Association for Information Systems

AIS Electronic Library (AISeL)

ICEB 2002 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-10-2002

Building an End-To-End Security Infrastructure for Web-Based Aerospace Components E-Trading

Stephen C. Shih

Follow this and additional works at: https://aisel.aisnet.org/iceb2002

Building an End-To-End Security Infrastructure for Web-Based Aerospace Components E-Trading

Stephen C. Shih
Department of Information Management Systems
College of Applied Sciences and Arts
Southern Illinois University
Carbondale, IL 62901-6614, USA
shihcs@siu.edu

Abstract

The research paper focuses on the development of a generic framework and architecture for building an integrated end-to-end security infrastructure and closed-loop solution to secure e-commerce and m-commerce. As an integral component, an intelligent decision support mechanism is developed in helping systems designers and managers make architectural, design, implementation, and deployment decisions on employing particular security solutions to issues and requirements arising in various e-commerce and m-commerce scenarios. In addition, this research identifies the key features, options and benefits of several security technologies as well as provide guidelines in managing the costs and complexities involved in the deployment of those security solutions. As an important groundwork for building a prototype based on the proposed research work, a study has been conducted to investigate the current B2B e-commerce operations between Pratt & Whitney (P&W) [15] (a division of United Technologies Corporation (UTC) [17]) and its partnering e-business and supply chain players in the aviation industry.

1. Research Objectives

Addressing the essential security issues and needs in e-commerce and m-commerce, an integrated and scalable security infrastructure is crucial to enable a company to reap substantial business values and financial benefits by safeguarding online transactions according to the policies, processes and procedures unique to its business.

As a significant research result, the proposed common framework will help a company achieve its security objectives in different dimensions as follows:

1) Construct an integrated, flexible and scalable security infrastructure that tightly fits in with other corporate e-business, supply chain management, customer relationship management, and enterprise resource planning (ERP) applications as well as with those of its customer and business partners.

2) Develop a security architecture with segmental entities (computers, local networks, private networks, public networks, etc.) to help isolate and identify the security issues, possible attacks, data vulnerability, and associated security requirements and in turn find attainable solutions to address specific requirements (specified assurance levels, security services, etc.) for each entity in various B2B interaction scenarios.

3) Reduce the chance of a security breakage by removing security issues from the application level and raising them to an architectural level.

4) Provide proactive and reactive security strategies, policies and guidelines.

5) Provide decision support capability [16] for selecting security tools and technologies as well as managing the costs and complexities involved in the technology deployment.

2. Background of E-Commerce Security in Aerospace Industry

B2B e-commerce for online trading of aerospace and aviation components is still in its infancy [9]. The potential of using the Web as a B2B commercial medium has been widely explored. However, a critical assessment of its B2B e-commerce challenges and issues has just started to receive attention. The new economy of ubiquitous B2B e-commerce usually introduces new risks [7], [8].

Based on the initial study, P&W's customers and suppliers can process online transactions through either private corporation e-business channels or via semi-private web-enabled exchanges (e.g., Cordiem [12] and Exostar [13]). E-business transactions in a B2B environment can happen in the context of a bilateral or multilateral exchange. Such a virtual marketing environment gives unprecedented open participation of business trading and information sharing. As submerging

under the uncharted waters, each type of exchange may raise significant issues and concerns threatening the objective of establishing a secure trading environment between P&W and its e-business counterparts (customers, suppliers, and other business partners). Without proper security measures and strategies, it will make e-marketplaces susceptible to such incidents as denial of service (DoS) attacks (which will halt on-line operations [10]), 'bid snatching' (wherein a set of malicious colluding agents halt another agent by using attractive bids to fraudulently 'snatch' and non-perform on all the targets' subcontracts), 'bid collision loops" (where a pair of agents halt online B2B transactions by establishing an infinite loop of colliding bids), and so on. This project effort specifically tackles one of the threads to this resource availability, the denial of service (DoS) attack [7], and suggests a viable solution to preventing possible loss of business due to the fact that P&W's data are made impossible to access by the legitimate customers or suppliers.

Electronic markets (e-markets) also give unprecedented scope to the deployment of relatively untested marketing and bidding mechanisms whose vulnerabilities have not been fully explored [18]. The consequences may thus bring forth the potential for serious disruptions in B2B operations of targeted business trading participants and/or the e-markets themselves.

3. E-Business Security Requirements

Addressing the potential risks and pressing issues of on-line B2B trading, this research project tackles a number of challenges in various e-commerce scenarios, such as client authentication, server authentication, authorization, etc. Proper access control is important. In other words, the company needs to know that the customers or suppliers who involve in a B2B dialogue are in fact who they claim they are, which can be referred to as "*client authentication*." On the other hand, when the customers or suppliers access a web site in the B2B e-marketplace, they want to make sure that they are indeed interacting with that site and not with an impostor. This is referred to as "*server authentication*." It is also necessary to control what information which business partners are allowed to access and/or modify. In addition, a reliable access for external players to gain access to a company's e-business ballpark and interact with the specified data is one of the critical requirements – all the legitimate B2B players should be able to access the required resources at any time under optimal performance.

Electronic data traveling on a complete supply chain and B2B environment requires more than access control. Authorization is recognized as another important security criteria and recognized as a problem with greater complexity than authentication and access control. The user privileges of the corporate customers and suppliers should be manageable and interchangeable across enterprise applications as well as other B2B communities of security domains. Furthermore, it is required that pertinent business rules and constraints should be dynamically weighed up coupling with fine-grained role privileges for initiating and committing required business transactions and processes.

"Integration" is a key to the proposed common framework for ensuring that all the security decisions (on authorization, authentication, auditing, etc.) that implement on each enterprise application and exchange point are consistent with those made across the entire B2B arena. The security infrastructure should be pervasive across the entire enterprise to establish greater communities of trust. As more and more business partners exchange trading information via various network connections (a private network, Internet, etc.), different security control services and standards are indispensable. The proposed security infrastructure is open in nature to ensure sound security interoperability – the capability of supporting heterogeneous security standards and platforms as well as different e-business interaction models and security services.

4. Research Methods

An engineering and scientific approach [11] is adopted to the research tasks undertaken in this project. Primarily, the following methods [1], [2], [3], [5] are used to validate the proposed framework:

1) **Conceptual Design.** To construct a conceptual security framework and an integrated, flexible and scalable security architecture that tightly fits in with P&W's enterprise resource planning applications as well as with those of its customer and business partners.
2) **Security Solutions Evaluation.** To evaluate a number of state-of-the-art security solutions and technologies (such as Entrust's Privilege Management Infrastructure integrated with XMI, ebXML, and Security Assertions Markup Language) and elaborate how the solutions fit into the entire security framework.
3) **Cases and Best Practices Study** [4], [6].
4) **Scenario-Building**. To develop a series of scenarios to test the security requirements of different segmental entities (computers, local networks, private networks, public networks, etc.) to help isolate and identify the security issues, possible attacks, data vulnerability, and associated security requirements and, in turn,

find attainable solutions to address specific requirements (specified assurance levels, security services, etc.) for each entity in various B2B interaction scenarios (Figures 1 and 2).

5) **Laboratory Experimentation [14] and Simulation**. To create an artificial environment, in order to isolate and control for potentially confounding variables; to conduct the study of a simplified, formal model of a complex e-commerce environment, in order to perform experimentation not possible in a real-world setting.

5. Research Results

Key outcomes of this research effort as well as major benefits from deploying the proposed framework are summarized in the following paragraphs:

5.1 An Integrated Security Framework

The developed framework **is** used to examine the explosion in B2B e-commercial activity on the Web especially for a company and its business trading partners. The framework provides a viable decision support mechanism in making architectural, design, implementation, and deployment decisions on employing particular security and connectivity solutions to issues and requirements arising in various B2B e-commerce scenarios.
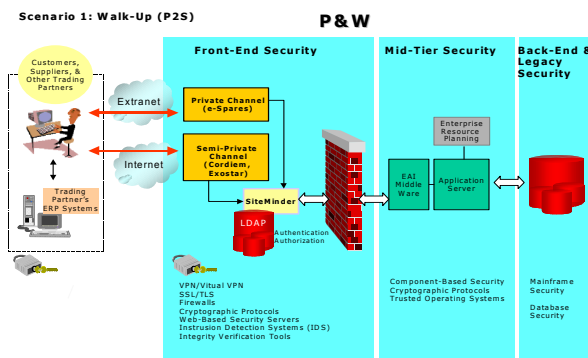

Figure 1. Aviation B2B E-Commerce Security Architecture: Transactional Scenario 1: Person/Human-to-Systems (P2S) Interaction.
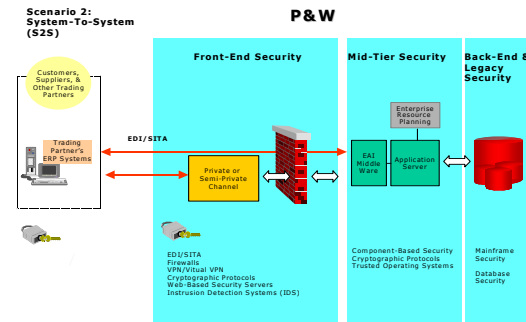

Figure 2. Aviation B2B E-Commerce Security Architecture: Transactional Scenario 2: Systems-to-Systems (S2S) Interaction.

5.2 A Decision Support System for Web Security Analysis

Security involves a total set of exposures in B2B e-commerce. Besides storing on computers, transactional data need to travel from within the perimeter of company's network (Intranet) to the space of its suppliers' and business partners' enterprise applications through Extranet or Internet as well as to voyage to the terrain of its customers via Internet. As a result, it is unattainable to maintain a robust security control by simply implementing an "one-size-fits-all" solution. Data traveling between diverse communication dimensions need to be secured differently. For instance, each of the communication points may have its own authentication and authorization policies and schemes. Accordingly, a decision support Expert System (ES) is to be developed to aid the corporate security analysts in finding a fitting security solution and configuring proper settings at each of the network points throughout the entire B2B chain. In the research, the security requirements are identified and categorized based on different needs on the two sides of an e-marketplace:

The Seller Side. The selling parties in the B2B e-marketplace are mostly interested in the identification and authentication of users (buyers). The sellers are concerned with acquiring adequate buyers' data and installing robust security measures for billing and other business transactional purposes, such as preventing the sender of a message from denying having sent it and mitigating the risks of so called Denial-of-Service attacks.

The Buyer Side. The participants on the buyer side in the e-Marketplace share a common interest in the

integrity and confidentiality of the information transmitted. Usually, buyers are more interested in reliable services and expect their privacy to be soundly protected. In most of the cases, they may prefer to use services without being identified and being monitored of their every single movement on the Web by the unrelated business parties.

Consequently, the first phase in the decision support ES construction focuses on the six essential security requirements shown as in Table 1.

Table 1. Security Requirements on Buyer's and Seller's Sides

	Security Category Code	Requirement	Description
Seller Side	A1	Authentication	Verifying that the trading partners are really who they claim they are. A process is necessary to proof the two parties involved in a B2B interaction are given a guarantee that they are indeed interacting with whom they think they are interacting.
	A2	Authorization	Ensuring that each business party is performing what it is authorized to do.
	A3	Availability	Tacking the Denial of Service (DoS) attacks .
	NR	Non-Repudiation	Preventing the sender of a message from denying having sent it.
Buyer Side	C	Confidentiality	Protecting the contents of messages or data transmitted over the Internet from unauthorized people.
	DI	Data Integrity	Shielding sensitive trading information from being modified or tampered by an attacker.

Based on specific security needs and scenarios, the decision support ES (with the code name, AirB2B SecurityGuru) will be assisting in finding corresponding security solutions. For instance, a viable authentication technology will be recommended to tackle A1 requirement while a proper authorization solution and an encryption solution is suggested to address the access control and the tampering issues, respectively. Furthermore, the user is allowed to enter English-like questions on any specific security problems via natural language processing.

As a powerful tool, the ES can give consultations in the following areas:

- Identify assets and vulnerabilities to known threats
- Identify likely attack methods, tools, and techniques
- Establish proactive and reactive strategies
- Develop an incident response plan
  - Developing incident handling guidelines.
  - Identifying software tools for responding to incidents/events.

5.3 Security Solution Matrices

One of important deliverables of this research effort is to construct a pertinent security solution matrix for providing information and assessment on various feasible solutions to security needs (at both the company side and trading partner's side) based on a given scenario.

5.4 A Security and Performance Analysis Model

Security is an important element in B2B interactions but performance is the price to be paid to meet the desired security criteria. Therefore, it is

important to determine the adequate level of security for special e-business exchange scenarios without incurring unnecessary costs and sacrificing too much system performance. In this research, the decision of the degree of security is modeled as an optimal function of resource protection, system performance and the security-related costs (infrastructure, implementation, maintenance and processing costs, etc.)

5.5 A Laboratory Experimentation and Simulation Environment

A laboratory environment is built to simulate various B2B interaction scenarios (system-to-system or person-to-system). Based on the existing security countermeasures and infrastructure, the lab environment helps identify vulnerabilities in various spots in the entire e-business chain (such as Internet connections, remote access points, connections to other business partners, physical access to network hardware, and user access points) and the type of treats. Performing such simulations and experiments will assist in determining the risk levels (system-level, network-level, or organization-level) and, in turn, seeking for a set of viable solutions (including technologies and processes) to address specific security attacks and needs.

In the developed simulation environment, a number of essential B2B Actors" are created to simulate how those key business trading actors interact with each other in various B2B transactions. Some of the key B2B actors identified in the first phase of this research effort are: CUSTOMERS, PARTNERS, SUPPLIERS, REGULATORS, MEDIATORS, and INTERNAL EMPLOYEES.

6. Conclusions

Besides the technical aspect of the B2B e-commerce discussed in this paper, an equally important organizational issue is to be dealt with to ensure a truly secured and safe e-marketplace for doing business on the Web -- *trusts* among business partners. To fully utilize the advantages of the open and ubiquitous technology of the Internet, trust makes it possible for extensively cooperative and collaborative endeavors among various players in the B2B e-marketplace. Trust is a key to positive interpersonal and inter-organizational relationships in various settings. Trust becomes even more central and critical to sustain everlasting business relationships, especially, when a great deal of sensitive business data are required to be shared among business partners over an Internet-based network. As a result, one of the future research efforts will be focusing on conceptualization of business trust model which should be cross-organizational in nature. Research work in other

disciplines (e.g., social science and organizational behavior) on trust will be studies and compared. Ultimately, the development of new e-business models for innovative business processes reengineering is perceived as one vital research activity for achieving to truly *trusted and trusting* B2B e-commerce environment.

References

1. Alavi M. & Carlson P. (1992) 'A Review of MIS Research and Disciplinary Development' J. Mngt Inf. Syst. 8,4 (Spring 1992) 45-62.
2. Baskerville, R. and A. T. Wood-Harper (1998) 'Diversity in information systems action research methods' European Journal of Information Systems 7, 2 (1998) 90-107.
3. Benbasat I. (1984) 'An Analysis of Research Methodologies' in McFarlan (1984), 47-88.
4. Benbasat I., Goldstein D. & Mead M. (1987) 'The Case Study Research Strategy in Studies of Information Systems' MIS Qtly 11,3 (September 1987) 369-386.
5. Cash, J.I. & Lawrence, P.R. (Eds.) (1989) 'The Information Systems Research Challenge: Qualitative Research Methods' Volume 1, Harvard Business School, 1989
6. Cavaye A.L.M. (1996) 'Case Study Research: A Multi-faceted Research Approach for IS' Information Systems J. (1996) 227-242.
7. Clarke R. (2001) 'Introduction to Information Security', February 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/IntroSecy.html
8. Clarke R. (2001) 'Trust in Cyberspace: What eCommerce Doesn't Get' at http://www.anu.edu.au/people/Roger.Clarke/EC/TrustCLE01.html.
9. Clarke R. (1997) 'Electronic Commerce Definitions', January 1997, at http://www.anu.edu.au/people/Roger.Clarke/EC/ECDefns.html .
10. Clarke R. (1997) 'Data Surveillance: Theory, Practice & Policy', July 1997, at http://www.anu.edu.au/people/Roger.Clarke/DV/ICIS97.html .
11. Clarke R. (1996) 'Appropriate Research Methods for Electronic Commerce', June 1996, at http://www.anu.edu.au/people/Roger.Clarke/EC/ResMeth.html.
12. Cordiem, http://www.cordiem.com/.
13. Exostar, http://www.exostar.com/.
14. Jarvenpaa S.L. (1988) 'The Importance of Laboratory Experimentation in Information Systems Research' Commun. ACM 31, 12 (December 1988) 1502-1504.
15. Pratt & Whitney, http://www.pratt-whitney.com/

16. Sprague R. (1980) 'A Framework for Research on Decision Support Systems' MIS Quarterly 4, 5 (1980) 1-26.
17. United Technologies Corporation, http://www.utc.com.
18. Zwass V. (1996) 'Electronic Commerce: Structures and Issues' Int'l J. Electronic Commerce 1,1 (Fall 1996) 3-23, at http://www.mhhe.com/business/mis/zwass/ecpaper.html .