Towards Flexible Credential Negotiation Protocols

Piero A. Bonatti[1], Sabrina De Capitani di Vimercati, and Pierangela Samarati[2]

[1] Dip. di Scienze Fisiche - Sezione di Informatica – Università di Napoli "Federico II"
Via Cinthia, I-80126 Napoli, Italy
bonatti@na.infn.it
[2] Dip. di Tecnologie dell'Informazione – Università di Milano
Via Bramante 65, I-26013 Crema, Italy
{decapita,samarati}@dti.unimi.it

Abstract. Accessing information over the Internet has become an essential requirement in modern economy, and unknown parties can come together on the Net and interact for the purpose of acquiring or offering services. The open and dynamic nature of such a scenario requires new protocols allowing parties to communicate and enforce security specifications related to access control conditions to be fulfilled. In this paper we discuss several issues to be investigated in the development of these flexible interaction protocols.

1 Introduction

Today's Globally Internetworked Infrastructure connects remote parties through the use of large scale networks, such as the World Wide Web. Execution of activities at various levels is based on the use of remote resources and services, and on the interaction between different, remotely located, parties that may know little about each other. In such a scenario, traditional assumptions for establishing and enforcing access control regulations do not hold anymore. For instance, a server may receive requests not just from the local community of users, but also from remote, previously unknown users. The server may not be able to authenticate these users or to specify authorizations for them (with respect to their identity). The traditional separation between *authentication* and *access control* cannot be applied in this context, and alternative access control solutions should be devised. Early approaches departing from this assumption proposed associating authorizations with keys rather than with users' identities. This family of *trust management systems* (e.g., PolicyMaker [BFL96], Keynote [BFIK98], REFEREE [CFL97]) use credentials to describe specific delegation of trusts among keys and to bind public keys to authorizations. While these approaches provide an interesting framework for reasoning about trust between unknown parties, assigning authorizations to keys may result limiting and make authorization specifications difficult to manage.

An alternative promising approach is based on the use of *digital certificates* (or *credentials*), representing statements certified by given entities (e.g., certification authorities), which can be used to establish properties of their holder

(such as identity, accreditation, or authorizations) [HFPS99]. Credential-based access control makes the access decision of whether or not a party may execute an access depend on properties that the party may have, and can prove by presenting one or more certificates (authorization certificates in [BFL96] being a specific kind of them). The development and effective use of credential based-access controls requires tackling several problems related to credential management and disclosure strategies, requiring the design of new protocols for parties to communicate what their requirements (information they request or disclose) to their counterpart. Several researchers have addressed the problem of establishing a Public Key Infrastructure (which is at the basis of credential-management); managing credentials and credential chains and developing strategies for automated trust negotiation, that is for determining the credentials to be required and released when interacting with other parties [SWW97, WCJS97a, WSJ00, YMW00, YS01, LWM01, ABFK98, BK02]

The successful use of credentials for enforcing access control, and the consequent application of all the different trust management strategies that can be though of, requires a fundamental problem to be solved: *parties must be able to communicate to others 1) what credentials/properties they enjoy and 2) what credentials/properties they require from the counterpart in order to grant them access to specific requests.* Since all these features are application-dependent and policy-dependent (both on the client's and on the server's side), the traditional protocols results too rigid and limited. It seems then useful to perform some automatic *inferences* on the parties' policies to achieve the necessary flexibility.

2 Open issues towards flexible negotiation protocols

The satisfaction of the requirements stated above, requires complementing traditional protocols with high-level flexible interaction protocols, enabling credential negotiation, credential understanding and explanation generation and handling, introducing a form of *negotiation* between clients and servers. In particular, it is important to devise how *security specifications (access rules) should be stated* in a way suitable with the new scenario; how they should *be translated for their communication* to the counterpart; and how the *parties communicate and reach consensus* in the transaction execution. Moreover, just like traditional security protocols, these new interaction protocols should give certain security guarantees (e.g., termination, correctness, no improper information disclosure).

Among the issues to be investigated, there are the following.

- *Ontologies.* Due to the openness of the scenario and the richness and variety of security requirements and credential-based properties that may need to be considered, it is important to provide parties with a means to understand each other with respect to the properties they enjoy (or request the counterpart to enjoy). Therefore, common languages, dictionaries, and ontologies must be developed [CGM99].
- *Client-side restrictions.* The traditional distinction of client and server becomes loose as every party can behave as either a client or a server depending

on the context. Also, while it is true that for each specific interaction there can be a clear distinction between the two roles, one assumption does not hold anymore: it is not only the server that establishes regulations. In traditional access control systems, clients need only to supply their identity (together with a proof for it), and servers need to support an access control system (i.e., include a system for stating and enforcing rules regulating access to their resources). Emerging scenarios require this latter ability to be supported by clients as well. Indeed, a client may—like a server—require the counterpart to fulfill some requirements. For instance, a client may be willing to release an AAA membership number only to servers supplying a credential stating that the travel agent is approved by AAA.

- *Credential-based access control languages.* Flexible and expressive languages able to express and reason about credentials need to be developed. Simple 'tuple-like' authorizations are obviously not sufficient anymore and richer languages are needed. Such languages may contain constructs to control negotiation.
- *Access control evaluation and outcome.* Users may be occasional and they may not know under what conditions a service can be accessed. Therefore, in order to make a service "usable", access control mechanisms cannot simply return "yes" or "no" answers. It may be necessary to explain why authorizations are denied, or - better - how to obtain the desired permissions.
- *Policy communication.* Since access control does not return a definite access decision, but it returns the information about which conditions need to be satisfied for the access to be granted, the problem of communicating such conditions to the counterpart arises. To fix the ideas, let us see the problem from the point of view of the server (the client's point of view is symmetrical). The naive way to formulate a credential request—that is, giving the client a list with all the possible sets of credentials that would enable the service—is not feasible, due to the large number of possible alternatives. In particular, the precise nature of the credentials might not be known in advance (as it happens with chains of credentials), and in the presence of compound credential requests such as "*one* ID *and one* membership certificate from a federated association", there may be a combinatorial explosion of alternatives, as each individual request can potentially be fulfilled in many possible ways.
- *Flow control.* Negotiations should not disclose "too much" of the underlying security policy, which might also be regarded as sensitive information. For instance, suppose that a given service is to be made accessible only to users who satisfy all the following conditions: 1) are registered at the server, 2) are US residents, 3) are members of a partner association. Instead of communicating all such requirements to the client, and therefore unrestrictedly disclosing the whole policy, the server could first ask the counterpart for her login name (prerequisite); if she is not registered, there is no reason to proceed further. The situation is particularly complicated since the information against which access control rules is evaluated can be communicated in

some cases and be considered sensitive in other cases. For instance, in the example above, the list of partner associations can be considered sensitive (and therefore used only for control at the server), or public (and therefore communicated to the user beforehand).
- *Negotiation strategy.* Credentials grant parties different choices with respect to what release (or ask) the counterpart and when to do it, thus allowing for multiple trust negotiation strategies[YS01]. For instance, an *eager* strategy, requires parties to turn over all their credentials if the release policy for them is satisfied, without waiting for the credentials to be requested. By contrast, a *parsimonious* strategy requires that parties only release credentials upon explicit request by the server (avoiding unnecessary releases).
- *Negotiation success.* The negotiation procedure should succeed whenever the policies of the two parties allow it. This aspect requires ensuring that the policy enforced by a party leads to the same result as the one communicated to the counterpart obtained from the original by removing sensitive information and conditions that could be evaluated only locally. Also, the interaction protocol between the parties must be guaranteed to terminate.

3 Conclusions and perspectives

Standard kinds of protocols will keep on playing a fundamental role in the key handling infrastructure, but they will have to be complemented by higher-level, flexible interaction protocols, enabling credential negotiation, credential understanding and explanation generation and handling. The technologies needed for such an enhanced infrastructure involve aspects of knowledge representation and reasoning, and should be made practical by adopting knowledge compilation techniques and fast, lightweight inference mechanisms. In this paper we have illustrated some issues to be investigated in this direction.

References

[ABFK98] C. Altenschmidt, J. Biskup, U. Flegel, and Y. Karabulut. Secure Mediation: Requirements and Design. In *Proc. of the 12th IFIP WG11.3 Working Conference on Database and Application Security*, Chalkidiki, Greece, July 1998.

[BFIK98] Matt Blaze, Joan Feigenbaum, John Ioannidis, and Angelos D. Keromytis. The Role of Trust Management in Distributed Systems Security. In *Secure Internet Programming: Issues in Distributed and Mobile Object Systems*. Springer Verlag – LNCS State-of-the-Art series, 1998.

[BFL96] Matt Blaze, Joan Feigenbaum, and Jack Lacy. Decentralized Trust Management. In *Proc. of 1996 IEEE Symposium on Security and Privacy*, pages 164–173, Oakland, CA, May 1996.

[BK02] J. Biskup and Y. Karabulut. A Hybrid PKI Model with an Application for Secure Mediation. In *Proc. of the 16th Annual IFIP WG 11.3 Working Conference on Data and Application Security*, King's College, Cambridge, UK, July 2002.

[BS02] P. Bonatti and P. Samarati. A Unified Framework for Regulating Access and Information Release on the Web. *Journal of Computer Security*, 2002. (to appear).

[CFL97] Y-H. Chu, Joan Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss. REFEREE: trust management for Web applications. *World Wide Web Journal*, 2(3):706–734, 1997.

[CGM99] Chen-Chuan K. Chang and Hector Garcia-Molina. Mind Your Vocabulary: Query Mapping Across Heterogeneous Information Sources. In *Proc. of the 1999 ACM-SIGMOD*, pages 335–346, 1999.

[HFPS99] R. Housley, W. Ford, W. Polk, and D. Solo. *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, rfc 2459 edition, January 1999. http://www.ietf.org/rfc/rfc2459.txt.

[JSSS01] S. Jajodia, P. Samarati, M.L. Sapino, and V.S. Subrahmanian. Flexible Support for Multiple Access Control Policies. *ACM Transactions on Database Systems*, 26(2):18–28, June 2001.

[LWM01] N. Li, W.H. Winsborough, and J.C. Mitchell. Distributed Credential Chain Discovery in Trust Management. In *Proc. of the Eighth ACM Conference on Computer and Communications Security*, Philadelphia, PA (USA), 2001.

[SWW97] K. E. Seamons, W. Winsborough, and M. Winslett. Internet Credential Acceptance Policies. In *Proceedings of the Workshop on Logic Programming for Internet Applications*, Leuven, Belgium, July 1997.

[WCJS97a] M. Winslett, N. Ching, V. Jones, and I. Slepchin. Assuring Security and Privacy for Digital Library Transactions on the Web: Client and Server Security Policies. In *Proceedings of ADL '97 — Forum on Research and Tech. Advances in Digital Libraries*, Washington, DC, May 1997.

[WCJS97b] M. Winslett, N. Ching, V. Jones, and I. Slepchin. Using Digital Credentials on the World-Wide Web. *Journal of Computer Security*, 1997.

[WSJ00] W. Winsborough, K. E. Seamons, and V. Jones. Automated Trust Negotiation. In *Proc. of the DARPA Information Survivability Conf. & Exposition*, Hilton Head Island, SC, USA, January 25-27 2000. IEEE-CS.

[YMW00] T. Yu, X. Ma, and M. Winslett. An Efficient Complete Strategy for Automated Trust Negotiation over the Internet. In *Proceedings of 7th ACM Computer and Communication Security*, Athens, Greece, November 2000.

[YS01] T. Yu and M. Winslett K.E. Seamons. Interoperable Strategies in Automated Trust Negotiation. In *Proc. of the Eighth ACM Conference on Computer and Communications Security*, Philadelphia, PA (USA), 2001.

This article was processed using the LaTeX macro package with LLNCS style