Towards an approach for Hybrid Trust Model

Philippe Jaillon, Marc Roelens, Xavier Serpaggi, Hoan Vu
Ecole Nationale des Mines de Saint-Etienne, G2I Division
158 cours Fauriel 42023 Saint-Etienne, France
{jaillon,roelens,xserppagi,vu}@emse.fr

Abstract

We present here an approach for a hybrid model of trust. Our idea on the trust model is that all evidences on interactions could be used to measure the trust on required actions before taking the decision. We use the policy language proposed by Krukow et al.[2], with some slight modifications to specify our trust model.

1. Hybrid Trust Management

We found that there are two approaches for trust management (TM). The first one is the credential-based TM and the second one is the experience-based TM. In the first approach, signed credentials are used to delegate rights between users in the system. In the second one, information about past interactions is used to measure the trust level in taking decision on actions.

We present a hybrid model for TM that is required in most real applications. With this model, the decision for an action of a principal is based on his policies and all information that he holds for verifying before taking the decision: the experience information of the past interactions, the recommendation of the other principals and the credentials of interaction partner.

The idea is that we consider the system as a logical framework and the model of TM is expressed by specifying the policy language.

2. Logical Framework Management

Our approach is inspired by the logical framework for reputation systems of Krukow et al [2]. The core of this framework consists of the event-structure for observations, the policy language and the dynamic model checking for verifying the policies and required actions. The policy language is a variant of LTL logic. The decision is taken based on the verification of policies and the experience information. For example, given an observed history \( H \), and a policy \( \psi \), \( H \models \psi \) mean that the observation set \( H \) satisfy the policy \( \psi \).

For applying our approach, we also consider observations on credentials, recommendation as events. These events are created and updated in the event-structure as usual events. The following case study will explain our idea in more detail.

3. Case study on the web-mail application

We describe here a case study about the web-mail application. The context is as follows: a user would like to check his mailbox in the mail server from an untrusted computer. He has the following risks: user can not verify the certificate of mail server that denotes it is the right one he wants to connect to; he may be cheated by intruders in authenticating. The outcomes of these risks are that his login information (login/password) may be stolen by the intruder.

We propose a set of policies, which manages all interactions of the user with the mail server through networks and it could be added in the web navigator as a plug-in for TM. Firstly, we propose the following events for modeling this system; authenticate, ignore: user authenticates or refuses to authenticate the server; cert-authentic, cert-forged, cert-unknown: verified result of the server certificate being authentic or forged or unknown; recommend-ok, recommend-not-ok: recommendation of a user about the server being good or not good. We can propose now some trust policies for the user’s security:

- The user authenticates the mail server by his login/pass either if the server certificate is authentic or the mail server is always recommended as a good one:
  \[
  \psi_2 \equiv X (\text{cert-authentic}) \land G (\text{recommend-ok}) \rightarrow \text{authenticate}
  \]
- The user will never authenticate the server when his certificate is forged or when the certificate can not be verified and if there is a negative recommendation:
  \[
  \psi_2 \equiv X (\text{cert-forged}) \lor X (\text{cert-unknown}) \land G (\text{recommend-not-ok}) \rightarrow \text{ignore}
  \]
- The user will never authenticate the server if he always had ignored this action in the past:
  \[
  \psi_3 \equiv G (\text{ignore}) \rightarrow \gamma \text{ authenticate}
  \]

4. Conclusion

In this abstract, we presented our approach for a hybrid trust model by using a policy language to specify policies of the system. We will also consider the policy negotiation problem based on this trust model.

5. References