「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

H24 年度
実績報告

河野健二

慶應義塾大学理工学部情報工学科・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. 研究実施体制

(1)「河野」グループ
① 研究代表者:河野 健二(慶應義塾大学理工学部情報工学科、准教授)
② 研究項目
・マルウェアの検知機構、障害の予兆検知

(2)「光来」グループ
① 主たる共同研究者:光来 健一 (九州工業大学大学院情報工学研究院、准教授)
② 研究項目
・OS の健全性回復機構、セキュリティアーキテクチャ

(2)「山田」グループ
① 主たる共同研究者: 山田 浩史(東京農工大学大学院工学研究院、准教授)
② 研究項目
・OS の健全性回復機構

§2. 研究実施内容

(文中に番号がある場合は(3－1)に対応する)

仮想化テクノロジー，セキュリティチップなど最新の技術動向を踏まえ,オペレーティングシステム(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研究開発および統合を行う．本プロジェクトでは，仮想化テクノロジーに軸足を置きつつ，OS のセキュリティ向上を目指した研究を推進している．仮想マシンモニタは OS 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 の動作を外部から観察することができる．こうした特徴を最大限に生かした基盤技術を研究開発することで，本プロジェクトで推し進めているオープンシステムディペンダイビリティ向上への貢献を狙う．

本年度は昨年度に引き続き，大きく 4 点の研究を推進した．また最終年度を見据え，成果の取りまとめ作業も開始した．一つ目は，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の層から検査する技術である．本プロジェクト内の D-RE 上における D-Visor および D-System Monitor を利用して実現する．本プロジェクトで研究しているマルウェア検知システムには，従来の個々の検体に対して対策を取る方式とは異なり，マルウェアのクラス(たとえばキーロガー，ボットという単位)で対策を取ればよいという特徴がある．本年度は，振る舞い監視というアイディアを拡張し，D-Visor や D-System Monitor だけでなく，他の D-RE のコンポーネントに対しても適応可能であるかを検討した．具体的には，OS カーネルに寄生するマルウェアではなく，ウェブブラウザに寄生するマルウェアを対象にその可能性を検討した．検討にさきだち，実際のウェブブラウザ寄生型マルウェアの振る舞いを解析するための機構を研究開発した．解析機構は，ウェブブラウザのプラグインの発行するシステムコールの監視や，イベントの挿入，コールバックのエミュレートを行い,詳細にマルウェアの活動を記録する．検知方式を確立するべく，実際のウェブブラウザ寄生型マルウェアの検体の振る舞いの調査を行った．加えて，これまで開発してきたキーロガー検知機構，およびメタデータ改竄型マルウェア検知機構については既に DEOS センターに納品済みであり，ドキュメントの整備を開始した．

二つ目は OS の健全性を高速に回復する機構である．本手法も仮想化技術を活用しており，D-Visor 上に組み込んでの実現を考えている．本年度は，OS カーネルのアップデートに伴うサービス中断を緩和する手法について研究を行った．通常，OS カーネルにパッチを適用すると，OS の再起動が求められ，その上で動作しているアプリケーションすべてを再起動しなければならない．本手法では，パッチ適用後，稼働している OS と同じ状態の仮想マシンを作りだし，そちらで再起動を行う．再起動後，スナップショットを取得し，稼働している． 今年度度はプロトタイプ実装を完了させ，実ワークロードを用いた密な実験を行った．5 種類の Linux distribution を用いた実験を通して，いずれの Linux に対しても提案方式は適用可能であり，91%～98%のダウンタイム削減に成功した．こちらのプロトタイプについても，ソースコードの整備やドキュメント化を推進した．

三つ目はセキュリティアーキテクチャに関する研究である．セキュリティソフトウェアを別の仮想マシンで動作させ，対象となる仮想マシンの挙動を監視するというアーキテクチャ(D-Visor と

D-System Monitor のアーキテクチャそのもの)について様々な角度から研究を行っている. 本年度は, D-System Monitor 自身のセキュリティ強化に取り組んだ. D-System Monitor が攻撃者に侵入されると, 監視対象の VM の情報が容易に漏洩してしまう. D-System Monitor への侵入を完全に阻止するのは現実的には難しいため、D-System Monitor に侵入されたとしても情報の漏洩を防げるようにする仕組みを仮想マシンモニタの D-Visor に実装する. 昨年度までに, 監視対象の VM のメモリをすべて暗号化する機構を実現した. 本年度は, D-System Monitor に必要最小限のメモリ内容のみをみせることで, 監視を実現しつつ, 情報漏洩を守る機構を実現した. 他にも, D-System Monitor に侵入されるリスクを減らす試みも行った. 従来, 管理 VM と呼ばれる VM が D-System Monitor の役割を担っており, 管理のための様々なサービスが動作しており, それらが攻撃対象となる危険があった. そこで,管理 VM とは別に D-System Monitor 用に専用の仮想マシンを用意し,対象の仮想マシンの監視を行えるようにした.

四つ目は障害の予兆を検知する手法についての研究である. これは, D-RE 内の D-Application Monitor への貢献を狙った研究である. パフォーマンス異常などの障害を対象に, 障害が顕在化する前段階の予兆を検知することを目指している. これまでに, サーバの応答時間を管理図という統計的手法を用いて処理することで, いくつかの障害予兆が検知できることがわかった. 本年度は, 障害の原因特定の手間を軽減する方法を研究した. これまでの研究において, プログラムが生成するログ内容と起きる障害とに相関があるという感触がある. そこで, ログを用いることで性能異常検知手法についての検討を行った. 基本的なアイディアは, ログの出現パターンと障害とを結びつけ, 過去に起きたことのある障害であれば, 以前利用した改善処置を施すというものである. まずは, Apache ウェブサーバを用いて, 性能異常を意図的に挿入し, ログの出現パターンを観察した. 起きた障害毎に出現パターンが異なっているという結果を得て, ログの出現パターンの類似性を検出する方法も検討した. 具体的には, 誤差逆伝播法を用いてニューラルネットワークで学習させることで, 類似性を検出することができた. 今年度は, 実際のサービスを模したベンチマークソフトを利用して, 方法の有効性を検証していく.

また, これらの研究活動と並行して, 本プロジェクトの活動をまとめたパンフレットの執筆を行った. 本パンプレットは Embedded Technology 2012 にて配布を行った. 他にも, 同イベントにてデモ発表を行った.

§3. 成果発表等

(3－1) 原著論文発表

・論文詳細情報

1. Hidekazu Tadokoro, Kenichi Kourai, and Shigeru Chiba: Preventing Information Leakage from Virtual Machines' Memory in IaaS Clouds, IPSJ Trans. on Advanced Computing Systems, Vol.5, No.4, pp.101-111, 2012.
2. Tomohisa Egawa, Naoki Nishimura, and Kenichi Kourai: Security Enhancement of Out-of-band Remote Management in IaaS Clouds, IPSJ Trans. on Advanced Computing Systems, to be published.
3. Takeshi Yoshimura, Hiroshi Yamada, and Kenji Kono:Using Fault Injection to Analyze the Scope of Error Propagation in Linux, In IPSJ Trans. on Advanced Computing Systems, to be publicshed.
4. Yusuke Takamatsu, Yuji Kosuga, and Kenji Kono: Automatically Checking for Session Management Vulnerabilities in Web Applications, In IPSJ Trans. on Advanced Computing Systems, to be published.
5. Hiroki Shirayanagi, Hiroshi Yamada, and Kenji Kono: Honeyguide: A VM Migration-aware Network Topology for Saving Energy Consumption in Data Center Networks, In Proc. of the 17th IEEE Symposium on Computers and Communication (ISCC'12), pp.460-467, 2012.
6. Kenichi Kourai, Takeshi Azumi, and Shigeru Chiba: A Self-protection Mechanism against Stepping-stone Attacks for IaaS Clouds, In Proc. of the 9th IEEE International Conference on Autonomic and Trusted Computing (ATC 2012), pp.539-546, 2012.
7. Takeshi Yoshimura, Hiroshi Yamada, Kenji Kono: Is Linux Kernel Oops Useful or Not? In Proc. of the 8th Workshop on Hot Topics in System Dependability (HotDep '12), 6 pages, 2012.
8. Kenichi Kourai and Takuya Nagata: A Secure Framework for Monitoring Operating Systems Using SPEs in Cell/B.E., In Proc. of the 18th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2012), pp.41-50, 2012.
9. Yusuke Takamatsu, Yuji Kosuga and Kono Kenji: Automated Detection of Session Management Vulnerabilities in Web Applications, In Proc. of Tenth Annual Conference on Privacy, Security and Trust (PST2012), pp.112-119, 2012.
10. Tomohisa Egawa, Naoki Nishimura, and Kenichi Kourai: Dependable and

Secure Remote Management in IaaS Clouds, In Proc. of the 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2012), pp.411-418, 2012.

11. Takeshi Yoshimura, Hiroshi Yamada, and Kenji Kono:Using Fault Injection to Analyze the Scope of Error Propagation in Linux, 第 24 回コンピュータシステムシンポジウム, 2012.
12. Hiroshi Yamada, Kenji Kono:Traveling Forward in Time to Newer Operating Systems using ShadowReboot,In Proc. of ACM Conference on Virtual Execution Enviroments (VEE '13), pp.121-130, 2013.

（3－2） 知財出願

① 平成 24 年度特許出願件数(国内 0 件)

② CREST 研究期間累積件数(国内 1 件)