 1 provides an introduction related to current security challenges. In particular, a security solution usually relies on a signature database. For example, an antivirus solution relies mainly on a virus signature database to detect viruses. An IDS relies heavily on a database of known attacks. The problem is how to detect previously unknown malicious code. Computer virtualization can contribute to solve this problem. In particular, virtualization makes it easy to create, copy and restore a virtual OS. Another feature is that virtualization makes it possible to monitor low-level activities on the BIOS level that would not be observable otherwise. This makes virtualization very useful to process both suspicious files and packets.

Chapter 2 discusses the main components of an IDS according to RFC 4766. Moreover, it presents IDS classifications according to two components, the data source and the analyzer. We also discuss the classification of wireless IDS, network behavior analysis based IDS and stateful protocol analysis based IDS.

Chapter 3 introduces our solution to detect malicious documents using a dynamic analysis system. We aimed to be able to detect malicious documents without the limitations of anti-virus solutions that require regular updates and usually cannot detect previously unseen malicious code. Therefore, we used virtualization along with Support Vector Machines (SVM), a machine learning classifier. The implemented solution opens the PDF file inside a PDF viewer in a virtual machine (VM) controlled

by a sandbox and then analyzes the sandbox report using SVM. We achieved a 99.49% prediction accuracy. We conclude that this solution is feasible and this approach can be used to detect other types of malicious documents as well.

Chapter 4 presents our solution to scan files exchanged between the different local computers. We implemented a basic IDS that captures network traffic to monitor the files being transferred to and from local systems. Unlike local anti-virus clients which are limited to one anti-virus vendor's engine, this file-level IDS can use multiple anti-virus engines and even more sophisticated automated anomaly detection systems that require large computing resources. This solution would help increase detection rate of malicious files accessed or sent by local systems.

Chapter 5 studies the feasibility of security virtual appliances from the performance point of view. One such example is a firewall setup in a VM. It can improve the security of its host, but it might suffer from virtualization performance overhead. We measured the bandwidth and latency and found the performance to be comparable to hardware counterparts. We concluded that this solution is feasible.

Chapter 6 proposes an IPS to protect against zero-day exploits. Zero-day exploits are attacks against servers using previously unknown software vulnerabilities; therefore, they are difficult to detect by relying on a signature database of known attacks. We propose creating a virtual server that mirrors the server that we want to protect. Each incoming packet would be delivered to the virtual server first, and only after ensuring that the virtual server is not compromised, it is to be delivered to the protected server. Testing the incoming packets can be achieved using Virtual Machine Introspection (VMI) for example. The proposed solution would provide protection against zero-day exploits.

Chapter 7 implements a prototype of our proposed solution to protect the privacy of smart device users. Smart device applications can leak various identifiers that can uniquely identify the user. Consequently, application vendors can track and compile data about user behavior. We propose using a modified gateway that can intercept packets containing such unique identifiers and remove any unique identifiers. We implemented a working prototype and obtained successful results with various applications. This solution can improve users' privacy without consuming the limited computing resources of the smart devices.

Chapter 8 summarizes our conclusion. In this research, we proposed and implemented solutions to help improve the security of both servers and computer systems. This research shows that computer virtualization can contribute to improving the security of systems. We showed that the performance of security virtual appliances is comparable to their hardware counterparts. By using a sandbox to open malicious documents in a VM and analyzing the sandbox reports, we showed that the detection accuracy is high. We also proposed that virtualization can be used to detect malicious packets. In brief, virtualization has a high potential to create or improve security solutions.

(和訳)

本研究の目的は、侵入検知システム(IDS)と侵入防止システム（IPS)において、現在のセキュリティ・ソリューションが抱える問題を改善するために、いくつかのアプローチについて研究することである。

第 1 章は、序論である。現在のセキュリティ・ソリューションが抱える問題について概説する。たとえば、IDS では、ウイルスを検出するために、主にウイルスに関するサイン・データベース（signature database）を用いる。このため既知のウイルスには対応できるが、今まで知られていなかった悪性ウイルスには無防備である。本研究では、コンピュータ仮想化を用いて、この問題を解決する。仮想化の以下の二点の特長について着目する。一つは、仮想 OS を構築して、コピーして、復活させることを簡単にする。もう一つの特長は、仮想化を用いなければ観察可能でない BIOS レベル上で低レベルの活動をモニターすることを可能にする。これらの特徴により、仮想化を用いると、疑わしいファイルやパケットを発見し、処理することができる。

第 2 章においては、IDS の 2 つの主要構成要素、つまりデータ・ソースとアナライザーについて述べる。これら 2 つの主要構成要素の構成法と内容によって IDS を、無線 IDS、ネットワーク振舞分析 IDS、ステートフル・プロトコル分析 IDS と分類し、概説する。

第 3 章「Detecting malicious documents using automated dynamic analysis」においては、サンドボックス（Sandbox）における挙動を専門家の手に解析をゆだねるのではなく、仮想計算機上でダイナミック解析を行いその解析結果を自動的に解釈し、マルウエアを検出する手法を提案する。具体的には、サンドボックスで PDF ビューアの中に PDF ファイルを解読して、サポート・ベクトル・マシン（Support Vector Machine ; SVM)を用いた機械学習によりマルウエアを分類する。その結果、99.49%の検出精度を得ている。この提案手法は、他のタイプの悪意のある文書検出にも有効である。

第 4 章「File-level IDS」では、ネットワーク・トラフィックを捕捉し計算機間で交換されるファイルを検査する IDS の基本構成を提案する。このファイル・レベル IDS では、大

規模な計算機資源を必要とする複数のアンチ・ウィルス・エンジン及び高度に自動化された例外発見システムを使用することができる。この提案手法により、悪意のあるファイルの発見率を上昇させることができる。

第 5 章「Feasibility study of security virtual appliances for personal computing」では、仮想化によるオーバーヘッドを評価するため、セキュリティ仮想機器の実現可能性を調査する。仮想化されたファイアウォールを用いた場合について、さまざまの動作環境でデータ伝送速度および処理時間を評価する。その結果、十分な伝送速度が確保できること及び利用者あたり十分な接続収容数が設定できることを示している。仮想化技法を用いたセキュリティ強化策は、現在市販されているハードウエア機器を用いても十分実現可能であることを確認している。

第 6 章「Preventing attacks in real-time through the use of a dummy server」では、ゼロデイ攻撃からサーバーを保護する IPS を提案する。ゼロデイ攻撃は、今まで知られていなかったソフトウェアの脆弱さを突いたサーバーへの攻撃である。したがって、既知の攻撃のサイン・データベースに頼ることは難しい。仮想化手法によりダミーサーバーを作成することを提案する。入力パケットは最初にダミーサーバーに届けられる。そして、ダミーサーバーが安全であることを確認した場合のみ、保護されたサーバーに届けられる。入力パケットの検査は、仮想マシン自己省察（Virtual Machine Introspection:VMI)を使う。

第 7 章「Privacy-aware gateway to prevent privacy leaks from smart devices」では、スマート端末のセキュリティ強化のために仮想機械を用いる手法を提案し、中間者攻撃（Man in the Middle Attack）を防ぐ手法について提案する。高性能なスマート端末は、利用者を特定できるいろいろな識別子を有しており、これらの貴重な情報の漏洩が懸念される。アプリケーション・ベンダーは、利用者の行動、嗜好等に関するデータを調査、編集することができる。本研究では、プライバシーに配慮したゲートウエイを作成し、そのようなユニークな識別子を含んでいるパケットの流出を防ぐことを提案する。プロトタイプを作成して、いろいろなアプリケーションを実行し、その有用性を確認している。

第 8 章においては、本研究で得られた結果をまとめるとともに残された問題、今後の研究の方向、応用の可能性等について述べる。本研究の結果を列挙する。サーバーとコンピュータシステムの安全性を改善するため、いくつかの解決策を提案し、実行する。コンピュータ仮想化がシステムの安全性改善に貢献できることを示す。セキュリティ仮想機器の性能がそれらの対応するハードウェア機器に相当することを示す。仮想計算機で悪意のある文書を解読するためにサンドボックスを使って、その結果を分析することによって、検出精度が高いことを示す。仮想化が悪意のあるパケットを検出するために有用であると提唱する。手短に言えば、仮想化には、セキュリティ・ソリューションを作成し改善する高い可能性がある。つまり、仮想化技法を用いると複雑な情報システムにおいてもセキュリティ強化が可能である。