発表概要

Javaにおけるインテグリティモデル

児島 尚[†] 丸山 宏[††] 西崎 真也[†]

Javaのセキュリティチェックシステムの核となるものの1つに，実行時におけるコールスタック検査システムがある．この方法では，「現在プログラムを実行しているのはだれ（コールスタック上のどのフレーム）か?」ということに基づきアクセス制限等を行っている．しかし，複雑なプログラムにおいては，プログラム実行中のある時点でのコールスタック状態を調べても発見できないようなセキュリティホールが存在することがある．そのようなセキュリティホールを防ぐ手段として，我々は変数どうしの依存関係をトレースするモデルを提案する．これはBibaのインテグリティモデルに基づいており，各変数に対して変数のインテグリティを示す属性を設け，変数どうしの代入等による依存関係によって，そのインテグリティが実行時に変化していくモデルである．インテグリティは大きいほど安全とされ，信頼されないプログラムにより値が更新されたりすると，その変数のインテグリティは下がり，信頼されない値と見なされる．最終的に，ファイル読み込み操作の引数に使われるような変数のインテグリティがチェックされ，閾値より小さいインテグリティの変数の場合，セキュリティ例外等を発生させる．このモデルにより効果的なセキュリティチェックが期待できる．我々はこのモデルをJavaにおけるインテグリティモデルと呼び，そのモデルに基づき，Javaソースコードに変数のインテグリティをトレースするためのコードを埋め込むようなプリプロセッサを実装した．

Java Integrity Model

Hisashi Kojima,[†] Hiroshi Maruyama[††] and Shin-ya Nishizaki[†]

Runtime call stack inspection is a major security check system in Java. This system checks a call stack at runtime, and applies access control to resources, which is determined by principals of frames on the call stack. But in the case of complicated programs, there are some security holes such that the security check system cannot detect them easily by checking a call stack. We propose a new security check system for avoiding such security holes. In the security check system, the security holes are detected by tracing dependency of variables. This system is based on the Biba's integrity model. Integrity denotes security level. If a value of a variable is updated by an untrusted program, then the integrity of the variable decreases and the value is regarded as untrusted. For example, for each formal parameter of file reading procedures, its integrity is checked. If it is lower than some fixed threshold, security exception is occurred. We call the security check system Java Integrity Model and implement a trancelator which embeds codes for integirity checking into Java source codes.

(平成12年6月16日発表)

† 東京工業大学大学院情報理工学研究科
Department of Computer Science, Gradutate School of Information Science and Engineering, Tokyo Institute of Technology
†† 日本アイ・ビー・エム株式会社東京基礎研究所
Tokyo Research Laboratory, IBM Japan