研究課題別評価

1. 研究課題名：広域分散環境のためのセキュアなオペレーティングシステム

2. 研究者氏名：河野 健二

3. 研究の狙い：

本研究の目的は、インターネットなどの開放性の高い分散環境においても、高いセキュリティを保証し、安心して利用できる計算機環境を提供することにある。インターネットなどの広域分散環境は、不特定多数のユーザが利用する環境であり、ユーザの匿名性がきわめて高い。従来のオペレーティングシステム (OS) は、あらかじめ登録された利用者のみから利用されることを想定しており、不特定多数のユーザにサービスを提供することは想定していない。そのため、広域分散環境の匿名性を悪用した不正アクセスに対して、従来の OS が提供する保護機構はきわめて無力である。 本研究のねらいは、従来の OS が提供してきたプロセス・モデル、保護のモデル、資源の管理方式を見直し、開放的分散環境に適した OS のモデルとその実現方式を確立することにある。開放的分散環境を念頭において、それらの諸概念を基本から設計し直し、新たなモデルに基づいた OS カーネルを提供する。

4. 研究結果：

本研究の成果は、1) 細粒度保護ドメインに基づく新しいプロセス・モデルの実現とその応用による新たな保護機構の実現、2) 資源を濫用する攻撃に対し、耐性を有する資源管理方式を実現した点、3) 高い堅牢性を有するインターネット・サーバの実現手法を提案した点の 3 点である。

4-1 細粒度保護ドメインとその応用

細粒度保護ドメインに基づいた新たなプロセス・モデルを実現し、その機構を応用したさまざまな保護機構の実現を行った。 プロセス・モデルは、OS の提供する抽象化の中でももっとも基本的な抽象化のひとつである。本研究では、そのプロセス・モデルを変革することにより、さまざまな保護機構の基盤となる機構を提供することができた。このプロセス・モデルを用いると、プログラムの実行を詳細にかつ効率的に監視できるようになり、従来では実現が困難であったさまざまな保護機構が実現可能となる。そのような保護機構の例として、実行可能コンテンツの監視, 柔軟かつ効率的なサンドボックス機構、UNIX における setuid プログラムの堅牢性向上が可能であることなどを示すことができた。

4-2 資源濫用攻撃に耐性を有する資源管理方式

資源濫用攻撃と呼ばれる不正攻撃に対し、耐性を有する資源管理方式の実現を行った。資源濫用攻撃とは、意図的に計算資源を濫用し、他のプログラムの応答性を著しく低下させる攻撃である。本研究では、資源濫用攻撃に耐性を有する資源管理方式として、優先度付き横取り可能な資源管理方式の提案を行った。この方式では、あるプロセスが資源を占有しても、ほかのプロセスが占有された資源を横取りすることができ、結果として資源の占有ができない。提案方式を Linux カーネルに実装し、資源濫用攻撃が行われても、プログラムの応答性が低下しないことを実証した。

4-3 堅牢性の高いインターネット・サーバの実現手法

インターネット・サーバの脆弱性は広く知られている。特に、バッファ溢れなどの常套的な攻撃手段の多くは、サーバの実装上の些細な誤りに起因する。本研究では、ドメイン特化言語の手法を用いて、インターネット・サーバの堅牢性を向上させる手法の開発を行った。

5. 自己評価：

細粒度保護ドメインに基づくプロセス・モデルを実現したことや、資源濫用攻撃に耐性を有する資源管理方式を実現したことによって、高いセキュリティ機構をもつオペレーティングシステムを実現するという当初の研究構想はある程度達成できたと考えている。特に、細粒度保護ドメインに基づいたプロセス・モデルはその柔軟性がきわめて高く、当初の予想を超えた応用性をもつことがわかった。さきがけの研究期間中にもいくつかの応用例を示したが、他にも多くの応用例があることが期待できる。今後はこれらの応用例を示し、細粒度保護ドメインに基づいたプロセス・モデルの有効性や有用性を実証していきたい。

資源濫用攻撃に耐性を有する資源管理機構は、十分に満足のいく結果が得られたとは言い難い。さきがけ研究期間中に提案・開発を行った機構は、既存のオペレーティングシステムの提供するプロセス・モデルをベースに資源割り当てモデルの設計や実現を行った。しかし、現実のアプリケーションは、複数のプロセスが互いに密接に連携しながら処理をすすめるため、既存のプロセス・モデルをベースとした資源管理方式では限界があることが判明した。この限界を打ち破るには、新たな資源割り当てモデルの考案、資源管理方式の実現、既存のアプリケーションとの親和性の問題などを解決しなければならず、多くの問題が山積みとなっている。さきがけ研究期間中にこれらの問題を解決できなかったことは残念であるが，新たな研究の鉱脈を発見できたことでよしとしたい。

堅牢性の高いインターネット・サーバの実現法は、安全性の高いオペレーティングシステムの実現法を考察する中で、副産物として得られた成果である。研究課題名にあるオペレーティングシステムの研究とは若干異なり、プログラミング言語の分野で用いられる手法をプラグマティックに適用した結果である。オペレーティングシステムの分野に、プログラミング言語の分野で発達しつつある手法を取り入れることができたという点で満足している。こうしたハイブリッド的なアプローチは今後ますます重要になってくると期待され、これからの研究手法の中に積極的に取り入れていきたいと考えている。

さきがけの研究期間中は、めぐまれた環境の中で存分に研究を進めることができ、多謝するとともに、これを糧に今後も研究活動を続けていきたい。

6. 研究総括の見解：

インターネットにおけるセキュリティ上の問題に対し、コンピュータを支える基盤であるオペレーティングシステムからのアプローチを行い、プロセス・モデルなどの基本的な概念の見直しからはじめ、コンピュータ科学の基幹的分野において重要な成果をあげたことは評価できる。また、今後の目標もしっかり捉えており、将来の研究推進が大いに期待できる。

7. 主な論文等：

K. Kono, T. Masuda: Efficient RMI: Dynamic specialization of object serialization, In Proceedings of IEEE 20th Int'l Conf. on Distributed Computing Systems (ICDCS), 308-315 (2000).

河野 健二, 益田 隆司：オブジェクト整列化の動的特化による効率的な RMI の実現, 情報処理学会論文誌 41 巻 10 号, 2916-2925 (2000 年).

品川 高廣, 河野 健二, 益田 隆司：実行可能コンテンツの安全な実行環境, 情報処理学会論文誌 43 巻 6 号, 1677-1689, (2002 年).

T. Shinagawa, K. Kono, T. Masuda: Flexible and Efficient Sandboxing Based on Fine-Grained Protection Domains, In Proceedings of Int'l Symp. on Software Security, 2002. Post proceedings will be published in Hot-Topic Series of the Springer LNCS.

W. Kaneko, K. Kono, T. Masuda: Preemptive Resource Management: Defending against Resource Monopolizing DoS, In Proceedings of Int'l Conf. on Parallel and Distributed Computing and Networks, 2003. To appear.

河野 健二: アプリケーション層プロトコルの実現を容易にするフレームワーク, 情報処理学会プログラミング研究会論文誌 掲載予定).