Intrusion Detection in Open Peer-to-Peer Multi-agent Systems

Shahriar Bijani and David Robertson

s.bijani@ed.ac.uk , dr@inf.ed.uk

Informatics School, University of Edinburgh. 10, Crichton St., Edinburgh, UK.

Abstract. One way to build large-scale autonomous systems is to develop open peer-to-peer architectures in which peers are not pre-engineered to work together and in which peers themselves determine the social norms that govern collective behaviour. A major practical limitation to such systems is security because the very openness of such systems negates most traditional security solutions. We propose a programme of research that addresses this problem by devising ways of attack detection and damage limitation that take advantage of social norms described by electronic institutions. We have analysed security issues of open peer-to-peer multi-agent systems and focused on probing attacks against confidentiality. We have proposed a framework and adapted an inference system, which shows the possibility of private information disclosure by an adversary. We shall suggest effective countermeasures in such systems and propose attack response techniques to limit possible damages.

Keywords: Security, Confidentiality, Multi-agent Systems, Electronic Institutions, P2P networks, Light Weight Coordination Calculus (LCC).

1 Introduction

We have focused on open peer-to-peer (p2p) multi-agent systems (MAS), in which *electronic institutions* [4] are used to form the interaction environment by defining social norms for group behaviour. An o*pen system* is a system that allows new components, which may have been created by different parties or for different objectives, not known at design time, to interact at runtime [5]. An open p2p *multi-agent system* is an *open system* in which autonomous peers can join and leave freely [4]. Open MAS have growing popularity (e.g. in social networks, e-commerce, social simulation and workflow systems) and are predicted to have many applications in the future [2]. In these open systems, peers may invent the protocols (*electronic institutions*) themselves and share them with others or use other (unknown) peers' protocols. We address confidentiality of open p2p MAS with dynamic protocols.

Although we focus on the open p2p MAS, we can extend the scope of our secrecy analysis without much difficulty to similar domains such as web services.

Even though openness in open systems makes them attractive for different new applications, new problems emerge, among which security is a key. Unfortunately

there remain many potential gaps in the security of open MAS and little research has been done in this area. The focus of the related work is mostly on mobile agents and using conventional security mechanisms (e.g. cryptography and PKI) in agent communication layer.

Traditional security mechanisms resist use in MAS directly, because of the social nature of them and the consequent special security needs[7]. Open MAS using dynamic protocols are particularly difficult to protect, because we can make only minimum guarantees about identity and behaviour of agents and conventional security mechanisms, like authentication and encryption, are at best a small (though necessary) part of the solution. We have focused on confidentiality which is an important subset of security and is critical in many applications (such as healthcare systems). To best of our knowledge, so far there are no attack detection/response systems or methods for open p2p multi-agent system that use dynamic electronic institutions.

An electronic institution is an organisation model for MAS that provides a framework to describe, specify and deploy agents' interaction environments. It is a formalism which defines peers' interaction rules and their permitted and prohibited actions. There are a few choreography-oriented languages, from which we selected LCC [6] (as an example) to implement electronic institutions. LCC (Lightweight Coordination Calculus) is based on π-calculus and logic programming to execute electronic institutions (interaction models) in a p2p style.

2 Overview of the Suggested Framework

Our suggested framework for the secrecy analysis of interaction models in an open p2p multi-agent system is shown inFig. 1. The first three steps are optional and they only will be necessary if we want to extend our work to support other open systems that do not use LCC to create their interaction protocols. We briefly describe the framework in the following steps:

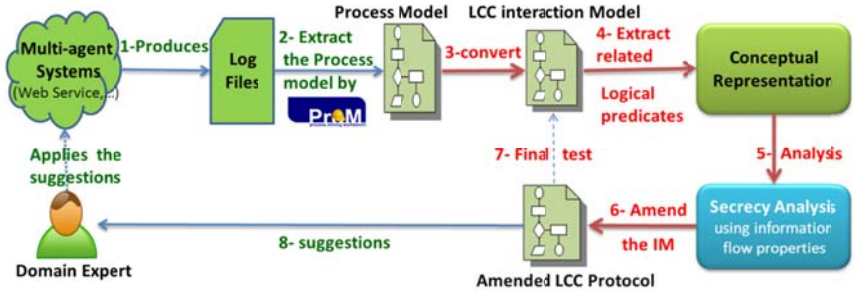

Fig. 1. A suggested framework for the secrecy analysis of open p2p multi-agent systems.

1. A multi-agent system (or a web service, a process management system …) produces log files while running.

2. The process model of the system is extracted by a process mining tool (ProM[1]).
3. The extracted process model is converted to LCC interaction models.
4. LCC interaction models are converted to a conceptual representation. (Section 3)
5. The secrecy of the conceptual representation (that represents the interaction model) is analysed using an inference system that shows what an adversary could infer from the interaction model. (Section 3)
6. The interaction model will be fixed if there is any information leak exists.
7. Steps 4 to 6 will be repeated to double check the amended interaction model.
8. The source of the information leak problem and the amended interaction model with some annotations will be sent to the domain expert of the original system.

3 Probing Attacks and Countermeasures

We analysed possible attacks on open p2p MAS as a part of our work and selected probing attack to address it. We redefine the probing attack [1] in conventional network security to be applicable in MAS. A probing attack in network security is an attack based on injecting traffic into the victim's network and analysing the results.

In our case, an adversary could infer information not only from the interaction model itself, but also from the local knowledge of other peers. An adversary could control other peers' behaviour in an interaction, by publishing a malicious interaction model. Furthermore, it could access the private local knowledge (e.g. decision rules and policies) of the victim peer by injection of facts to the peer's knowledge-base, asking queries and analysing the queries result.

The first step in our secrecy analysis is converting interaction models to simpler logical representations in order to illustrate only the related parts of the LCC code to the security evaluation. What we need for our conceptual representation is a more minimal interpretation of LCC, which reflects information leaks or helps to find knowledge leakage. We should interpret interaction models for each scenario differently, to be able to discover information leaks and consequently to achieve more accurate secrecy analyses.

After the conceptual representation of interaction models we could analyse them to detect any possibility of a probing attack. We are going to use a security type system to analyse information flow properties in LCC interaction models. Meanwhile we used the Becker's inference system [3] for *detectability*[2] to analyse secrecy, because it was compatible with our conceptual representation. Although this inference system has been created for credential-based authorisation policies (such as Datalog), with some modifications, it could also be used to detect probing attack on open MAS. We want to know if an adversary injects expressions into the agent's private knowledge-base and asks a query, what else the adversary will infer from the knowledge-base. To answer this question we used the inference system in [3].

---

[1] ProM is an open-source framework for implementing process mining tools in a standard environment (www.processmining.org). We selected it as a working example of process mining systems.

[2] Detectability (or non-opacity) is an information flow property that shows the ability to infer a specific predicate from a set of rules.

Two reasons that security problems might lead to probing attacks on choreographic systems are: (1) no distinguishing notion of private and public data in choreography languages (such as LCC) and (2) no mechanism for information leakage control in their interaction models. Hence, two countermeasures to these problems are adding some access control features to the language and secrecy analysis of interaction models. The first solution for LCC is to label information in it and to add attack prevention rules in the LCC interpreter.

The second solution for probing attacks is secrecy analysis of interaction models using techniques such as using the introduced inference system to detect injection attacks before using the interaction models. This analysis could be implemented as a separate interaction model that receives other interaction models and after extracting the corresponding logical representation, check possibility of information leak using the inference system.

4 Conclusion and Future work

We propose a programme of research that addresses secrecy of open peer-to-peer multi-agent systems by devising ways of probing attack detection and damage limitation. To analyse information leaks in these agent systems, we have suggested a conceptual representations of interaction models and adapted an inference system, which shows the possibility of private information disclosure by an adversary. Finally we have proposed two solutions to prevent and detect probing attacks in open p2p multi-agent systems. We intend to develop a security type system for LCC language to analyse information leakage in agents' interaction models. The evaluation of the suggested techniques has two stages. In the first stage, we will try to find detection and response methods for probing attacks and evaluation would be empirical by simulation of these techniques. In the case that no convincing detection method exists, we will analytically show it and disconfirm the hypotheses, as the second stage.

References

[1] R. Anderson, M. Kuhn. Tamper resistance: a cautionary note. Proc. of USENIX Workshop on Electronic Commerce 2, 1-11. 1996.

[2] A. Artikis, M. Sergot, J. Pitt, Specifying norm-governed computational societies, ACM Tran. on Computational Logic (TOCL), v.10 p.1-42, 2009.

[3] M.Y. Becker. Information Flow in Credential Systems. IEEE Computer Security Foundations Symposium (CSF), 171-185. 2010.

[4] M. Esteva, et.al. Engineering open multi-agent systems as electronic institutions. Proc. of the National Conference on Artificial Intelligence, 1999.

[5] S. Poslad, M. Calisti. Towards improved trust and security in FIPA agent platforms. Workshop on Deception, Fraud and Trust in Agent Societies. 2000.

[6] D. Robertson, Multi-agent coordination as distributed logic programming. International Conf. on Logic Programming, France, 2004.

[7] S. Robles Trust and Security. Issues in Multi-Agent Systems: the AgentCities.ES Experience, Basel, 2008.