（様式１１）

博士学位論文審査結果要旨

平成２８年8月２５日

研究科、専攻名　バイオ・情報メディア研究科　コンピュータサイエンス専攻

学位申請者氏名　Noor Afiza Binti Mat Razali

論文題目　Remote Detection Method of Operating Environment in Cyber Security Attack and its Countermeasure

和文題目　サイバーセキュリティ攻撃における動作環境の遠隔検出法とその対抗策

審査結果の要旨

研究の背景として、インターネットの普及によりネットワークを介したディジタル通信においてネットワークセキュリティの問題が発生している。インターネットの利用者は今や絶えずサイバー攻撃の脅威にさらされているといって過言でなく、この脅威に対する対策が急務である。本研究は、サイバー攻撃の攻撃者が自分をより有利な形で攻撃を行うために、攻撃に先立って攻撃対象システムの動作環境を予め遠隔で突き止めておこうとする行動に対して、被攻撃側がそのような攻撃があることを察知して対抗策（攻撃側に対して自分の動作環境を偽装する）講ずる手段を提供することに関する。

このようなサイバー攻撃を仕掛けるに当たって、攻撃者は攻撃対象システムが仮想計算機（以下、Virtual Machine (VM)）環境下で動作していることを嫌う傾向がある。それは被攻撃側がVM 環境で動作していると仮想ハニーポットを仕掛けられて攻撃側の素性を暴かれたり、VM モニタの監視機能によって攻撃を妨害されたりするためである。このため攻撃側は攻撃に先立ち攻撃対象システムの動作環境が実マシンか VM かを遠隔から検知しようと試みる。その検知する手段の一つが、通信パケットに付加されるタイムスタンプ値の分布の特徴を調べる方法である。これは、攻撃側が攻撃に先立って攻撃対象システムに大量のタイムスタンプ要求を送り付け、帰ってきたタイムスタンプ値の分布の特徴を調べることにより、攻撃対象システムの動作環境が実マシン環境か VM 環境かを識別する方法である。VM 環境で動作していると VM モニタのオーバヘッドや他 VM との競合などにより実行の遅れが発生し、タイムスタンプ値の分布に実マシンとは異なる特徴が現れる。これを分析することにより、攻撃対象が実マシン環境か VM 環境かを識別することが可能となる。本研究は、この実マシン環境と VM 環境でのタイムスタンプ値の分布の特徴の違いを分析し、さらにその差異を殆どなくして区別をつかなくすることにより、実際は実マシン環境でありながら VM 環境であると偽装する手段を提案した。

タイムスタンプ値の分布の特徴の違いにより攻撃対象システムの動作環境を識別する方法に関する先行研究では、タイムスタンプを 2 種類要求し（IP タイムスタンプと ICMP タイムスタンプ）、その 2 種類のタイムスタンプ値の差異（同じパケットに異なる値のタイムスタンプ値が返される）を分析する方法を提案している。パケットに格納されるタイムスタンプ値の精度はミリ秒であるが、この先行研究の方法では被攻撃側のマシンの性能が向上してタイムスタンプ値の差異がミリ秒より細かくなると、同一のパケット内の 2 種類のタイムスタンプ値に差異が発生しなくなって、この方法は有効でなくなるという問題があった。

そこで本研究では 1 種類のタイムスタンプ（主に ICMP タイムスタンプ）を使い、被攻撃側のシステムの性能が上がっても無効とならない方法を提案した。この方法では、連続するタイムスタンプの値の間隔に注目する。CPU の性能が上がると同じミリ秒の間に複数のパケットが送出されるようになり、同じタイムスタンプ値を持った複数のパケットが連続して送られるようになる。そのような連続してタイムスタンプ値が同じパケットの個数の分布を分析することにより、被攻撃側が実マシンか VM 環境かを識別することができる。実マシンでは実行が速いため同じミリ秒の間により多くのパケットが送出されるため、連続して値が同じタイムスタンプを持つパケット数が多いところに分布が偏る（最頻値は 4 個程度）。一方、VM 環境では実行が遅いため同じタイムスタンプ値のパケット数は少ない方に偏る（最頻値は 2 個程度）。この違いによって実マシン環境か VM 環境かを識別できる。

第 2 の研究は、被攻撃側がこのタイムスタンプ値の分布を故意に変化させて、実際は実マシン環境で動いているにもかかわらず VM 環境で動いているように偽装する方法を提案した。タイムスタンプ要求付のパケットが大量に送り付けられたら、それはタイムスタンプを用いた実行環境を遠隔検出する攻撃を受けていると判断し、タイムスタンプ付きの応答パケットの送出間隔を故意に遅らせて VM 環境であると装う方法を提案した。実験により VM 環境でのタイムスタンプ値の分布の特徴は予想できるので、故意にその分布に近づけることにより VM 環境であると偽装できることを示した。

既述の 2 つの研究では、攻撃対象システムのオペレーティングシステム（OS）をサーバ等の標準的な OS である Linux で行ったが、第 3 の研究ではこれをスマートフォンやタブレット端末で急速に普及を伸ばしている Android OS で行った。Android OS をスマートフォンの実機とサーバ上に構築した VM のゲスト OS として組み込んで、タイムスタンプ値の分布の特徴を調べた。スマートフォンの性能はサーバの約 0.6 倍程度と遅いため、同一のタイムスタンプ値を持つパケットは全く発生せず、引き続くパケットのタイムスタンプ値は 1～5 ミリ秒の間隔があった。そこでこのタイムスタンプ値の間隔の分布を実マシンと VM 環境とで比較することで、スマートフォンの実マシン上で動作しているかサーバの VM 環境で動作しているか識別できることを確認した。

本研究をまとめると、攻撃対象システムの動作環境を遠隔で検出する方法として、1 種類のタイムスタンプ値の分布の特徴を分析して動作環境が実マシン環境か VM 環境かを検出できることを確認した。これを応用して、被攻撃側の応答パケットの送出を故意に遅らせることにより、タイムスタンプ値の分布の特徴を VM 環境での分布の特徴に似せて VM 環境であることを偽装する方法を提案した。さらに OS が Android OS の場合について、タイムスタンプ値の分布の特徴の違いを用いて動作環境がスマートフォンの実マシンかサーバの VM 環境のどちらであるかを検出できることを示した。これらの研究は、研究室の中ではあるがすべて実験によって確認されており信頼性は高く、実際のサーバ攻撃に対する防衛策として応用上も価値の高い研究であると評価できる。

また、学位審査公開発表会などにおける発表および応答も妥当なものであり、審査委員会は本論文の著者に対して博士（コンピュータサイエンス）の学位を授けるのに十分な能力と学識、語学力を有していることを認めるものである。

審査委員　主査

東京工科大学大学院　教授　　木下 俊之　　印