Agent-Based Privilege Negotiation for E-commerce on World Wide Web

Richard Au, Ming Yao, and Mark Looi

Information Security Research Centre
School of Software Engineering and Data Communications
Queensland University of Technology
Brisbane, Qld 4001, Australia
{w.au, m.yao, m.looi}@qut.edu.au

1 Introduction

The World Wide Web (Web) is an important channel for business-to-customer transactions in E-commerce. Most commercial organisations have the basic goal to outreach as many potential customers as possible and establish business relationships with them. Before granting privileges to access some protected resources, organisational systems must facilitate the ability to assess the trustworthiness of entities (users or applications) they encounter. For E-commerce on the Web, a typical service provider faces a wide spectrum of potential users without any pre-existing relationship. The question of interest is how these processes of trust establishment and authorisation can be conducted effectively and efficiently.

2 A New Agent-Based Authorisation Framework

Applying the concept of mobile agents, we design a new authorisation architecture that supports automated privilege negotiation in the Web environment.

Referring to figure 1, our framework consists of four main components:

- An infrastructure of domain-based security servers for trust distribution across different administrative domains [3].
- Authorisation tokens for secure delivery of user credentials [1].
- Secure Client Agent Environment(SCAE) for hosting multiple agents and providing them with execution resources and security protection [2].
- A family of privilege negotiation agents for establishing trust and authorisation.

2.1 Privilege Negotiation Agents for Distributed Authorisation

In this paper, we propose a novel family of *Privilege Negotiation Agents* which can migrate from various servers to the client's secure agent platform. These agents are trusted representatives of their parent servers and they work collaboratively in the negotiation process for trust establishment and authorisation. The family consists of three types of members:

J.M. Cueva Lovelle et al. (Eds.): ICWE 2003, LNCS 2722, pp. 68–71, 2003.

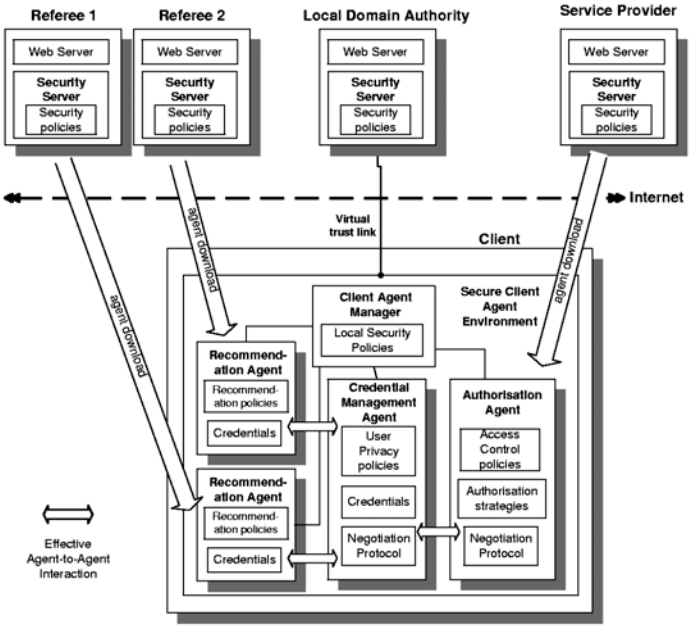

Fig. 1. Agent-based Authorisation Framework

- **Authorisation Agent(AA) from Service Provider** – It performs the enforcement of access control with functions of:
  - Assessing authorisation credentials from client.
  - Providing access control and resource information to clients.
  - Making authorisation decision.
  - Keeping authorisation states in the workflow of the access.
- **Credential Management Agent(CMA) from Client** – It works on behalf of the user and performs the following tasks:
  - Managing the credentials delivery and storage.
  - Making requests to referee servers for recommendations.
  - Enforcing user privacy policies.
- **Recommendation Agent(RA) from Referee Server** – It provides certified credentials according to its recommendation policies and CMA's request.

2.2 Advantageous Features

Our user-centred and agent-based approach to authorisation can enhance distributed access control systems in the following ways:

- User Customisation - The use of agents provides better support for heterogeneous environments as it can express more the user's context and provide more interactions with the servers.

- Security and User Privacy - Authorisation based on credentials can be of higher security than traditional identity-based systems as more user attributes are included. In our user-centred approach, the disclosure of user's credentials is highly controllable by the user. So user privacy can be well protected and anonymity can be supported.
- Dynamic extension of application functionality - The Privilege Negotiation Agents are tailor-made specifically for that particular application and they provide a powerful tool for the user to access remote services and resources in the customised way he needs.

3 Privilege Negotiation Protocols

When a new user at a browser attempts to acquire some services/resources at a destination site, he may not have sufficient, if any, privileges/credentials to gain the access. In that case, the agent-enabled Web server will start the registration process by sending an Authorisation Agent(AA) to the client secure agent platform. The AA carries along some access control policies and strategies corresponding to the user's access request. It works as an authorised and trusted representative of the service provider in the privilege negotiation process.

To illustrate the agent interactions, we use propositional symbols to express various services and credentials.

$$S \leftarrow P\ (C_1,....,C_n)$$

The above expression denotes that resource/service S has an authorisation policy $P(C_1,....,C_n)$ and P is a Boolean expression involving user credentials, $C_1,....,C_n$, required. If sufficient credentials are submitted so that P becomes true, then S is granted. It is also possible to have $C \leftarrow P(C_1,....C_n)$, which shows a policy P for combining a number of credentials into another one, C. In practice, a policy may be either *public* (i.e. can be disclosed to users at any time) or *confidential* (i.e. disclosure are restricted).

Based on the client's request for service S, AA can ask for the necessary credentials according to its authorisation policy P_{AA}.

$$\mathbf{AA} : S \leftarrow P_{AA}(C_1,....,C_n)$$

On the client platform, the Credential Management Agent(CMA) works on behalf of the user. It enforces the user privacy policies and manages credential delivery and storage, etc. CMA holds information of a finite set of credentials that are kept by the user and/or the referee servers.

$$\mathbf{CMA}: \{C_1,.....C_m\}$$

Upon receiving the credential requirements from AA, CMA can contact the appropiate referee servers and invite download of Recommendation Agents

(RA). When all the agents AA, CMA and RA are present on the client platform, they can work collaboratively and conduct privilege negotiation dynamically. RA provides recommendation (certified credential) R according to the user's request Q, his existing credentials C_m and local recommendation policy P_{RA}. (Note: C_m may be submitted by client or stored in the server repository, depending on individual system.)

RA: $R \leftarrow P_{RA}(C_m, Q)$

When necessary, RA or AA can make suggestions to CMA for inviting more RA to join in the negotiation. Based on the user privacy policy P_{CMA}, CMA can either discard or forward the recommendation R to AA as certified credential C. It is also possible to develop mechanisms to allow CMA to forward only a selected portion of R to AA and hide the other parts [4]. With CMA as an intermediary, trust establishment and authorisation can be completed without revealing irrelevant credentials to the service provider. Also user privacy can be well protected.

CMA: $C \leftarrow P_{CMA}(R)$

AA can collect a set of submitted credentials from a user, $\{C_1,....C_k\}$, and evaluate it using all the authorisation policies. When $P_{AA}(C_1,....C_n)$ becomes true, access right to service S will be granted to the client by AA itself or the service provider server. Otherwise AA can make further request to the client asking for extra credentials.

4 Future Work and Conclusion

In this paper, we have proposed a new credential-based authorisation framework using *Privilege Negotiation Agents* to enhance the authorisation service in the Web environment. For further research, we can put efforts to develop an universal set of languages with formal semantics for expressing policies and credentials for interactions between various agents and servers.

References

1. Au, R., Looi, M. & Ashley, P. (2000) *Cross-Domain One-Shot Authorisation Using Smart Cards*. Proceedings of 7th ACM Conference on Computer and Communication Security, pages 220–227.
2. Au, R., Yao, M., Looi, M. & Ashley, P. (2002). *Secure Client Agent Environment for World Wide Web*. Proceedings of Third International Conference on E-commerce and Web Technology, LNCS 2455, Springer, pages 234–244.
3. Au, R., Looi, M. & Ashley, P. (2001) *Automated Cross-organisational Trust Establishment on Extranets*. Proceedings of the Workshop on Information Technology for Virtual Enterprises(ITVE' 2001), pages 3–11.
4. Brands, S. (2002) *A Technical Overview of Digital Credentials*. URL: citeseer.nj.nec.com/brands02technical.html