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

H22 年度
実績報告

平成 20 年度採択研究代表者

河野 健二

慶應義塾大学理工学部情報工学科・准教授

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研究開発および統合を行う．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 の振る舞いとを付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の層から検査する技術である．昨年度までに蓄積したキーロガーやファイル改ざんを行うルートキットを検出する技術を応用し，今年度はボットの存在を検出する機構についての研究を推し進めた．もうひとつは，OS カーネルの健全性を回復するための基盤技術についての研究である．再起動によるカーネルや仮想マシンモニタの健全性回復を高速化する手法に焦点をあて，本年度は，OS 再起動の高速化の研究に取り組んだ．昨年度に作成したプロトタイプをチューニングすることで，再起動に伴うダウンタイムをさらに短縮することができた．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るべき機能に関する研究である．本年度は，セキュリティ機構を他の仮想マシンにオフロードする際に，既存のセキュリティ機構に変更を施すことなしで監視対象の仮想マシンの検査を可能にするための支援機構についての研究・開発を行った．4 つ目の研究はサービス運用時において，障害の予兆を検知する手法に関する研究を行った．リクエストの応答時間に着目し，管理図と呼ばれる統計的手法を用いることで迅速にパフォーマンス異常を検出する．実運用を模したベンチマークソフトウェアに適用したところ，障害予兆を検知し，障害解析の手助けとなることが判った．

これらの機構はシステム運用時に効果を発揮し，当該研究領域で検討をしているシステムアーキテクチャである DEOS アーキテクチャの中でも，D-Visor や D-System Monitor，D-Application Manager に貢献する． いずれの研究も現在進行中であり，来年度以降もこれらの研究は継続し，知見を蓄える予定である．

また，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サブコアチームドキュメントの執筆を行った．また，全体統合に向けて，特に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を開始した．

§2. 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(慶應義塾大学理工学部、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, 障害の予兆検出

(2)「光来」グループ(研究機関別)

①研究分担グループ長: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

・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

§3. 研究実施内容

(文中に番号がある場合は(4－1)に対応する)

本年度は，当該研究領域で検討しているシステムアーキテクチャ「DEOS アーキテクチャ」において，仮想マシンモニタ層であるD-VisorとD-System Monitor，およびアプリケーションの挙動を監視する D-Application Manager に関する技術の研究開発を行った．D-Visor・D-System Monitor の狙いは OS カーネルの正常な振る舞いを保証し，OS カーネルが提供するセキュリティ機構を正しく動作させることにある．D-Application Manager はアプリケーションを監視し，障害の予兆が現れたらいち早く警告し，迅速な障害対策を促す．いずれもシステムのディペンダビリティ向上のためには必須のコンポーネントである．

OS 自身のセキュリティを強化する手法として，本年度は仮想マシンモニタを利用してマルウェアを検知する手法に関する研究を行った．D-System Monitor の一部であり，本手法の特徴は個々のマルウェアの検体に対しての対策ではなく，マルウェアのクラス(キーロガー，ボットという単位)で対策を取れる点にある．これにより，従来に比べると，対策のために要する手間を減らすことができる．これは，DEOS アーキテクチャと並んで検討しているシステムのディペンダビリティ向上のためのライフサイクルである DEOS プロセスを回す頻度を従来に比べ大幅に減らすことを意味し，ディペンダビリティのさらなる向上に貢献する．

昨年度までに行った研究から，仮想マシンモニタのレイヤでキー入力といった様々なイベントをOS に挿入し，その振る舞いを観察することで，キーロガーやルートキットといったマルウェアを検知できることが判っている．本年度はボットに対してその適用能力を検証した．まず，インターネットから実際のボットを 22 体収集し，様々なイベントを挿入し，その挙動を詳細に観察した．ボットは犯罪組織等に用いられる本格的なマルウェアであり，その検体の収集，挙動の分析が非常に困難であり，継続的に研究を進めていく予定である．今年度の分析結果により，ボットはチャットのためのプロトコルを用いて通信することが多いため，キーボード割り込みを挿入することで，ボットの通信量を意図的に増やせることが判った．そのため，挿入したキーボード割り込みと発生した通信との相関を観察することで，OS 内のボットを検知可能であるというところまで解析が済んだ．また，昨年度までに研究開発を行ったキーロガー検知機構とファイルシステム改ざん型ルートキット検知機構については，本領域の中島チームにソースコードを渡し，同チームで研究開発している仮想マシンモニタとの統合作業を行っている．

次に，OS カーネルの健全性を高速に回復するための基盤技術の研究を行った．本機構は，D-System Monitor の一部である．本技術は，OS カーネルの健全性を定期的に高速回復することで，セキュリティ対策が講じられるまでの間も，サービスを提供しつづけられるようにする．サービスの可用性を高めることで，システム全体のディペンダイビリティ向上を計る．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不揮発性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．これら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を被り, サービスによっては頻繁に再起動することはできない.

本年度は, 仮想マシン再起動に伴うダウンタイムを削減する手法 FlashReboot の最適化を行い, さらなるダウンタイムの短縮化に取り組んだ. FlashReboot は仮想マシンのスナップショット機能を利用し, OS やサービスアプリケーションが起動した直後の状態のスナップショットを取得しておき, 再起動する際には, 不揮発装置の状態を考慮しながら, そのスナップショットを復元する. これまでは素朴にスナップショット機能を利用していたため, FlashReboot に要するダウンタイムの多くがスナップショットの復元に費やされていた. そこで, OS のメモリ情報を利用してスナップショットの復元に要する時間を短縮する最適化を施した. バッファキャッシュやフリーページといった soft state なメモリをスナップショットに加えることをやめ, 復元するメモリ量を大幅に減らす. このようにすることで, ダウンタイムの大幅な削減に成功した.

3 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るべき機能に関する研究である. D-Visor, D-System Monitor の一部であり, D-System Monitor 内で動作するセキュリティソフトウェアの稼働をサポートすることでディペンダビリティの向上を狙う. 本年度も昨年度に引き続き, セキュリティ機構のオフロードに関する研究を実施した. 別の仮想マシンでセキュリティ機構を動作させることで, もしサービスを提供している仮想マシンが攻撃で乗っ取られても, セキュリティ機構のログ等は別の仮想マシンに保存されているため, 攻撃の痕跡を安全に保存することができる. 従来, セキュリティ機構をオフロードすると, 監視したい仮想マシンの情報を別仮想マシンから取得する必要があるため, 既存のセキュリティ機構を大幅に変更する必要があった. この問題を解決するべく, 既存のセキュリティ機構に変更を加えることなくオフロードが可能な支援機構の研究・開発を行った. 具体的には, 監視対象の仮想マシンをスキャンし, ファイルシステムのネームスペースやプロセスリストを作り出す. 作成した監視対象の仮想マシンの情報に対して既存のセキュリティ機構を適用することで, 安全かつ従来通りの動作をすることができる. オフロードをする度にセキュリティ機構を大幅に変更するのは非現実的であるため, 既存のソフトウェアとの親和性を高めることで, システム全体のセキュリティを向上させることを狙った研究である.

また, インターネットサーバを対象に障害の予兆を検知する手法に関する研究を行った. 本手法は D-Application Manager によって利用されることを想定している. 障害の予兆を検知することで, 迅速に原因究明や障害対策のサイクルへと進むことができる. リクエストの応答時間のぶれに着目し, 管理図と呼ばれる統計的手法を用いることで, 細やかなパフォーマンス異常を検知する. 実システムを模したベンチマークに適用したところ, 昨年度に検出したデータベーススキーマの不具合のみならず, コネクション数の設定ミスによる異常や, 誤った SQL クエリの発行による異常等を検出することができた. 本手法による異常検出はかなりよい手応えであり, 今後も研究を継続する予定である.

本年度は, 研究活動と並行してプロジェクト白書, ならびにサブコアチームドキュメントの執筆も行った. プロジェクト白書については, 主として 5.4 セキュリティ, 5.5 仮想化技術とその応用の節

を記述した．また，サブコアチームドキュメントに関しては，VM サブコアチームとエビデンスサブコアチームのドキュメントを同領域チームの中島チームや倉光チームと執筆した．

§4. 成果発表等

（4－1） 原著論文発表

●論文詳細情報

1. Takahiro Kobayashi, Hiroshi Yamada and Kenji Kono: Quick Reboot-based Recovery for Commodity Operating Systems in Virtualized Server Consolidation, In Proc. of EuroSys 2010 Workshop on Isolation and Integration for Dependable Systems (IIDS'10), Apr 2010.
2. Satoshi Iwata, Kenji Kono: Narrowing Down Possible Causes of Performance Anomaly in Web Applications, In Proc. of the 8th European Dependable Computing Conference (EDCC '10) , Apr. 2010.
3. Kenichi Kourai: CacheMind: Fast Performance Recovery Using a Virtual Machine Monitor, DSN 2010 Workshop on Proactive Failure Avoidance, Recovery and Maintenance (PFARM), June 2010.
4. Takahisa Kitagawa, Miyuki Hanaoka, and Kenji Kono: AspFuzz: A State-aware Protocol Fuzzer based on Application-layer Protocols, In Proc. of 15th IEEE symposium on Computers and Communications (ISCC'10), June 2010.
5. 岩田 聡, 河野 健二: ウェブアプリケーションの性能異常兆候検出への管理図の適用, 情報処理学会論文誌:コンピューティングシステム, Vol 3, No 3, pp.221--234, Sep 2010.
6. 石川豊, 山田浩史, 浅原理人, 花岡美幸, 河野健二: アプリケーション層プロトコルの状態を考慮した広域ネットワーク上での仮想マシン移送, 第 22 回コンピュータシステム・シンポジウム(ComSys 2010), November, 2010 年.
7. Kenichi Kourai and Shigeru Chiba : Fast Software Rejuvenation of Virtual Machine Monitors, IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Computer Society Digital Library, May 2010. (preprint)
8. Hidekazu Tadokoro, Kenichi Kourai, and Shigeru Chiba, A Secure System-wide Process Scheduler across Virtual Machines, In Proc. of 16th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'10), Dec. 2010.
9. Yuji Kosuga, Miyuki Hanaoka, Kenji Kono, Generating Effective Attacks for Efficient and Precise Penetration Testing against SQL Injection, IPSJ Transactions on Advanced Computing Systems(ACS), Vol.1, No.2, pp69--82, February, 2011
10. Kenichi Kourai, Fast and Correct Performance Recovery of Operating Systems Using a Virtual Machine Monitor, In Proc. of 2011 ACM International Conference on Virtual Execution Environments (VEE 2011), March 2011.

11. 石川 豊, 山田 浩史, 浅原 理人, 花岡 美幸, 河野 健二, アプリケーション層プロトコルの状態を考慮した広域ネットワーク上での仮想マシン移送, 情報処理学会論文誌:コンピューティングシステム, Vol.4, No.2, pp.12--pp.24, March 2011
12. 吉田 哲也, 山田 浩史, 佐々木 広, 河野 健二, 中村 宏, マルチコア CPU の電力消費特性を考慮した仮想 CPU スケジューラ, 情報処理学会論文誌:コンピューティングシステム, Vol.4, No.2, pp.25--pp.39, March 2011

(4－2) 知財出願

① 平成22年度特許出願件数(国内 0 件)

② CREST 研究期間累積件数(国内 0 件)