「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」
平成 20 年度採択研究代表者

平成 20 年度
実績報告

河野　健二

慶應義塾大学　理工学部　准教授

耐攻撃性を強化した高度にセキュアな OS の創出

1. 研究実施の概要

仮想化テクノロジー，セキュリティチップなどの最新の技術動向を踏まえ，OS カーネルそのものの健全性を担保するための要素技術の開発および統合を行う．仮想マシンモニタは OS 層とは明確なハードウェア・インターフェースで分離されており，OS の動作をいわば外部から観察することができる．たとえば，OS カーネルの持つ重要なデータ構造の完全性を検証したり，ユーザランドで観測される OS の振る舞いと，仮想マシンモニタ層で観測される OS の振る振る舞いとを突き合わせて動作異常を検出することができる．

本年度は主に次の 4 点について研究を行った．ひとつは，ゲスト OS がマルウェアに感染しているかどうかを仮想マシンモニタ層から検査する技術である．特にキーロガーと呼ばれるスパイウェアの一種や,隠れファイルの存在を検出する機構について研究を行った．もうひとつは，OS カーネルの健全性を回復するための基礎技術についての研究である．本年度は再起動による OS カーネルの健全性回復を高速化する手法に焦点をあて，バッファキャッシュの扱いを工夫することで再起動の高速化を行った．三つ目の研究は，ゲスト OS の安全性を担保するために仮想マシンモニタが備えているべき機能に関する研究である．本年度は新たなセキュリティ機構を導入した際に CPU 時間の課金情報を正確に扱えるようにする VM スケジューリングの手法について研究を行った．四つ目の研究はマルウェアの解析を支援するツールの研究である．本年度はマルウェアの解析を支援するコードエミュレータの開発を行い，難読化や暗号化の施されたシェルコード（リモート攻撃の端緒となる攻撃コード）の振る舞いを分析できるようになった．

本年度は研究初年度であり，その期間も半年と短かったため上記の研究の多くは現在進行中の状況である．来年度以降も引き続きこれらの研究を継続していく方針である．

2. 研究実施内容（文中にある参照番号は 4.(1)に対応する）

仮想マシンモニタのレイヤからマルウェアを検知する手法として次のふたつのタイプのマルウェアに焦点をおいて研究を行った．ひとつはキーロガーと呼ばれるスパイウェア

の一種であり，ユーザの入力したキーストロークを記録しパスワードやクレジットカード番号などを盗み出すことを目的としたマルウェアである．もうひとつはルートキットといわれるマルウェアのうち，ウィルス等に感染したファイルを隠蔽するタイプのものを対象として研究を行った．

通常，キーロガーはキー入力があるとそのキー入力を横取りし，ハードディスク等に入力されたキーの内容を記録する．人間のキー入力の速度はコンピュータの処理速度に比べて著しく低速である上，キーロガーそのものの動作は比較的単純であり，必要とされる計算リソースも極めて少ない．その結果，キーロガーの動作は極めてステルス性が高く，観測可能な副作用はほとんど引き起こさない．本研究では仮想マシンモニタのレイヤで，人間では不可能なほどの高速なキー入力をねつ造し，キーロガーの動作そのものを増幅する．大量のキー入力を受けたキーロガーはそれらの入力を記録するため大量のディスク I/O を行う．キー入力のねつ造とディスク I/O の増加の間に統計的に有意な相関がみられれば，高い確率でキーロガーに感染しているといってよい．実際のキーロガーでは定期的にキー入力を収集するタイプのものも多いため，さらにタイマ割り込みをねつ造することによってゲスト OS 内の時間の流れも高速化し，そうしたタイプのキーロガーでも検知できるように工夫を行った．実際に 56 種類のキーロガーの検体を収集し，これらのキーロガーに対して提案手法が有効に機能するかどうかを検査した結果，すべてのキーロガーを正しく検出することができた．キーロガーを検出する従来手法の多くは既知の検体しか検出できなかったり，あるいは難読化や暗号化の行われた検体に対しては無力であった．提案手法はキーロガーの実現方法に依存しないため，こうした制限はない．

ファイルの存在を隠蔽するルートキットを検出する手法の研究開発も行った．こうしたルートキットの多くは OS カーネル内に常駐し，システムコールの返値を改ざんすることでファイルの存在を隠蔽する．たとえば，ディレクトリ内に存在するファイルの一覧を得るシステムコールの返値から，隠蔽したいファイルについての情報を取り除くことでファイルの存在を隠蔽する．本研究では，ゲスト OS による直接のディスク I/O を禁止し，すべてネットワークファイルシステムを介してディスク I/O を行うようにする．仮想マシンモニタを利用しているため，ファイルサーバのために別のマシンを用意する必要はなく，同一マシン上の別の仮想マシンにファイルサーバを置けばよい．このような環境にすることで，仮想マシンモニタのレイヤでファイルサーバとの通信をすべて横取りし，ルートキットによる改ざんのない状態でのファイルシステムの情報を入手する．さらに，システムコールの返値を横取りして両者を比較することで隠れファイルの存在を検出する．この手法を用いて数種類のルートキットに対して有効性の確認を行ったところ，すべてのルートキットを適切に検出することができた．キーロガーの検知手法と同様に，提案の手法はルートキットの実現方法に依存しない汎用性の高い手法となっている点に特徴がある．

次に，不正攻撃による障害の発生した仮想マシンを迅速に回復させる手法についての基礎的研究を行った．感染や攻撃の痕跡を残さないようにするため，ハードディスク等の 2 次記憶装置に感染することを避け，メモリ上にのみ感染するタイプのマルウェアが存在する．こうしたマルウェアの場合，たとえば上記のルートキット検出手法を利用しても検出は不可能である．こうしたタイプのマルウェアに感染した場合，仮想マシンを再起動する

という手法が簡便であるにもかかわらず，極めて有効な手段であることが知られている．しかし，仮想マシンの再起動は OS やアプリケーションの再起動を伴うため，長期間のダウンタイムが必要となり，提供しているサービスによっては頻繁に再起動を行うことができない．こうした実運用上の障壁を取り除くため，再起動の高速化は有効なアプローチのひとつである．本年度はバッファキャッシュの扱いを工夫することによって，再起動に伴うダウンタイムの低下を回避する手法の実現を行った．通常，仮想マシンを再起動すれば OS が保持していたバッファキャッシュも初期化されるため，再起動後には大量のディスク I/O が発生し，ダウンタイムが長期化する一因となっている．本研究では再起動前の状態にバッファキャッシュを戻してやることで，ディスク I/O の多発を回避している．この手法はデータセンターなどのサーバ集約環境で有益だと考えている．

本研究プロジェクトでは，さまざまなセキュリティ機構を組込み可能な仮想マシンモニタを提供することを目的の一つとしている．サービス拒否攻撃による被害を避けるためには，仮想マシンモニタ自身が正確なリソースアカウンティングが行えるようになっている必要がある．本年度は CPU 時間に限定してより正確なリソースアカウンティングのための基礎的研究を行った．来年度以降，より詳細なアカウンティングのための諸技術の確立を目指す．

最後に，マルウェアの解析に必要なツールの開発も行った．現在のマルウェアは難読化，暗号化などがなされており人手での解析が難しい．さらにデバッガがアタッチされると動作を停止するなど，既存の解析技術が適用しにくいようになっている場合が多い．本研究では，リモート攻撃の端緒となるシェルコードに焦点をあて，ネットワークパケット中に含まれるシェルコードを擬似実行することで，シェルコードの振る舞い解析を行うツールの開発を行った．

3. 研究実施体制

(1)「河野」グループ

①研究分担グループ長：河野　健二（慶應義塾大学、准教授）

②研究項目

マルウェアの検知機構，不正攻撃からの回復機能，マルウェア解析技術．

(2)「光来」グループ

①研究分担グループ長：光来　健一（九州工業大学、准教授）

②研究項目

不正攻撃からの回復機能，サービス拒否攻撃対策としてのリソースアカウンティング

4. 研究成果の発表等

（1）論文発表（原著論文）

1. Makoto Shimamura, Kenji Kono: "Yataglass: Network-level Code Emulation for Analyzing

Memory-scanning Attacks", Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), July, 2009, To appear.

2. Yoshida Tetsuya, Hiroshi Yamada, Kenji Kono: "Using a Virtual Machine Monitor to Slow Down CPU Speed for Embedded Time-Sensitive Software Testing" IPSJ Transactions on Advanced Computing Systems, 2009, To appear.
3. Miyuki Hanaoka, Kenji Kono, Toshio Hirotsu: "Performance Improvement by means of Collaboration between Network Intrusion Detection Systems" Communication Networks and Services Research Conference (CNSR), May, 2009, To appear.

（2）特許出願

平成 20 年度 国内特許出願件数：0 件（CREST 研究期間累積件数：0 件）