Trust Realisation in Multi-domain Collaborative Environments

Oluwafemi Ajayi, Richard Sinnott and Anthony Stell
National e-Science Centre
University of Glasgow
G12 8QQ, United Kingdom
{o.ajayi, r.sinnott, a.stell}@nesc.gla.ac.uk

Abstract

In the Internet-age, the geographical boundaries that have previously impinged upon inter-organisational collaborations have become decreasingly important. Of more importance for such collaborations is the notion and subsequent nature of trust - this is especially so in Grid-like environments where resources are both made available and subsequently accessed and used by remote users from a multitude of institutions with a variety of different privileges spanning across the collaborating resources. In this context, the ability to dynamically negotiate and subsequently enforce security policies driven by various levels of inter-organisational trust is essential. In this paper we present a dynamic trust negotiation (DTN) model and associated prototype implementation showing the benefits and limitations DTN incurs in supporting n-tier delegation hops needed for trust realisation in multi-domain collaborative environments.

1 Introduction

As the world becomes a global village where the increasing need to share and access resources becomes more apparent, so also is our need to establish trust between parties across organisation boundaries. Although we have achieved some mastery in controlling access to resources that are within our autonomy, we are yet to come to grasp with distributed access control where collaborating remote users and institutions are involved. Existing distributed access control solutions include the use of centralised access control lists where all collaborating partners come together to negotiate and agree on privileges amongst other things on access to shared resources. Other solutions involve delegating some responsibility of access right management to trusted remote individuals in assigning privileges to their (remote) users [1, 2].

Often these solutions, which entail negotiations and delegations are constrained by organisations, people and static rules. These constraints often result in a lack of flexibility in what has been agreed, or difficulty in reaching agreement or once established, in maintaining agreements. Similarly, these solutions often reduce the autonomic capacity of collaborating organisations because of the need to satisfy collaborating partners demands and thereby increase security risks or reduce the quality of security policies.

These solutions bring to the forefront the issue of trust. Specifically trust realisation between organisations, individuals, entities or systems that are present in multi-domain authorities and multi-policy enforcement points. One approach that promises trust realisation is trust negotiation [3]. Trust Negotiation provides a means of establishing trust between strangers (non trusted entities) through an iterative but cautious disclosure of digital credentials [4, 5].

In this paper we review and analyse the dynamic trust negotiation (DTN) model[6] to show the effect and limitation of n-tier delegation hops for trust realisation in multi-domain collaborative environments. We would show how n-tier delegation hops help to limit the disclosure of access control policies during trust negotiations. In Section 2 we review the dynamic trust negotiation (DTN) model. Section 3 introduces and discusses the benefits and limitations of *circles of trust* and *trust contracts*. Section 4 shows how DTN limits access control disclosure. Experimental analysis of DTN is introduced in Section 5 and Section 6 presents our conclusions.

2 Dynamic Trust Negotiation

Dynamic trust negotiation (DTN) introduced by [6], is the process of realising trust between strangers or two non-trusting entities, e.g. institutions, through locally trusted intermediary entities. Trust is realised when an entity delegates its digital credentials to trusted intermediary entities through which it can interact with non-trusted entities. This intermediary entities can in

6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)
0-7695-2841-4/07 $25.00 © 2007 IEEE

turn delegate to other intermediary entities resulting in what we call n-tier delegation hops. The trust negotiation process involves trust delegations through intermediary trusted entities on behalf of non-trusting entities. Any entity can serve as a negotiator for other entities provided it is trusted by the two non-trusting entities or by their intermediaries.

DTN explores how credentials can be negotiated as the basis to support collaborative research between autonomous, distributed resources. It addresses the heterogeneous and autonomous issues of trust management like credentials and policies in multi-domain environments. DTN negotiates credentials between trusted parties also known as a *circle of trust* COT [6], who act as mediators on behalf of strangers and thus bridge trust gaps. This bridge also reduces the risk associated with disclosing policies to strangers.

As an example of *circle of trust*, consider the following scenario. Alice from the Glasgow Royal Infirmary hospital - hereafter referred to as domain GRI - is an investigator on a cancer clinical trial. She wants to recruit patients onto specific trials and in doing so needs to query patient consented health records in Scotland. To achieve this, she logs in onto the trial portal and her credentials (privileges/attributes/roles...) are pulled from her domain. The trial portal initiates a credential negotiation request with all other domains that GRI trust such as Southern General Glasgow hospital (SGG). SGG returns patient records that satisfies GRI request based on Alice's credentials and delegated privileges at SGG. SGG also negotiates with other domains it trust such as RIE using Alice's SGG delegated privileges. Similarly, Royal Infirmary Edinburgh (RIE) negotiates with other domains it trust using SGG's RIE delegated privileges. Thus GRI, SGG, RIE are *trust pathways*. The request process continues with nodes joining the trust pathways until all possible trust paths are exploited. These negotiated credentials such as $RIE.investigator$ are forward to GRI, which then makes query request with these credentials on behalf of Alice.

$$\begin{aligned} GRI.investigator &\leftarrow Alice \\ GRI.circleOfTrust &\leftarrow SGG \cup SGH \cup GRH \\ SGG.circleOfTrust &\leftarrow RIE \cup IRH \\ GRI.investigator &\leftarrow SGG.delegatedInvestigator \\ &\qquad \cap RIE.investigator \end{aligned}$$

where Southern General Hospital is referred to as SGH; Gartnavel Royal Hospital as GRH; and Inverclyde Royal Hospital as IRH.

Digital credentials, which are similar to their paper counterpart are digital assertions about a credential owner signed by the credential issuer. Most digital credentials today are implemented as X.509 certificates [7]. The credential is signed using the issuer's private key and the signed credential is verified with the issuer's public key. A credential contains attributes that describe properties of the owner asserted by the issuer. Credentials also contain the public key of the credential owner through which the owner can demonstrate its ownership by the corresponding private key. Negotiating these sensitive credentials without any human intervention is the basis of trust establishment [3, 8].

We define trust in the context of access control as possession of authentic and valid credentials necessary for access control at an end point. An end point is a target with access control policies defined by the target resource providers. A credential is either valid and authentic or only authentic. Authentic credential implies a verifiable and un-tampered credential, while a valid credential implies a semantically correct credential that is acceptable, useable and tenable to an end point. A satisfiable credential is a valid credentials that satisfies an access policy. Trust negotiation aims at delivering valid credential that are both authentic and able to satisfy an access policy.

3 Negotiating Access Control Policies

3.1 Circle of Trust

In the DTN model, the concept of *circle of trust (COT)* [6, 9] for trust negotiation was introduced. The COT shown in figure 1 is a network of locally trusted intermediary peers that a peer (or entity) trust, collaborates with through one or more trust-contracts between each peer. A trust contract is an agreement that exists between two entities. This sphere of trusted peers enable interactions between peered and non-peered domains.

Through COT trust can be realised. Consider two peers P_1 and P_2, where P_1 is a requester and P_2 is a resource provider in another domain. P_1 and P_2 has $\{P_3, P_4, P_6, P_7\}$ and $\{P_3, P_4, P_5\}$ in their COT respectively. For P_1 to access P_2 resources, they will need to be trusted by P_2. In addition, P_2 will need to understand and trust credentials from P_1. Since P_1 has trust relationships with $\{P_3, P_4\}$, which are also in trust relationship with P_2, P_1 will initiate a trust negotiation with P_2 through $\{P_3, P_4\}$. Hence trust is realised by exploring overlapping COTs between P_1 and P_2.

$$P_1 \leftarrow (P_3 \vee P_4) \leftarrow P_2$$

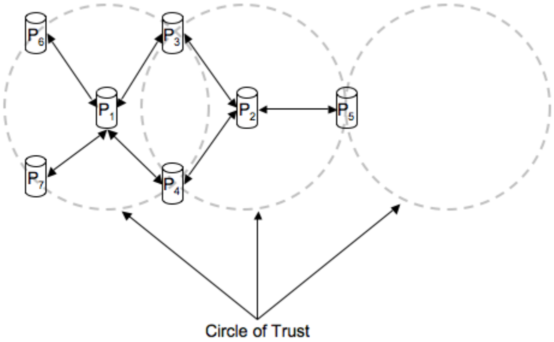

Figure 1: Circle of Trust

That is trust is realised between P_i and P_j when:

$$P_i \leftarrow P_j : \quad COT(P_i) \cap COT(P_{i+1}) ... \cap COT(P_j) \neq \{\}$$

COT improves the likelihood of successful negotiations as peers can cache trust chains from previous negotiations, which will reduce likelihood of future negotiations failing. The cache can also speed up future trust negotiations. However, this additional benefit of COT is yet to be explored in our current model and our experiment analysis in section 5 exclude this improvement.

As will be seen in section 5, the advantages of having COT is quickly overshadowed as the number of overlapping COT increases. This is because the more hops you have, the less likely peers will be delegating privileges in open decentralised collaborative systems.

Despite this limitation, COT provides an additional benefit. Overlapping COTs can help to abstract virtual organisations through which trust can be discovered and realised dynamically. In virtual organisations, relational hierarchy often exist, which can be modelled over the underlying COTs.

3.2 Trust Contract

The presence of multiple domain authority and policy enforcement introduces a policy semantics divide between domains, that is knowing that $org1.investigator = org2.investigator$. Trust contracts $($TC)[6] are static agreement between two peers that map credentials between domains. Trust contracts provide one mechanism to overcome this semantic issue of what a credential from one domain means (or should mean) in another domain. Trust contracts require of course that overlapping COTs exist.

One approach to modelling this relationships is through non-negative, bi-directional, acyclic graph as shown in figure 2. The network is denoted as G(V,E), which abstracts trust negotiation that augment an authorisation layer. The graph itself represent an abstract model of a collaborative environment.

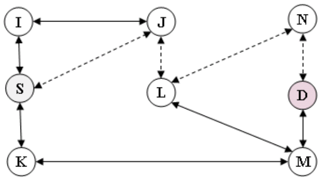

Figure 2: A network of collaborating health organisation

The Node set V is an abstraction of an autonomous domain in a network of domains. A node refers to an end point in a communication chain and consists of security credentials. The Edge set E represents the direction of trust, which consists of policies and constraints. The Edge also signifies the existence of a Trust-Contract (TC) between two Nodes, which is shown as a bi-directed arc between two Nodes. A tc is an agreement between two nodes (u, v) that states the mapping/relationship between two credentials (c^u, c^v). That is:

$$tc = (u, v) \text{ where } u, v \in V$$

That is,

$$f : c^u \rightarrow c^v : tc \mapsto f(tc)$$

A *set* of $tc \in TC$ exists between two nodes when more than one credential mapping is agreed between them, that is:

$$TC = (\{u_0, v_0\}, \{u_1, v_1\}, ..., \{u_k, v_k\})$$

3.2.1 Credential Equivalence

Trust contracts was introduced as possible solution to credential equivalence problem of resource sharing among autonomous domains. Credential (R) equivalence span semantics and heterogeneity issues. TC credential equivalence are based on the following rules.

1. Transitive membership rule:

   $R \leftarrow R_1$ and $R_1 \leftarrow R_2 \Rightarrow R \leftarrow R_2$

   This rule means that R_1 is a member of R and R_2 is a member of R_1, then R_2 is a member of R. As an example,

   $org1.investigator \leftarrow org2.healthpractitioner$
   $org2.healthpractitioner \leftarrow org3.specialist$
   $\Rightarrow org1.investigator \leftarrow org3.specialist$

6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)
0-7695-2841-4/07 $25.00 © 2007 IEEE

2. Linking delegation rule: $R \leftarrow R_1 \cdot R_2$

   This rule means an entity that has R_2 can act as R if the entity also has R_1. As an example,

   $org1.investigator \leftarrow org1.nurse \cdot org1.clinician$
   $org1.nurse \leftarrow org2.nurse$
   $org1.clinician \leftarrow org2.clinician$
   $org2.nurse \cdot org2.clinician \leftarrow org3.investigator$
   $\Rightarrow org1.investigator \leftarrow org3.investigator$

3. Intersection rule: $R \leftarrow R_1 \cap \cdots \cap R_k$ implies an entity that has $R_1, R_2, ...,$ and R_k is a member of R. At most times the least upper bound of the intersections is inferred.

4 Limiting Disclosure of Access Control Policies

In trust negotiation, peers limit what credentials are disclosed by means of various negotiation strategies. In [3], two strategies were proposed: *eager* and *parsimonious*. In eager negotiation strategy requires a party to discloses all of its credential to the other non-trusted party right at the initiation of a negotiation. The benefit of this strategy is that it assures a negotiation will succeed where successful negotiation is possible. Successful negotiation refers to the point when all credential disclosure policies are satisfied. This strategy however discloses more credentials than are potentially necessary thereby reducing party privacy. On the other hand, the parsimonious negotiation strategy enables a party to disclose its credential only after it has been requested and after necessary disclosure policy for that credential has been satisfied. This strategy increases party privacy and reduces the risk of unnecessary credential disclosure. However, this strategy can result in credential negotiation deadlock as explained in [10], which occurs whenever there is cyclic credential interdepency.

A solution to the problem of disclosing sensitive credentials is to limit what is disclosed to a total stranger and to gradually establish trust [11]. In dynamic trust negotiation (DTN), credentials are only disclosed to intermediary parties, which are trusted with the expectation that privileges would be delegated to it that wouldn't be directly to non-trusted parties. Further as negotiations take place from one intermediary party to another, the privacy of the requester is even more protected.

Similarly by the nature of trust contracts, it implies that credentials should not be unnecessarily disclosed, as both parties are aware of their contract. These contracts limit what credentials can be accepted and which credential can be delegated. Trust can only be negotiated within the constraints of these contracts. However these constraints only hold during party interactions and do not restrict what inferences parties can make with credentials during negotiations. These inferences enable parties to compute inter-contract relationships, which can subsequently improve the likelihood of successful negotiations.

5 Experimental Results

Several experiments were conducted in a simulated P2P environment to further analyse the DTN model and it's associated properties. Our simulator was ran on a dual 2.4GHz Xeon processor machine with 2GB of memory running Scientific Linux OS. We simulated various scale of interconnected P2P systems of up to 1,000 nodes with various degree of overlapping COTs. In all conducted experiments we achieved similar negotiation effect. In this paper we present results from experiments of 2 to 14 overlapping COTs P2P system.

Peers in the simulator are autonomous, each with unique node properties like services, resources, address, etc. Each peer in our simulation has randomly chosen number of credentials (X.509 certificates) with a maximum of 20 in their local security infrastructure e.g. an LDAP server. Each peer has randomly chosen nodes in it's COT, without any priorities or hierarchies between nodes. Randomly generated number of trust-contracts tc: $1 \leq tc \leq thresh$ are established between each peer and peers that exist in their COT. Where $thresh$ is a threshold percentage of credentials in each peer LDAP. The COT and tc are used in each peer randomly generated access policy rule. Every peer has a deny rule for any remote credential from non-COT peers and also for any non-tc remote credential from COT peers.

Randomly two peers P_i and P_j, $i \neq j$ were chosen for each trust negotiation. P_i initiates a request with its local credential, $C_i^{P_i}$ for P_j's resource (i.e. credential). The request is made to all peers in P_i's COT. The result of each trust negotiation is recorded at the P_j. We run 10,000 negotiations divided into 50 rounds for each simulation and results were collated for each simulation. Each data point shown in the following figures represents the average of 20 simulations with different random seeds.

Figure 3 shows the result when the number of COT involved in the trust negotiation increases. The number of successful negotiations at the target fell exponentially to an asymptotic state. Similarly failed negotiations at the target shows that the number of negotiations reaching the target is rapidly affected by the

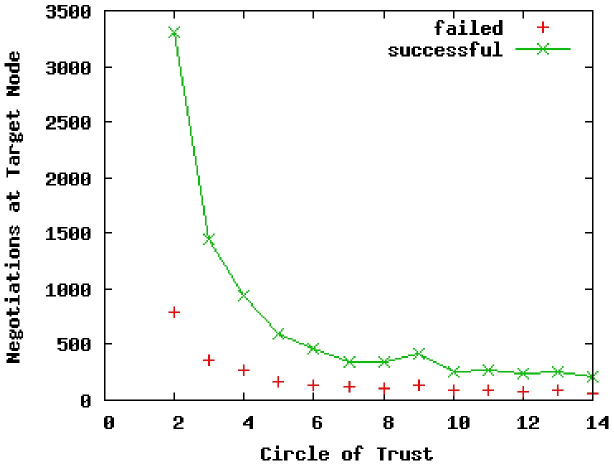

Figure 3: Circle of trust vs. negotiations

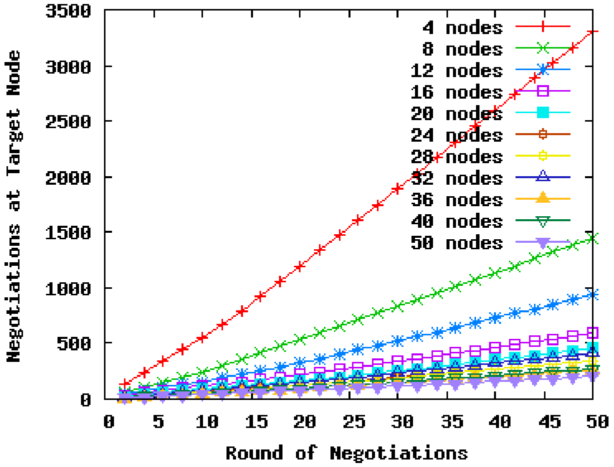

Figure 4: Effect of hops on negotiations

increase in *COT*. We noted a 10-30% successful negotiation rate where *COT* is not more than 5.

N-tier delegation hops effect in the system were compared. Figure 4 shows the result when various number of nodes (hops) are involved in the trust negotiation. The result shows that successful negotiation is dependent on fewer numbers of hops. These result agrees to the effect of *COT* on the system. It should be noted that currently no hierarchy exists between these negotiated credentials. Based on these results we intend to enhance the DTN model through achieving balance between *COT* and negotiation hops. We also intend to look at the effect of role-based access control as opposed to attribute-based access control that was used in this experiment.

6 Related Work

Automated trust negotiation (ATN) [3] is a promising approach for trust establishment between strangers through an exchange of digital credentials. However credentials are sensitive information that need to be protected through the use of disclosure policies. These disclosure policies inevitable require negotiation strategies as each entity tries to protect what credentials are released. However for a negotiation to succeed entities are expected to operate using the same family of disclosure strategies[12].

Several approaches[8, 13, 10, 14, 15] to trust negotiations have been proposed to support access control policies in an open decentralised environment. Some approaches investigated trust negotiation framework in the context of a peer-to-peer environment. [10] introduced a *locally trusted third party* (LTTP) which acts like a cache and mediator between two entities for the purpose of successful trust negotiations in peer-to-peer systems. Similarly [13] introduces a *sequence prediction module* that caches and manages used trust sequences from previously trust negotiations. While [14] proposes a trust chain based negotiation strategy (TRANS), which dynamically constructs trust relationships using a *trust proxy* that can cache common credentials or partial trust chain information from previous negotiations.

7 Conclusion

In this paper we reviewed and analysed the DTN model showing the pros and cons of *circle of trust (COT)* as well as *trust contracts*. We showed how these can be used to realise and build trust between non-trusting entities; how credential semantics between domains can be bridged; and how access control disclosure can be limited.

In the future, we would like to investigate the effect of role-based access control in the DTN model and hope to the likelihood of successful negotiations. We also intend to implement trust chains caching by peers to support future trust negotiations and peers that can dynamically link trust-contracts locally to improve future trust negotiations.

Ultimately we plan on exploring these models to support the area of clinical trials and epidemiological studies.

Acknowledgements

This work is supported by a grant from the Medical Research Council (MRC) UK and is undertaken as part of the Virtual Organisation for Trials of Epidemiological Studies (VOTES) project.

References

[1] L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke, "A Community Authorization Service for Group Collaboration," in *POLICY '02: Proceedings of the 3rd International Workshop on Policies forDistributed Systems and Networks (POLICY'02)*, (Washington, DC, USA), p. 50, IEEE Computer Society, 2002.

[2] R. Sinnott, J. Watt, J. Koetsier, D. Chadwick, O. Otenko, and T. Nguyen, "Supporting decentralized, security focused dynamic virtual organizations across the grid," in *Proceedings of 2nd IEEE International Conference on e-Science and Grid Computing, Amsterdam, December 2006*, 2006.

[3] W. H. Winsborough, K. E. Seamons, and V. E. Jones, "Automated Trust Negotiation," *DARPA] Information Survivability Conference and Exposition (DISCEX)*, vol. 01, p. 0088, 2000.

[4] E. Bertino, E. Ferrari, and A. Squicciarini, "Trust Negotiations: Concepts, Systems, and Languages," *Computing in Science and Engineering*, vol. 06, no. 4, pp. 27–34, 2004.

[5] W. Winsborough and J. Jacobs, "Automated Trust Negotiation Technology with Attribute-based Access Control," in *In Proceedings of DARPA Information Survivability Conference and Exposition, 2003*, vol. 02, pp. 60–62, 22-24, Apr. 2003.

[6] O. Ajayi, R. Sinnott, and A. Stell, "Formalising Dynamic Trust Negotiations in Decentralised Collaborative e-Health Systems," in *Proceedings of the 2nd International Conference on Availability, Reliability and Security, (ARES07), Vienna, Austria*, IEEE Computer Society, Apr. 2007.

[7] "ITU-T Recommendation X.509 — ISO/IEC 9594-8: Information Technology Open Systems Interconnection the Directory: Public-key and Attribute Certificate Frameworks," 3, May 2001.

[8] W. Winsborough and L. Ninghui, "Safety in Automated Trust Negotiation," in *In Proceedings of IEEE Symposium on Security and Privacy, 2004*, pp. 147–160, 2004.

[9] O. Ajayi, R. Sinnott, and A. Stell, "Trust Realisation in Collaborative Clinical Trials Systems," in *HealthCare Computing Conference HC2007, Harrogate, England*, Mar. 2007.

[10] S. Ye, F. Makedon, and J. Ford, "Collaborative Automated Trust Negotiation in Peer-to-Peer Systems," in *P2P '04: Proceedings of the Fourth International Conference on Peer-to-Peer Computing (P2P'04)*, (Washington, DC, USA), pp. 108–115, IEEE Computer Society, 2004.

[11] K. Seamons, M. Winslett, and T. Yu, "Limiting the disclosure of access control policies during automated trust negotiation," in *Proc. Network and Distributed System Security Symposium, San Diego, CA*, Apr. 2001.

[12] T. Yu, M. Winslett, and K. E. Seamons, "Interoperable Strategies in Automated Trust Negotiation," in *CCS '01: Proceedings of the 8th ACM conference on Computer and Communications Security*, (New York, NY, USA), pp. 146–155, ACM Press, 2001.

[13] E. Bertino, E. Ferrari, and A. C. Squicciarini, "Trust-X: A Peer-to-Peer Framework for Trust Establishment," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 827–842, 2004.

[14] J. Li, J. Huai, J. Xu, Y. Zhu, and W. Xue, "TOWER: Practical Trust Negotiation Framework for Grids," *2nd IEEE International Conference on e-Science and Grid Computing*, Dec. 2006.

[15] V. Bharadwaj and J. Baras, "Towards Automated Negotiation of Access Control Policies," in *Proceedings of the Fourth International Workshop on Policies for Distributed Systems and Networks (Policy 2003)*, IEEE Computer Society Press, 2003.