E-SECURITY ISSUE

Priyadharshini Arumugam,
Assistant Professor in Computer Science
VLB Janakiammal College of Arts and Science

ABSTRACT

E-Commerce refers to the exchange of goods and services over the Internet. All major retail brands have an online presence, and many brands have no associated bricks and mortar presence. Electronic Business (e-Business) is revolutionizing the way of communication between internal and external stakeholders in an organization. E-business can lead to competitive advantage and at the same time, increase profitability. There are several factors resulting on the success of e-business. One of the most important factors is trust. The electronic business provides enormous advantages. In this paper we discuss a secure system accomplishes its task with no unintended side effects, by classifying the user security concerns into Class A, Class B and Class C impersonation types. We suggest that these vulnerabilities can be linked to a weakness in the user security model. Hence, without forsaking the active model we propose a goal-oriented approach to address the user security needs of the system. Furthermore, a review of the existing solutions depicts insufficient capabilities to minimise all the three classes of impersonation challenges. Hence, we propose that an appropriate blend of existing methods will minimise the types of impersonation threats and improve user security in e-business and also address security concerns in web services

Keywords: E-Business, Security, Problems

INTRODUCTION

Electronic Business which is commonly referred to as e-business, which is the utilization of information and communication technology (ICT) in conduct business on the internet, not only buying and selling but also servicing customers and collaborating with business partner. The electronic business helps the organisation in satisfying their customer needs and expectations. Security reliance plays a vital role in the key success of the e-business and the issues faced are the significant problem on the way to the e-business success.

1. SECURITY OVERVIEW

A computer-based system has three primary valuable assets to protect; they are the hardware, software and data assets. A secure system accomplishes its task with no unintended side effects. The computer security threats which exploit the vulnerabilities of computer assets are interception, interruption, modification and fabrication. The fundamental security goals which ensure that the hardware, software and data assets are not compromised by the threats include Confidentiality (C), Integrity (I), Availability (A) Legitimate Use (L), Auditing Or Traceability (A/T),Non-repudiation(NR)

Confidentiality: Providing access privileges to users in accessing the data.
Integrity: Restricting alteration rights to the original data.
Availability: Data accessible and operational whenever it is required.
Legitimate use: Includes identification, authorisation, and authentication
Auditing or traceability: Process of examining the transactions
Non-Repudiation: ability of an originator or recipient of a transaction to prove to a third party that their counterpart did in fact take the action in question.

Thus, a compromise in the C-I-A-L-A/T-NR security goals may lead to a compromise of the critical assets. Since E-Business is widely implemented by various organisations in order to simplify the purchasing process by the customers. There are many ways in which the customers can be attacked by hackers, crackers, and disgruntled insiders. Some of the common threats include hacking, cracking, masquerading eavesdropping, spoofing, sniffing, Trojan horses, viruses, bombs, wiretaps, etc.

2. USER SECURITY IN E-BUSINESS

One of the problems of the current e-business security implementation is that components of e-business infrastructure tend to be looked at individually and separately for security purposes. The current common "security policy" implemented by most e-businesses runs like this: assemble a catalogue of threats and vulnerabilities and then shop for technology tools that alleviate those concerns. Security solutions are targeted at counteracting specific groups of threats and vulnerabilities. However, what is needed are comprehensive solutions that will produce peace of mind to the business and trust and confidence in customers and partners. A typical three-tier e-business architecture comprises the client, web and commerce servers, and database servers. A systematic implementation of e-business security must ensure that each of these components is secure. This requires security policy and implementation at three levels: network security, system level security and transaction level security.

Due to the high-stake nature of E-Business, the system bases much of its security on knowing that only a legitimate customer can gain access to the online transactions. Thus, one of the characteristics of an e-business system is the ability to securely provide a payment gateway which is delivered at the right time and to the correct customer. User security plays a vital role in e-business; as it ensures that only the correct customers access their card details for online transaction. To fulfil this role, the user security process poses two challenges (identity and authentication) to the customers. Thus, the ability of the customer to provide the correct responses will give the security system an assurance that the correct customers are taking the transaction. In this section, the questions provided by the security system and the common types of responses are explored. Figure 1 depicts the questions posed to the customer during an online transaction.

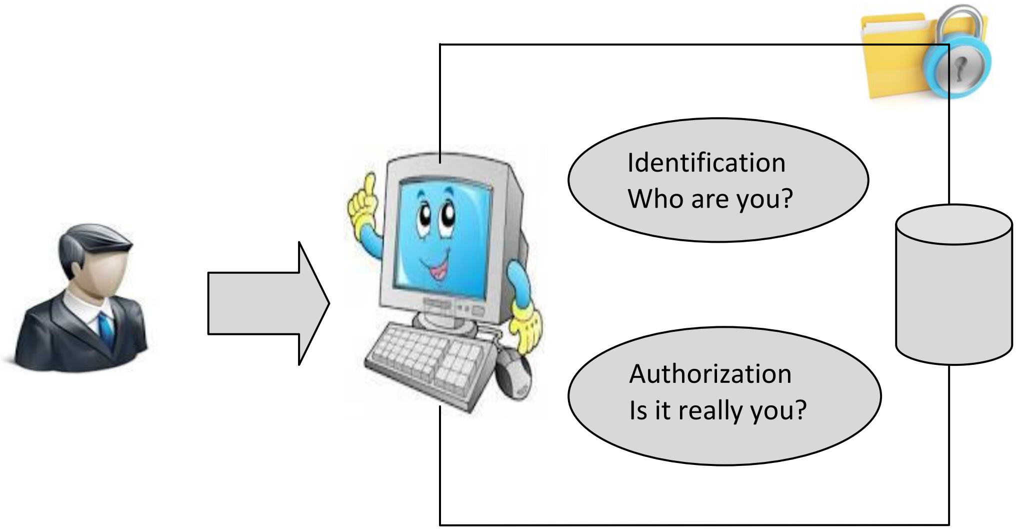


Figure 1: User security in E-Business

2.1 Identity

The term identity refers to the state or fact of remaining the same one or ones, as under varying aspects or conditions. When an Ecommerce security system solicits an answer to the "who are you?" question; it simply requires that the customer provides a unique response which distinguishes him/her from every other customer. A typical form of response used in e-security is the username (e.g. customer log-in ID). A username is not secret information and it can be shared or stolen for fraudulent purposes. In addition, providing a username only method makes the e-security system an easy hurdle for the customers. In an identity only system, the customers are required to provide one answer; however, this response does not ensure correctness of the customer. In order to ensure correctness, the e-security system solicits an additional response to confirm the claimed identity.

3.2. Authentication

In e-security, it is insufficient to assume correctness of a customer details based only on an identity. As depicted in figure 1, the e-security system requires prove that the identity claimed actually belongs to the owner who stored the information. Hence, when the security system solicits an answer to the "is it really you?" question; it simply requests an evidence of the claimed identity. Authentication data is often a secret which should be known to the customer and the security system alone. User authentication is a widely discussed subject both in secured and non assessment online environments. In general, user authentication is classified into three categories:

(1) Something the user knows (knowledge),

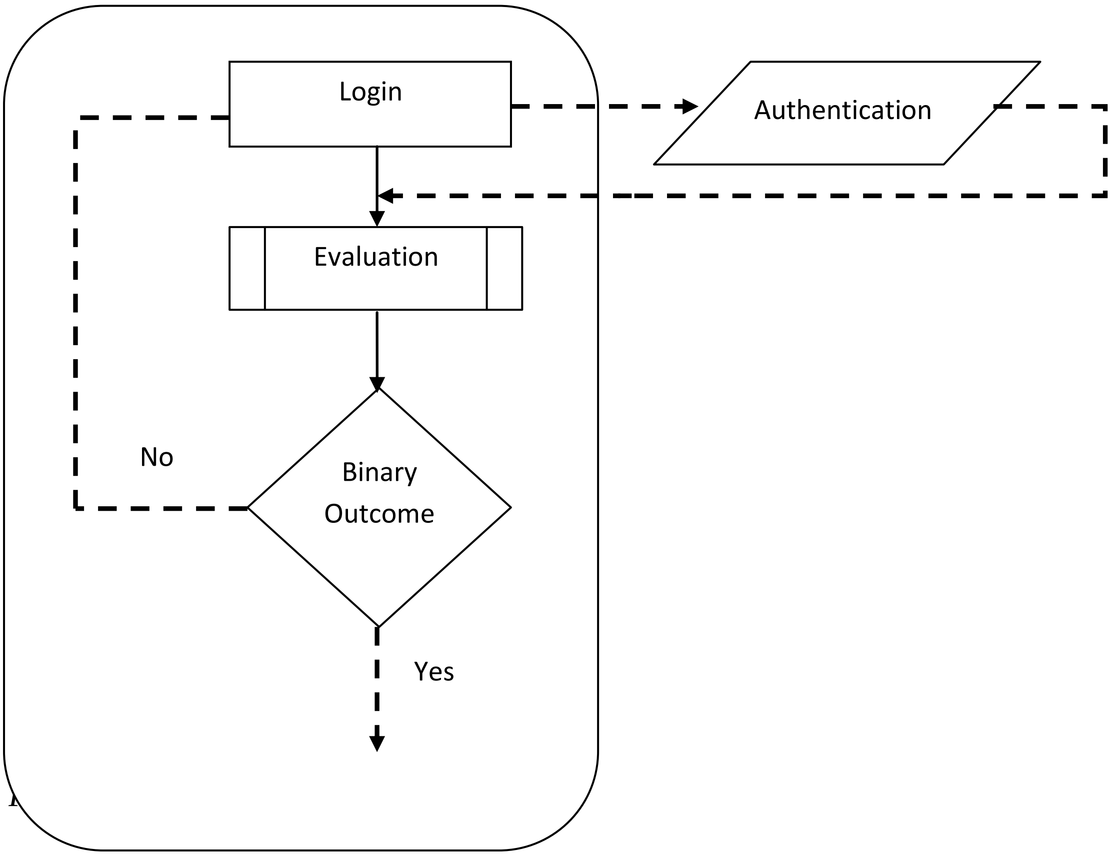
(2) Something the user has (possession) and

(3) Something the user is (biometrics).

Common pairs in e-security depict a username used as a form of identity and one or more of the above authentication methods employed as proof for a claimed identity. By doing this, the user security phase can solicit answers from the customers in order to satisfy the requirement of the security system i.e. to ensure that only correct customer to initiate the online transaction.

The Username and Password Paradigm

In online transactions, the username/password pair is the most popular and inexpensive method of identifying and authenticating users. The success of the username/password pair is attributed to its ease of use, such that no special device is required for data collection. These have an advantage such that it can be easily implemented using software methods which are conceptually simple for the user to understand. In addition, the users are able to choose an easy-to-remember combination for their convenience. Thus, the simplicity of a password makes it susceptible to a wide range of attacks.



The players

In a typical e-Commerce experience, a shopper proceeds to a Web site to browse a catalogue and make a purchase. This simple activity illustrates the four major players in e-Commerce security. One player is the shopper who uses his browser to locate the site. The site is usually operated by a merchant, also a player, whose business is to sell merchandise to make a profit. As the merchant business is selling goods and services, not building software, he usually purchases most of the software to run his site from third-party software vendors. The software vendor is the last of the three legitimate players. The attacker is the player whose goal is to exploit the other three players for illegitimate gains. Figure:3 illustrates the players in a shopping experience.

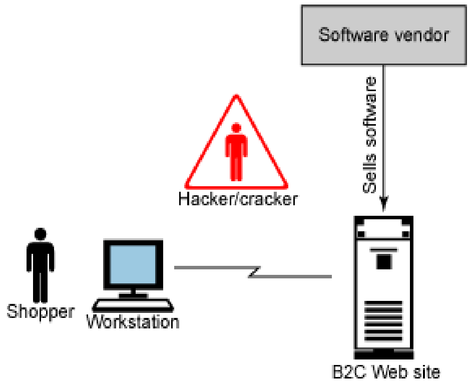


Figure: 3 The Players

The attacker can besiege the players and their resources with various damaging or benign schemes that result in system exploitation. Threats and vulnerabilities are classified under confidentiality, integrity, and availability. A threat is a possible attack against a system. It does not necessarily mean that the system is vulnerable to the attack. An attacker can threaten to throw eggs against your brick house, but it is harmless. Vulnerability is a weakness in the system, but it is not necessarily known by the attacker. For example, only you know that you have left your front door unlocked. Vulnerabilities exist at entry and exit points in the system. In a house, the vulnerable points are the doors and windows. When the burglar threatens to break into your house and finds the vulnerability of the unlocked door, he is exploiting the assets in the house.

3. CLIENT THREATS

a) Active content

Active content refers to programs that are embedded transparently in web pages and that cause action to occur. Active content can display moving graphics, download and play audio, or implement web-based spreadsheet programs. Active content is used in e-commerce to place items one wishes to purchase into a shopping cart and to compute the total invoice amount, including sales tax, handling, and shipping costs. The best known active content forms are Java applets, ActiveX controls, JavaScript, and VBScript. Since active content modules are embedded in web pages, they can be completely transparent to anyone browsing a page containing them. Anyone can embed malicious active content in web pages. This delivery technique, called a *trojan horse*, immediately begins executing and taking actions that cause harm.

Embedding active content to web pages involved in e-commerce introduces several security risks. Malicious programs delivered quietly via web pages could reveal credit card numbers, usernames, and passwords that are frequently stored in special files called cookies. Because the internet is stateless and cannot remember a response from one web page view to another, cookies help solve the problem of remembering customer order information or usernames or passwords. Malicious active content delivered by means of cookies can reveal the contents of client-side files or even destroy files stored on client computers.

b) Malicious codes

Computer viruses, worms and trojan horses are examples of malicious code. A trojan horse is a program which performs a useful function, but performs an unexpected action as well. Virus is a code segment which replicates by attaching copies to existing executables. A worm is a program which replicates itself and causes execution of the new copy. These can create havoc on the client side.

c) Server-side masquerading

Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack (in which the masquerader issues responses to mislead the user about its identity).

4.1 Communication channel threats

The internet serves as the electronic chain linking a consumer (client) to an e-commerce resource (commerce server). Messages on the internet travel a random path from a source node to a destination node. The message passes through a number of intermediate computers on the network before reaching the final destination. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure, and non-hostile.

4. Site development best practices

This section describes best practices you can implement to help secure your site.

a) Security policies and standards

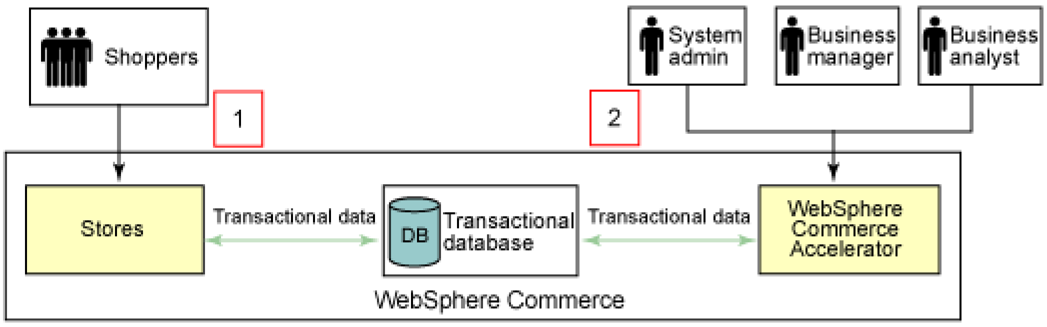
There are many established policies and standards for avoiding security issues. However, they are not required by law. Some basic rules include:

- Never store a user's password in plain text or encrypted text on the system. Instead, use a one-way hashing algorithm to prevent password extraction.
- Employ external security consultants (ethical hackers) to analyze the system.
- Standards, such as the Federal Information Processing Standard (FIPS), describe guidelines for implementing features. For example, FIPS makes recommendations on password policies.
- Ensure that a sufficiently robust encryption algorithm, such as triple DES or AES, is used to encrypt all confidential information stored on the system.
- When developing third-party software for e-Commerce applications, use external auditors to verify that appropriate processes and techniques are being followed.
- Recently, there has been an effort to consolidate these best practices as the Common Criteria for IT Security Evaluation (CC). CC seems to be gaining attraction. It is directly applicable to the development of specific e-Commerce sites and to the development of third party software used as an infrastructure in e-Commerce sites.

Security best practices remain largely an art rather than a science, but there are some good guidelines and standards that all developers of e-Commerce software should follow.

b) Using threat models to prevent exploits

When architecting and developing a system, it is important to use threat models to identify all possible security threats on the server. Think of the server like your house. It has doors and windows to allow for entry and exit. These are the points that a burglar will attack. A threat model seeks to identify these points in the server and to develop possible attacks.Threat models are particularly important when relying on a third party vendor for all or part of the site's infrastructure. This ensures that the suite of threat models is complete and up-to-date.



c) Using an online security checklist

Use this security checklist to protect yourself as a shopper:

- Whenever you logon, register, or enter private information, such as credit card data, ensure your browser is communicating with the server using SSL.
- Do not shop at a site when the browser does not recognize the server's SSL certificate. This check is done by your browser the first time your URL becomes HTTPS for the site. If the certificate is not recognized, then your browser presents a pop-up message to inform you.
- Use a password of at least 6 characters, and ensure that it contains some numeric and special characters (for example, c0113g3).
- Avoid reusing the same user ID and password at multiple Web sites.
- If you are authenticated (logged on) to a site, always logoff after you finish.
- Use a credit card for online purchases. Most credit card companies will help you with non-existent or damaged products.
- A bricks and mortar store with an online brand is most likely a legitimate site. However, the site may still have vulnerabilities.

6. CONCLUSIONS

The development and improvement of technologies have brought successful towards e-business. High technologies have attracted people misuse the technologies such as hackers and cybercrime which they can access to e-business privacy easily. Thus, e-business companies should build trust and using security during the business transaction. To provide value to the customers through service and goods provided, research found

that companies should build up trust and security to protect their customers. Benefits of application trust and security include improved customer service, build customers trust, avoid the misuse of technologies, protect customer's privacy and maintain the companies' reputation. In order to create an effective infrastructure for securing E-business, it requires a comprehensive development of several elements including laws, policies, industry self regulation, technical standards and law enforcement. These elements may provide positive environment and infrastructure to support the growth of e-business and relation with customers. Therefore, Governments and businesses need to work together to improve consumer trust and security are attempt to increase transactional efficiency and effectiveness in all aspects of the design, production, marketing and sales of products or services for existing and developing good relation through the utilization of current and emerging electronic technologies, which will gain the more confidence in e-business. Additionally, the government itself needs to re-examine existing regulations to ensure protection for the e-business.

7. REFERENCES

1. Alan, D. S. and William, T. R., 2002, "E-Lending: Foundations of financial and consumer marketing in an information intensive society," *Journal of e-Business and Information Technology*, Vol. 3, No. 1, pp.5-19.

2. Davidson, M. A., 2001, "Database security for e-Business," *Oracle9i Security Overview*, U.S.A.: Oracle Corporation.

3. Eben, O, 2003, *A Systematic Approach to e-Business Security*, University of New Brunswick, Fredericton, Canada.

4. Lord, P., Mary, A. and Kristy, B., 2002, *Managing e-Business Security Challenges*, An Oracle White Paper, U.S.A.: Oracle Corporation