発表概要

ロード時バイナリ変換によるセキュリティ強制方式

渡部卓雄[†] 永藤直行[†] 山田聖[††]

柔軟な分散計算システムを構築するための便利な抽象化機構としてさまざまな形態の異動コードが注目されてきた．固定的なネットワークシステムから移動・遍在計算機環境へとシフトするうえで，移動コードの重要性が増している．しかし，実際の応用システムで移動コードを採用するうえで，解決しなければならないセキュリティ上の問題はまだ多い．さらに，移動コードを用いてシステムを構成するためには，コードの移動がひきおこすさまざまな変化に対処できる必要がある．そしてセキュリティモデルもそのために拡張可能（あるいは適応的）である必要があり，さらにそういったセキュリティモデルのためのポリシー記述はむずかしい．今回の発表では，まずアプリケーション依存のセキュリティポリシーについて述べ，次にそういったポリシーを強制する方法の提案について説明する．対象とする移動コードは，ここではJavaクラスファイルとする．我々の方式は，主としてロード時のバイトコード変換によって監視付き実行を行うコードを挿入するものであるが，そのためのポリシーをPolarisという特別な言語によって記述する．Polarisは基本的には有限状態プロセス言語であるが，変数間のデータ依存関係を扱えるようになっている．これによって監視のコストを抑えることができる．記述の具体例として，我々が構築しつつある拡張可能メールクライアントの一部を示す．

本プロジェクトのwebサイト：http://www.psg.cs.titech.ac.jp/sc/

A Security Enforcement Method by Load-time Binary Translation

Takuo Watanabe,[†] Naoyuki Nagatou[†] and Kiyoshi Yamada[††]

Mobile code has been regarded as a convenient abstraction mechanism to construct flexible/evolvable distributed computing systems. It has now gained prominence, mainly due to the current shift from stationary to mobile/ubiquitous computing environment. Although designing a system using mobile code is appealing, its deployment is still a security risk. Further, a system using mobile code is inherently dynamic; we need an extensible/adaptable security model. In this talk, we first claim that application-dependent and special-purpose security policies are increasingly important especially for modern distributed computing environment. Then we present a set of techniques that may be used to enforce such policies on mobile objects (Java classes). The main technique is a load-time bytecode modification that enforces user-defined policies via monitored execution. The policies are written in a language called Polaris, which is basically a finite process language enhanced to deal with data-dependencies among variables. Use of data-dependencies reduced the cost of monitoring. As an example, we show a code portion from our extensible e-mail client system.

Web site of this project: http://www.psg.cs.titech.ac.jp/sc/

（平成13年10月23日発表）

† 東京工業大学情報理工学研究科計算工学専攻
Department of Computer Science, Tokyo Institute of Technology
†† 北陸先端科学技術大学院大学情報科学研究科
School of Information Science, Japan Advanced Institute of Science and Technology