Security Requirements for Online Stores: 
Development of Use Cases and Security Use Cases

Drew Hwang
Computer Information Systems
California State Polytechnic
University, Pomona
Pomona, California, USA
dhwang@csupomona.edu

Ming Wang
Information Systems
California State University, Los Angeles
Los Angeles, California, USA
ming.wang@calstatela.edu

Zhongmin Ma
Computer Information Systems
California State Polytechnic
University, Pomona
Pomona, California, USA
zma@csupomona.edu

Abstract: Online retailing is considered as one of the most prevalent business models of electronic commerce today, but security concerns are making negative impact on online retailing sales. Integrating security requirements early into the development of online stores is a vital task. This paper presents a framework that integrates online store system architecture and system goals to capture store functionalities in a systematic and modular manner. Using this framework, online store developers can systematically and effectively develop use cases and security use cases early in the development lifecycle.

Keywords: E-commerce Applications; Online Stores, Web Application Security; Security Requirements Elicitation

1. Introduction

Online retailing is considered as one of the most prevalent business models of e-commerce today. But as Internet users are increasingly dismayed and frightened over the rising rates of a variety of Internet threats, security concerns are making negative impact on online retailing sales (Gartner Group, 2006). According to CyberSource Corp., a division of Visa Inc., retailers’ revenue lost to online fraud reached an estimated $3.5 billion, up 3% from 2011 and 30% from 2010 (Cybersource, 2012).

Today’s web platform suffers higher risk introduced through its exposure to anonymous users and the involvement of various parties (i.e., suppliers, distributors, customers, and partners), thus making ecommerce systems a target for both accidental and intentional distortion, distribution and deletion of critical transaction data (Anton and Earp, 2000). Although the environmental factors contributing to the security problems cannot be ignored, the failure of secure web engineering has received tremendous attention. Research has found that insecure web applications are being developed by web programmers who either lack of adequate security training (Firesmith, 2003) or interest in eliciting security requirements (Mouratidis et al., 2005). In many cases traditional software requirements techniques are found to be difficult to apply (Mouratidis et al., 2005), and the testing methodologies for the audit and control of web development were overly insufficient (Mansour and M. Houri, 2006).

Rigorous efforts have been made to develop approaches that integrate security requirements early into software development, and these approaches undoubtedly have their merits (Haley et al., 2008; Huang et al., 2012). In order to facilitate the integration process of security requirements, many of these approaches explicitly define a set of well-defined tasks to follow and typically recommend the use of system goals and such artifacts as use cases, security use cases, and misuse cases (Tondel et al., 2008). System goals are success factors for a system. In requirements engineering system goals are generally considered essential in the development of system requirements. For the use of the artifacts, however, Firesmith (2003) cautions that system developers should focus on security use cases in the process, because misuse cases are only effective in analyzing security threats. Thus, the nature of misuse cases would inevitably make the development of security use cases a hit-and-miss task.

This paper presents a framework that integrates store system architecture and systems goals to capture store functionalities in a modular manner. Using this framework, online store developers can systematically and effectively develop use cases and security use cases early in the development lifecycle. The reminder of the paper is organized as follows. Section 2 discusses the system architecture of online stores. Section 3 reports a synthesis and summary of system goals for online stores. Section 4 illustrates how the framework integrates both the system architecture and the system goals of
online stores and provides an example of how to use the framework to develop use cases and security use cases. Section 5 explains some of the recommendations of the framework and concludes.

2. System Architecture of Online Store

"E-Commerce" is commonly viewed as the sale and purchase of products and services over the internet, which includes the sharing of business information, maintaining business relationship, and conducting business transaction by way of Internet based technology. "Online retailing" can be defined a business model of e-commerce that uses Internet-based technologies to "facilitate efficient and effective shopping, purchasing and delivery of goods or service". Shopping is browsing and searching; purchasing is ordering and paying; delivery is post-sale service.

Several attempts in the literature have been made to formulate system architecture of online stores. To analyze business-related Internet strategies, Lieu and Barnett (2000) divided functions of e-commerce websites into three structural phrases of marketing activities: pre-order, online sales, and after sales. In Rowley's (1996) view, an Internet online transaction is generally consisting of five structural components: promotion, one-to-one contact, closing, transaction, and fulfillment. Taking a customer-oriented approach to commercial website design, Wan (2000) expanded and modified Rowley's component structure to focus on four core structural processes: promotion (advertising, brand identity), pricing (catalog), transaction (ordering, delivery, logistic, payment), and services (information search, advice). Finally, Yeung and Lu (2004) developed an analytical grid framework to address the functionality of commercial websites in general. The grid covers a multitude of websites functions across a wide range of electronic commerce activities including advertising, sales, customer service, distribution, financing, and market research. The grid also classifies website functions into four types: information, communication, downloading, and transaction.

In summary, the system architecture of online stores is consisted of the following modules:

- **Catalog**: Customers are able to navigate, filter, and search product categories within a single or multiple levels of category structure.
- **Marketing**: To increase Internet awareness and competitiveness, online stores are often designed and structured in a way to effectively pursue a Search Engine Optimization (SEO) campaign.
- **Communication**: Businesses use various ways (e.g., RSS feed, FAQ, Help desk, etc.) to communicate with their current and potential customers.
- **Transaction**: Each visitor is assumed to be carrying a "shopping cart". During the shopping process, the customer can maintain the shopping cart by deleting an item, increasing the purchased quantity of an item, or simply emptying the whole cart to start it over. Once the shopping is done, the customer will proceed to the payment process where he/she supplies necessary information related to payment, shipping, and discount.
- **Fulfillment**: Products sold online should ultimately be transferred to the buyer terrestrially or digitally.
- **Support**: Online stores may allow the customers to maintain their account information and access to other business information such as order status, payment status, delivery schedule, and many others. Customers may also be able to request and process return and/or refund online.
- **Administration**: Many advanced online stores allow the store owners to maintain their product catalog, product information, and promotion choices and policies online.

3. System Goals of Online Stores

This paper uses Delone and Maclean's (2003) model of IS success to synthesize and organize these various success metrics. The Delone and Maclean's model proposes that Information Quality, System Quality, and Service Quality are the three key dimensions that would affect e-commerce success.

3.1. Information Quality

- **Information Availability**: While availability is not a new attribute of information, the importance of information availability as a system goal has grown tremendously due to the criticality of systems that are now operating in the distributed computing environment.
- **Organization of Information**: Online store content should be structured using effective and intuitive taxonomy, naming and labeling. Well-defined categories always make it easier for customers to find what they are looking for.
• **Quality of Information:** Information presented on an online store captures the perceptions of consumer regarding the characteristics of the website content as accuracy, comprehensiveness, reliability, relevance, and usefulness. In fact, these measures represent different aspects of the quality of the information.

3.2. System Quality

• **Usability:** With the emergence of the Internet there has been additional pressure for the design to be usable, because often there is no opportunity to train customers to use the software.

• **Layout:** The layout of an online store refers to the underlying website structure (e.g., tree structure) that would significantly impact a retailer's overall performance.

• **Navigability:** A successful online store should employ an efficient and effective scheme of navigability to enable consumers to find information or products in a way that is meaningful to them.

• **Usefulness and Ease of Use:** Perceived usefulness refers to the degree to which a person believes that a particular information system would enhance his or her job performance by reducing the time to accomplish a task or providing timely information, while perceived ease of use refers to the degree to which a person believes that using a particular system would be free of effort.

• **Experience:** As Internet shopping grows, the action of online shopping has become an experience more than a task.

• **Playfulness:** A satisfied customer not only comes from an extrinsic reward of purchasing products or services but also from personal and emotional reward from purchasing-derived pleasure or enjoyment.

• **Interactivity:** Today's ecommerce activity is basically a function of interactivity between customers and business enterprises.

• **Search Capability:** A successful online store should incorporate friendly and powerful search capability that enables consumers to locate the product they want more efficiently and effectively.

• **Personalization:** Personalization such as personalized search facility and catalog can be integrated into the store design to increase long-term relationship with the consumers and the store's long-term benefits.

• **Decision Support:** An online shopping store can provide decision support capabilities for searching, comparing, and finally recommending a product to the customers.

• **Technology:** The extent to which the technology simplifies the site and makes the visit successful can be evaluated on both reliability and progressiveness.

3.2. Service Quality

• **Responsiveness:** Online store responsiveness means functionalities (e.g., online order tracking, FAQ, etc.) designed to prompt delivery and response to the concerns or inquiries of its customers.

• **Trust:** Providing accessible privacy information reduces the information asymmetry gap between merchants and consumers and leads consumers to purchase from online retailers who better protect their privacy. Confidentiality has been the primary goal of information assurance, because there has been and continues to be a desire for systems to be trusted.

4. The Use of the Framework

Based on the store system architecture and system goals, a 2 x 2 framework in a matrix format (see TABLE 1) can be formed, with the horizontal axis distinguished between store architectural modules and the vertical axis of the matrix distinguished between system goals. In the framework each intersection in the grid represents a functional scenario for an online store to develop its functionalities (i.e. use cases) to achieve its system goals, whereas each function and data asset to be developed must also be examined to address security concerns (i.e., security use cases). Thus, this framework can be used for systematic and effective development of use cases and security use cases for online stores.

Note that the framework is rather broad and flexible. Using this framework, online store developers must systematically examine either all the working domains or those that would best represent the online store’s interest and technological competency. As an illustration, this paper illustrates the use of the framework by examining the “Catalog” module. For the taxonomy of web-based security use cases, this paper adopts those formulated by Firesmith (2003), which include Identification, Authentication, Authorization, Immunity, Integrity, Intrusion, Non-repudiation, Privacy, and Audit. The process of identifying use cases and security use cases for the “Catalog” module is consisted of three steps. The first step is to identify possible system goals in the three quality dimensions of the Delone and Maclean's model of IS success (i.e., information, system, and service), followed by the identification of store functions and data assets to be
created to achieve these system goals. In the last step security use cases are developed by analyzing potential security vulnerabilities and threats associated with each functional scenario.

Assume that an online store decides to enhance the quality of its catalog browsing to achieve the following system goals:

- **Information Quality**: To publish an online catalog that makes product structure and product information available through an effective scheme of information organization and of high quality; to provide relevant and useful product review information.
- **System Quality**: To employ adequate technologies in the design of the online catalog that has an effective layout and offers site features such as ease of use, search capability, decision support, and interactivity.
- **Service Quality**: To offer prompt responsiveness by enabling customer to send direct product request and receive instant inventory notification.

To meet these system goals, the online store must develop and employ a number of functions and data assets as shown in FIGURE 1. For example, in order for customers to be notified instantly when the inventory is back in stock, the online store needs to develop the “Inventory Notification” function that utilizes three databases: “Customer,” “Product,” and “Inventory Notification Request”.

Finally, these functional scenarios as use cases are examined carefully to identify potential security vulnerabilities and threats and to develop security use cases accordingly (see TABLE 2). For instance, assumes that the online store intends to use AJAX (Asynchronous JavaScript and XML) technology to enhance the ease of use and interactivity (i.e., system quality goals) of its catalog browsing, the store will have to examine the “Product Navigation” and “Product Search” functions for vulnerabilities that would result in malicious input and unauthorized access through AJAX tunneling. As a result, three access-control security use cases (i.e., Identification, Authentication, and Authorization) are developed. When the online store, in another example, chooses to support customer purchasing decision through comparing competitors’ pricing, the store should then examine the “Competitor Pricing” function for vulnerabilities and threats that would threaten the integrity of the “Competitor Price” database and the viability of its audit tail. Such an examination will lead to the development of a security use case for Integrity and another for Audit.

5. Conclusions and Limitations

This paper presents a framework that integrates store system architecture and systems goals to capture store functionalities in a systematic and modular manner. Using this framework, online store developers can systematically and effectively develop use cases and security use cases early in the development lifecycle, thus avoiding the hit-and-miss pitfall form the inadequate use of misuse cases.

This framework in practice has two limitations. First, the framework reflects a scope of functionalities that would be limited over time. Online store developers should consider the two dimensions of the framework as open-ended, so that the system architecture and system goals can be modified and updated as technology advances, website design paradigm shifts, or marketing competition changes. Second, it is recommended that the framework further integrate other backend and logistics functionalities which are also needed to run an online store. This is especially important when e-commerce systems are becoming an integral part of the whole enterprise architecture for many modern businesses.

References


