Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 86 (2015) 35187-35191

ISSN: 2229-712X

An empirical study on secure and multiple web service collaborations

Nalini Priya.G[1], M V Rathnamma[2] and Balamurugan Balusamy[3]

[1]Saveetha University, Chennai, India.

[2]Sri Sai Institute of Tech. & Science, Kadapa, India.

[3]VIT University, India.

ARTICLE INFO

Article history:

Received: 4 July 2012;

Received in revised form:

14 September 2015;

Accepted: 19 September 2015;

Keywords

Authentication,
Multi-Party Interactions,
Secure Service Collaborations,
Web Services,
E-Commerce,
Online shopping.

ABSTRACT

The objective of this study is to investigate the factors affecting secure and multiple web service collaborations. Online shopping is one such area where the need arises to perform secure communications with several other trading partners. In this study we have chosen a popular Chinese internet E-commerce company that offers online shopping and other internet related services. We have compared the current model which they have adopted to perform those collaborations and also proposed the benefits they would obtain if changes are made in their communication patterns.

Introduction

The use of the internet as a shopping and purchasing medium has seen unprecedented growth. Most experts expect the global electronic market to dramatically impact commerce in the twenty first century.

In addition to this tremendous growth, the characteristics of the global electronic market constitute a unique opportunity for companies to more efficiently reach existing and potential customers by replacing traditional retail stores with Web-based businesses. Many physical obstacles hinder companies in their efforts to reach global markets. Therefore, the World Wide Web (WWW) enables businesses to explore new markets that otherwise cannot be reached. Consequently, Electronic Commerce (EC) has emerged as the most important way of doing business for years to come. This term was first used by Kalakota and Whinston [4]. They state that EC has two distinct forms: Business-to-business and business-to consumer. Much of the growth in revenues from transactions over the Internet has been achieved from business-to-business exchanges leading to the accumulation of an impressive body of knowledge and expertise in the area of business-to-business EC [5], [6]. Unfortunately, this is not the case for business-to-consumer EC. With the exception of software, hardware, travel services, and few other niche areas, shopping on the Internet is far from universal even among people who spend long hours online [7], [8]. A recent survey reported by Krochmal [9], found that only 18% of U.S. households have made a purchase online.

Moreover, many companies already practicing EC are having a difficult time generating satisfactory profits. For example, many e-companies such as Amazon.com have successfully attracted much attention but have not been able to convert their competitive advantage into tangible profit [10].

The applications and services involved in the process are typically heterogeneous and may be provided and maintained by different organisations. As an organisation has its own security mechanisms and policies to protect its local resources, the application across multiple organisations has to operate amongst multiple, heterogeneous security realms. A security realm is a group of principals (people, computers, services etc.) that are registered with a specified authentication authority and managed through a consistent set of security processes and policies.

Because organisations and services can join a collaborative process in a highly dynamic and flexible way, it cannot be expected that every two of the collaborating security realms always have a direct cross-realm authentication relationship. A possible solution to this problem is to locate some intermediate realms that serve as an authentication-path between the two separate realms that are to collaborate. However, the overhead of generating an authentication-path for two distributed realms is not trivial. The process could involve a large number of extra operations for credential conversion and require a long chain of invocations to intermediate services.

Eguo.com, founded in April 1999 by Yongqing Zhang, is a Chinese Internet e-commerce company to offer consumers online shopping, delivery and other Internet related services. It focuses on items that have rapid turnover, repeat purchases, and high margins without inventory costs. Now, eguo offers 30 lines of consumer products, about 60,000 products including foods, CDs, books, tickets, digital products, groceries, cosmetics and electronics, sports and outdoor equipment, etc, and its business has expanded to US, Japan, Korea, India and HK.

Eguo promotes itself as an online convenience store on “little something for everyone” with a guaranteed delivery time within the Beijing area. Eguo.com is one of the largest e-commerce websites in China today. In late 2007, eguo.com had about three million registered users, and page impressions topped 200 thousand per day with over five million Yuan sales

Tele:
E-mail addresses: kadavulai@gmail.com

per month. By now, Eguo has been the famous brand of business to consumer ecommerce enterprises in Beijing.

OPERATION MODEL OF EGUO

Eguo provides the payment option of C.O.D, card (only China Merchants Bank and Industrial and Commercial Bank of China) payments and remittance currently. Eguo will provide customers with more choice for payment in the future. Eguo has launched the famous "Eguo one hour" delivery service in Beijing since April 2000, which means products ordered in the website will be delivered to consumers within one hour in Beijing (within the 4th Ring Road). "Eguo one hour" delivery service brought much convenience to the consumers, since then, many Fast Moving Consumer Goods companies such as Pepsi; Uni-president started the cooperation with Eguo. Eguo created the concept of independent logistics. Based on the independent logistics, Eguo founded its delivery system using the hub and approach with one advanced central warehouse center, an efficient customer service center and a few dense distribution centers within the 4th Ring Road to meet the goals of one hour delivery guarantee. Meanwhile, by utilizing this system with advanced IT technology, Eguo could manage the customer service effectively.

As an online retail platform, Eguo not only provides cheap goods for customers, but also offers maximal convenience and best services to customers by cooperating with the traditional producers and using advanced IT technology to realize the goal of "serve for common people with practicality and benefit". Eguo deals with customer service in the way of call center, MSN, E-mail and BBS.

Reiter and Stubblebine in [16] argue that an authentication process in a large-scale distributed system often needs the assistance of a path of security authorities as it is difficult to locate a single authority to authenticate all the principals in the system. They suggest using multiple paths to increase assurance on authentication. It is important to notice here that a Session Authority or SA in our system differs significantly from the security authority in [16]. A security authority is used to enforce security policies and processes for a security realm so as to prevent attacks from accessing the applications and resources within that realm. In contrast, an SA is associated with a business session (management system), independent of any local security realm. It has much simpler functionalities than a security authority, aiming to provide secure real information to session partners which may belong to different security realms.

TECHNOLOGY, MANAGEMENT AND CAPITAL MODEL OF EGUO

As an e-commerce service provider, Eguo developed the retail and e-commerce Logistics Management System, as shown in figure 1, based on its practice on e-commerce retail. Eguo provides the simple version of the system to its partners for free. With the use of the Logistics Management System, its partners could management their products and inventory exactly and its customers could get more choices and the lowest price. The system includes such modules as supplier management, product management, purchasing management, inventory management, return management, customer management and sales management, etc. Eguo developed the ERP system in the late of 2005. With the Compiere as the technology platform, eguo's ERP system works stably and emphasizes particularly on e-commerce application. By the application of ERP system, Eguo could allocate its resources including people, goods, funds, equipment and information properly and streamline the business process.

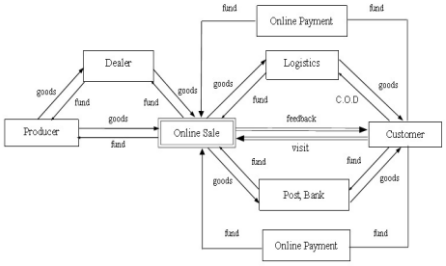


Figure 1. Eguo online retail system

The organization structure of Eguo is shown as figure 2. Functions of each department are as follows:

General Manager

Draw the development strategy and annual plan, etc.

Cooperation Department

Supplier management, customer relationship maagement.

Sales Department

Sell goods develop market, VIP management.

Website Development Department

Development and maintenance of eguo's website.

Technology Department

Construct the network, maintain the server.

Customer Service Department

Pre-sale service, after sale service.

Human Resources Department

Recruitment, training

Financial Department

Finance management.

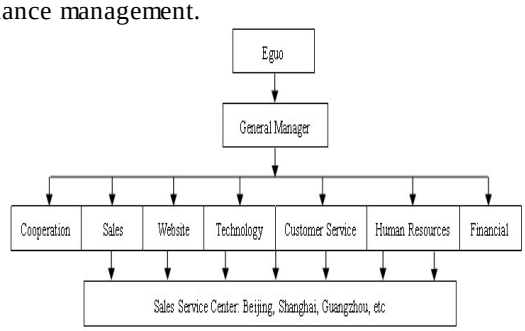
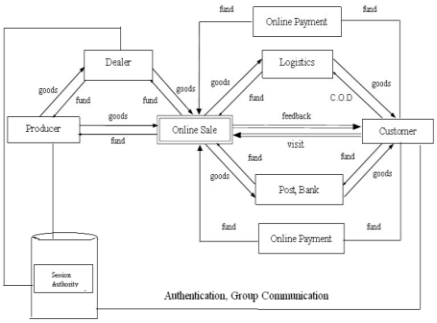


Figure 2. Organization structure of Eguo

With the fast growing customers, Eguo expands fast at a sales growth rate of 30 percent per year. The revenue of Eguo mainly came from the earnings of sales, ads and franchise fee, and the sales earnings were in the majority.

PROPOSED MODEL



The proposed model is the modified version of EGUO web service functionality. We have added our Session Authority concept that provides authentication and other secure group communication services. The following are the main 4 modules of the Session Authority concept. We won't go in to the implementation details of the modules. But they provide a clear cut explanation of the overall process of the session authority concept.

Multi-Party Session

A multi-party session may have two or more session partners for the intended collaboration. A partner can search for and invoke new services at runtime. Before a service (instance) is accepted as a new partner, an HCRA process is needed. However, unlike a two-party session, authentication for the existing partners of a multi-party session could be simplified significantly without requiring credential conversion and the establishment of any authentication path. This is because session partners can make use of their session memberships to authenticate each other even if they belong to different security realms. A shared session key or individual secret keys may be used to enforce a secure collaboration amongst session partners. Consider the example of Fig 1 again. When *SI* attempts to contact *CI*, it does not have to authenticate itself with the local authentication system of *CI* because both *SI* and *CI* are members of the same session. *SI* can simply use its session membership to prove its identity to *CI*. This simplified authentication process is called Simplified Cross-Realm Authentication (SCRA). The HCRA process has to be repeated $(n - 1)$ times for a multi-party session with n security realms, but up to $(n - 1) \times (n - 2)/2$ authentication processes can be simplified as SCRA based on session memberships, thereby reducing both cost and complexity significantly. However, managing and coordinating a multi-party session is more complex in nature, in comparison with handling two parties only. A multi-party session management system needs to address the issues with *message routing* and *secret keys for communications*. A *Session Authority* (SA) is also required to provide reliable real-time information (e.g. memberships) about session partners [9].

Message Routing

Message routing is concerned with the issues of dispatching messages to the intended service instance which maintains corresponding states. In practice, a service may handle requests from different requestors concurrently. When all the requestors invoke operations provided by the same port, the messages are sent to the same address (e.g. the same URL). In this case, additional correlated information is needed, which helps the underlying middleware to determine which interaction a message is related to and to locate the corresponding service implementation object to handle the message.

A simple approach is to exploit a correlated token, shared by the communicating partners, for identifying the related messages transported within the collaboration. A shared token is sufficient to the identification of session partners on the both sides of two-party collaboration. However, session partners (i.e. service instances) in a multi-party session may be generated by the same service with the same address. It is difficult to distinguish them using a single token. In contrast with the token-based solution, an ID-based solution assigns every session partner with a unique identifier, thereby distinguishing all the partners unambiguously. In practice, a token-based solution is usually used to decide whether an instance is actually working within a business session while an ID-based scheme is employed to identify individual session partners in the case that fine-grained instance identification is needed.

Secret Keys

In a two-party session, authentication typically consists of several rounds of operations and message passing, and the session key used in the subsequent communication between the two partners is normally a by-product of the authentication process. However, in a multi-party session, SCRA is a highly simplified process and does not include the automatic generation of secret keys.

An obvious approach is to generate a single secret key for a given multi-party session and then distribute it to all the session partners. Once the session key is generated, it can be used to simplify the authentication process amongst the existing session partners, thereby avoiding HCRA. Hada and Maruyama's protocols in [9] are an example of this type of solution with the support of a Session Authority. However, if a partner loses the secret key, the security of the whole session will be compromised. Moreover, session partners may leave and join a session dynamically. When a partner leaves from its session, the shared secret key must be refreshed in order to ensure that any previous partner cannot gain any further information from the session. Similarly, when a new partner joins the session, the secret key must also be refreshed in order to ensure that any new partner cannot obtain any previous information transferred within the session. The issues related with secret key revocation have been discussed in many papers on secure group communications (e.g. [15][20]).

Another possible solution is to generate a shared secret key for every pair of session partners (e.g. using the Diffie-Hellman public key algorithm [18]). This scheme is more costly but it avoids the issue with key revocation.

Session Authority

A Session Authority (SA) is a service that provides reliable real-time information (e.g. session memberships) for a given multi-party session. For example, the SA may be employed to notify that a partner has left from the session, by contacting all the partners that have collaborated with the previous partner. An SA service could be associated conveniently with, or implemented as part of, a multiparty management system. This can be implemented using different methods with different features and characteristics such as fault-tolerance, scalability and cost-effectiveness. These methods include centralized management, decentralized architecture for better scalability, and fully distributed information provision for improved fault-tolerance. As an example of the SA implementation, our authentication protocols are designed to conform to the WS-Coordination specification [3] in which an SA is an extension of a *coordinator*. In WS-Coordination both centralized and decentralized coordinators are discussed. An SA may act as a centralized service that handles requests from all the session partners within a business session; alternatively, an SA may manage the session partners within a local domain only, and a group of decentralized SA's can then manage collectively the whole business session, thereby avoiding the problem of concentrating the SA operations in a single place.

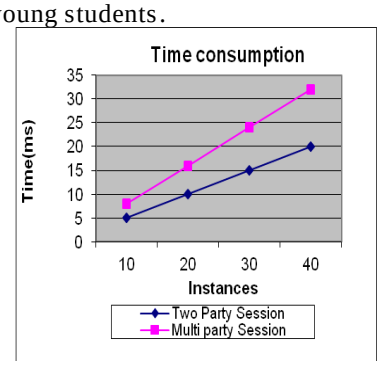
Implementation Details

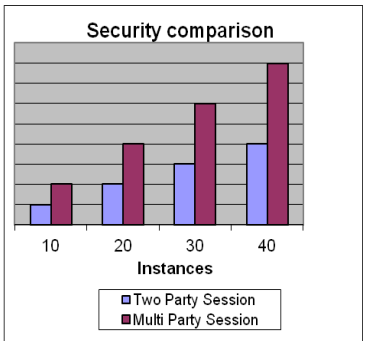
Beside the correctness analysis, we also need to examine whether our authentication system is feasible enough for practical real-world applications. Consequently, a series of experiments has been implemented to assess the overheads imposed by the authentication mechanisms and the scalability of our proposed system. Because the system is designed to be deployed on service-oriented middleware, we will evaluate the compatibility of our system with existing message-level security protocols.

We made a comparison evaluation for security and performance overhead for authentication using two party and multi party session. The results of which are displayed in the following figures.

Perhaps, eguo's success is due to its cooperation with traditional manufactures. Now, the number of companies cooperated with eguo is increasing continually, and a range of industries is involved with diversified cooperation way. In addition to the cooperation with traditional companies, eguo cooperated with universities also. Eguo has started its cooperation with universities since 2004 such as Beijing Jiaotong University, Beijing Union University, China Agriculture University.

University of Finance and Economics, China University of Geosciences, Beijing University of Aeronautics and Astronautics, Beijing University of S&T, Beijing Institute of Technology, etc. Eguo offered a chance of internship or starting a business to students from these universities. Students from these universities could have an intern, work or start a business in eguo. Eguo has recruited 1000 internship students including sophomore, juniors and seniors since the foundation of the innovation park. 80 percent of eguo's current staffs came from the interns. As an innovation park of young people especially university students, eguo offers a free business platform, virtual host without space limit, an online tool for user management, suggestions from e-commerce experts and office room, while young entrepreneurs offer ideas, and the profits will be halved by eguo and young students.





Conclusion

In practice, a dynamic business process may involve many applications and services which belong to different organizations and security realms. The dynamic authentication process between organizations could be highly complex and time-consuming if some intermediate authentication paths have to be created and credentials have to be converted. When there is no existing authentication relationship in place between two organizations, it will be practically difficult for a system to enable any secure collaboration between services from the two organizations in a just-in-time fashion.

Based on the above analysis, the reason of eguo's success can be summarized as the following three points:

First, unlike the failures of many dot com companies, eguo limited it most service scope in Beijing, and strategically placing its distribution centers, so it could realize the promise of "one hour delivery". By this way, eguo overcame logistics obstacle of e-commerce, and consumers could experiment with the advantages of ecommerce.

Second, with the innovative cooperation way, eguo heightened its brand awareness and attracted many traditional partners and young talents. By the cooperation with tradition companies, eguo offers a growing wide variety of goods including convenience goods, which encouraged general customers that might not be accustomed to shop online to purchase in the website of eguo. With the cooperation with universities, eguo reinforced its brand popularity during the young people and attracted many high quality employees.

Third, with application of the advanced IT technology, eguo could manage goods, inventory and customers effectively, and allocate its resources including people, goods, funds, equipment and information properly and streamline the business process. But will it succeed in the future with the expanding of goods? Is it restricted the development by limiting the delivery scope?

References

[1] S. Bajaj, G. Della-Libera, B. Dixon, M. Dusche, M. Hondo, M. Hur, C. Kaler, H. Lockhart, H. Maruyama, A. Nadalin, N. Nagaratnam, A. Nash, H. Prafullchandra, and J. Shewchuk, "Web Services Federation Language (WS-Federation)," available from http://msdn2. microsoft.com/en-us/library/ms951236.aspx, Jul.2003.

[2] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," *ACM Trans. on Computer Systems*, Feb. 1990, pp. 18-36.

[3] F. Cabrera, G. Copeland, T. Freund, J. Klein, D. Langworthy, D. Orchard, J. Shewchuk, and T. Storey, "Web Services Coordination (WS-Coordination)," available from http://www.ibm.com/developerworks/library/ws-coor/, Aug. 2002.

[4] I. Cervesato, A.D. Jaggard, A. Scedrov, and C. Walstad, "Specifying Kerberos 5 Cross-Realm Authentication," *Proc. Workshop on Issues in the Theory of Security*, Long Beach, California, USA, 2005, pp. 12 – 26.

[5] N. Cook, S. Shirvastava, and S. Wheater, "Distributed Object Middleware to Support Dependable Information Sharing between Organisations," *Proc. International Conference on Dependable Systems and Networks*, Maryland, USA, Jun. 2002, pp, 249- 258.

[6] K. Czajkowski, D. Ferguson, I. Foster, J. Frey, S. Graham, I. Sedukhin, D. Snelling, S. Tuecke, W. Vambenepe, "The WS Resource Framework Version 1.0," available from http://www.globus.org/wsrf/specs/ws-wsrf.pdf, 3 May 2004.

[7] D. Georgakopoulos and M. Hornick, "An Overview of Workflow Management: From Process Modelling to Workflow Automation Infrastructure," *Distributed and Parallel Database*, Springer, Mar. 2005, pp. 119-153.

[8] Li Gong, "Increasing Availability and Security of an Authentication Service," *IEEE J. Selected Areas in Communication*, vol. 11, no. 5, June, 1993, pp. 657-662.

[9] S. Hada and H. Maruyama, "Session Authentication Protocol for Web Services," *Proc. Symposium on Application and the Internet*, Jan. 2002, pp. 158-165.

[10] M. Hondo, N. Nagaratnam, and A. J. Nadalin, "Securing Web Services," *IBM Systems Journal.*, 2002.

[11] M. Huhns and M. P. Singh, "Service-Oriented Computing: Key Concepts and Principles," *IEEE Internet Computing*, vol. 9, no. 1, Jan. 2005, pp. 75-81.

[12] O. Kornievskaia, P. Honeyman, B. Doster, and K. Coffman, "Kerberized Credential Translation: A Solution to Web Access

Control," *Proc. 10th USENIX Security Symposium*, Washington, DC, USA, Aug. 2001.
[13] N. Li, W. Winsborough, and J.C. Mitchell, "Distributed Credential Chain Discovery in Trust Management," *J. Computer Security*, vol. 11, no. 1, 2003, pp. 35-86.
[14] P. C. van Oorschot, "Extending Cryptographic Logics of Belief to Key Agreement Protocols," *Proc. the 1st ACM Conference on Computer and Communications Security*, Fairfax, Virginia, USA, Nov. 1993, pp. 233– 243.
[15] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," *ACM Comput. Surveys*, vol. 35, no. 3, Sep. 2003, pp. 309-329.
[16] M. K. Reiter and S. G. Stubblebine, "Resilient Authentication Using Path Independence," *IEEE Trans. Computers*, vol. 47, no. 12, Dec. 1998, pp. 1351-1362.
[17] W. Stallings, *Cryptography and Network Security: Principles and Practices*, Prentice Hall, Upper Saddle River, New Jersey, 1999.
[18] M. Steiner, G. Tsudik, and M. Waidner, "Diffie- Hellman Key Distribution Extended to Group Communication," *Proc. of the 3rd ACM Conference on Computer and Communications Security*, New Delhi, India, Mar. 1996, pp. 31-37.
[19] H. Sun, Y. Zhu, C. Hu, J. Huai, Y. Liu, and J. Li, "Early Experience of Remote and Hot Service Deployment with Trustworthiness in CROWN Grid," *Proc. APPT*, 2005, pp. 301-312.
[20] C. K. Wong, M. G. Gouda, and S. S. Lam, "Secure Group Communications Using Key Graphs," *Proc. ACM SIGCOMM '98 Conf. Applications, Technologies, Architectures, and Protocols for Computer Comm.*, 1998, pp. 68-79.
[21] V.Bertocci, G.Serack and C.Baker, "*Understanding Windows Cardspace: An introduction to the concepts and challenges of digital identities*" Addison-Wiley, 2007
[22]Jiangtao Li, Ninghui Li, XiaoFeng Wang, Ting Yu3 "*Denial of Service Attacks and Defenses in Decentralized Trust Management*", International Journal of Information Security, vol 8.pp 88-101,2009