Université Nice SOPHIA ANTIPOLIS

i3S sophia antipolis

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Sophia Antipolis, December 9th, 2016

REPORT ON THE PHD DISSERTATION OF MRS. THI-MAI NGUYEN

This report reviews the contributions of Mrs. Thi-Mai NGUYEN in her thesis dissertation entitled *"A Model-Driven Engineering Approach to Build Secure Information Systems"*. The work of Thi-Mai NGUYEN deals with the interesting topic of security-by-design with respect to the implementation of access control mechanisms and their formal validation. This manuscript, which is 182 pages long, is made up of 7 chapters, including an introduction and a conclusion. It discusses three main contributions: (1) how to model and visualize static and dynamic access control rules using UML and B with a separation of concerns, (2) how to automatically translate graphical models into their B formal counterpart, and (3) how to derive an executable code out of the B Platform Independent Model into a Platform Specific Model based on an aspect-oriented instrumentation of the functional code. The manuscript also contains a bibliography of 10 pages. It is written in English.

EVALUATION OF THE MANUSCRIPT AND CONTRIBUTIONS

Chapter 1: Introduction (5 pages)

This introductory chapter discusses the security challenges faced by developers when they have to develop a software that must satisfy specific security requirements. While the thesis title hints at security in the large, Mrs. NGUYEN's work more specifically focuses on logical (and mostly role-based) access control. There is no debate on the fact that the scenarios addressed by Mrs. NGUYEN constitute a very important topic today given the long-term objective of producing secure-by-design systems, at the various levels of abstraction involved in their design and development. This chapter also briefly introduces the model-driven approach followed in the rest of the manuscript. While rather short, this chapter does a good work in motivating the research undertaken and introducing the contributions and the organization of the following chapters.

Chapter 2: Background (20 pages)

This chapter introduces basic knowledge and concepts regarding the various techniques used, namely the B method for specification and proofs, the Model-Driven Engineering approach, access

control policies and more specifically Role Based Access Control, and finally Aspect-Oriented Programming, which is used for code instrumentation.

Chapter 3: State of the Art (40 pages)

This very long chapter quite pedagogically describes the existing techniques regarding the specification and enforcement of role-based access control policies and discusses their shortcomings. Regarding specification, this chapter notably distinguishes between graphical models like UML together with OCL, and textual modeling languages, like Alloy, Z-, and B-based approaches. Formal approaches based on B, which are further used in the thesis, come with the promise of a more scalable validation through theorem proving, in comparison with approaches following a model-checking validation. This section also discusses the tools supporting the formal specification of access control models with some of these approaches. This section also touches at the topic of access control enforcement by discussing library-based implementations, annotation based approaches, and finally aspect-based instrumentations. The latter discussion however only scratches the surface of the state of the art in the domain.

Chapter 4: Formal Development of a Secure Access Control Filter (21 pages)

This chapter discusses the first main contribution of the candidate, namely how to specify access control requirements based on UML and how to formalize such diagrams with B. The approach is inspired by a previous work separating the functional model from the static and from the dynamic access control requirements specifications. In her contribution, Mrs. NGUYEN builds upon the UML activity diagram in order to capture a history of past accesses for dynamic access control rules. Static and dynamic rules get translated into B using multiple machines to progressively refine the specification. This chapter is finally concluded by discussing the effectiveness of the formal verification performed by the Proof Obligations Generator of AtelierB. While the results obtained illustrate the high degree of automation of these proofs, the example considered is rather small for a complete validation in comparison with realistic access control policies. Mrs. NGUYEN also does not provide performance figures that would indeed prove the better scalability of B's theorem proving approach in this matter.

Chapter 5: A Tool for the Generation of a Secure Access Control Filter (17 pages)

This chapter introduces the second main contribution of the thesis, namely how to combine the B semantics of the functional model together with the static and dynamic access control requirements. This is notably made possible through automating the writing of a so-called access control filter with an extension of the B4MSecure tool. This chapter actually nicely illustrates the concepts introduced in Chapter 4 and makes the formalization much more accessible through concrete examples. While the process is nicely discussed and illustrated, this chapter lacks a description of the translation algorithms between UML and B models. Similarly to Chapter 4, this chapter would benefit from a large scale experiment with a realistic policy in order to evaluate the size of the specification and to assess whether it remains manageable for developers.

Chapter 6: A Formal Approach to Derive an AOP-Based Implementation of a Secure Access Control Filter (38 pages)

This chapter finally introduces the third main contribution of Mrs. NGUYEN, namely how to instrument the specification obtained into code. The approach followed is actually quite original in

this chapter as the enforcement of the security specification is actually implemented through static and dynamic checks over policy and application attributes stored in a separate relational database. The checks themselves are introduced through aspect weaving in order to support the separation of concerns discussed throughout the manuscript between the functional model and the security models. While the work covers very nicely implementations using logical access control mechanisms, one however wonders how it would translate to access control mechanisms based on encryption, a rather hot topic in the field. The performances of the actual implementation, both in terms of additional storage and execution time, are here much more critical than for the previous contributions, since the access control mechanisms introduced have a direct impact on the application at runtime. Still, this problem is never discussed in the chapter. Aspect-Oriented Programming also comes with a lingering question, as pointed out by Mrs. NGUYEN in her conclusion for this chapter: how to formalize the weaving itself in order to be sure that it does not introduce a weakness into the software generated?

Chapter 7: Conclusions and Future Work (3 pages)

This chapter finally very concisely summarizes the three contributions of Thi-Mai NGUYEN in this thesis. Mrs. NGUYEN hints at a certain number of future directions, namely refinement automation, and more complex policies, including notably delegation and prerequisites that are indeed frequently used in the industry. Even before addressing such important topics, I would certainly recommend formalizing the transformation algorithms developed in the tools and performing larger scale experiments to better assess the approach.

SYNTHESIS AND CONCLUSIONS

The research work undertaken by Thi-Mai NGUYEN is very interesting given the perspective of applying the methodology developed to industrial software development. This would make it possible to produce secure-by-design and proven applications according to a separately specified access control model. The dissertation is pleasant to read and shows Mrs. NGUYEN's academic knowledge of the field of access control specification and formalization as well as that of aspect-oriented programming, which is further proven by her good publication record (2 international conference papers). For all these reasons, and based on the work presented in this manuscript, I therefore recommend to authorize Thi-Mai NGUYEN to defend her thesis.

Yves ROUDIER
Professeur des Universités
Laboratoire I3S - CNRS - Université de Nice Sophia Antipolis