Distributed security in closed distributed systems

The goal of the present thesis is to discuss, argue and conclude about ways to provide security to the information travelling around computer systems consisting of several known locations.

When developing software systems, security of the information managed by these plays an important role in their design. There should always exist techniques for ensuring that the required security properties are met. This has been thoroughly investigated through the years, and many varied methodologies have come through.

In the case of distributed systems, there are even harder issues to deal with. Many approaches have been taken towards solving security problems, yet many questions remain unanswered. Most of these problems are related to some of the following facts: distributed systems do not usually have any central controller providing security to the entire system; the system heterogeneity is usually reflected in heterogeneous security aims; the software life cycle entails evolution and this includes security expectations; the distribution is useful if the entire system is "open" to new (a priori unknown) interactions; the distribution itself poses intrinsically more complex security-related problems, such as communication, cryptography, performance and reliability. We do not expect to solve all of these, but we shall approach the first three.

In this dissertation, we take the view of a distributed system from a high-level of abstraction. We then focus on the interactions that can take place between the locations, and aim at providing security to each of these individually. The approach taken is by means of access control enforcement mechanisms, providing security to the locations they are related to. We provide a framework for modelling so. All this follows techniques borrowed from the aspect-orientation community.

As this needs to be scaled up to the entire distributed system, we then focus on ways of reasoning about the resulting composition of these individual access control mechanisms. We show how, by means of relying on the semantics of our framework, we can syntactically guarantee some limited set of global security properties. This is also restricted to distributed systems in which the set of locations is known a priori. All this follows techniques borrowed from both the model checking and the static analysis communities.

In the end, we reach a step towards solving the problem of enforcing security in distributed systems. We achieve the goal of showing how this can be done, though we restrict ourselves to closed systems and with a limited set of enforceable security policies. In this setting, our approach proves to be efficient.

Finally, we achieve all this by bringing together several fields of Computer Science. These include aspect orientation, model checking and static analysis, and of course some ingredients of logics and formal methods as well. All this is in an attempt to approach a software engineering problem, such as security in distributed systems. This shows how the full field of Computer Science can benefit from combining its subfields.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology, Computer Science and Engineering
Authors: Hernandez, A. M. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Number of pages: 198
Publication date: 2012

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Globally reasoning about localised security policies in distributed systems

In this report, we aim at establishing proper ways for model checking the global security of distributed systems, which are designed consisting of set of localised security policies that enforce specific issues about the security expected. The systems are formally specified following a syntax, defined in detail in this report, and their behaviour is clearly established by the Semantics, also defined in detail in this report. The systems include the formal attachment of security policies into their locations, whose intended interactions are trapped by the policies, aiming at taking access control decisions of the system, and the Semantics also takes care of this.

Using the Semantics, a Labelled Transition System (LTS) can be induced for every particular system, and over this LTS some model checking tasks could be done. We identify how this LTS is indeed obtained, and propose an alternative way of model checking the not-yet-induced LTS, by using the system design directly. This may lead to over-approximation thereby producing imprecise, though safe, results. We restrict ourselves to finite systems, in the sake of being certain about the decidability of the proposed method.

To illustrate the usefulness and validity of our proposal, we present 2 small case-study-like examples, where we show how the system can be specified, which policies could be added to it, and how to decide if the desired global security property is met.

Finally, an Appendix is given for digging deeply into how a tool for automatically performing this task is being built, including some implementation issues. The tool takes advantage of the proposed method, and given some system and some desired global security property, it safely (i.e. without false positives) ensures satisfaction of it.

Position paper: A generic approach for security policies composition

When modelling access control in distributed systems, the problem of security policies composition arises. Much work has been done on different ways of combining policies, and using different logics to do this. In this paper, we propose a more general approach based on a 4-valued logic, that abstracts from the specific setting, and groups together many of the existing ways for combining policies. Moreover, we propose going one step further, by twisting the 4-valued logic and obtaining a more traditional approach that might therefore be more appropriate for analysis.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Hernandez, A. M. (Intern), Nielson, F. (Intern)
Number of pages: 4
Publication date: 2012
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Designing, Capturing and Validating History-Sensitive Security Policies for Distributed Systems

We consider the use of Aspect-oriented techniques as a flexible way to deal with security policies in distributed systems. We follow the approach of attaching security policies to the relevant locations that must be governed by them, and then combining them at runtime according to the interactions that happen. Recent work suggests using Aspects in this way to analyse the future behaviour of programs and to make access control decisions based on this; this gives the flavour of dealing with information flow rather than mere access control. We show in this paper that it is beneficial to augment this approach with history-based components, as is traditional in reference-monitor-based approaches to mandatory access control. Our developments are performed in an Aspect-oriented coordination language, aiming to describe the Bell-LaPadula policy as elegantly as possible. Furthermore, the resulting language has the capability of combining both history-sensitive and future-sensitive policies, providing even more flexibility and power. Moreover, we propose a global Logic for reasoning about the systems designed with this language. We show how the Logic can be used to validate the combination of security policies in a distributed system, either with or without exploring the entire state space.

History-sensitive versus future-sensitive approaches to security in distributed systems

We consider the use of aspect oriented techniques as a flexible way to deal with security policies in distributed systems. Recent work suggests to use aspects for analysing the future behaviour of programs and to make access control decisions based on this; this gives the flavour of dealing with information flow rather than mere access control. We show in this paper that it is beneficial to augment this approach with history based components as is the traditional approach in
reference monitor based approaches to mandatory access control. Our developments are performed in an aspect-oriented coordination language aiming to describe the Bell-LaPadula policy as elegantly as possible. Furthermore, the resulting language has the capability of combining both history- and future-sensitive policies, providing even more flexibility and power.

**General information**
State: E-pub ahead of print
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Hernandez, A. M. (Intern), Nielson, F. (Intern)
Pages: 29-43
Publication date: 2010

**Host publication information**
Title of host publication: ICE2010 : Third Interaction and Concurrency Experience
Volume: EPTCS 38
Main Research Area: Technical/natural sciences
Conference: DisCoTec2010 : ICE2010 Satellite Workshop, CWI, Amsterdam, 01/01/2010
http://arxiv.org/abs/1010.5567v1
Source: orbit
Source-ID: 266368
Publication: Research - peer-review › Article in proceedings – Annual report year: 2010

**Enforcing Mandatory Access Control in Distributed Systems using Aspect-Orientation**

**General information**
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Hernandez, A. M. (Intern), Nielson, F. (Intern)
Pages: 62-64
Publication date: 2009

**Host publication information**
Title of host publication: 21st Nordic Workshop on Programming Theory Proceedings
ISBN (Print): 978-87-643-0565-4
Main Research Area: Technical/natural sciences
Conference: 21st Nordic Workshop on Programming Theory, Lyngby, Denmark, 14/12/2009 - 14/12/2009
Source: orbit
Source-ID: 257448
Publication: Research › Conference abstract in proceedings – Annual report year: 2009

**Projects:**

**Formal approaches for Aspect-Oriented Systems**
Department of Informatics and Mathematical Modeling
Period: 01/06/2009 → 28/09/2012
Number of participants: 6
Phd Student:
Hernandez, Alejandro Mario (Intern)
Supervisor:
Nielson, Hanne Riis (Intern)
Main Supervisor:
Nielson, Flemming (Intern)
Examiner:
Probst, Christian W. (Intern)
De Nicola, Rocco (Ekstern)
Hankin, Chris (Ekstern)

**Financing sources**
Source: Internal funding (public)
Name of research programme: *Forskningsrådsfinansiering*
Project: PhD