An Architecture Approach to Dependable Trust-based Service Systems

Suronapee Phoomvuthisarn
supervised by Yan Liu

National ICT Australia (NICTA), Australia, & School of Computer Science and Engineering, University of New South Wales, Australia
{suronapee.phoomvuthisarn, jenny.liu}@nicta.com.au

Abstract. *A key challenge in emerging service-oriented computing is the need to establish trust-based loosely coupled partnerships between previously unknown services. A dependable trust framework is essential to capture and maintain realistic trust information based on different requirements of participating services. Most existing trust management frameworks assume that the participating services perform cooperative behavior rather than have strategic behavior for their own interests. In this paper, we propose a novel architecture approach to integrate auction mechanisms into trust framework in order to prevent benefits from untruthful incentives. This is achieved by defining an auction-based trust negotiation protocol and realizing it in the trust framework. This research also aims to examine the impacts that the resulting architecture has on the attributes of dependability in particular trustworthiness, performance and reliability as well as their dependencies. Test cases that capture the key scenarios of these quality attributes are devised and exercised to collect empirical evidence.*

1. Introduction

In emerging service-oriented systems that require exchanging the information with other participants, especially previously unknown services, trust management framework is needed for particular services to allow others to access its resource. To capture and maintain trust information that is distributed over these environments, a dependable trust application is needed for establishing trust to satisfy the security requirements of all the participating services. However, participating services in trust negotiation are not merely to perform cooperative behavior, they also have strategic behavior. For example, some services have their own incentives to reveal their information. In some cases, they might untruthfully reveal their trust information to the service provider, leading to arbitrage opportunities for access to resources. One challenging question is how to prevent the gain from untruthful strategic behavior in order to achieve welfares for all the participants.

Existing trust frameworks have been proposed such as Trust-Serv [1], TrustBuilder [2], and Requirements-Driven Trust Framework [3]. These frameworks mainly focus on

trust negotiation strategies and access control policy. However, existing trust frameworks have not addressed how to prevent strategic behavior. The extension to the existing frameworks should be in place to prevent this strategic behavior from untruthfully revealing their trust information.

Auction mechanism is a suitable technique to solve real-world problems especially in market trading so as to achieve specific resource allocation goals. In this research, we propose an architecture approach integrating VCG (Vickrey-Clarck-Groves) auction mechanism with an existing trust framework [3] to prevent strategic behavior. This also involves defining a new trust negotiation protocol that encapsulates each steps of VCG auction mechanism. Due to the extra computing incurred by VCG, the resulting architecture has an impact on several attributes of dependability, in particular, trustworthiness, performance, and reliability. Moreover, they can have dependencies. For example, when using VCG, extra communication message may impose extra delay to response time and also impact mean time to failure, and therefore the increasing trustworthiness may come at a cost of performance and reliability. In this work we also consider these architectural dependencies and evaluate our solution using an established architecture evaluation method [4].

Our contribution is complementary to existing trust framework with the extra capability to prevent strategic behavior. The use of auction mechanisms induces an effective trust negotiation by preventing a trust-based application from being exploited by incentive services while ensuring accurately trust information captured. This leads to more trustworthy system, as well as more efficient trust negotiation using lightweight mechanisms rather than sophisticated implementations for capturing trust information. Also the novel architecture will be optimized to support performance and reliability.

The rest of the paper is organized as follows. We start with related work in Section 2. The motivating scenario is described in Section 3. The research method is presented in Section 4. We then propose the architecture and negotiation protocol in Section 5. Evaluation plan is discussed in Section 6. This paper concludes at Section 7.

2. Related Work

Existing trust frameworks have mainly focused on trust negotiation strategies and access control policy. Key among existing related work includes Trust-Serv [1], TrustBuilder [2], and Requirements-Driven Trust Framework [3]. Trust-Serv, a model-driven trust framework, uses state machines to represent and determine credential exchanges for access to resources [1]. TrustBuilder uses credential disclosure trees and negotiation strategies to facilitate protection of credential information during negotiation [2]. Finally, Requirements-Driven Trust Framework, our existing work, combines trust negotiation and trust level computation together based on the service requirement [3]. This framework is very suitable for a distributed environment where trust is negotiated based on the service requirements of each domain involved. However, existing trust frameworks have not

addressed how to prevent strategic behavior. In this research, we propose a novel architecture approach integrating VCG (Vickrey-Clarck-Groves) auction mechanism with requirements-driven trust framework [3] to prevent strategic behavior.

3. Motivating Scenario

In this section, we provide a simple scenario to explain how VCG auction mechanism can be used to prevent strategic behavior of services. We postulate an application where several travel agents are competing for deals to manage group travels. A customer as a traveling group can register the request with a travel agent brokering service. Travel agents compute with each other by using their web services to provide its quote to the broker with its credit. Hence, an appropriate identity should be provided to the broker to check for credits. The higher the submitted credit, the higher sensitive credentials needed to prove their identities.

Suppose the particular travel agent untruthfully reveals its credit to the broker, this agent would get the deal. In this case, the system is untrustworthy because of its lacking capabilities to prevent this strategic behavior. One solution is to implement VCG in trust management framework that prevents any gain from untruthfully revealed information. In VCG, the bidder who submits the highest bid wins the auction and pays the second-highest bid [5]. This principle of VCG is that "lying does not pay", which means bidding something other than the bidder's true value is never beneficial and sometimes was detrimental with penalty. Suppose all travel agents truthfully send their credits to the broker. Let's say, agent A, B, C, D submits 10, 20, 50, and 60 credits with the same quote, respectively. In this case, D has been chosen to get the deal and is required to prove the credentials based on 50 credits. The agent D will have the net utility gain of 60 minus 50 which is 10 credits. Note that the credentials to be exposed for 50 credits would be less trustworthy than 60 credits. If agent D service sends its credit more than 50, the result remains the same. If agent D sends its credit less than 50, it loses the competition. If other travel agents such as agent B send its credits higher than 60, suppose 80 credits, it would get the deals but have to pay the net utility gain of 20 minus 80 which is negative and eventually a loss. Therefore, all travel agents are content to send their truth credit.

4. Research Method

In this research, an architecture approach is proposed to develop the solutions for dependable trust-based service oriented applications. A negotiation protocol encapsulates VCG auction mechanism is defined and realized in relevant VCG mechanism components. These components interact with trust components in an architecture framework. It is also aimed to optimize this architecture with regards to the impact on the attributes of dependability which are trustworthiness, performance, and reliability. The

improvement solution will be based on observing the dependencies among these qualities of attribute using test cases. Further architecture improvement will be devised given the empirical evidence. The proposed research methods consist of three stages as follows:

4.1 An architecture approach is conducted at the architecture level to develop the novel architecture for dependable trust-based service oriented application. The essence of this stage is to build a reference trust framework architecture integrating with auction mechanisms, in particular, VCG mechanism to prevent strategic behavior. This is achieved by developing negotiation protocol encapsulating with VCG and realizing it in relevant VCG components. The primary concern with the resulting architecture is to ensure the separation of concerns between trust and VCG components. Trust and VCG components have to overlap in functionality as little as possible so that trust-based application can be maintainable and extensible with other auction mechanisms. Although the resulting architecture can help preventing strategic behavior, there is a possibility that a poorly-designed architecture might degrade the composition capability of the original trust framework. Loosely-coupled component-based approach can be used to decompose system into functional components to support extensibility and maintainability. Our plan is to develop a basic trust management architecture as a prototype with the motivation scenarios deployed. Then, the auction mechanism is integrated into the trust negotiation protocol and interacts with the trust management framework. It should be tested that the VCG mechanism is efficient for preventing strategic behavior.

4.2 The core architecture is extended with performance and reliability qualities of attribute. The essence of this stage is to examine the dependencies of performance, reliability, and trustworthiness based on the impacts that resulting architecture has on. One such challenge is to address the dependencies of these attributes of dependability which may incurs trade-off in the architecture design and implementation. For example, increasing trustworthy trust-based application with auction mechanisms might decrease system performance in response time and increase points of failure that affect reliability. Our solution is to use the basic prototype as a test-bed to further identify and pinpoint any architecture issues incurred by the computation of the auction mechanism. Test cases are devised to observe and measure the performance and reliability of this architecture. Moreover, the dependencies or even correlations between trustworthy, performance and reliability are studied. The root cause is then resolved either at architecture design or at the implementation level.

4.3 Evaluation is conducted at the empirical level to firstly evaluate appropriateness auction mechanisms of the extended architecture used for preventing strategic behavior. We then evaluate the value of other dependability attributes, performance and reliability. One challenge is that trustworthiness is a qualitative attribute. It is quite subjective to evaluate the trustworthiness of trust framework. MEMS [4] has proposed the scenario-based architecture evaluation method used to evaluate both quantitative and qualitative attributes, hence, we will adapt MEMS to justify the value of these attributes. The plan is to devise three case studies with each having the emphasis on trustworthiness, performance and reliability. All case studies are to be

modeled after real-world scenarios in service oriented architectures. At the end, architecture design and implementation guidelines are provided with regards to different characteristics of service oriented applications.
Section 5 discusses the current progress in the first step.

5. The Architecture

A conceptual trust management architecture is proposed to prevent strategic behavior. This section discusses the current progress in the first step of the method. We also exemplify this architecture using the auction-based trust negotiation scenario.

Trust-based application has to be extensible while negotiation protocol has to be maintainable when changing in auction mechanisms. This is achieved by using loosely-coupled component-based approach that decomposes system into functional components with well-defined interface used for communication between components. The key components of this architecture are Trust Engine and VCG Engine.

Trust Engine is responsible for trust negotiation between services. This engine involves establishing the services that will be exchanged between the participating services and establishing a negotiated trust level for service access. It consists of the following components:

- Trust Negotiation Module is responsible for checking the validity of *trust tokens*, a set of selected credential(s), based on specified *trust token type*, a set of attributes and the range of values they should be constrained to [3]. If all attributes in the certificates satisfy all *trust token types*, they are proved to be valid. For example, the broker's *trust token types* based on 50 credits are ({firm's age > 10}, {location = U.S.A.}). In the context of this example, travel agent B has to provide the credential(s) stating that B's company has been established for over 10 years and its location is in USA.
- Trust Level Computation Module is responsible for computing trust level that service provider has on service requester.

Auction Engine is responsible for computing the appropriate trust level that service provider has on service requester based on auction mechanisms calculation. It consists of the following components:

- VCG Mechanism Computation Module is responsible for computing trust level based on VCG auction mechanism that can be categorized into single-item and multi-item.
- Utility Calculation is responsible for calculating the net utility gain for services.

As a result, in this architecture Trust Level Computation Module uses the VCG Mechanism Computation Module to compute the appropriate trust level of particular resources service requester requests. The service that sends the highest credit will be required to send the credential(s) based on the second-highest credit submitted. In this case, credit is the trust information that will be translated into trust value. The higher the credit, the higher the trust value will be. After each VCG steps, the selected service then continues to exchange the certificates based on each *trust token types* required for trust

level of particular resources. The higher the trust level, the higher sensitive credentials needed to prove their identity.

6. Evaluation Plan

The basic architecture has been implemented with a set of travel agent web services using Apache Axis1.0. Trust negotiation protocol is implemented using JXTA technology which includes a set of open peer-to-peer protocols. In this earlier stage, to demonstrate the trust management framework capabilities when using VCG auction mechanism, the plan is to implement two prototypes with and without VCG deployed. The testing is presented as follows:

- Utility test evaluates the practical usage of the architecture in the case that it can efficiently avoid untruthfully strategic behavior.
- Overhead test evaluates the performance in terms of response time of the architecture when using VCG.

7. Conclusion

In this early stage, we envision a conceptual architecture of trust-based service oriented application integrating with VCG auction mechanism. Our architecture introduces the solutions of dependable trust-based application that can prevent strategic behavior. The notion of VCG induces an effective trust negotiation by preventing a trust-based application from being exploited by incentive services.

References

1. Skogsrud, H., Benatallah, B., Casati, F., "Model Driven Trust Negotiation for Web Services", IEEE Internet Computing, November-December 2003, Pages 45-52.
2. Yu, T., Winslett, M., Seamons, K. E., "Supporting Structured Credentials and Sensitive Policies through Interoperable Strategies for Automated Trust Negotiation", ACM Transactions in Information Systems Security, Vol. 6, No.1, February 2003, Pages 1-42.
3. Phoomvuthisarn, S., "Trust and Role Based Access Control for Secure Interoperation ("TracSI")", Communications and Information Technologies, 2007, 17-19 Oct. 2007 Page(s):1458 - 1463
4. Liu, Y., Gorton, I., Bass, L, Hoang, C., Abanmi, S., MEMS: A Method for Evaluating Middleware Architectures, QoSA, June 27-29, 2006, Sweden. Lecture Notes in Computer Science, Volume 4214/2006, 2006.
5. Ye, S., Makedon, F., Ford, J., "VCG computational Mechanism", in Proceedings of the 4th International Conference on Peer-to-Peer Computing, 2004. 25 Aug. 2004 Page(s):108 – 115