Privacy-Preserving Trust Management Mechanisms from Private Matching Schemes*

Oriol Farràs, Josep Domingo-Ferrer, and Alberto Blanco-Justicia

Universitat Rovira i Virgili
Department of Computer Engineering and Maths
UNESCO Chair in Data Privacy
Av. Països Catalans 26, 43007 Tarragona, Catalonia
{oriol.farras,josep.domingo,alberto.blanco}@urv.cat

Abstract. Cryptographic primitives are essential for constructing privacy-preserving communication mechanisms. There are situations in which two parties that do not know each other need to exchange sensitive information over the Internet. Trust management mechanisms make use of digital credentials in order to establish trust among these strangers. We present a method to reach an agreement on the credentials to be exchanged in which the parties can control the disclosure of their credential preferences. Our method is based on secure two-party computation protocols for set intersection.
Keywords: Trust Management; Secure Two-Party Computation; Set Intersection; Privacy.

1 Introduction

Interactions between parties that involve exchanging sensitive information are part of everyday life. Taking a medical test, paying with a credit card or asking for directions are examples of such interactions. In all of these cases an individual or organization $\mathcal{C}$ reveals some information to another individual or organization $\mathcal{S}$ so that $\mathcal{S}$ can provide a service to $\mathcal{C}$. Clearly, an exchange of personal information is more likely to take place if there is trust between the interacting parties. For instance, people agree on revealing medical data to a doctor in a medical center, but not to anyone or anywhere. These interactions are easy to carry out face to face and in a

* This work was partly supported by the Government of Catalonia under grant 2009 SGR 1135, by the Spanish Government through projects TIN2011-27076-C03-01 "CO-PRIVACY" and CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", and by the European Comission under FP7 project 'Inter-Trust". The second author is partially supported as an ICREA Acadèmia researcher by the Government of Catalonia; he is with the UNESCO Chair in Data Privacy, but he is solely responsible for the views expressed in this paper, which do not necessarily reflect the position of UNESCO nor commit that organization.

specific context, but they are challenging if performed over the Internet, where personal identification is not obvious and the physical context is simply not there.

A first approach is securing the communication using cryptographic protocols. Using these techniques in combination with public key infrastructures provides users interacting with remote parties with the certainty that they are communicating with the real service provider. Furthermore, encrypting communication prevents third parties from eavesdropping on the transmitted contents. This has been the basis of secure digital communications and e-commerce, but recent reports show that authentication is not always enough for users to trust service providers [16, 22].

The special Eurobarometer on data protection and electronic identity [22] shows that the majority of Europeans are concerned about their behavior being recorded via payment cards, mobile phones or mobile Internet. Moreover, 43% of the respondents claim they have been asked more personal information than necessary in order to access online services.

Therefore, there is a need to design new access control systems in which not only the identity of the parties is revealed and assured, but trust is built through the exchange of valid credentials that contain attributes of the parties. Trust management mechanisms make use of digital credentials in order to establish trust between strangers. Trust negotiation schemes are protocols for establishing trust between parties unknown to each other through the exchange of credentials and personal information; in such negotiation protocols, the disclosure of this information is performed according to access control policies determined by the parties.

Trust management is a building block of many industry-led frameworks. One example is the Interoperable Trust Assurance Infrastructure (Inter-Trust, [11]), a project that seeks to develop a framework to support trustworthy applications in heterogeneous networks and devices, based on the enforcement of interoperable and changing security policies. Trust negotiation (Fig. 1) is essential in Inter-Trust to reach agreements on the security policies, the so-called Service Level Agreements (SLAs). Inter-Trust will incorporate trustworthiness by integrating legal, social and economic concerns, thereby allowing applications and devices to negotiate and be constrained by such concerns.

A critical issue in trust management is to preserve the privacy of the users. During the trust establishment process, the parties can try to learn information about each other. On the one hand, the service requesters can try to obtain information about the preferences of the service providers:

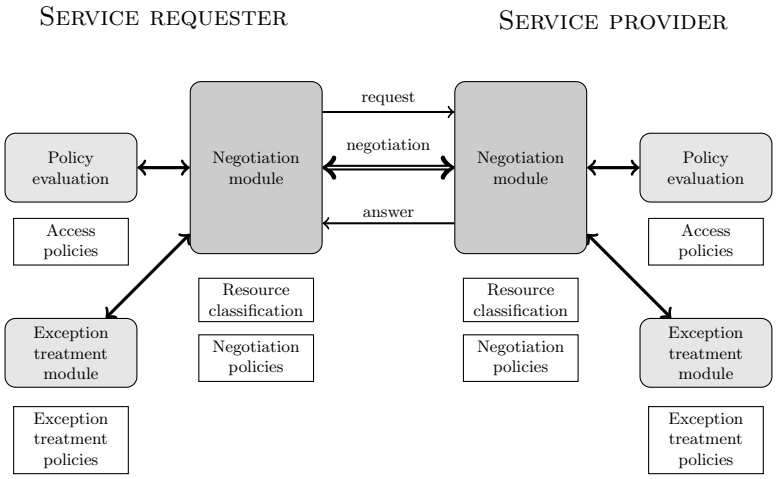

Fig. 1. Negotiation module of Inter-Trust

if the requesters indicate their wish to use specific options, the server is forced to show the different acceptable options. Since the revealed options may reflect the business model and the target customers considered by the provider, service providers are reluctant to show full descriptions of their access policies. On the other hand, requesters do not want to provide information on the credentials they own unless those credentials are essential for the transaction.

In summary, service providers are reluctant to show their access policies, and clients want to disclose as little private information as possible. Therefore, during the trust establishment process no party should learn any information about the access policies or preferences of the other parties beyond what is strictly required for trust establishment. Solutions based on trust negotiation mechanisms [7, 9, 13–15, 19, 23, 25] control the disclosure of user preferences by showing the access control policies in a sequential way. However, trust negotiation mechanisms are oriented to controlling credential disclosure, but the users may obtain information on the access control policies by playing with the system. Trust management mechanisms based on secure multiparty computation [17, 20, 27] provide higher privacy protection.

1.1 Our Results

We address the problem of constructing a privacy-preserving mechanism for choosing the credentials to be exchanged. Moreover, we consider that privacy preservation should be achieved as effortlessly as possible. Therefore, our goal is to come up with an efficient and privacy-preserving mech-

anism to determine the optimal set of informations to be disclosed, according to the preferences of the two parties. We present a method that is based on secure two-party computation protocols for set intersection. Specifically, it is constructed from the private matching schemes in [8].

In our proposal, the client sends a list of options to the server in a private way. Each option is a combination of credentials the client would agree to show. The server has a correspondence list that, for each accepted combination of client credentials, specifies the credentials the server would show. Using secure multiparty computation techniques, client and server compute the matching options. Then the server sends to the client the options that match the client's preferences. In this way, the server does not learn the preferences of the client, and the client only learns the specific access policies that match her selected options. Using the Paillier homomorphic cryptosystem [21], the total number of exponentiations needed is $O(s + t \ln \ln s)$, where s and t are the number of options specified by the client and the server, respectively.

The rest of this paper is organized as follows. In Section 2 we present an introduction to trust management. Section 3 is devoted to private matching schemes. We present our results in Section 4. Section 5 lists conclusions and open problems.

2 Trust Management

Remote communications over the Internet often require the interacting parties to trust each other, especially when the communication involves the exchange of private, confidential, or sensitive information. Traditional approaches to establish trust assume that the parties are known to each other before the communication takes place. Organizations often sign a SLA and collaboration contracts before engaging in the exchange of services and information. This approach is not always possible, because the assumption that the parties are known to each other is not always true, especially in open environments such as the Internet and the Web [25].

Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are cryptographic protocols that provide trust and security to communications over the Internet. These protocols begin with a negotiation or *handshake* phase in which the two parties (normally a client and a server) agree on an encryption algorithm and a shared key to encrypt the communication. Also, during this phase the two parties exchange digital certificates in order to authenticate each other. Even though the use of TLS is widespread, users do not fully trust Internet service providers, as

discussed in the previous section. Therefore, there is a need to improve existing strategies and/or devise new methods for establishing trust.

More recent approaches to establishing trust are the *Automatic Trust Negotiation* (ATN) protocols. ATN is based on the exchange of digitally signed credentials to establish trust and make access control decisions. Digital credentials are an extension of traditional electronic certificates that only prove the identity of a user. Credentials can include additional attributes, and hence they can certify more properties of that user, such as age, permission to perform a certain activity, membership to a certain organization, etc. In the full version of this paper we provide an introduction to cryptographic credentials, access control policies, negotiation techniques, and secure multiparty computation.

3 Private Set Intersection

Secure multiparty computation allows a set of parties to compute a joint function of their inputs in a secure way without requiring a trusted third party. During the execution of the protocol the parties do not learn anything about each other's input except what is implied by the output itself.

There are two main adversarial models: honest-but-curious and malicious. In the former model, the players follow the protocol instructions but try to obtain information about other players' inputs from the messages they receive. In the latter model, the adversary may deviate from the protocol in an arbitrary way. Aumann and Lindell [1] introduced a new model, the covert adversary model. A covert adversary may deviate from the protocol in an attempt to cheat, but such deviations are detected by honest parties. In this context, the parties may be considered rational, that is, acting according to their interests. In game-theoretic terms, it is assumed that players only try to maximize their utility functions; hence, all possible deviations from the correct protocol execution have this goal.

The intersection of two sets can be obtained by using the generic constructions based on Yao's garbled circuit [26]. This technique is very generic, because it allows computing any arithmetic function, but for most of the functions it is inefficient. Many of the recent works on two-party computation are focused on improving the efficiency of these protocols for particular families of functions. Freedman, Nissim, and Pinkas [8] presented a more efficient method to compute the set intersection that was called *private matching scheme*. The idea of Freedman, Nissim, and Pinkas [8] was used in many other works to improve the computation of set operations. Kissner and Song [12] presented secure multiparty compu-

tation protocols for computing set intersection, multi-set intersection and other combinatorial operations. They presented constructions for honest-but-curious adversaries and malicious adversaries. Hazay and Lindell [10] presented a construction that is secure in the covert model. There are also other interesting constructions, such as [4, 18].

4 A Privacy-Preserving Trust Management Scheme

In this section we present a new mechanism for privacy-preserving trust management. We consider the following situation. A client $\mathcal{C}$ wants to buy a service from a server $\mathcal{S}$. $\mathcal{S}$ needs some personal and financial information about $\mathcal{C}$ to perform the transaction. However, $\mathcal{C}$ is reluctant to show private information to $\mathcal{S}$, because $\mathcal{C}$ is not sure that $\mathcal{S}$ trustworthy.

The mechanism we construct is a protocol based on the private matching scheme of Freedman, Nissim, and Pinkas [8]. Our protocol is secure in the honest-but-curious model.

Our proposal allows parties $\mathcal{C}$ and $\mathcal{S}$ to agree on the information they have to exchange to perform the transaction in a private way. Broadly speaking, $\mathcal{C}$ first sends an encrypted message to $\mathcal{S}$ that declares which credentials and personal information she would be inclined to reveal to $\mathcal{S}$. $\mathcal{S}$ cannot read the message, but he can create an encrypted message containing the options declared by $\mathcal{C}$ in which he agrees, and the information $\mathcal{S}$ would reveal in each case. The interest of our protocol lies in the protection of the preferences of each party. That is, $\mathcal{S}$ does not learn the preferences of $\mathcal{C}$, and $\mathcal{C}$ only learns the specific access policies that match her selected options.

Let $E_{\mathcal{C}}$ and $E_{\mathcal{S}}$ be the domains of credentials and personal data of $\mathcal{C}$ and $\mathcal{S}$, respectively. Define $D_{\mathcal{C}} = \mathcal{P}(E_{\mathcal{C}})$ and $D_{\mathcal{S}} = \mathcal{P}(E_{\mathcal{S}})$, where, for any set A, $\mathcal{P}(A)$ is the power set of A.

First $\mathcal{C}$ defines different combinations of elements from $E_{\mathcal{C}}$ that she would be ready to show to $\mathcal{S}$. Let $X = \{a_1, \ldots, a_s\} \subseteq D_{\mathcal{C}}$ be the set of such options. Independently, $\mathcal{S}$ defines $Y = \{(b_1, c_1), \ldots, (b_t, c_t)\} \subseteq D_{\mathcal{C}} \times D_{\mathcal{S}}$, the acceptable combinations $(b_i, c_i) \in D_{\mathcal{C}} \times D_{\mathcal{S}}$ according to his preferences. That is, for every acceptable combination of elements b_i from $D_{\mathcal{C}}$, $\mathcal{S}$ would show $c_i \in D_{\mathcal{S}}$. Observe that $(b_i, c_i) \neq (b_j, c_j)$ for every $1 \leq i < j \leq s$, but b_i and b_j (or c_i and c_j) may be equal.

Our scheme can be constructed by means of the Paillier cryptosystem [21]. It exploits its homomorphic property whereby, given three elements m_1, m_2, m_3, it is possible to compute efficiently $Enc(m_1 + m_2)$

and $Enc(m_1 \cdot m_3)$ from $Enc(m_1)$, $Enc(m_2)$, and m_3. Our protocol is as follows:

1. $\mathcal{C}$ computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$.
2. $\mathcal{C}$ sends $Enc(p_0), \ldots, Enc(p_s)$ to $\mathcal{S}$, where p_i is the coefficient of degree i of p.
3. For every $1 \leq j \leq t$, $\mathcal{S}$ picks a random element $r_j \in \mathbb{Z}_n$ and computes $Enc(r_j \cdot p(b_j) + (b_j||c_j))$. Then $\mathcal{S}$ sends the ciphertexts to $\mathcal{C}$.
4. $\mathcal{C}$ decrypts the t ciphertexts.

The result of each decryption is an element from X attached to an element of $D_{\mathcal{S}}$ or a random element.

4.1 Discussion

The parameters for the Paillier cryptosystem are $n = p \cdot q$, where p and q are large primes satisfying the properties in [21]. Then we describe $X \in \mathbb{Z}_n$ and $Y \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$. A way to encode an option in $\mathbb{Z}_n$ is the following. First, we establish an order among the credentials. Given an option $\{\text{cred}_{i_1}, \text{cred}_{i_2}, \ldots, \text{cred}_{i_u}\}$ for some $i_1 < i_2 < \ldots < i_u$, we consider $x = \sum_{j=1}^{u} 2^{i_j}$. If the domain $D_{\mathcal{C}}$ (or $D_{\mathcal{S}}$) is much larger than the number of realistic options, we can use a hash function [8]. The amount of exponentiations needed is $O(s \cdot t)$, and it can be reduced to $O(s + t \ln \ln s)$ [8].

The protocol is secure in the honest-but-curious adversary model. Following [8] we can create a protocol that is secure in the malicious adversary model by means of zero-knowledge proofs. The resulting protocol is much less efficient.

We consider that the previous solution is to be deployed in the typical client-server context, where the client is usually at a disadvantage. Hence, we offer higher protection to the client's privacy than to the server's privacy. However, there are other situations in which we need to guarantee a more equitable treatment. In this case, private matchings also provide a natural solution for privacy-preserving trust management. A solution would be a private matching in which the inputs contain the preferred options about one's own credentials and the other party's credentials. That is, $X, Y \subseteq D_{\mathcal{C}} \times D_{\mathcal{S}}$. A solution along this line was presented in [17].

In this work we present a method for agreeing on the credentials to be exchanged, but we do not analyze the way the credentials are exchanged and disclosed. There are many schemes for *fair exchange* of information between different parties. Some recent proposals consider schemes that are secure in the covert model, as for instance [3, 5, 6].

5 Related Work

Yao *et al.* [27] presented Point-Based Trust, a trust management mechanism built from a tailored secure multiparty computation protocol. The owner of a resource values the amount of sensitive information of each credential, and the output of the protocol provides an acceptable combination of the credentials that minimizes the owner's privacy loss. A drawback of this scheme is that this quantitative approach does not take into account the dependencies among credentials. For instance, a credential A may be useless without a credential B, or A and B may contain the same information.

In a privacy-reconciliation protocol [17, 20], each party holds a private input set in which the elements are ordered according to the party's preferences. The goal of a reconciliation protocol on these ordered sets is to find all common elements in the parties' input sets that maximize the joint preferences of the parties. The main drawback of these schemes is efficiency. The computation of the best option is, in general, a hard problem and so the protocols are less efficient than the scheme presented here. Moreover, adding privacy protection to reconciliation protocols can increase their running time by two orders of magnitude [17, 24].

6 Conclusions

In this paper we have presented a privacy-preserving mechanism for trust management. This work is restricted to the two-party case. Given the preferences of each party on credential disclosure, our method provides a proposal on the credentials to be exchanged that is consistent with the parties' preferences. The privacy of the parties is preserved because their preferences are protected by a secure two-party computation protocol for set intersection that is secure in the honest-but-curious model.

Future work might consider the combination of this trust management method with fair exchange mechanisms and the integration of these building blocks into more general frameworks. Moreover, it would be interesting to extend this construction to the covert adversarial model.

References

1. Y. Aumann and Y. Lindell, "Security against covert adversaries: efficient protocols for realistic adversaries", in *Journal of Cryptology*, 2010, 23(2), pp. 281–343.
2. F. Autrel, F. Cuppens, N. Cuppens-Boulahia, and C. Coma, "MotOrBAC 2: a security policy tool", in *Third Joint Conference on Security in Networks Architectures and Security of Information Systems (SARSSI)*, 2008, pp. 273-287.

3. L. Buttyán and J.-P. Hubaux, "Rational exchange - a formal model based on game theory", in *WELCOM*, 2001, pp. 114–126.
4. D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, "Efficient robust private set intersection", in *ACNS*, 2009, pp. 125–142.
5. J. Domingo-Ferrer, "Rational privacy disclosure in social networks", in *MDAI*, 2010, pp. 255–265.
6. J. Domingo-Ferrer, "Coprivacy: an introduction to the theory and applications of co-operative privacy", *SORT-Statistics and Operations Research Transactions*, special issue, pp. 25–40, 2011.
7. C. Dong and N. Dulay, "Privacy preserving trust negotiation for pervasive healthcare", in *Pervasive Health Conference and Workshops*, 2006, pp. 1–9.
8. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection", in *EUROCRYPT*, 2004, pp. 1–19.
9. K. B. Frikken, J. Li, and M. J. Atallah, "Trust negotiation with hidden credentials, hidden policies, and policy cycles", in *NDSS*, 2006.
10. C. Hazay and Y. Lindell. "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries", in *TCC*, 2008, pp. 155–175.
11. Interoperable Trust Assurance Infrastructure (Inter-Trust). EU Project FP7-ICT 317731, 2012-2014. `http://www.inter-trust.eu`
12. L. Kissner and D. X. Song, "Privacy-preserving set operations", in *CRYPTO*, 2005, pp. 241–257.
13. A. J. Lee, M. Winslett, J. Basney, and V. Welch, "Traust: a trust negotiation based authorization service", in *iTrust*, 2006, pp. 458–462.
14. A. Lee, M. Winslett, and K. Perano, "TrustBuilder2: a reconfigurable framework for trust negotiation", in *Third IFIP WG 11.11 International Conference on Trust Management (IFIPTM)*, 2009, pp. 176–195.
15. J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials", in *ACM Trans. Inf. Syst. Secur.*, 13(1), art. no. 2, 2009.
16. MEF Global Privacy Report 2013.
17. U. Meyer, S. Wetzel, and S. Ioannidis, "Distributed privacy-preserving policy reconciliation", *ICC*, 2007, pp. 1342–1349.
18. A. Miyaji and M. S. Rahman, "Privacy-preserving two-party rational set intersection protocol", in *Informatica*, 36(2):277–286, 2012.
19. W. Nejdl, D. Olmedilla, and M. Winslett, "PeerTrust: automated trust negotiation for peers on the semantic web", in *Secure Data Management*, 2004, pp. 118–132.
20. G. Neugebauer, L. Brutschy, U. Meyer, and S. Wetzel, "Design and implementation of privacy-preserving reconciliation protocols", in EDBT/ICDT Workshops, 2013, pp. 121–130.
21. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes", in *EUROCRYPT*, 1999, pp. 223-238.
22. "Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union", June 2011
23. A. Squicciarini, E. Bertino, E. Ferrari, F. Paci, and B. Thuraisingham, "PP-trust-X: a system for privacy preserving trust negotiation", in *ACM Trans. Inf. Syst. Secur.*, 10(3), art. no. 12, 2007.
24. J. Voris, S. Ioannidis, S. Wetzel, and U. Meyer, "Performance evaluation of privacy-preserving policy reconciliation protocols", in *POLICY*, 2007, pp. 221–228.
25. W. H. Winsborough, K. E. Seamons, and V. E. Jones, "Automated trust negotiation", in *DISCEX*, 2000, vol. 1, pp. 88-102.

26. A.C.-C. Yao, "How to generate and exchange secrets", in *FOCS*, 1986, pp. 162–167.
27. D. Yao, K. B. Frikken, M. J. Atallah, and R. Tamassia, "Point-based trust: define how much privacy is worth", in *ICICS* , 2006, pp. 190–209.