研究課題別評価

1. 研究課題名 :オープンネットワークのための基盤システムソフトウェア

2. 研究者氏名 :加藤　和彦
ポスドク研究員 :大山　恵弘(研究期間 :2001.4.1～2003.3.31)

3. 研究の狙い：
本研究は、オープンなネットワーク環境で稼動することを最初から前提としたソフトウェア体系の再構築と、その体系に基づいた実際的な基盤ソフトウェアを設計開発することを目的とする。具体的には以下の研究を行う。

- オープンネットワーク環境を前提とした基盤ソフトウェアの構成モデルを新たに構築する。オペレーティング・システム、ミドルウェア、アプリケーションソフトウェアのそれぞれが提供すべき機能の系統的な再構成を行う。
- アプリケーション独立に資源アクセス制御および資源消費制御を行うための方式を開発する。この方式は、さまざまなプラットフォームおよびアプリケーションにおいて必要となる資源の拡張的な定義技術を含む。また、資源アクセスを行うための API の統一的な記述とその安全な実行法、およびポリシーモジュールによる実行時検査機構を開発する。
- 資源アクセス制御および資源消費制御機構を有効に利用するためのポリシープログラミング技術を開発する。ポリシー記述をコンポーネントモジュール化し、再利用性を高める方法を開発する。

4. 研究結果：
従来のオペレーティング・システム環境およびアプリケーションソフトウェアの構成を根本的に変えるのではなく、従来環境との互換性を保ちながら、かつ、オープンなネットワーク環境において安全にソフトウェアを流通・実行させる方法論を研究した。その結果、以下のような研究結果を得ることができた。

1. オープンネットワーク環境上でソフトウェアを安全に流通・実行するための構成モデルの設計とその実装を行い、SoftwarePot システムと名付けた。オペレーティング・システムおよびアプリケーションには変更を加えず、ミドルウェア層において実現する方式を開発した。
2. アプリケーション独立に資源アクセス制御を行う方法として、システムコールの捕捉によって実現する方式を開発した。仮想計算環境を作り上げることによって、ファイルやネットワーク等の計算機資源を仮想化し、アプリケーションの実行時のアクセスを制御する。仮想化機能においては、ユーザが柔軟に定義を与えることができるようになっている。
3. 計算機資源へのアクセス制御を行うポリシーを動的に切り替える機構、および、専門家によるポリシー作成を支援する GUI 環境を開発した。また、ポリシーを動的に生成するアプローチの一貫として、ソフトウェア・コンポーネントごとに正常動作検査ポリシーを自動作成し、コンポーネントを利用して構築されたソフトウェアの正常動作モデル作成において再利用する方

法を開発した。

5. 自己評価：

ほぼ予定した計画通りに研究を遂行することができたと自負している。最初の 10 ヶ月に、問題分析や過去の研究のサーベイや、予備的な検討、実験、試験的な設計を行い、その結果、ファイルシステムごとサンドボックスに入れ、仮想化し、移動可能とするという基本設計の着想を得ることができた。この着想により、既存のソフトウェア環境と極めて互換性高く、安全にソフトウェアを流通・実行し、セキュリティポリシー記述を比較的容易に行い、実際的な安全性を確保することが可能となった。その後の研究期間は、この着想に基づいて設計を進め、実装と評価を繰り返しながら、実用性の高いシステムへと仕上げていった。またポリシープログラミングを容易化させる研究も並行して行い、いくつかの成果を得ることができた。

試みながらも、アプローチをうまく見つけられなかったのは、資源消費制御を OS カーネルに改変を加えることなしに実現する方法である。これは世界的に見ても、未だによい方法が見つかっていない研究課題であり、今後の課題としたい。

私はこれまでに約 20 年間に渡っていくつものシステムソフトウェア開発に関する研究を行ってきたが、その中で今回の研究が最も他の同分野の研究者・開発者からの評判が高い。平成 15 年 10 月よりCREST研究（「情報社会を支える新しい高性能情報処理技術」（研究総括：田中英彦 東京大学教授））の支援を受けているが、CREST研究として採択となったのも、幸いにして、本さきがけ研究での研究成果が評価を受けたためである。研究総括やアドバイザーの先生方の御指導・御鞭撻があったからこそであり、心より感謝している。

本さきがけ研究においては、私の専門とする研究分野以外の数多くの研究者の発表を聞き、刺激を受け、議論をすることができた。今回の研究で開発した SoftwarePot システムは、本さきがけ研究の領域名である「協調と制御」を、ソフトウェア・セキュリティの分野において、正に実現している。外部由来のソフトウェア環境と内部由来のソフトウェア環境が、ユーザの制御下で（すなわちセキュリティポリシーの制御下で）協調し合う SoftwarePot の着想は、今回のさきがけ研究を開始して後に得たものであり、領域会議等での議論が影響を与えている部分があると思われ、大変に感謝している。CREST 研究のタイトルは「自律連合型基盤システムの構築」というものであり、「自律と連合」という発想も「協調と制御」という領域名から影響を受けている部分がある。

最後にポスドク参加型の有効性であるが、私にとって極めて有効であり、得られた研究成果は、この制度のおかげであったと言っても過言ではない。ポスドク研究員として参加して頂いた大山恵弘氏には、東京大学大学院理学系研究科博士課程情報科学専攻を修了してすぐに 2 年間、当プロジェクトに参加して頂くことができた。同氏が極めて高い才能を有することは、同氏が本年 4 月に出身研究室の助手として採用されたことからも窺われよう。連日続いた同氏との白熱した議論、同氏の驚嘆すべき調査能力と実装能力のおかげで SoftwarePot の研究を立ち上げることができた。現在の CREST 研究の主要メンバーとしても参加して頂いている。ポスドク参加型の恩恵を存分に享受することができ、心より感謝している次第である。

6. 研究総括の見解：

オープンな環境における基盤ソフトウェアの基本設計を根本から見直して、そのモデルに基づいたソフトウェアである“SoftwarePot”という構成モデルを研究開発・実装し、かなり完成度の高い

レベルのソフトウェア実行システムとして実現したことは極めて高く評価できる。
SoftwarePot は従来のよりも低コストで、資源をより細かな単位で仮想化できる点、さらに、Linux, Solaris, PocketPC, Windows に対応する実装を行っている点など高い評価を得ている。

7. 主な論文等：

1. 大山恵弘, 神田勝規, 加藤和彦, 安全なソフトウェア実行システムSoftwarePotの設計と実装、コンピュータソフトウェア, 日本ソフトウェア科学会,Vol. 16, No. 6, pp. 2-12, 2002年11月.
2. 阿部洋丈, 加藤和彦. セキュリティポリシーの動的切替機構を持つリファレンスモニタシステム. コンピュータソフトウェア, 日本ソフトウェア科学会, Vol. 20, No. 3, pp. 2-16, 2003年5月.
3. 大山恵弘, 王維, 加藤和彦. 異常検知システムにおける正常動作データのモジュール化. 情報処理学会論文誌, Vol. 44, No. SIG 10 (ACS 2), pp. 36?47, 2003年7月.
4. 阿部洋丈, 大山恵弘, 岡瑞起, 加藤和彦, 静的解析に基づく侵入検知システムの最適化, 情報処理学会論文誌 :コンピューティングシステム 採録決定).
5. 5. K. Kato, Y. Oyama, K. Kanda, and K. Matsubara, Software Circulation using Sandboxed File Space-Previous Experience and New Approach. *Proc. of 8th ECOOP Workshop on Mobile Object Systems*, June 2002, Malaga, Spain.
6. 6. K. Kato and Y. Oyama, SoftwarePot: An Encapsulated Transferable File System for Secure Software Circulation, Proc. of Int. Symp. on Software Security, Springer, LNCS-2609, 2003. pp. 112?132.

論文 :28件 (上記含む)
口頭発表 :15件

特許

1. 出願番号 :特願2001-380629, 発明者 :加藤和彦、大山恵弘,
   発明の名称 :安全なソフトウェア流通システム,出願日 :2001年12月13日
   (2002年12月に、米国出願を含むPCT出願中)