博士論文要旨

論文題名：
仮想化技術に基づいたマルウェア解析のための
システムコールトレース手法に関する研究

立命館大学大学院情報理工学研究科
情報理工学専攻博士課程後期課程

ふりがな おおつき ゆうと
氏 名　大月 勇人

コンピュータとネットワークの普及に伴い，マルウェアの脅威が問題となっている．その対策のためにはマルウェアの解析を行い，特徴を理解する必要がある．しかし，解析を妨害する機能を持つマルウェアの解析は困難である．マルウェアを実行してその挙動を観測する動的解析では，解析下にあることを検出するアンチデバッグ機能や他のプロセスへ感染する機能が解析時の課題となる．これらの機能を持つマルウェアの解析が可能な既存解析システムは，観測オーバヘッドが大きく短時間での解析が困難である．そこで，本論文では解析時の課題を解決し，かつ低オーバヘッドでの挙動観測を実現することを目的として，軽量な仮想計算機モニタをベースとするシステムコールトレーサ Alkanet と，システムコールの呼出し元識別手法 BTS トレースを提案する．

Alkanet は，仮想計算機モニタ BitVisor をベースとし，Windows XP 上で動作するマルウェアに対して透過的な挙動観測を可能とするシステムコールトレーサである．Alkanet は，典型的なアンチデバッグ手法の 94%に対して耐性があることを確認している．また，典型的なプロセス感染型マルウェアが感染時にスレッドを挿入することに着目し，マルウェアが作成したスレッドを追跡する機能も有しており，既存システムよりも多様なマルウェアを解析可能である．さらに，ベンチマーク評価により，Alkanet は実機の 78%の動作性能であり，既存システムと比べて十分な速度で挙動観測が可能であることを確認した．

BTS トレースは,被感染プロセス内に潜むマルウェアの挙動の識別精度を向上するための手法である．プロセス感染型マルウェアは，正規のプロセスのメモリ空間内に自身のコードを挿入し，そのプロセスに悪意ある挙動を実行させる．そこで，BTS トレースでは，マルウェアが感染したメモリ領域を識別し，その領域を起源とするシステムコールを識別する．BTS トレースは，プロセッサが持つ Branch Trace Store 機能により記録された分岐命令の情報に基づいて関数呼出し階層を取得する BTS トレース本体と,Windows が持つメモリ管理情報と発行されるシステムコールの情報から感染領域を識別する手法から成る．Alkanet に本手法を適用することで，正規プロセスに潜んで動作するマルウェアの挙動を正規プロセス本来の挙動と正確に識別可能であることを確認した．

なお，本研究の有効性は，既に x64 版 Windows 7 および 10 などでも検証済みである．

Abstract of Doctoral Thesis

Title：
Research on System Call Tracing for Malware Analysis based on Virtualization Technology

Doctoral Program in Advanced Information Science and Engineering
Graduate School of Information Science and Engineering
Ritsumeikan University

ふりがな おおつき ゆうと
氏 名 OTSUKI Yuto

Malware has become a major security threat on computers. Understanding malware characteristics by malware analysis is required for taking measures against the threat. However, it is difficult to analyze malware that has the functions to disturb the analysis. Recent malwares have anti-debugging functions or infect other running processes. These functions are issues in dynamic analysis which executes malware and observes its behavior. Existing systems that have the ability to analyze such malware have suffered from large observation overhead. Therefore, to observe malware behavior without the influence from the disturbing functions and large overhead, "Alkanet" and "BTStrace" are proposed in this paper. Alkanet is a system call tracer based on the lightweight virtual machine monitor BitVisor. Alkanet can transparently observe malware running on Windows XP. 94% of typical anti-debugging techniques are ineffective against Alkanet. Alkanet observes malicious behavior focusing on thread because typical process-infecting malware injects threads into the target process. Alkanet can analyze more various malware than conventional systems. A benchmark evaluation shows that Alkanet has 78% performance of the physical machine. This result indicates that Alkanet runs faster than other analysis systems.

BTStrace makes it possible to distinguish behavior of malware hiding in the benign processes more accurately. Process-infecting malware hides their malicious codes in the memory space of other processes. Even if a running process is benign, the executed codes may be malicious. BTStrace finds malicious regions in the memory space and detects system calls originating in the regions. The proposed method consists of two functions. The first one extracts a call hierarchy from branch records which are stored by processor's Branch Trace Store. The other finds malicious regions based on Windows's memory management data and information of invoked system calls. Alkanet extended with BTStrace could distinguish system calls originating in malicious regions from other system calls by evaluation experiments.

Furthermore, it has been already confirmed that the proposed methods are adaptable for Windows 7 x64 and Windows 10 x64.