CHALMERS | UNIVERSITY OF GOTHENBURG

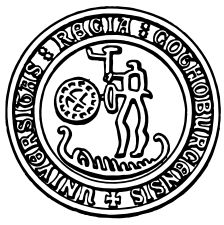
Lightweight Enforcement of Fine-Grained Security Policies for Untrusted Software

Phu H. Phung

Thesis for the Degree of Doctor of Philosophy to be defended in public in lecture room EC, ED&IT-building, Rännvägen 6B, Gothenburg on **Monday**, **October 10th**, **2011** at **10:15**.

Faculty opponent: **Associate Professor V.N. Venkatakrishnan**
University of Illinois at Chicago, USA.

The thesis is available at:
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg, Sweden
Telephone: +46 31 772 1000



Lightweight Enforcement of Fine-Grained Security Policies for Untrusted Software

Phu H. Phung
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg

Abstract

This thesis presents an innovative approach to implementing a security enforcement mechanism in the contexts of untrusted software systems, where a piece of code in a base system may come from an untrusted third party. The key point of the approach is that it is *lightweight* in the sense that it does not need an additional policy language or extra tool. Instead, the approach uses the aspect-oriented programming paradigm – a programmatic means to modify the behaviour of an application based on *aspects* – to specify security policies and *embed* the policies into untrusted software. As a result, security policies can be fine-grained and application-specific, and can be *inlined* into the untrusted software without modifying the base system, in order to detect and prevent unintended behaviour of the software at runtime. The approach has been elaborated in two particular untrusted software contexts in this thesis.

Firstly, we have developed the approach in the context of a vehicle software architecture, where a third-party application can be installed and executed in a vehicle system. We have shown that various classes of fine-grained security policies can be specified and enforced in such a system by the approach. The security assurance provided by the enforcement mechanism is promising for deployment in an existing vehicle software system. Furthermore, we have identified a number of potential threats in the vehicle software architecture and developed countermeasures in terms of security policies. We have demonstrated the deployment of countermeasures to prevent possible attacks.

Secondly, we have studied web application security. We propose a novel enforcement method called *lightweight self-protecting JavaScript* by applying the lightweight approach in the context of web security. The method prevents or modifies inappropriate behaviour of JavaScript execution in web pages by intercepting security relevant API calls. Unlike other approaches to enforcing policies for JavaScript, the enforcement and policy code are provided as a library and therefore do not require a modified browser. Furthermore, the approach does not employ runtime parsing or transformation of code, and thus has low runtime overhead. We also present an application of the method in the context of untrusted JavaScript such as *mashups* by proposing a two-tier sandbox architecture in which untrusted JavaScript code can be loaded and executed dynamically. The execution of untrusted code is monitored by modular and fine-grained security policies defined via an adaptation of self-protecting JavaScript to ensure security for the hosting page.

Keywords: *security policy enforcement, vehicle software security, web-application security, JavaScript security, untrusted software*