Specificating and Verifying an Attribute-based Usage Control Approach regarding Open and Dynamic Computing Environments

Christos Grompanopoulos
Department of Applied Informatics
University of Macedonia

This dissertation is submitted for the degree of

Doctor of Philosophy
This Dissertation Advisory Committee (DAC) consists of the following members (listed alphabetically):

• Professor Athanasios Manitsaris
  (Dept. of Applied Informatics, University of Macedonia, Greece.)

• Assistant Professor Christos Georgiadis
  (Dept. of Applied Informatics, University of Macedonia, Greece.)

• Associate Professor Ioannis Mavridis (PhD Supervisor)
  (Dept. of Applied Informatics, University of Macedonia, Greece.)

This Dissertation Defence Committee (DDC) consists of the following members (listed alphabetically):

• TODO
I would like to dedicate this dissertation to my family, for their love, endless support and encouragement.
First and foremost, I would like to express my sincere appreciation and gratitude to my supervisor, Associate Professor Ioannis Mavridis. His guidance and support all these years and during the completion of this dissertation have been invaluable. Even in difficult times, a meeting with him always reinvigorated my enthusiasm and raised my spirits.

I am also extremely grateful to the members of my dissertation committee, Professor Athanasios Manitsaris and Assistant Professor Christos Georgiadis, for their time and dedication in reviewing my work and for their advice throughout my dissertation.

I would also like to thank my colleague and friend Antonios Gouglidis at the Department of Applied Informatics of the University of Macedonia, for sharing his thoughts and feelings during the completion of this laborious but very rewarding journey.

Finally, I would also like to take this opportunity and express my profound gratitude to my parents and all of my family for their continuous support and encouragement.
Abstract

Computing systems are always evolving in order to keep pace with the requirements that are posed by new computing environments. The widespread of networking technologies transformed the standalone computer model into the client-server computer model. Social trends as frequent traveling and social networking, led to the creation of small-sized computing devices that are equipped with sensors to recognize their surrounding environment and adapt accordingly their operations. Therefore, novel computing modes are emerged, as ubiquitous computing and the Internet of Things. The aforementioned type of systems set new requirements in several areas, including also the area of security. Security is an area of great importance in all computing systems. From a computer security, and particularly from an access control point of view the evolution of computing systems induces the creation of Open and Dynamic Computing Environments (ODCE). They are characterized as open since there are no boundaries between the legitimate and illegal users of a system. And dynamic since the configuration of these systems is constantly changing. Despite the importance of access control in ODCE there are a few proposals that addressed their analysis and identification of new requirements. Therefore, also existing access control modes are not able to fully support these requirements.

In this dissertation, we analyze existing access and usage control approaches to identify a number of unique characteristics posed by ODCE. Secondly, we formally define an attribute based usage control model for ODCE that is designed based on the identified requirements. Last but not least, we check the proposed model for its correctness, i.e., the adherence of
the model to its initially defined specifications.

Specifically, we provide information on the RBAC, ABAC and UCON models, which are mostly applicable in the examined case of ODCE. The presented work on the specification of models renders the aforementioned information valuable regarding the modeling of access or usage control systems since it can help in the identification of required specifications of access/usage control models for ODCE, and further, it examines state-of-the-art models and verification techniques to check the correctness of the designed or produced models in respect to their initial specifications. In turn, we highlight through representative usage scenarios the additional requirements that are introduced when attempting to utilize the UCON family of models in modern computing environments. To meet the requirements posed by ODCE, the proposed UseCON model incorporates a number of significant features compared with existing access/usage control models. Firstly, UseCON’s extended expressiveness over the existing usage control models is the result of utilizing information originating from either a single or a set of both direct and indirect entities in the creation of the usage allowance decision. Secondly, UseCON inherently supports the utilization of historical information of usages through the automatic management of use entities. We further elaborate on the enhanced expressiveness in UseCON. A number of examples are given to demonstrate the enhanced capabilities of the UseCON model. The simplification of the policy administration process and the support of enhanced policy rules regarding their expressiveness, are included in the advantages of the proposed model. Furthermore, we provide a safety analysis of UseCON’s formal TLA+ specification to prove the correctness of the UseCON model. The verification of consistency, safety and liveness properties for the core model and its internal operations for correctness was done by providing a formal specification of the UseCON model in TLA+, and using the TLC model checker. Lastly, we provide information on the declaration of models in TCL and elaborate on some performance metrics and in the internal procedures of the TCL model checker.
References


32. Antonios Gouglidis and Ioannis Mavridis. On the definition of access control require


69. OASIS. Oasis extensible access control markup language (xacml) tc, 2011.


74. Li Li Qu, Yin Zhang, Feng Wang, Mi Kyung, and Han Ratul Mahajan. Trusted computer system evaluation criteria. In National Computer Security Center, 1985.


82. R. Sandhu. The ascaa principles for access control interpreted for collaboration systems. In


85. 234412.


98. Eric Yuan and Jin Tong. Attributed based access control (abac) for web services, 2005.


