Title: Automatic security policy enforcement in computer systems

Author: K. Adi, L. Hamza, L. Pene

PII: S0167-4048(17)30228-6
DOI: https://doi.org/10.1016/j.cose.2017.10.012
Reference: COSE 1224

To appear in: *Computers & Security*

Received date: 7-5-2017
Revised date: 29-9-2017
Accepted date: 29-10-2017

Please cite this article as: K. Adi, L. Hamza, L. Pene, Automatic security policy enforcement in computer systems, *Computers & Security* (2017), https://doi.org/10.1016/j.cose.2017.10.012.

Automatic Security Policy Enforcement in Computer Systems

K. Adi, L. Hamza, and L. Pene

Computer Security Research Laboratory

Computer Science and Engineering Department

Université du Québec en Outaouais, Québec, Canada.

Vitae

Kamel Adi holds a Master degree in theoretical computer science from Pierre et Marie Curie (Paris VI) University and a Ph. D. degree in computer security from Laval University, Quebec, Canada. He is currently a full professor in the Department of Computer Science and Engineering at the University of Quebec in Outaouais, Canada. Kamel Adi is also the co-director of the Computer Security Research Laboratory at Université du Québec en Outaouais, Canada. His research activities focus on the development and application of formal methods for solving problems related to computer security and computer networks.

Lamia Hamza is a Ph.D. student and assistant teacher at University of Bejaia, Algeria. She received an engineer diploma in computer sciences from the University of Setif, Algeria, and a M.Sc. in networking and distributed systems from the University of Bejaia, Algeria. Lamia joined the Computer Security Research Laboratory during her research internship at Université du Québec en Outaouais, Canada. She continues to collaborate with other team members on topics of common interest. Her current research involves computer security and formal methods.

Liviu Pene received his Master degree in computer science from Université du Québec en Outaouais, Canada. He is currently a Ph.D. student and a member of the Computer Security Research Laboratory team at Université du Québec en Outaouais, Canada. Liviu's most recent research explores subjects related to the verification and enforcement of computer and network security policies through formal methods.

Abstract. This paper proposes a formal framework for automatic security policy enforcement in computer systems. In this approach, systems and their interactions are formally modelled as process algebra expressions with a new dedicated calculus inspired from the ambient calculus. Security policies are specified with the aid of a dedicated modal logic. We demonstrate how, for a given security policy expressed by a logical formula, our calculus allows to verify whether the specification meets the security policy requirements. If it does not, the optimal enforcement for