Domain : Programming-Testing-ProvingDomain

Model-based Testing of Operating-System-Level Security Mechanisms

Year: 2012
Starting: 1.10.2012

Aadvisor: WOLFF Burkhart,
Laboratory: LRI ForTesSE, University Paris-Sud
Collaborations: EU Project EURO-MILLS

Abstract
Security Mechanisms on operating system level play a major role in modern virtualization environments: Memory Separation, control of shared memory, control of send-receive event relations between specific groups of threads and processes (or generally speaking: information flow properties) have to be enforced on different layers of abstraction.

Based on prior experience of model-based testing of security infrastructures with HOL-TestGen system, this Phd work attempts to adapt and extend model-based testing techniques to Operating-system level security mechanisms. In particular, it has to be explored if the required security properties can be expressed in the policy-language UPF.ContextThis Phd is part of the EU Integrated Project EURO-MILLS (consisting of 14 partners in Germany, Austria, Belgium, France, the Netherlands) whose primary goal is to provide a small virtualization platform (based on the operating system PikeOS) intended to allow the secure decomposition of complex embedded systems into independent components. The secondary goal is to achieve EAL7 certification for this virtualization platform by applying formal verification; for this purpose, a combination of proof and test techniques is envisaged, where the Partner U-PSud plays a major role.Objectives- Develop Security Models relating to the (Isabelle) Pike-OS Model to be developed in the project

Working Plan:

- Develop specific testing techniques and infrastructure
- for test-generation in the context of OS systems.
- integrate test-data generation into the industrially used workflow.

Extra informationPublications:

- [1] Achim D. Brucker, Burkhart Wolff: On Theorem Prover-based Testing. Accepted the 07-08- 2011. In Formal Aspects of Computing (FAOC). DOI: DOI: 10.1007/s00165-012-0222-y. Springer, 2011.
- [2] Achim D Brucker, Lukas Brügger, Paul Kearney and Burkhart Wolff. An Approach to Modular and Testable Security Models of Real-world Health-Care Applications. Series Proceedings of the ACM Symposium on Access control models and technologies, ACM, 2011, pages 133-142. SACMAT 2011.
- [3] Achim D Brucker, Lukas Brügger, Paul Kearney and Burkhart Wolff. Verified Firewall Policy Transformations for Test Case Generation. Software Testing, Verification, and Validation, 2010 International Conference on 0:345-354, 2010.

Prerequisites

- Knowledge in Formal Methods, Logic, Functional Programming
- Interest in Modeling and Programming with Isabelle/HOL