Security Issues, Challenges and Solutions for E-Commerce Applications over Web

Mimansa Gantayat\(^1\), Chandan Kumar Giri\(^2\)

\(^1\)Department of Computer Science & Engineering, Centurion University of Technology and Management, Odisha, INDIA
\(^2\)Associate Professor, Department of Computer Science & Engineering, Centurion University of Technology and Management, Odisha, INDIA

ABSTRACT

E-commerce becomes a catchphrase in the world of internet. Many organizations all over the world appeared on the internet to offer everything thinkable. It refers to the process of buying, selling products or services over internet. This becomes most popular among the customers due to the speed and easy services as well as the doorstep conveyance. These activities such as selling online can be directed at consumers or other businesses. B2C (Business to Consumer) and B2B (Business to Business) refers to the online sales of good, services to the consumers and information between businesses. The main obstruction in the growth of e-commerce is information or data security, cyber fraud and integrity. Hence, poor security on e-commerce web servers and in users computer is core issue to be resolved for the rapid growth of e-commerce. This paper provides the security issues, challenges and solution for e-commerce application over web to improve consumer’s confidence in e-commerce.

Keywords-- E-Commerce, Attacks, Threats, Security Issues and measures, Digital E-commerce

I. INTRODUCTION

In the advancement of e-commerce, security has always been the hub and key issue still as information and system is additional essential outline for online business managing. As e-commerce refers to a wide range of online business activities for products and services for which security is the basic need to secure the information over internet. Internet becomes the comprehensive source for any type of business and commercial transaction through e-commerce website. It enables different range of business to exchange trading goods and services between corporations. These services include ‘click and buy’ methods using computers as well as various mobile devices or smart phones. This term takes in to account not just the act of purchasing goods and / or availing services through an online platform but also all other activities which are associated with any transaction such as delivery, payment enablement, supply chain and device management.

E-commerce has defied the traditional structure of business trading with consumers bringing to the fore various business models which has empowered customers. In its present state, M-commerce can be viewed as the extension of conventional, internet based e-commerce which adds a different zest to accommodate different end users. Delivery of electronic commerce capabilities is directly into the consumer’s hand, anywhere via wireless technology [1].

If a customer wants to use e-commerce website then following things need to be checked.

- A URL address that begins with https:// in place of http://
- By Symbol (lock icon) or by a message
- A Browser that notify the customer that he/she is in secure site
II. TYPE OF E-COMMERCE

Business-to-Consumer (B2C)

In B2C Web sites, the level of activity can range from very inexpensive operations of a Web site with only company and contact information, all the way to the investment of millions of dollars (as well as substantial operating funds) in a site that can handle marketing and sales transactions, after-sales service, and customer relationship management. E-Business levels range from the least involvement to the most advanced and most effective in terms of customer relationship management.

Benefits of B2C E-Commerce Solutions –

- Elimination of intermediaries – Businesses, particularly manufacturers, can offer lower and more affordable goods to consumers by selling products directly, eliminating distributors and retailers that add to the cost of the products.
- Flexibility in pricing – Price tags can be adjusted easily and instantly, benefitting the business and the customer. You also have the ability to strategically cross-sell, discount, and provide coupons and other online/offline specials.
- Professional image – Even if you have a small business, your e-commerce site can enhance your reputation by projecting a larger picture and allowing you to compete on a level playing field.
- Extended reach – Opening up an online storefront can effectively extend your presence to a great number of prospects, particularly those unable to access your local bricks and mortar store.

Business-to-Business (B2B)

B2B e-commerce also written as e-Commerce, e-Commerce or similar variants), short for business-to-business, electronic commerce, is selling products or services between businesses through the internet via an online sales portal. In general, it is used to improve efficiency for companies. B2B activities tend to be different from B2C, since they involve higher volumes, contractual relationships, and the establishment of permanent digital linkages between trading partners. The advent of the Internet greatly reduced the cost of exchanging this type of information, but it also allowed the use of on-line supplier catalogues and one-to-one Internet linkages between supplier organizations and procurement functions in buyer organizations.

Benefits of B2B E-Commerce Solutions –

- Purchasing supplies – By creating an online account for your business with supply stores you can purchase office supplies and equipment online and save time and money by automating the purchasing process.
Purchasing direct materials – These are materials that go into the production or manufacturing of your products. Establishing a relationship with a vendor and purchasing online may help reduce costs[5].

Selling products or services to new vendors – Having an online e-commerce presence opens up more opportunities to extend your reach and gather new vendors beyond your bricks and mortar offerings.

Leveraging your existing web presence – If you already have B2C operations, you can extend them to business clientele – perhaps by providing private areas for special pricing, delivery options, etc. However, this additional functionality is not trivial and could require rebuilding your online store at a significant cost.

Fig. 4.B2B E-Commerce Diagram

III. E-COMMERCE SECURITY

E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. Today, privacy and security are a major concern for electronic technologies. Web e-commerce applications that handle payments (online banking, electronic transactions or using debit cards, credit cards, PayPal or other tokens) have more compliance issues, are at increased risk from being targeted than other websites and there are greater consequences if there is data loss or alteration[6].

Online shopping through shopping websites having certain steps to buy a product with safe and secure. The e-commerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the e-commerce systems personnel to read and implement[2]. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture. These programs can be installed on a remote computer by the simplest of means email attachments. Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for e-Commerce providers.

IV. SECURITY ISSUES

Security is an essential part of any transaction that takes place over the internet. Customer will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions.

Confidential – Information should not be accessible to unauthorized person. It should not be intercepted during transmission.

Integrity – Information should not be altered during its transmission over the network.

Availability – Information should be available wherever and whenever requirement within time limit specified.

Authenticity – There should be a mechanism to authenticate user before giving him/her access to required information.

Non-Repudiability – It is protection against denial of order or denial of payment. Once a sender sends a message, the sender should not able to deny sending the message. Similarly the recipient of message should not be able to deny receipt.

Encryption – Information should be encrypted and decrypted only by authorized user.

Auditability – Data should be recorded in such a way that it can be audited for integrity requirements.

Measures to ensure Security

Major security measures are following –

Encryption – The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations. Security is on the mind of every e-commerce entrepreneur who solicits, stores, or communicates any information that may be sensitive if lost. An arms race is underway: technologists are building new security measures while others are working to crack the security systems. One of the most effective means of ensuring data security and integrity is encryption[3].

Digital Signature – Digital signature ensures the authenticity of the information. A digital signature is a e-signature authentic authenticated through encryption and password. It helps in E-commerce.
**Security Certificates** – Security certificate is unique digital id used to verify identity of an individual website or user. Due to this we can know about the user details.

**Secure Socket Layer (SSL)**

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

**Secure Hypertext Transfer Protocol (SHTTP)**

SHTTP extends the HTTP internet protocol with public key encryption, authentication and digital signature over the internet. Secure HTTP supports multiple security mechanism providing security to end users. SHTTP works by negotiating encryption scheme types used between client and server. S-HTTP does not use any single encryption system, but it does support the Rivest-Shamir-Adleman public key infrastructure encryption system. SSL works at a program layer slightly higher than the Transmission Control Protocol (TCP) level. S-HTTP works at the even higher level of the HTTP application. Both security protocols can be used by a browser user, but only one can be used with a given document. Terisa Systems includes both SSL and S-HTTP in their Internet security tool kits [4].

**Security issues in e-commerce application**

There are following types of security issues in any e-commerce application which needs to be addressed

**Malicious Code:**

**Viruses:** They have ability to replicate and spread to other files; most also deliver a “payload” of some sort (destructive or benign); include macro viruses, file-infecting viruses, and script viruses.

**Worms:** They are designed to spread from computer to computer.

**Trojan Horse:** They appears to be benign, but then does something other than expected.

**Bots:** It can be covertly installed on computer; responds to external commands sent by the attacker.

**Unwanted Programs:** These are installed without the user’s in Volume formed consent. Following are its types.

**Browser parasites:** It can monitor and change settings of a user’s browser [7].

**Adware:** It calls for unwanted pop-up ads.

**Spyware:** It can be used to obtain information, such as a user’s keystrokes, e-mail, IMs, etc.

**Phishing and Identity Theft:** Any deceptive, online attempt by a third party to obtain confidential information for financial.

**Gain:** Most popular type [e-mail scam letter] – It is one of fastest growing forms of e-commerce crime.

**Hacking and Cyber vandalism:** Hacker Individual who intends to gain unauthorized access to computer systems.

**Cracker:** Hacker with criminal intent (two terms often used interchangeably).

**Cyber vandalism:** Intentionally disrupting, defacing or destroying a Web site.
VI. CHALLENGES OF E-COMMERCE

<table>
<thead>
<tr>
<th>E-Commerce Site Name</th>
<th>Attacks</th>
<th>Algorithm Use</th>
<th>Overall Security Threat</th>
<th>Vulnerability to Hardware/Software</th>
<th>Public Key Infrastructure Use or Not</th>
<th>Encryption Code Use or Not</th>
<th>Digital Certificates Use or Not</th>
<th>Digital Signatures Use or Not</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMAZON</td>
<td>DDoS attack</td>
<td>Learning Algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>SNAPDRAGN</td>
<td>SQL injection attack</td>
<td>Read algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>PAYTM</td>
<td>Intellectual Property Theft</td>
<td>MIT algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>MUNTRA</td>
<td>Cyber attacks</td>
<td>LSTM algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>HOME</td>
<td>Cyber attacks</td>
<td>BAHM algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>INFREEM</td>
<td>Denial of Service (DoS) attack</td>
<td>ML algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>TABONG</td>
<td>Cross-site Scripting (XSS)</td>
<td>Encapsulation algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>KXML</td>
<td>Buffer overfl ow attack</td>
<td>CTXPFW algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>STOPCUSES</td>
<td>Impersonation attack</td>
<td>GZIP (GNU zip) algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>VISON</td>
<td>Impersonation attack</td>
<td>GZIP (GNU zip) algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>UVIX</td>
<td>URI interception attack</td>
<td>Symmetric algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>PREMATES SHOPPING</td>
<td>Session hijacking</td>
<td>Sequence Algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>REDHFS</td>
<td>Directory browsing</td>
<td>Learning Algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>HOMESTAY</td>
<td>Interning</td>
<td>NL algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>LYNX</td>
<td>SQL injection attack</td>
<td>R.S. Algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>MEDIA HOME</td>
<td>SQL Query Focusing</td>
<td>NL algorithm</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
</tbody>
</table>

Fig. 6. Table of E-Commerce Sites & Security Level

VII. RC6 METHOD, USEFUL IN ENCRYPTION

RC6 is a symmetric key block cipher derived from RC5. It was designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin to meet the requirements of the Advanced Encryption Standard (AES) competition by the National Institute of Standards and Technology (NIST). The algorithm was one of the five finalists, and was also submitted to the NESSIE and CRYPTREC projects. Though the algorithm was not eventually selected, RC6 remains a good choice for security applications. It is proprietary of RSA Security. The design of RC6 began with a consideration of RC5 as a potential candidate for an AES submission. Modifications were then made to meet the AES requirements, to increase security, and to improve performance[12].

To attack RC6 the best approach available to the cryptanalyst is that of exhaustive search for the b-byte encryption key. The more advanced attacks of differential and linear cryptanalysis, while being feasible on small-round versions of the cipher, do not extend well to attacking the full 20-round RC6 cipher. The RC6 key schedule is secure through mixing, one way function and no key separation. Therefore, RC6 provides a solid, well tuned margin for security. RC6 facilitates and encourages analysis by allowing rapid understanding of security and making direct analysis straightforward. It also enables easy implementation by allowing compilers to produce high quality code for software implementations, and by preventing complicated optimizations and providing good performance with minimal effort for hardware implementations. RC6 is known to have good performance on 8, 16 and 32-bit platforms. RC6 can easily be implemented in such a way as to be vulnerable to "timing attacks"[13]. Many modern processors have constant-time rotation and multiplication instructions. Other processors may have a rotation or shift time that depends linearly with the amount of rotation, but in this case it is usually easy to arrange the work so that the total compute
time is data-independent (for example, by computing a rotate of \( t \) bits using a left-shift of \( t \) bits and a right-shift of \( w-t \) bits). In either case, the RC6 encrypt/decrypt time is data-independent, causing any potential timing attacks to fail. RC6 does not have a non-linear transformation s-box.

Fig. 8. Symmetric layer of R6 Method

VIII. SOLUTIONS & CONCLUSION FOR E-COMMERCE

Choose a secure e-commerce platform. Following steps are

- SSL certificates are a must for transactions. To validate our credit cards we use a payment gateway that uses live address verification services right on our checkout. This prevents fraudulent purchases by comparing the address entered online to the address they have on file with their credit card company.
- Don't store sensitive data. There is no reason to store thousands of records on your customers, especially credit card numbers, expiration dates and CVV2 [card verification value] codes.
- Employ an address and card verification system. Enable an address verification system (AVS) and require the card verification value (CVV) for credit card transactions to reduce fraudulent charges [8].

- Require strong passwords. While it is the responsibility of the retailer to keep customer information safe on the back-end, you can help customers help themselves by requiring a minimum number of characters and the use of symbols or numbers.
- Layer your security. One of the best ways to keep your business safe from cybercriminals is layering your security. Start with firewalls, an essential aspect in stopping attackers before they can breach your network and gain access to your critical information. These measures will ensure that your ecommerce environment is protected from application-level attacks like SQL (Structured Query Language) injections and cross-site scripting (XSS).
- Provide security training to employees. Employees need to know they should never email or text sensitive data or reveal private customer information in chat sessions as none of these communication methods is secure. Employees also need to be educated on the laws and policies that affect customer data and be trained on the actions required to keep it safe.
- Use tracking numbers for all orders. To combat chargeback fraud, have tracking numbers for every order you send out.
- Perform regular PCI scans. Perform regular quarterly PCI scans through services like TrustWave to lessen the risk that your ecommerce platform is vulnerable to hacking attempts. If you're using third-party downloaded software like Magento or PrestaShop, stay on top of new versions with security enhancements.
- Patch your systems. "Patch everything immediately—literally the day they release a new version."
- Make sure you have a DDoS protection and mitigation service. With DDoS [Distributed Denial of Service] attacks increasing in frequency, sophistication and range of targets, commerce sites should turn to cloud-based DDoS protection and managed DNS services to provide transactional capacity to handle proactive mitigation and eliminate the need for significant investments in equipment, infrastructure and expertise.

REFERENCES


