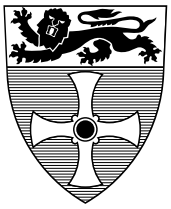
UNIVERSITY OF
NEWCASTLE



University of Newcastle upon Tyne

COMPUTING SCIENCE

A Formal Approach to Dependable Evolution of Access Control Policies in Dynamic Collaborations

J. W. Bryans, J. S. Fitzgerald, P. Periorellis.

TECHNICAL REPORT SERIES

No. CS-TR-1027 June, 2007

TECHNICAL REPORT SERIES

No. CS-TR-1027 June, 2007

A Formal Approach to Dependable Evolution of Access Control Policies in Dynamic Collaborations

Jeremy W. Bryans, John S. Fitzgerald, Panos Periorellis.

Abstract

Network-enabled dynamic collaborations between businesses are increasingly common, and can evolve rapidly. We propose a formal approach to maintaining information security during evolution, while enabling participants to evolve their access control policies with the coalition.

Printed and published by the University of Newcastle upon Tyne,
Computing Science, Claremont Tower, Claremont Road,
Newcastle upon Tyne, NE1 7RU, England.

Bibliographical details

BRYANS, J. W., FITZGERALD, J. S., PERIORELLIS, P..

A Formal Approach to Dependable Evolution of Access Control Policies in Dynamic Collaborations
[By] J. W. Bryans, J. S. Fitzgerald, P. Periorellis.

Newcastle upon Tyne: University of Newcastle upon Tyne: Computing Science, 2007.

(University of Newcastle upon Tyne, Computing Science, Technical Report Series, No. CS-TR-1027)

Added entries

UNIVERSITY OF NEWCASTLE UPON TYNE
Computing Science. Technical Report Series. CS-TR-1027

Abstract

Network-enabled dynamic collaborations between businesses are increasingly common, and can evolve rapidly. We propose a formal approach to maintaining information security during evolution, while enabling participants to evolve their access control policies with the coalition.

About the author

Jeremy Bryans has been a post doctoral research associate in Computing Science at Newcastle University since 2002. His background is in Theoretical Computer Science. His research has addressed the security of computer-based systems, particularly Dynamic Coalitions.

John Fitzgerald is Reader in Computing Science at Newcastle University. His research addresses the use of formal methods in early stages of development for complex systems, particularly systems that may reconfigure in response to threats. He leads work on resilience-explicit computing in the ReSIST Network on Resilience in IST. He is Chairman of Formal Methods Europe.

Panos Periorellis joined the department in June 2000 as a research associate after successfully completing his Ph.D. in the area of Enterprise Modelling under the supervision of Prof. John Dobson. Panos was promoted to Senior research Associate in March 2004 and started work on the GOLD project looking into issues of trust, privacy and security.

Suggested keywords

DEPENDABLE EVOLUTION,
ACCESS CONTROL POLICIES,
DYNAMIC COALITIONS

A Formal Approach to Dependable Evolution of Access Control Policies in Dynamic Collaborations

Jeremy W. Bryans, John S. Fitzgerald, Panos Periorellis
School of Computing Science, Newcastle University, UK
{Jeremy.Bryans, John.Fitzgerald, Panayiotis.Periorellis}@newcastle.ac.uk

Abstract

Network-enabled dynamic collaborations between businesses are increasingly common, and can evolve rapidly. We propose a formal approach to maintaining information security during evolution, while enabling participants to evolve their access control policies with the coalition.

1 Introduction

There is an increasing tendency for businesses to move away from the model of a small set of trusted collaborators towards opportunistic ad-hoc collaborations. These dynamic collaborations form around needs and opportunities in the market place, and evolve or are disbanded as these needs and opportunities evolve or disappear. This capacity to quickly create business-focused networks offers many benefits, but there are many inherent risks. Today's collaborator may become tomorrow's competitor; or two firms may simultaneously be collaborators on one product and competitors on another. As collaborators they will want to share certain information; as competitors there will be much information that cannot be divulged.

Our goal is to assist the participants in collaborations to control the evolution of their access control policies as they join and leave collaborations. As collaborations evolve, policies must necessarily evolve. At each step, each potential member is forced to make a trade-off between the risks and the benefits. We aim to make each of these evolutionary steps as dependable as possible, by providing tools and techniques to help in assessing this trade-off.

2 Our Approach

The approach we propose is outlined in Figure 1. Initially, a collaboration presents a proposed workflow to an access control policy generator. It produces an access control policy, which must be met in order for the workflow to run to completion. The policy will then divided into multiple policies, one for each collaboration member. For each member, these are the adaptions which need to be made to their access policy in order that the collaboration can execute the workflow.

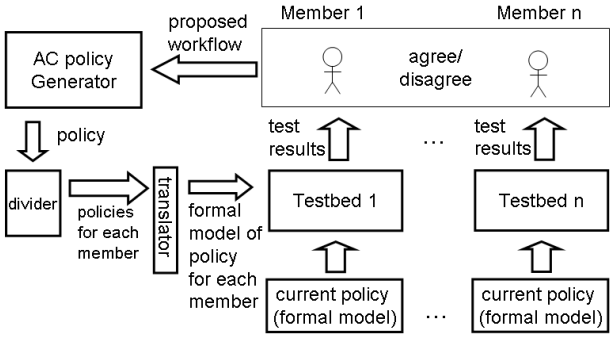


Figure 1. Evolving policies in collaborations

The next step is to translate each of these policies into its formal representation, and pass these to the individual members. Each member has to decide independently if the proposed adaptions to their current policy are acceptable. They are faced with two questions: 1) What access privileges need to be granted to other members in the course of executing this workflow? and 2) Will adding these new privileges to my existing access control policy violate my information security policy?

We propose using testing of formal models of the access control policies to provide support in answering these questions. The tests used will be a set of access requests together with the expected responses. These will be derived from the member's information security policy.

Within the testbed, a model of the proposed adaptions is combined with a formal model of their current access control policy. If this combination passes all the tests then the proposed workflow should be acceptable. Otherwise, any failures are presented to the decision maker.

If any member decides that the policy is unacceptable,

they can do more than simply signal disapproval. For every test that fails they may use the formal model to investigate precisely why it failed, and which particular parts of the access control policy were invoked. They can use this information to propose alternative workflows to the collaboration.

Once all members agree on a workflow, they add the new access control policy to their current policies. They may then begin to execute the workflow.

3 Implementation

In order to realise the policy validation approach outlined above, we require a way of generating access control policies from workflow descriptions. We expect to use an off-the-shelf tool such as the one described in [3] for this, adapting it to divide the output into separate policies for the individual members. For the analysis phase, we require a common framework for the policies. In our current work we are using the OASIS standard access control policy language XACML [5]. The analysis of these policies requires that the policy language has a formal semantics that is susceptible to analysis. We are using the model-oriented formal specification language VDM++ [4] and its associated tools as a basis for this. VDM++ specifications separate data and functionality, allowing us to clearly describe the access control policies and evaluation functions over them. Whilst VDM++ supports data and functional abstraction to the extent that the full language is not executable, there is a clearly defined executable subset. The VDM++ tool support (VDMTools) includes an interpreter that permits the execution of VDM++ policy evaluation functions over scripts containing test cases. We have developed a translator from XACML to a semantics in VDM [2]. An initial testing framework for context free policies (those which make no reference to information outside of that in the request) than has been constructed [2] and is being extended to context dependent policies (where the behaviour of the policy may be conditional on external variables.) Figure 2 shows a fragment of VDM++ invoking a test on a policy by evaluating a request on the policy decision point (PDP).

4 Next steps

Currently our approach is based on testing of policies. We would like to extend this to include the possibility of proving that policies meet key information security objectives. Automating this would depend on proof technology for VDM++ which is currently being developed.

Our work allows the decision maker to to see the implications of changes to access control policies. We would like to extend it to explore wider questions of information flow within dynamic collaborations. We could allow the user to experiment with various policies, such as those governing collaboration membership, information transfer or delegation of duties and privileges within a collaboration. In [1] we present a way of formally modelling a range of dynamic collaborations in order to investigate information flow properties between the members. Combined with the work presented here this would allow us to add a predictive capability to the work, allowing the decision maker to ask "what-if" questions based on possible future scenarios. For this, it would be important to present an intuitive graphical interface to the user. The API provided by VDMTools will provide a basis for this.

```
protected RunTest: () ==> ()
RunTest () == (
dcl pdp : PDP := CompanyPDP;
dcl req  : Request :=
  new Request(Anne,hazard_analysis,review);
dcl env : Env := new Env(
    author_haz_an.GetExp() |-> <BoolArray>,
    author_haz_an.GetExp() |->
       Anne.GetExp() |-> true,
         Bob.GetExp() |-> false);
dcl eval : Evaluator :=
  new Evaluator(req,pdp,env);
AssertTrue(eval.evaluateRequest() = <Deny>));
```

Figure 2. A VDM++ test on a policy

Acknowledgments: We are grateful for the support from the GOLD project and DSTL colleagues, in particular Tom McCutcheon, Helen Phillips and Olwen Worthington.

References

[1] J. W. Bryans, J. S. Fitzgerald, C. B. Jones, and I. Mozolevsky. Formal modelling of dynamic coalitions, with an application in chemical engineering. In *2nd International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA)*. IEEE, 2006. To appear. Also available as Newcastle University Technical Report CS-TR-981.

[2] J. W. Bryans, J. S. Fitzgerald, and P. Periorellis. Model based analysis and validation of access control policies. Technical Report CS-TR-976, Newcastle University, School of Computing Science, July 2006.

[3] D. Domingos, A. Rito-Silva, and P. Veiga. Authorization and access control in adaptive workflows. In *ESORICS*, 2003.

[4] J. Fitzgerald, P. G. Larsen, P. Mukherjee, N. Plat, and M. Verhoef. *Validated Designs for Object–oriented Systems*. Springer, New York, 2005.

[5] OASIS. eXtensible Access Control Markup Language (XACML) version 2.0. Technical report, OASIS, Feb 2005.