Lightweight Inlined Reference Monitors for Securing Extensible and Open Systems

Phu H. Phung

The licentiate seminar will be held in hall EE, ED-building, Rännvägen 6B, on **Friday, January 16th, 2009 at 10:15**.

Discussion leader: **Prof. Frank Piessens**, Katholieke Universiteit Leuven, Belgium.

This thesis is available at the Department of Computer Science and Engineering, Chalmers University of Technology and Göteborg University, SE-412 96 Göteborg, Sweden. Telephone: +46 31 772 1000
Lightweight Inlined Reference Monitors for Securing Extensible and Open Systems

PHU H. PHUNG
Department of Computer Science and Engineering
Chalmers University of Technology and Göteborg University

Thesis for the degree of Licentiate of Engineering, a Swedish degree between M.Sc. and Ph.D.

Abstract

This thesis studies an alternative implementation of a security reference monitor in the contexts of extensible and open systems. A security reference monitor is a classic approach to imposing a security policy on an otherwise untrusted system by using a trusted component which intercepts security-relevant resource requests and applies a security policy to decide whether to grant such requests.

Recently, an application-level approach to implementing reference monitors has emerged. This is the so-called inlined reference monitor (IRM) approach where the software is rewritten to embed (inline) the policy within it. This thesis presents an alternative implementation of the IRM approach by using aspect-oriented programming. We call this the lightweight inlined reference monitor approach, since it does not require modification of the base system, and does not need an additional security policy language. The contexts of this thesis are extensible and open software systems in which software components are allowed to extend the functionality of others, and to integrate external, or third-party services. Firstly, we have studied such an extensible system in a vehicle software scenario, and analysed the safety-security characteristics for such a system. The analysis has resulted in guidelines for policy design for securing vehicle software systems. Secondly, we have proposed a lightweight IRM approach to providing vehicle software security. We have shown that the security assurance provided by the lightweight IRM approach is promising for deployment in an existing vehicle software system. Lastly, we have applied the lightweight IRM approach to the context of JavaScript (web browser) security, where we show how to control and modify the behaviour of JavaScript to make it self-protecting.

Keywords: Inlined Reference Monitors, Vehicle Software Security, JavaScript, Security