IJCTA, 10(9), 2017, pp. 67-70 ISSN: 0974-5572
© International Science Press

A study of Ecommerce Security

Minal D. Kalamkar*

ABSTRACT

Ecommerce is nothing but electronic commerce or transactions through internet. With the increase in number of online transactions, there is a need of computer and information security that prevents financial frauds, hacking, phishing and different types of web attacks. Online payments made secure which involves authenticity, confidentiality, privacy, integrity and non repudiation. Ecommerce security deals with prevention of unauthorised access to ecommerce assets. Also protecting the data from any modification, alteration or deletion. With the changing technology & business models, definition of Ecommerce security is still endeavour. Java Script is widely used for client side programming language which is used to develop many web applications. The vulnerabilities in web applications are the main target for invaders. In this paper, I've taken the overview of Ecommerce, security issues in Ecommerce, web vulnerabilities & its solutions.

Index Terms: Firewall, proxy, vulnerability, web attacks, web security.

1. INTRODUCTION

In India, people started trading over internet in late 1990.Ecommerce started growing and becoming popular due to its infrastructural cost and operational time. It also promotes the product worldwide. Based on type of the application, the business over Internet can be categorised into B2B, B2C, C2B, C2C, B2G /G2B.[9] To support growing Ecommerce business , use of Virtual Private Network(VPN), Extranet were introduced. With the changing technology, mobile devices are playing major role in Ecommerce (EC). It is called as mobile commerce or m-commerce. It is predicted that purchase made by mobile devices making 25% of market by 2017.[11]

Along with the use of EC as a medium to conduct business, it is also referred as a new economic model.

2. EDI

Electronic Data Interchange deals with automated exchange of structured business documents like purchase orders or Invoices, between an organization and its trading partners.[10] It is intended for paperless documents and to improve efficiencies. EDI is defined by IDEA (International Data Interchange Association) as "transfer of structured data, by agreed message standards, from one computer system to another by electronic means". In other words, EDI focuses automation of transactions. With EDI all demerits of traditional business such as increase in processing time, low accuracy, high labor cost and increased uncertainty can be overcome.

3. PAYMENT SYSTEM

The online payment can be done using payment instruments like credit/debit cards, smart cards, e- money and electronic fund transfer.

There are many methods for online payment like net banking, payment wall, PayPal, Google wallet, mobile money wallet.

* Asst. Professor, Dept. of Computer Science, T.M.V., Pune, *Email: minaldk@gmail.com*

The components of payment System are a) Payment instruments –that refers to media or methods for online payments. b) Institutional framework – for efficiency and effectiveness. c) Legal & regulatory framework –to regulate procedures and payment activities adhering to laws. d) Communication Infrastructure – affects efficacy of payment system e) users-individual or corporate.

4. ELECTRONIC COMMERCE ATTACKS

There is always a risk to Ecommerce security from attacks like script attacks, input validation attacks, DNS attacks and Eavesdrops. Attacks can be categorised as active & passive. Encroacher observes the network traffic for the passive attacks like traffic analysis and eavesdropping. In man in the middle attack (MiM), communication between two parties is altered by invader. Whereas denial of services (DoS), unauthorised access, session hijacking, rogue access point are active attacks.

In DoS attack, perpetrator makes users deprived of resources or services by making them temporary unavailable. It’s like exploiting the server resources by making fake requests. In unauthorised attack, the attacker makes unauthorised access to network. Session hijacking takes place in real time and it captures the session data. Replay attacks also captures the session data but in passive time. In rogue access point, attacker mounts a rogue access point to gain access to the network.[1]

5. SECURITY THREATS

There are three types of threats:[2]

- Denial of Services(DoS)
- Unauthorised access
- Theft and fraud

I) Two types in DoS attacks: spamming & viruses. Spamming is related with sending unsolicited emails to individual. While Viruses, worms, Trojan horses are the software programs which causes malfunctioning of computer.

II) Unauthorised access: Illegal access to the system, applications or data, message spoofing.

III) Theft and fraud: Theft of software and hardware, financial frauds, data fraud.

6. E-COMMERCE SECURITY

E-commerce security provides protection to e-commerce assets from unauthorized access, use, alteration, or destruction. 6 dimensions of e-commerce security are: [12]

1. Integrity: prevention against unauthorized data modification. Information should be exactly same as sent by sender to receiver.
2. Non repudiation: prevention against denial by any party in an agreement.
3. Authenticity: authentication of data source. It is the ability to identify identity of both parties while doing transactions over internet.
4. Confidentiality: protection against unauthorized access. In other words, only authorised user can access the protected data.
5. Privacy: provision of data control and disclosure
6. Availability: It is prevention against data delays or data removal. Also it represents you are authorised user to resources.

Techniques used for security are Authorization, Authentication, Encryption and Auditing.

In spite of security, hackers will try to breach the security. And therefore security must be maintained by using firewalls, Secure Socket Layer (SSL) protocol for encryption of the streams used in communication, having strong passwords, encrypting the sensitive data and external security audit. [3]

7. LITERATURE SURVEY

Web applications that are concerned with handling financial transactions are at greater risk. There is a threat of data loss or modification done by attackers. Security is prime concern whenever we talk about ecommerce. In this paper, the author has discussed digital ecommerce cycle that involves buying products using shopping cart, placing order, making payment with different types of cards, dispatching the product from warehouse to final delivery. Along with this he has discussed ecommerce security issues and threats like denial of services (DoS), theft & fraud, unauthorised access, security measures, & guidelines for online shopping that advise to ensure if we are using secure web site for shopping, to see web site's privacy & security policies, precautions that should be taken while using payment cards, rules for securing password, phishing alerts, shipping policies and E-Sign Act[4] etc.

To carry out ecommerce, many web applications have been developed. But these web applications came up with their own vulnerabilities. Cross site scripting is among top five vulnerabilities. This paper represents the solution for Cross Site Scripting (XSS) attacks by providing client side XSS sanitizer. The author claims that this sanitizer is able to detect cross site scripting vulnerabilities at client side. [5] It consists of four modules viz. DOM (Document Object Module) module, input field capture module, link and text area module, XSS notification module. DOM module access current web page's DOM hierarchy. It works with input capture module for capturing the different input fields. The input analyzer module categorises the input into links and textarea fields. The link and textarea module pass all links and input text to XSS vulnerability checking module. Thus XSS vulnerabilities are notified to user by highlighting it in red color.

Many researchers came up with different techniques to identify JavaScript vulnerabilities. In this paper[6] author presents technique based on signatures & regular expression. Signature based detection system contains predefined static rules i.e. if iframe with opacity 0 (CSS property) is used then code is said to be vulnerable. And the regular expression search for patterns and recognises the tag to identify the vulnerabilities in the web page.

In this paper[7] author claims that Noxes is the first client side solution for reducing XSS attacks without relying on web application providers. Noxes acts as a web proxy that gives HTTP requests on user's behalf using automated & manually generated rules to block XSS attacks. Noxes allows client to implement filter rules for web in three ways. First, by creating rules manually like to allow abc.com or to block xyz.com web site. Secondly, by introducing firewall. And finally, by generating snapshots of profile of browsing. Noxes finds & accumulate the domains which have been surfed. Based on this information client can generate the filter rules.

To resolve the security issues like SQL injections, price manipulation, weak authentication and authorization, Cross Site scripting, the author [8] proposed methodology using AES algorithm. In SQL injection attacks, malware authors introduce SQL character in user's input. Result of SQL injection can disclose backend technology or to access restricted areas of site or can steal credit card no.s, transaction details. In price manipulation, attacker can use web application proxies like ACHILLE S, to manipulate the price stored in hidden HTML field. Using XSS attacks, intruder can steal sensitive information or session ID. Weak authorization & authentication is the main target to breach the web security. For e.g., attacker can sniff the traffic if session ID is passed over without SSL (Secure socket layer). The author develop the AES algorithm which is symmetric key algorithm that is more secure than its predecessor DES (Data Encryption Standards).

8. CONCLUSION

With the growing technology and changing life style, Ecommerce is becoming part of daily life activities in urban cities. There is a need of information security as number of transactions over internet is increasing constantly. Ecommerce security is protection of ecommerce asset from unauthorised access. So by using different encrypting algorithms, SSL, Firewalls, security audit we can prevent the hackers from unauthorised access. This paper includes study of what is E-Commerce, EDI, security measures, and threats, web vulnerabilities, Cross site scripting (XSS) attacks & its solution.

REFERENCES

[1],[3] P. Jindal , Amit Kumar and Dr. Shishir Kumar- Security issues in E-Commerce. Pioneer Journal, 8th National Conference, (2011).

[2],[4] M. Niranjanamurthy and DR. D. Chahar - The study of E-Commerce Security Issues and Solutions. International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, July 2013.

[5] D.K. Patil and K.R. Patil- Client side Automated Sanitizer for Cross Site Scripting Vulnerabilities. International journal of Computer Applications, Vol.121, July 2015.

[6] S.Jain, D. S.Tomar and D. R. Sahu- Detection of JavaScript Vulnerability At Client Agen. International journal of scientific and technology research, Vol. 1, pp. 36-41, August 2012.

[7] A.Monika and D.Raman - Justified Cross-Site Scripting Attacks Prevention from Client Side. International journal on Computer Science and Engineering, Vol. 6,pp. 267-270, July 2014.

[8] R.Puri and Sheetal Kalra- Web Security in Ecommerce against various vulnerabilities using AES algorithm. International journal of innovation sciences and research, Vol. 4, pp. 090-095,March 2015.

[9],[10] Er.A Misra and Dr. W.K. Sarwade, A textbook on E-Commerce, A.K. Publications.p 20, p306

[11] https://en.wikipedia.org/wiki/E-commerce

[12] http://www.uky.edu/~dsianita/390/390wk4.html