Cross-Enterprise Policy Model for e-Business Web Services Security

Tanko Ishaya[1] and Jason R.C. Nurse[2]

[1] The University of Hull, Scarborough Campus, Filey Road, Scarborough, YO11 2AZ, UK
[2] Department of Computer Science, University of Warwick, Coventry, CV4 7AL, UK
T.Ishaya@hull.ac.uk, jnurse@dcs.warwick.ac.uk

Abstract. Contemporary e-Business applications comprise of dynamic extensible and interoperable collection of services, Web Services and information shared by collaborating entities performing various transactional tasks. Securing these services offerings is therefore of crucial importance. To address security requirements, there has been a plethora of proposed solutions, ranging from hardware devices and security specifications to software applications. Most of these security solutions are largely technology focused with little or no evaluation and integration of policies and procedures of these collaborating entities. This research investigates the use of an approach that integrates documented cross-enterprise policies with current security technology, to enhance the overall security requirements of businesses that decide to use web services. A policy model for enhancing web services security is developed evaluated and presented.

Keywords: security, security policies, security model, web Services, cross-enterprise, e-Business, web-based applications.

1 Introduction

Electronic Business (e-Business) has undoubtedly become the fastest growing means of doing business in today's economy. An assessment of the UK e-business field in [15], noted that over two-thirds of UK companies are doing business online, a 50% increase from 2002. There is also a considerable increase in the level of collaboration between e-businesses, with service offerings such as e-banking, online order processing and even e-payments –particular through the use of Web services (hereafter referred to as WS) technology. An example of e-Business use of WS is the streamlined communications between airline, hotel and car rental companies discussed in [12]. Using WS technology, the interactions between these distinct companies is dynamically available in real time and possibly all through one single interface to the customer.

Electronic Data Interchange (EDI) has enabled cross-enterprise interactions (see [9]) before the existence of WS; main benefit available with WS is their ability to facilitate interoperability between heterogeneous systems due to their use of standardized protocols and open technologies. WS provides the ability to allow for seamless integration of services and business processes across disparate types of enterprises.

D. Weerasinghe (Ed.): ISDF 2009, LNICST 41, pp. 163–171, 2010.

While WS presents e-Business with dynamic and interoperable service integration, the security dilemmas that they pose are enormous. As noted in [13], WS presents a new avenue for attack not addressed by current security infrastructure. This security issue is compounded by the fact that an individual, isolated approach to security by each e-Business is no longer sufficient as each one's approach must now readily interoperate with the others' at any moment in time. The seriousness of this security issue is stressed by numerous authors in [2], [11] and [14] with [6] linking this issue as the limiting factor on widespread deployment of WS. Hartman et al. (2003) proposed a 'structured approach' to achieving secure joint WS offerings. This approach requires each e-Business to clearly define a set of security requirements for its services; the level of functionality that needs to be exposed; and then the special mechanisms to be put in place to fulfill each participating entity's needs. Essential to this proposed solution is also the concept of Enterprise Application Security Integration (EASI) techniques as they aid considerably in providing a common security framework for integrating many different technology solutions (Hartman et al., 2003). A shortcoming of this approach is that it places so much emphasis on the mechanisms/technologies to be used (e.g. the EASI framework), but not the overarching requirements that must be fulfilled to enable the highest security level of WS intercommunications. In addition to technology implementations, one key requirement for secure service interactions is the need for overarching cross-enterprise business policies. This requirement is especially crucial in arranging and supporting these sometimes complex and highly sensitive intercommunications.

Policies that focus on a higher level than the technology solutions to be implemented form another protective layer. The benefit of these policies is that once established they help to maintain a high level of trust between all participating companies. This trust is sustained by enabling the exchange of information to always occur in an expected and understood manner. The presence of this trust is a crucial requirement to the realisation of the seamless integration of services promised by WS technologies. While, there are considerable developments in WS security policies, these developments consider policies at the technology layer and thus do not address the higher-level policy layer, which was introduced in the paragraph above.

Given the significance and value of an additional way to secure WS, the focus of this research is to investigate whether an approach to WS security oriented on agreed-on cross-enterprise policies can significantly aid in providing protection against fraud, lawsuits and other business risks. The approach adopted for the research is a combination of empiricism and hermeneutics research methodologies. A specific WS-based scenario (in the form of a case study) that demands an extremely high level of trust between entities is presented. Members of this scenario include an e-university, an e-bank and an e-hotel (which is defined as a provider of temporary accommodation for students). The purpose of this particular case scenario is to allow this research to identify some of the most crucial aspects that should be considered in the creation of any reliable WS security model. The model has been implemented through a proof of concept prototype, which is currently being evaluated.

The remainder of this paper is organized as follows: Section 2 presents related work and suggests shortcomings that could be overcome by enterprise policies; in Section 3, the case study developed in this paper is described and the proposed policy model presented. Finally, Section 4 concludes this paper and outlines future work.

2 Related Work

This research is based on three related areas of work, e-Business and its security concerns, the adoption of WS for e-Business, and current approaches used in securing WS. These have been reviewed and presented in the following sections.

2.1 e-Business and Its Security Concerns

e-Business is undoubtedly one of the most discussed topics in the business and information technology (IT) fields today. Interestingly however, there seems to be no globally accepted definition with some authors linking e-Business primarily with internal operations [9] and others with both internal and external business processes [5]. The latter perspective conveys a more complete and accurate description of our view of e-Business. IBM is one of the many entities that support this internal and external orientation, thus defining e-Business as: "The process of using Web technology to help businesses streamline processes, improve productivity and increase efficiencies. Enables companies to easily communicate with partners, vendors and customers, connect back-end data systems and transact commerce in a secure manner". This definition highlights key constituent elements such as the use of Web technologies, internal and external communications and the overarching concept of the requirement for security.

e-Business has experienced a phenomenal growth over the last decade. The large-scale integration of business processes within the UK has experienced a massive 40% increase from 2002 [15]. Similarly, this considerable increase is being experienced all over the world. For example, the US e-Business sector estimates an average increase of 18.6% per year in online retail sales between 2005 and 2009 (eMarketer-b, 2006). As advancements in technologies enable easier online integration between companies, an increasing number of businesses have embraced the use of Internet technologies in order to gain competitive advantage. The wide adoption of these technologies comes with significant challenges- including security [7].

Web security has been broken into three components [3], namely the clients, the servers (or more generally, the server-side) and the communications pathways. These three components constitute the vulnerable areas thoroughly analysed in [9] also identifies six requirements that must be addressed and then the appropriate mechanisms implemented to fulfill. From a business perspective, one common temptation in the pursuit of security is simply to find and implement the latest range of highly rated security technologies. These could range from new intrusion detection systems to the installation of complete antivirus packages. This approach however is inadequate as technologies by themselves do not and cannot solve the security problem. To successfully address these threats a more complete and layered approach is necessary which takes into account laws and industry standards, policies and procedures and also, technology solutions (see [9]).

2.2 Approaches to Web Services (WS) Security

Web services have been defined using different terms and terminologies. For example, as a standardized way of integrating web-based applications using XML, SOAP,

WSDL and UDDI [6] and [13] and as a platform-independent, loosely coupled, self-contained programmable Web-enabled application that can be described, published, discovered, orchestrated and programmed using XML artefacts for the purpose of developing distributed interoperable applications [11]. However, all varying definitions of WS, emphasizes on interoperability, machine-to-machine or service-to-service interaction, mechanism for service description and discovery, platform-independence and the fact that they are self-contained (i.e. expose functionality not implementation (Hartman et al. 2003). In addition to the interoperability characteristics, WS are easy and inexpensive to implement since they use open technologies; and (b) they can significantly reduce the cost of business-to-business (B2B) communications.

While, the use of WS has substantial advantages to e-Business, they also come with many challenges – one of which is the security vulnerabilities that e-Businesses are exposed to in [1] and [11].

Until recently, technology mechanisms were the main approach for achieving WS security [8]. Technology solutions were quickly needed to respond to immediate security threats. With the wide adoption of WS in e-Business and other large-scale web-based applications, a holistic approach to WS security became apparent because of the inter-business integration allowed by WS, plus the high level of communications now readily expected, the use of agreed-on cross-organisational policies becomes an even more critical consideration. As increasing amounts of e-Businesses adopt WS and thus open their precious internal processes and workflows, trust between organisations is a crucial requirement. Thus frameworks such as the Web Services Security roadmap proposed by IBM, Microsoft and VeriSign became a roadmap for research and development in WS where policy component including the overall system design and implementation mechanisms all play critical roles (Hartman et al., 2003). A model-driven approach to define WS security architecture was proposed and explained in Nakamura et al. (2005). This approach does not provide a method with which to produce software requirements.

The main aim of this research therefore is to investigate the use of agreed-on, cross-enterprise policies in Web services (WS) security, to determine whether they can significantly aid in enhancing the security currently provided. The next section presents the proposed security model.

3 Web Services Security Model

Section 2 examined Web services (WS) security and assessed the role and use of policies in these security solutions. Given the significance and the need for the use of policies, this section describes a policy-based WS security model. To achieve this aim, the main approach adopted has been a careful definition of a specific WS-based case scenario followed by a detailed analysis of its interactions and requirements.

The case features an e-university, its e-bank and an e-hotel and by its very nature, demands an extremely high level of trust between all entities. With these aspects as a basis, the proposed high-level model is then defined with emphasis placed on some generic cross-enterprise policies. These policies act to provide a more clear illustration of the model's focus, but also to provide general policies that can be applied to most WS scenarios.

Section 3.1 presents the case scenario and its analysis followed by a detailed analysis of requirements in Section 2.2. Section 3.3 presents a proposed model.

3.1 e-Business Case Scenario

The business scenario used in this research consists of the various transactions that occur between four main entities - a student, an e-University, the e-University's e-Bank, and an e-Hotel. For completeness, two other entities are highlighted, these being the student's e-Bank and the e-hotel's e-Bank.

Figure 3.1, is a graphical representation of all these entities followed by a basic description of each participating entity. This scenario assumes that e-University did have previous business relations with e-Bank and the e-hotel. However, previous communication did not use WS technologies to facilitate the cross-organisational communication.

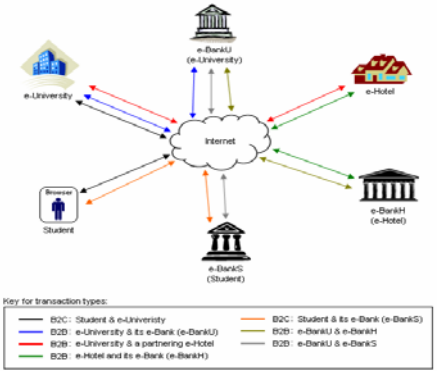

Fig. 3.1. Graphical Representation of the case Scenario

- Student and his/her e-bank (e-BankS). A student represents a person who is either a prospective student applying to the e-university or a current student of the e-university. A student uses the university's site to: (a) apply, register and access course content online; (b) to arrange for course fee payments; and (c) to find and arrange payment for temporary accommodation.
- E-University and its e-bank (e-BankU). E-University is a university (or more generally, an e-business) that offers online education to students. It also acts as an interface for students that allow them to do task (b) and (c) above. Its e-bank plays a critical role in enabling and handling the payment instructions received at the university's web site. In effect, all these instructions are passed to the e-bank for processing. Once completed, it is expected to inform the e-university and other necessary parties.
- E-Hotel and its e-bank (e-BankH). E-Hotel is essentially a business that holds information on a number of accommodation properties available for rent to students of e-University. Its e-bank's purpose is to support its online transactions especially the receiving of payments in lieu of student accommodation fees.

Having identified the main entities, the following steps are a walk-through of how these entities work together:

- **Step 1: Student contact with e-University** – Students may be required to be at the e-university campus for either examinations or for a prescribed residential course. To find temporary accommodation for the duration of their stay, they access the university's website and login using a username and password. By logging in, they are able to browse; upon logging in they see a list of properties available for temporary rental.
- **Step 2: E-University contact with e-Hotel** –Once a property has been selected; a payment instruction is made by the student at the university's web site to start the booking process. This instruction primarily uses the student's bank details, which are stored on e-University's records.
- **Step 3: E-University contact with its e-bank (i.e. e-BankU)** – Upon receiving this payment instruction, e-University passes the student's and e-Hotel's bank account details to e-BankU with the instructions for processing. e-BankU validates and verifies each incoming instructions using steps 4 and 5 below.
- **Step 4: E-BankU contact with Student's e-bank (i.e. e-BankS)** – E-BankU contacts the student's e-bank and arrange for the funds to be taken from their account. The amount may be stored at e-BankU temporarily.
- **Step 5: E-BankU contact with e-Hotel's e-bank (i.e. e-BankH)** – The next step involves taking a specified percentage of this amount, which the e-university charges to the e-hotel as a referral fee, then transferring the remaining amount to e-Hotel's account at e-BankH.
- **Step 6: E-BankH contact with e-Hotel** – Having successfully received the payment from e-BankU in respect of the accommodation booking, e-BankH informs e-Hotel of the payment receipt.
- **Step 7: E-Hotel contact with e-University** – Once the e-Hotel receives this confirmation for accommodation fee payment; it contacts the e-university to verify that the booking for a specific student (identified by name) and property is now complete. It also updates it records to show this that this property is no longer available.
- **Step 8: E-BankU contact with e-University** – Upon completion of the payment process originally instructed by the e-university, e-BankU sends an acknowledgement to the university.
- **Step 9: E-University contact with e-Hotel** – This acknowledgement in addition to the verification received from the e-hotel acts to confirm the booking process. Now, the full accommodation booking details (e.g. specific property and time of stay) and the necessary student's details (e.g. name, contact information) are sent from e-University to e-Hotel for it to update the necessary records.
- **Step 10: E-University contact with Student** – Finally, the e-university notifies the student of the successful booking of the selected accommodation by email.

With the general case scenario outlined, functional requirements for each of the entities have been analyzed leading to the definition of the main security requirements presented in the next section.

3.2 Security Requirements

Based on the functions of each entity's system and the main services it should provide an assessment is now made into where exactly, aspects of security would be needed. From a policies point of view perspective, all e-businesses (or organisations) must typically have their internal policies. Below is an outline of five top-level, security-specific policies for e-University, e-Bank and e-Hotel. The list is not intended to be exhaustive but to focus on the specific areas that will be considered for this scenario.

1. All of e-University's information and services is categorized into two main classifications:
    a. Public – declared public knowledge by someone with the authority to do so
    b. Confidential – all other information. This information is further divided into:
        i. HIGH priority – declared at this level by someone with the authority to do so. Very sensitive information that must be highly secured
        ii. LOW priority – all other information. Security here is also required but at a reduced and basic level

    For all confidential information, it should be secured whether in storage or in transit.
2. Remote access to the company's internal information and services (web site being an example) which deemed to be confidential must be accessed in a secure manner and by authorised entities.
3. An e-business and thus always open via the Internet, measures should be taken to ensure persistent and consistent availability of services.
4. All personnel are to be classified into specific user groups that link to their job roles and responsibilities in the organisation.
5. Measures should be taken to ensure that persons can only access the accounts, data, information, system capabilities to which they have been strictly authorised.

These general policies have been analyzed into specific low-level security requirements for each participating organization – e-University, e-Bank, and e-Hotel used to define the proposed model in the next section.

3.3 The Model

The first policy is to ensure that each business has its own security policies, A layered approach defined in [7] and [9] has been adopted to secure each individual business entity according to their defined requirements.

Having secured the individual e-business Business, the next aspect is to secure communications between entities. One option to address this aspect is to simply perform the necessary service bindings to the consumer/provider's service and let the business's security setup interact with the consumer/provider's Web service. However, as highlighted in the literature review section, this approach only focuses on the technology solution to service interactions. Thus, an approach that allows participating organisations to partner and define a framework (agreed-upon policies) with which the security of the entire communications (internal and external to each

business) is proposed. External communications are defined as everything that goes on external to an e-Business within the service interactions.

The goal of this policy oriented security framework would be to give each entity some level of assurance for security of the overall WS communications especially those outside their own control. By partnering and defining cross-enterprise policies, one substantial achievement to be made is that of a new level of trust between all entities. These agreed-on policies would clearly outline requirements for the overall WS communications and purport a level of trust beyond that attainable with technology solutions. Figure 3.2 is a diagrammatic representation of the proposed model.

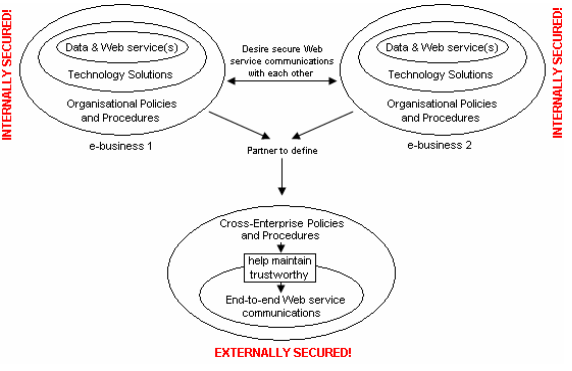

Fig. 3.2. A Model for enhancing WS security

From Figure 3.2, each business entity is required to ensure that their businesses are internally secured. Once this is done and they are ready to offer their services externally they essentially 'Desire secure Web service communications'. At this point, they then move to partner to define cross-enterprise policies and procedures that help maintain trustworthy end-to-end WS communications. The process of partnering to define cross-enterprise policies may require that additional security policies and mechanisms be in place for some or all organizations. The model also defines a set of generic Cross-Enterprise Policies and procedures applicable to a wide range of WS scenarios.

4 Conclusion and Future Work

The proposed model is currently being implemented and evaluated in a two-step process. The first step assumes that each business has its own internal policies, procedures, and technology solutions to protect its data and now, Web services. The next step is the definition and application of the cross-enterprise policies and procedures that will enhance the overall security of the WS communications. These policies can be seen to provide a wrapper to allow for this enhanced level of security.

The vast benefits attainable through Web services (WS) usage in e-business will undoubtedly make this pair a force in the future. As show however, one hindrance to WS widespread adoption is the new security concerns it introduces. Unless concerns

are adequately addressed, the advantages possible with WS will be remain as theory and never put into widespread practice. This WS security formed the basis of this report paper and its research investigated into the use of cross-enterprise policies for enhancing the currently provided security solutions

Future work considers two specific areas: (a) continued development of the proposed Web services security model, especially the generic cross-enterprise policies; and (b) the critical and thorough evaluation of this model.

References

1. Bebawy, R., et al.: Nedgty: Web services Firewall. In: IEEE International Conference on Web Services, ICWS 2005 (2005)
2. Boncella, R.: Web Services for E-Commerce. Communications of the Association for Information Systems 4(11), 4–14 (2000)
3. Boncella, R.J.: Web Services and Web Services Security. Communications of the Association for Information Systems 6(14), 344–363 (2000)
4. Cavanaugh, E.: Web services: Benefits, challenges, and a unique, visual development solution, http://www.altova.com/whitepapers/webservices.pdf (accessed 3 June 2006)
5. Chaffey, D.: E-Business and E-Commerce Management, 2nd edn. Pearson Education Limited, Essex (2004)
6. Chatterjee, S., Webber, J.: Developing Enterprise Web Services: An Architect's Guide. Prentice Hall PTR, New Jersey (2004)
7. Davidson, M.A.: Security for eBusiness. Information Security Technical Report 6(2), 80–94 (2001)
8. Krawczyk, K., Weilgus, M.: Security of Web Services. In: International Conference on Dependability of Computer Systems (DEPCOS-RELCOMEX 2006), pp. 183–190 (2006)
9. Laudon, K.C., Traver, C.G.: E-commerce: business, technology, society, 2nd edn. Addison Wesley, Boston (2004)
10. Nakaruma, Y., Tatsubori, M., Imamura, T., Ono, K.: Model-driven based security based on web services security architecture. In: IEEE International Conference on Services Computing (SCC 2005). IEEE Computer Society, Orlando (2005)
11. Papazoglou, M.P., Ribbers, P.M.: e-Business: Organizational and Technical Foundations. John Wiley & Sons Ltd., West Sussex (2006)
12. Pulier, E., Taylor, H.: Understanding Enterprise SOA. Manning Publications, California (2005)
13. Rowan, L.: Security in a Web Services World in Network Security, June 2005, vol. 2005(6) (2005)
14. Steel, C., Nagappan, R., Lai, R.: Core Security Patterns. Prentice Hall PTR, Englewood Cliffs (2005)
15. Young, K.: UK firms surf the e-business wave (2005), http://www.itweek.co.uk/vnunet/news/2144211/uk-business-internet-soaring (accessed 29 May 2006)