A Decentralized Access Control Model for Dynamic Collaboration of Autonomous Peers

Stefan Craß(✉), Gerson Joskowicz, and Eva Kühn

Institute of Computer Languages, TU Wien, Argentinierstr. 8, Vienna, Austria
{sc,gj,ek}@complang.tuwien.ac.at

Abstract. Distributed applications are often composed of autonomous components that are controlled by different stakeholders. Authorization in such a scenario has to be enforced in a decentralized way so that administrators retain control over their respective resources. In this paper, we define a flexible access control model for a data-driven coordination middleware that abstracts the collaboration of autonomous peers. It supports the definition of fine-grained policies that depend on authenticated subject attributes, content properties and context data. To enable peers to act on behalf of others, chained delegation is supported and permissions depend on trust assumptions about nodes along this chain. Besides access to data, also service invocations, dynamic behavior changes and policy updates can be authorized in a unified way. We show how this access control model can be integrated into a secure middleware architecture and provide example policies for simple coordination patterns.

Keywords: ABAC · Delegation · P2P · Coordination middleware

1 Introduction

Modern distributed systems are often not managed by a single organization, but require collaboration of multiple stakeholders that provide data and offer services. Due to evolving application requirements and availability of different providers for specific tasks, distributed workflows should be dynamically configurable and enable ad-hoc coordination. Examples for such complex interactions include cloud-based business-to-business transactions, peer-to-peer (P2P) networks that enable efficient data replication, and connected smart devices.

As mutual trust cannot be assumed in such dynamic communication networks, a suitable access control model is necessary that enables participants to specify who can access their data and services. To address the flexibility of distributed systems with dynamically changing security requirements, each member shall be able to manage its own access control policy independently of others [1]. This requires an authentication concept that supports identity providers from different security domains, which may be linked to different trust levels. In order to cope with indirect access on behalf of other users, support for delegated identities is needed. For instance, a customer may want to access a company's data

B. Thuraisingham et al. (Eds.): SecureComm 2015, LNICST 164, pp. 519–537, 2015.
DOI: 10.1007/978-3-319-28865-9_28

storage via a cloud service. The company may allow a trusted cloud service to read data associated with the delegating customer, while denying direct customer access in order to make security administration simpler and more reliable.

In order to adhere to the principle of least privilege, permissions shall be specifiable in a fine-grained way. Access decisions may depend on the environmental context (e.g. previous interactions), while the administration of policies itself shall be governed with meta-level policies [2]. For instance, resource owners may delegate their administrator privileges to other trusted users, or a cloud provider may allow users to control access to their deployed services themselves.

Current security mechanisms for distributed systems usually rely on centralized servers, which limits their use to networks controlled by a unified administration. There still is a lack of powerful security models for the collaboration of autonomous peers in dynamic scenarios. Although some research has been done on decentralized authentication and authorization [3,4,5], most approaches do not model fine-grained access control policies that support content- and context-based rules as well as arbitrary forms of delegation.

In this paper, we present a flexible and expressive security concept that targets the dynamic coordination of autonomous components in a fully decentralized environment. We assume that applications are designed using a data-driven coordination model [6], which hides the complexity of remote communication and provides intelligible abstractions for service invocation and data access. Application logic is encapsulated in decoupled software components termed *peers*, whose interactions are specified declaratively. Although the security mechanisms are shown in the context of this specific architecture, the concept is applicable to any business process that is implemented using interconnected components.

We propose an extended middleware architecture for this coordination model called *Secure Peer Space* that enables decentralized authorization with support for complex delegation chains and fine-grained access control rules. Rules depend on the accessed content, the environmental context and the subject. We combine elements of attribute-based and discretionary access control, as decisions are based on authenticated attributes, while each owner of a peer may govern access to its own services and data. In contrast to usual access control concepts that place controls on few entry points, we support access control at any involved component of a workflow. The access control model is suitable for cross-organizational collaboration, as it provides a way to specify trust in attributes from distributed sources. It is also possible to depict multitenant scenarios, as users may dynamically inject sub-peers into another peer if permitted by its owner. The security mechanisms, including policy administration, are largely bootstrapped using existing coordination features of the middleware.

The paper is structured as follows: Section 2 describes the addressed coordination middleware. On top of that, Section 3 presents a security concept and a middleware architecture for the Secure Peer Space. Section 4 provides examples for the usage of this secure middleware in the form of reusable coordination patterns. Section 5 discusses the benefits of the presented approach and compares it to related work. Finally, Section 6 concludes the paper and outlines future work.