Deploying E-Commerce and its Security Challenges ; The Nigerian Situation

By

Modesta. E. Ezema
Lecturer 1
Department of Computer Science
University of Nigeria, Nsukka
Enugu State, Nigeria

and

Ifenyinwa Ngozi Arinze
Department of Computer Science
Anambra state university, Uli
Anambra state
Nigeria
and
Chikaodili Helen Ugwuishiwu
Department of Computer Science
University of Nigeria, Nsukka
Enugu State, Nigeria

ABSTRACT

Information Technology has revolutionized the world and Nigeria has not been left out. Nigerians are embracing the internet. Thus, with the introduction of the Cashless Policy which has been deployed in the country since this year', e-commerce will soon be the face of business transactions in Nigeria. This may naturally lead to many traditional crimes being aided or abetted through the use of computer network, and wrongdoing previously never imagined surfacing because of the incredible capabilities of information systems. Enterprises must provide secure services for their customers in e-commerce. Providing secure services can be so extensive and difficult, that using the appropriate models can facilitate implementation. This paper will be looking at such issues as to how to protect a customer's database and transaction information; how to create a secure shopping chart and payment system; how to create and implement a secure database for online transactions, as well as other managerial and technical issues.

Keywords: Internet, online shopping, credit card, e-commerce security,, malware.

I INTRODUCTION

The Internet has created a new economic ecosystem the e-commerce marketplace, and it has become the virtual main street of the world. Electronic commerce, commonly known as e-commerce or e-comm, is the exchange of goods and services over electronic systems enabled by the Internet and other computer networks. E-commerce however is more than just buying and selling online. It tends to include the entire process of marketing, selling, supply chain management, , online transaction processing, electronic data interexchange (EDI),etc.[1] At the dawn of January 1, 2012, the pilot scheme of mobile money, one of the financial services introduced by the Central Bank of Nigeria, via a CBN circular Ref. No. COD/DIR/GEN/CIT/05/031 dated 20th April, 2011, to achieve a cashless economy took off in Lagos, the commercial nerve centre of the country. Other financial services under this payment platform are consumer accounts information and updates, alerts, which have been in existence but not widely subscribed to by account holders. Payment of bills, person-to-person transactions and remittances in different forms also form part of the cashless economy drive. With the introduction of the mobile payment, Nigeria is only keying into a fast evolving global payment system. The mobile money platform is a

technology driven payment system that will open up several other business opportunities in the economy

Business which occurs online can occur between businesses, this is called business to business (B2B). It can also take place between business to consumers , this is normally referred to as business to consumers (B2C). It could also be consumer to consumer (C2C)

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. E-commerce Security ensures that business transactions are authenticated, access to resources such as Web pages are available for registered or selected users, communication channels are encrypted, and, in general, ensuring the privacy and effectiveness of transactions.

II E-COMMERCE SECURITY ELEMENTS

When using computer network for transactions, the sender and recipient need to ensure the confidentiality of information exchanged. Security is a main issue influencing people to purchase online. Consumers generally are reluctant to give their personal financial information during an online transaction because they fear that it will be intercepted by hackers during transmission;[2] Traditional security products such as virus scanners and firewalls do not provide adequate protection against unknown threats and the thousands of mutations and variations of Spyware and viruses available to hackers on the Internet.

With the Internet being used in so many ways in e-commerce, the security control of new applications and technologies requires an entirely new paradigm. Security, in this environment of constantly evolving threats, can only come from having complete control of the Internet connections including the ability to specify which applications, known and unknown, can be trusted to use the Internet, to ensure security of data transmitted in a network. E-commerce Security Elements is further expressed under the following sub headings for clarity and guidance.

A The Integrity of the Information

Integrity refers to the quality of information available on say a company's website. Integrity of information available is important as people use this information to make decisions and take actions. To assist with sound decision making, information must have value. For it to be valuable, information should be accurate, verifiable, timely, organized, accessible, useful, and cost-effective. For instance if a customer sees the cost of a product at a particular web site, the price must be consistent . A website where what you see is not what you get will definitely lose the confidence of it customers.

B. The Validity of Information

E-commerce will have a direct bearing on the validity of the information to individuals, co-operations or the country's economic interests and reputation. The validity of the transaction price, period, and the number of hours as part of the agreement is particularly important.

C The Authenticity of the Transaction Status

Internet transactions are geographically distant. There must be mutual understanding. To make transaction a success, there must be trust. In fact the transaction must be real. Authentication is an important issue for users of electronic commerce. Consumers must have faith in the authenticity of the merchant, and merchants must have faith in the authenticity of the consumer. Without authentication, any individual could pose as a merchant, and besmirch a merchant's good name by failing to deliver goods and piling up credit card bills. Without authentication, an individual could pose as a willing buyer, accept the goods, and then repudiate the transaction. Authentication is critical to achieving trust in electronic commerce.

D The Reliability of the System:

E-commerce System must be a computer system that is reliable with advance facilities to prevent computer failure, procedural errors, transmission errors, hardware failures, software errors, computer viruses and natural disasters resulting from human carelessness. Finally, it must ensure system security and reliability.E-commerce tends to be at a higher echelon for risk and attacks. This is so because. E-commerce is the transaction of goods and services; and the payment for those goods and services over the Internet. Therefore, the physical place where all of these transactions occur is at the Server level. The server can be viewed as the central repository for the "e-commerce place of business" (which consists of the actual website which displays your products and services, the customer's database, and the payment mechanism). If there are any attacks to this server,, there is the potential threat that you could lose everything. Thus, being proactive about security is indispensible to ensure reliability of transactions.

The Internet has enabled the growth of e-commerce and it is all too easy to do business with anyone located anywhere in the world. As a result it has brought about some security issues as you do not know whom you are doing business with. Someone with malicious intent can easily release a virus into your system or do something else that shuts down your Website.

III DIFFERNCE FORMS OF SECURITY FOR E-COMMERCE

To protect your business from such concerns, e-commerce systems use different forms of security.

These forms of security that e-commerce uses includes the following;

A. Securities to Access Control

Access control security measures ensure that only data that is authorized enters and leaves a computer system in a network.[4]Access control is the process by which an administrator can regulate and monitor user's access to intranet or Internet services. It supplies a much broader range of network security options than packet filtering alone. screening router decides whether to forward or drop each Internet Protocol (IP) packet. There is also inspection technologies that could use other information to decide whether to forward an IP packet or not. The use of circuit-level and application-level gateways provides additional access control security. E-commerce must establish mutual trust and secure access between the parties in an e-commerce transaction by authenticating users, authorizing access, and enforcing security features. E-commerce site must then authorize access to onl,y those parts of the site that an individual user needs to accomplish his or her particular transactions. Thus, individual usually will be given access to all resources of an E-commerce site except for others people's accounts, restricted company data, and webmaster administration areas.

B Communications Security

Cryptographic security protocols that operate at different layers of the computer system's communications protocol stack provide another level of security for e-commerce systems. At the network access layer, a Point-to-Point-Tunneling Protocol (PPTP) could provide security, and at the transport layer, a Secure Sockets Layer (SSL) could help with communication security. There are also other protocols that operate at or above the application layer.

C Firewalls

E-commerce systems also use firewalls as a security device. A firewall is a highly resistant system that a business places between its internal network and an external network, through which all traffic passes. Only traffic that the firewall authorizes will pass into the e-commerce system. Typically, a firewall system consists of one or more of the e-commerce system's host systems and routers, and also uses other security measures. For instance, instead of using constant passwords, the firewall might use more advanced ways of authentication.

IV FORMS OF THREATS IDENTIFIED WITH E-COMMERCE

Threats to E-Commerce servers fall into two general categories It can be either malicious or(technical) transmission attacks [5] It is important that you understand the risks facing your e-commerce system, and the potential impact of any security incident.. The procedures and controls you put in place to protect your site should help minimize both.

In terms of the former, the motivation is primarily psychological. The intent is to gather personal information from people for the sheer purposes of exploitation (such as obtaining Credit Card and Bank Account information; Phishing schemes, obtaining usernames and passwords, etc.). With the later, anything related to the Internet can cause problems. This can be anything from a network not configured properly to data packets being lost, especially in a wireless access environment. Even poorly written programming code upon which your E-Commerce site was developed can be very susceptible to threats. Most E-Commerce Servers utilize a Windows Operating System (such as Windows 2000 and 2003 Server), a Web Server Software to host the E-Commerce Site (such as Internet Information Services, or IIS), and a database (such as Access 2000 or SQL Server 2000) which contains your customer information and transaction history. These platforms have had various security flaws associated with them, which has made them wide open to threats and attacks. As a result, there has been a move in the business community to adopt more robust and secure platforms. A prime example of this is the use of Linux as the operating system, Apache as the Web Server Software,

and My SQL as the database (these are database languages created from the Structured Query Language, or SQL).

With the former, malicious, or rogue programming code is introduced into the server in order to gain access to the system resources. Very often, the intent of Malicious Code Attacks is to cause large scale damage to the E-Commerce server. With the later, the threats and risks can be classified as either as active or passive. With passive threats, the main goal is to listen (or eavesdrop) to transmissions to the server. With active threats, the intent is to alter the flow of data transmission or to create a rogue transmission aimed directly at the E-Commerce server.

A . MALICIOUS CODE OR MALWARE

What causes breach, damage, infiltration of information in computer systems is referred to as Malicious Code or rather Malware**.** [6] As internet and e-mail become an ever increasing part of our 21st-century lives, the myriad dangers and risk that come with them are increasing too, make sure you know how to detect and deal with threats that face us . We have difference forms of these codes which includes;

1.) Viruses and Worms:

The most common threats under this category are the worms and viruses. In the media today, we keep hearing about these words on almost a daily basis, and there is confusion that the two are related, and synonymous. However, the two are very different. [3] Viruses are

programs written to change the way computer systems or mobile devices work without the knowledge of the owner A virus needs a host of some sort in order to cause damage to the system. A virus attaches itself to executable code and is executed when the software program begins to run or an infected file is opened. Thus a virus can be attached to a file hence once that file is opened, the virus can then cause the damage. This damage can range from the deletion of some files to the total reformatting of the hard drive.

However, worms are very much different. A worm does not need a host to replicate. Rather, the worm replicates itself through the Internet, and can literally infect millions of computers on a global basis in just a matter of hours. A perfect example of this is once again the MS Blaster worm. Worms by themselves do not cause damage to a system like a virus does. However, worms can shut down parts of the Internet or E-Commerce servers, because they can use up valuable resources of the Internet, as well as the memory and processing power of servers and other computers.

2.) Trojan Horses

A Trojan Horse is a piece of programming code that is layered behind another program, and can perform covert, malicious functions. For example, your E-Commerce server can display a "cool-looking" screen saver, but behind that could be a piece of hidden code, causing damage to your system. One way to get a Trojan Horse attack is by downloading software from the Internet. This is where you need to be very careful. There will be times (and it could be often) that patches and other software code fixes (such as Service packs) will need to be downloaded and applied onto your E-Commerce server. Make sure that whatever software is downloaded comes from an authentic and verified source, and that all defense mechanisms are activated on your server.

3.) Logic Bombs:

A Logic Bomb is a version of a Trojan Horse, however, it is event or time specific. For example, a logic bomb will release malicious or rogue code in an E-Commerce server after some specific time has elapsed or a particular event in application or processing has occurred.

B TRANSMISSION THREATS

Transmission threat can be anything related to the way data are transmitted from the internet that can cause problems. This can be anything from a network not configured properly to data packets being lost, especially in a wireless access environment. Even poorly written programming code upon which your E-Commerce site was developed can be very susceptible to threats

1). *Internet protocol Spoofing (IP Spoofing)*

The intent here is to change the source address of a data packet to give it the appearance that it originated from another computer. With IP Spoofing, it is difficult to identify the real attacker, since all e-commerce server logs will show connections from a legitimate source. IP Spoofing is typically used to start the launch of a Denial of Service Attack.

2.) Denial of Service Attacks

The main intention of denial of service attack is to deny your customers the services provided on your E-Commerce server. There is no actual intent to cause damage to files or to the system, but the goal is to literally shut the server down. This happens when a massive amount of invalid data is sent to the server. Although the server can handle and process so much information at any given time, it is unable to keep with the information and data overflow. As a result, the server becomes "confused", and subsequently shuts down. Another type of Denial of Service Attack is called the Distributed Denial of Service Attack (DDoS). [7] A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. In this scenario, many computers are used to launch an attack on a particular E-Commerce server. The computers that are used to launch the attack are called "zombies." These "zombies" are controlled by a master host computer. It is the master host computer which instructs the "zombie" computers to launch the attack on the E-Commerce Server. As a result, the server shuts down because of the massive bombardment of bad information and data being sent from the "zombie" computers.

3.) Ping of Death

When we surf the web, or send e-mail, the communications between our computer and the server takes place via the data packet.[8] Technically speaking, the Ping of Death attack involved sending IP packets of a size greater than 65,535 bytes to the target computer. It is the data packet that contains the information and the request for information that is sent from our computer to other computers over the Internet. The communication protocol which is used to govern the flow of data packets is called Transmission Control Protocol/Internet Protocol, or TCP/IP for short. The TCP/IP protocol allows for data packets to be as large as 65,535 bytes. However, the data packet size that is transmitted across the Internet is about 1,500 bytes. With a Ping of Death Attack, a massive data packet is sent-65,536 bytes. As a result, the memory buffers of the E-Commerce server are totally overloaded, thus causing it to crash.

4.) SYN Flooding Attack (synchronization flooding attack)

When we open up a web browser and type in a web address, or click "send" to transmit that e-mail from our own computer (referred to as in this section as the "client computer"), a set of messages is exchanged between the server and the client computer. These set of exchanges is what establishes the Internet connection from the client computer to the server, and vice versa.

This is also known as a "handshake." To initiate this internet connection, a SYN (or synchronization) message is sent from the client computer to the server, and the server replies back to the client computer with a or synchronization acknowledgement (SYN ACK) message. To complete the Internet connection, the client computer sends back an ACK (or acknowledgement) message to the server. At this point, since the E-Commerce server is waiting to receive the ACK message from the client computer, this is considered to be a half-open connection. It is at this point that the E-Commerce server becomes vulnerable to attacks. Phony messages (which appear to be legitimate) could be sent to the E-Commerce server, thus over loading its memory and processing power, and causing it to crash.[9] Then SYN flag of a TCP segment is activated when a host is initiating a new TCP connection. The connection establishment is successfully completed when the 3-way handshake method is performed as seen below:

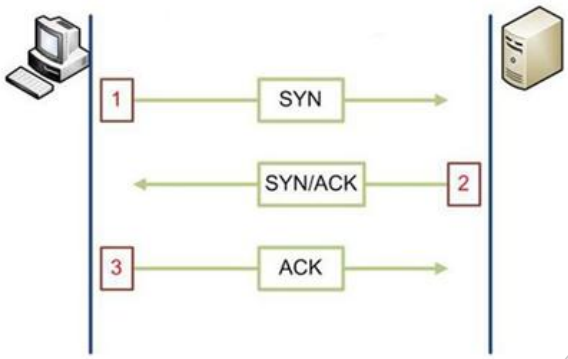

Fig 1 transmission Communication protocol 3 – way handshake

An attacker could deliberately flood the server with TCP SYN segments without acknowledging back the server's SYN response. As a consequence the server's session table is filled up with ongoing session requests driving its resources to the edge making it unable to accept legitimate connection requests until its TCP inactivity timer is reached where it would start dropping incomplete sessions.

This kind of attack is usually originated by a spoofed source IP address making it harder to track down the attacker. A schematic explanation of the TCP SYN attack is presented below:

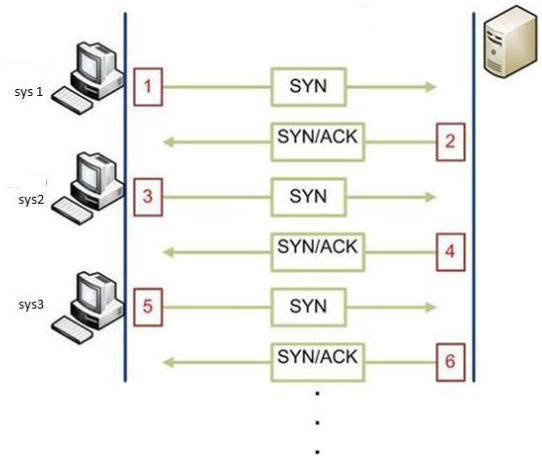

Fig 2 TCP/SYN attack

5.) Phishing Attacks;

One of the biggest threats to your E-Commerce customers is that of phishing. Specifically, Phishing can be defined as the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. For instance , fraudulent e-mail could be sent to your customers claiming that their online account is about to expire, or their username and password has been compromised in some fashion, or that there is a security upgrade that will take place affecting their online account. After they are tricked into believing the content of the Phishing e-mail, the customer then clicks on the link, and submits all of their confidential information. All Phishing e-mail contains a link, or a web address, in which the customer clicks on thinking that they are going to a secure and legitimate site (people who launch Phishing schemes also called "Phishers". They can copy the HTML code from your e.commerce site, making it look authentic in the eyes of the customer. The truth is, that all confidential information submitted is collected by the "Phisher", who is bent upon creating havoc and damage to your e-commerce business.

An example that we witness everyday in this country is the phony emails from your presumed bank telling you to update your account online when sometimes you don't even have an account with that particular bank .Other threats posed to E-Commerce servers include a few listed below:

6.) Data Packet Sniffing

This refers to the use of Data Packet Sniffers, also known simply as "sniffers." While it is an invaluable tool to the Network Administrator for troubleshooting and diagnosis, an attacker can also use a sniffer to intercept the data packet flow and analyze the individual data packets. Usernames, passwords, and other confidential customer's data can then be hijacked from the E-Commerce server. This is a very serious problem, especially in wireless networks, as the data packets literally leave the confines of the network cabling and travel in the air. Ultimately, Data Packet

Sniffing can lead to hijacking sessions. This is when the attacker eventually takes control over the network connection, kicks off legitimate users (such as your customers) from the E-Commerce server, and ultimately gains control of it.

7.) Port Scanning

This is listening to the network ports of the E-Commerce server. When conducting such a scan, an attacker can figure out what kind of services are running on the E-Commerce server, and from that point figure out the vulnerabilities of the system in order to cause the greatest damage possible.

8.)Trapdoors/Backdoors

In developing the code for an e-commerce site, developers often leave "trapdoors" or "backdoors" to monitor the code as it is developed. Instead of implementing a secure protocol in which to access the code, backdoors provide a quick way into the code. While it is convenient, trapdoors can lead to major security threats if they are not completely removed prior to the launch of the e-commerce site. Remember, an attacker is always looking first for vulnerabilities in the e-commerce server. Trapdoors provide a very easy vulnerability for the attacker to get into, and cause system wide damage to the e-commerce server.

V . STRATEGY OF E-COMMERCE SECURITY

As e-commerce security problems are caused by many factors, to solve the security problem from different aspects, offers a variety of countermeasures. A. Security strategy to ensure the safety communications must be the necessary measures to guard against them.

A Communication links

We can use communication links like the following a firewall, proxy server, Virtual Private Network (VPN) technology; in the identification and authentication, encryption and authentication techniques will go a long way in controlling e-commerce crime.

B Legal Protection:

As e-commerce activities involves commodity transaction and security issues it should be protected by law. [10] Not only should the laws be applicable to innovations in E-commerce but they should also be sensitive to the legal developments taking place worldwide including consumer protection. The Nigerian Police and the Judiciary System must arise and help authenticate this service. If people know that they will get real justice for fraud they will be careful in perpetuating these acts

VI CONCLUSION

As e-commerce transactions are not direct, it is bound to have security implications. Thus, the healthy development of e-commerce depends on the establishment and perfection of social ethics. E-commerce transaction system is a highly integrated man-machine system, therefore in addition to network security, management of the system is also very important, as it plays a decisive role. Thus, the whole system of power distribution management and supervision, management training and assessment, ethical and professional standards must draw up complete training regulations, management jobs in order to enhance the spirit of love in e.commerc transactions.

References

1.)"Will Cashless Economy Work? Available at http:// http://www.nigeriafilms.com/news

2.) http://www.peterindia.net/ITSecurityView.html

3.) M.E Ezema , H.C. Inyiama Contemporary Malicious Code Detection-Techniques

International Journal of Engineering Research and Technology http://www.ijert.org

4.)http://www.novell.com/documentation/nbm37/?page=/documentation/nbm37/over/data/ae70rc0.html

5.)identifying e-commerce threats and vulnerabilities http://www.findlaw.co.uk/law/small_ business/business_operations/e_commerce/securing_your_e_commerce_systems/558.html

6) www.kaspersky.com/threats

7.) http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

8.) http://compnetworking.about.com/od/networksecurityprivacy/l/bldef_pingdeath.htm

8.)9http://www.trainsignal.com/blog/ping-of-death-and-dos-attacks

10.) Parviz Bagheri and K.H. Hassan, 2012. E-Commerce and Consumer Protection in Iran: A Legal Framework. *International Business Management, 6: 317-324.* http://medwelljournals.com/abstract/?doi=ibm.2012.317.324