「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

H23 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 主たる共同研究者: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, OS の健全性回復機構, 障害の予兆検出

(2)「光来」グループ
③ 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）
④ 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. 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.

本年度は主に次の 4 点について研究を行った. 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, メッセンジャーの通信プロトコルである IRC 通信を悪用するボットの検知手法について研究を行った. 本手法では, ユーザがメッセージを受信したときの応答時間, ならびに入力速度とボットの振る舞いとに着目する. ボットはプログラムであるために, IRC 通信を受信した際に人間より応答時間が極めて速く, またメッセージ送信量が著しく多い. この点に着目しながら, IRC 通信を常に監視することで, 該当マシンにボットが潜んでいるか否かを判定する. 閾値を用いた検知方法ながら, 実インターネット上から採取した 22 種類のボットすべてを検知することができた. また, 近年増加しているウェブブラウザ寄生型マルウェアの検知手法を確立するために, インターネット上から実際のウェブブラウザ寄生型マルウェアを採取した.

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 OS をそのスナップショットの状態にすることで, アップデートと同等の効果を得る. 設計に関しては今年度中に終えることができたので, 来年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い本方式の検証を行う.

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, 既存のセキュリティソフトウェアを修正することなく, 別の仮想マシンから対象の仮想マシ

ンを監視可能にする仕組みを研究開発した. 別の仮想マシンから対象の仮想マシンの実行環境を提供することにより, あたかもセキュリティソフトウェアが対象の仮想マシン上で動作しているような状況を作り出す. 他にも, 仮想マシンのマイグレーションを行っても, 監視を継続し続けられる仕組みについても研究開発を行った. これにより, 監視をしながらも, マイグレーションを用いた柔軟な資源管理が可能になる.

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. 管理図が警告を発した前後の応答時間の変化の類似性に着目することで, 同じ原因で警告を発しているリクエストをグルーピングする. こうすることで, 同じグループのリクエストを処理している共通のコンポーネントのみを調査すればよくなり, 障害の原因究明の負担をより軽くなる. 実システムを模したベンチマークである RUBiS を用いて実験したところ, 提案手法により, サーバのコネクション不足という異常の原因が不適切な KeepAliveTimeout 値であることを特定することができた.

また, これらの研究活動と並行して, 本年度は当該研究領域で作成したドキュメントであるプロジェクト白書, ならびに本(Chapter 6.4 Security Mechanism)の執筆を行った. また, 中島チームと集中的に議論を行い, 各チームが個別に研究開発していた機構の統合し, Embedded Technology 2011 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. Takahisa Kitagawa, Miyuki Hanaoka, and Kenji Kono: A state-aware Protocol Fuzzer based on Application-layer Protocols. In IEICE Trans. on Information and Systems, Vol. E94-D, No.5, pp.1008-1017, May 2011.
2. Miyuki Hanaoka, Kenji Kono, Toshio Hirotsu, and Hirotake Abe: Performance Improvement by Coordinating Configurations of Independently-managed NIDS, International Journal of Computer Science and Network Security, Vol.11, No.5, pp.1-11, May, 2011
3. Satoshi Iwata, Kenji Kono: Clustering Performance Anomalies in Web Applications Based on Root Causes, In Proc. of the 8th IEEE/ACM International Conference on Autonomic Computing (ICAC '11) (Short Paper),

IEEE/ACM, Jun 2011.
4. Kazuya Yamakita, Hiroshi Yamada, and Kenji Kono: Phase-based Reboot: Reusing Operating System Execution Phases for Cheap Reboot-based Recovery, In Proc. of the 41st Annual IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN '11), pp.169—180, Jun 2011.
5. Hiroshi Yamada and Kenji Kono: Traveling Forwards in Time to Newer Operating Systems using ShadowReboot, In Proc. of the 2nd ACM SIGOPS Asia-Pacific Workshop on Systems (APSys '11), July 2011.
6. Takeshi Yoshimura, Hiroshi Yamada, and Kenji Kono: Can Linux be Rejuvenated without Reboots?, In Proc. of the 3rd International Workshop on Software Aging and Rejuvenation (WoSAR '11)
7. Shuntaro Tonosaki, Hiroshi Yamada, and Kenji Kono: Efficiently Synchronizing Virtual Machines in Cloud Computing Environments, In Proc. of the 3rd IEEE International Conference on Cloud Computing Technology and Science (CloudCom '11),
8. Kenichi Kourai and Shigeru Chiba: Fast Software Rejuvenation of Virtual Machine Monitors, IEEE Transactions on Dependable and Secure Computing (TDSC), Vol.8, No.6, pp.839-851, November/December 2011.
9. Satoshi Iwata and Kenji Kono: Clustering Performance Anomalies Based on Similarity in Processing Time Changes. In IPSJ Trans. on Advanced Computing Systems, Vol. 5, No. 1, pp.1-12
10. 糟谷 正樹, 河野 健二: ブラウザのアドオンを利用したアドウェアのイベント注入による振る舞い解析, 情報処理学会論文誌, Vol. 52, No. 12, pp.3775-3785
11. 花岡 美幸, 河野 健二: ネットワーク侵入検知システムの協調による性能と耐障害性の向上, 情報処理学会論文誌: コンピュータシステム(ACS), Vol.5, No.1, pp.13-26.
12. Kazuya Yamakita, Hiroshi Yamada, and Kenji Kono: Lightweight Recovery from Kernel Failures using Phase-based Reboot, In IPSJ Trans. on Advanced Computing Systems, Vol. 5, No.2, pp.121 – 132

（3－2） 知財出願

① 平成 23 年度特許出願件数（国内 1 件）

② CREST 研究期間累積件数（国内 1 件）