

## **“Threats to E-Commerce Servers-Part I”**

This article starts our new series on E-Commerce security. This article as well as future articles will now be focusing on different areas with regards to E-Commerce Security. We will be looking at such issues as to how to protect your customer database and transaction information; how to create a secure shopping cart and payment system; how to write good programming code for an E-commerce site which has strong security features; how to create and implement a secure database for online transactions, as well as other managerial and technical issues.

### *Overview of Article*

This article will examine the various threats which exist to E-Commerce Servers. The next article, which will be Part II, will focus upon solutions which can be implemented to protect your E-Commerce server from such threats. Specifically, this article is divided into the following sections: (1) An Overview into E-Commerce; (2) The Security Issues with E-Commerce-The Human Element; (3) The Threats Posed to E-Commerce Servers.

### *An Overview into E-Commerce*

All of us remember the heydays of the late 1990's. We had the Internet Boom, the .com craze, venture capital money being pumped into technology startups like oil gushing out of a well, the stock market at all time highs, etc. Well, those days have come and gone, and all of us I am sure have learned painful lessons from that time period, in the last couple of years. However, there is one legacy from the Internet Boom that has survived, and will continue to be a very dominant force in the worldwide economy. That legacy is known as E-Commerce.

The term E-Commerce can be a nebulous one, and can possess different meanings to people and businesses. For example, to some entities, E-Commerce can mean simply having a video conference over the Internet; conducting an online chat session with a customer; simply putting up a website where your products and services are displayed; or just e-mailing a price quote to a potential customer. However, for purposes of this article as well as future articles, the term E-Commerce will be defined as:

*“The conducting of business communication and transactions over networks and through computers. As most restrictively defined, electronic commerce is the buying and selling of goods and services, and the transfer of funds, through digital communications. Electronic commerce also includes buying and selling over the World-Wide Web and the Internet, electronic funds transfer, smart cards, digital cash, and all other ways of doing business over digital networks.”*

Source: (1)

Although the craze for E-Commerce occurred during the Internet Boom, as you can see from the definition, the core concept of buying, selling, and paying over the Internet still exists today, and will for a long time to come. A perfect example of the above definition is E-bay. It is probably by far the largest and most popular E-Commerce site in the world. The following statistics reveal how prevalent E-Commerce is today, and will be in the future:

*The Dollar Volume of E-Commerce*

In 2004	<p>*On Thanksgiving Day: E-Commerce transactions were greater than \$75 million, a 40% increase over 2003 (Source: 2)</p> <p>*On Black Friday, E-Commerce transactions on VISA credit cards and debit cards was \$234 million compared to \$183 million in 2003, a 28.1% increase (Source: 3)</p> <p>*The Monday after Black Friday, E-Commerce transactions were about \$406 million (Source: 4)</p>
By 2005	*E-Commerce transactions will reach an expected \$12.5 billion (Source: 5)
By 2006	* E-Commerce transactions will reach an expected \$13 billion (Source: 6)
By 2008	*E-Commerce sales of <b>just</b> apparels and accessories will reach an expected \$12 billion (Source: 7)

*The Security Issues with E-Commerce-The Human Element*

There are security issues associated with E-Commerce. An entire book could be written about them, however future articles will address the security issues as they relate to the specific topic on hand. In this article, I am going to focus a little bit on the human element.

My biggest mantra to business owners is that the first line of defense against security threats is to be proactive in taking steps to protect your place of business. You can have all of the fanciest and most expensive security equipment that is available, but it does not mean anything unless you are proactive. The bottom line is why wait for something to happen first, then enhance your security? Why not take a stand now before something does happen? A perfect example of this is the recent MS Blaster worm. When it became known that this worm was prevalent, software patches became available for download to protect your computer(s) before it hit you. Well, unfortunately, many people disregarded these software patches, and did not download them until after they were hit with the worm.

In my meetings with contacts and potential clients, people are aware of security to some degree, and they know that it is a “hot topic” issue in today’s world. When I ask them about their security infrastructure, they openly admit that they know they have flaws in it. But then when I ask them about implementing a change to enhance or further strengthen their security system, the reluctance then sets in. If security is such a “hot button” issue, why is there then the reluctance to change or enhance your security system when you know it can be greatly improved? Well, it all comes down to human psychology: (1) The fear of change or trying something new; and (2) We live in a reactive society. To put it bluntly, we will only change our ways until something catastrophic occurs and which directly affects us at a great cost. Remember, there is a lot at stake—especially your customer’s loyalty to you and your bottom line. Why risk all of that when all is needed is a change to a more proactive mindset about security for your business? In fact, given the statistics in the previous table, ultimately there will be no other choice but to have a proactive security conscience, since E-Commerce will be such a dominant force in the global economy.

Therefore, the primary goal of the articles in this series is two fold: (1) To make you, the business owner, aware of the types of security threats and risks that are out there; and (2) To make you have a proactive mindset with regards to security.

### *The Threats Posed to E-Commerce Servers*

E-commerce tends to be at a higher echelon for risk and attacks. This is so because according to our definition, 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 your “E-Commerce Place of Business”[which consists of the actual website which displays your products and services, the customer database, and the payment mechanism]. If there are any attacks to this server, in one blow, there is the potential you could lose everything. Thus, being proactive about security takes on a much greater magnitude now.

Threats to E-Commerce servers fall into two general categories: (1) Threats from an actual attacker(s); and (2) Technological failure. In terms of the former, the motivation is primarily psychological. The intent is to garner personal information from people for the sheer purposes of exploitation (such obtaining Credit Card and Bank Account information; Phishing schemes, obtaining usernames and passwords, etc.). With the latter, 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 either PostgreSQL or MySQL as the database (these are database languages created from the Structured Query Language, or SQL). These latter platforms will be explored in much more detail in subsequent articles.

We will now examine the various threats and risks that are posed to E-Commerce servers. Also, we will look at some threats posed to your customers who use your E-Commerce server to buy goods and services.

The direct threats to E-Commerce servers can be classified as either (1) Malicious Code Threats; and (2) Transmission Threats. 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 latter, 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.

## **Malicious Code Attacks**

### Viruses and Worms

The most common threat 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. A virus needs a host of some sort in order to cause damage to the system. The exact definition is “. . . a virus attaches itself to executable code and is executed when the software program begins to run or an infected file is opened.” (Source: 8). So for example, a virus needs a file in which to attach itself to. 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. The key to thing to remember about viruses is that they cannot by themselves spread-they require a host file.

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. A question that is often asked about worms and viruses is which of the two are worse. This is a difficult question to answer, as the criteria for which is worse depends upon the business environment. However, one thing is certain: in terms of the rate of propagation and multiplicity, worms are much worse than viruses.

## 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.

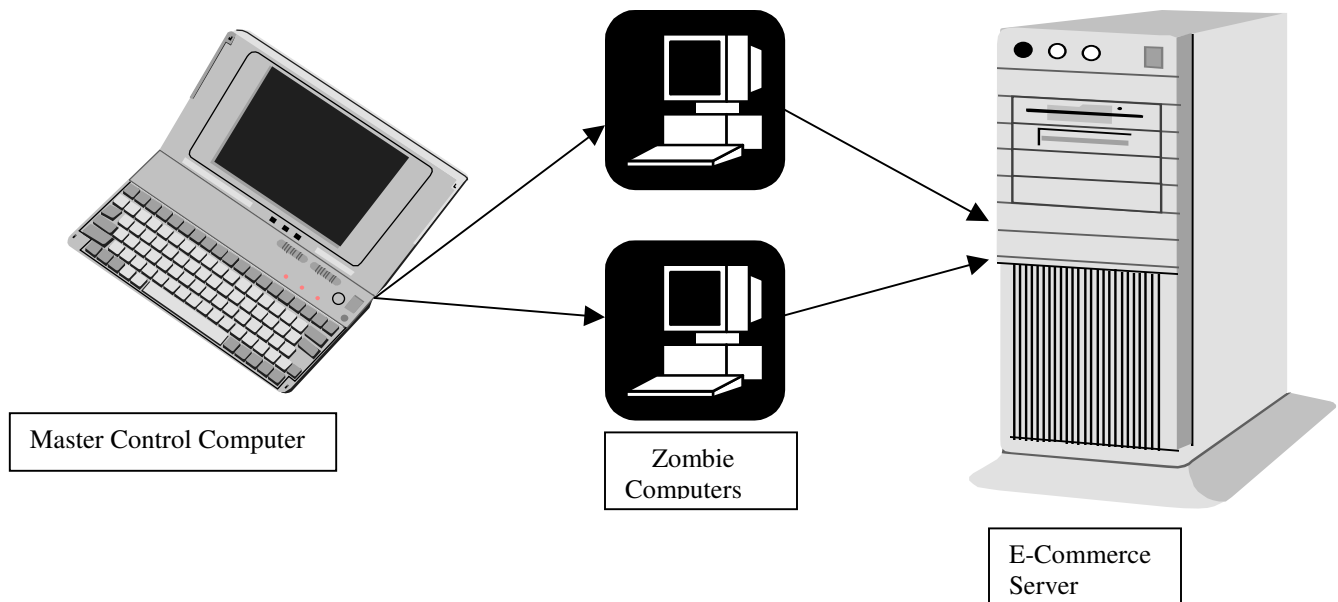
## Logic Bombs

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.

## **Transmission Threats**

### Denial of Service Attacks

With a Denial of Service Attack, the main intention 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. Because 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. 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. A Distributed Denial of Service Attack is diagrammed as follows:



*Diagram of A Distributed Denial of Service Attack*

### 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. 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.

### SYN Flooding

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 SYN ACK (or synchronization acknowledgement) 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 awaiting to receive the ACK message from the client computer, this is considered to be a half-open connection. It is at this point in which the E-Commerce server becomes vulnerable to attacks. Phony messages (which appear to be legitimate) could be sent to the E-Commerce server, thus overloading its memory and processing power, and causing it to crash.

## **Threats to Your E-Commerce Customers**

### 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.” (Source: 9). So, for example, 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 secure and legitimate site (people who launch Phishing schemes [also known as “Phishers”] can copy the HTML code from your E-Commerce site, making it look authentic in the eyes of the customer). The truth is, all of the confidential information submitted is collected by the “Phisher”, who is bent upon creating havoc and damage to your E-Commerce business.

I have seen many examples of Phishing schemes. I routinely get Phishing e-mails from banks saying that my online bank account is going to receive a security upgrade, and that I need to submit my username and password after clicking on the link provided. The irony is that I don't even have an online bank account from the banks mentioned in the Phishing e-mail. The year 2004 will probably be known as the year for the explosion of Phishing scams. According to one group that monitors Phishing e-mails, it first picked up 250,000 Phishing e-mails per month at the start of 2004. Now it has gone up to five million. Phishing “. . . has firmly established itself as a threat to any organization or individual conducting business online.” (Source: 10).

### **Other Threats To E-Commerce Servers**

There are other threats posed to E-Commerce servers, a few are listed here. These threats will be further discussed in subsequent articles.

#### 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 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.

### 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.

### 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.

### 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.

Our next article, “Threats to E-Commerce Servers-Part II”, will provide solutions to the threats detailed in this article. Remember, security is an issue which cannot be taken for granted anymore in today’s business environment. It is a necessity to be proactive, and to avoid threats and risks, before they really hurt you.

Sources:

- (1) <http://www.nref.com/dictionary.html>
- (2) <http://www.itfacts.biz/index.php?id=P2129>
- (3) <http://www.itfacts.biz/index.php?id=P2124>
- (4) <http://www.itfacts.biz/index.php?id=P2129>
- (5) <http://www.itfacts.biz/index.php?id=P775>

(6) <http://www.digits.com/articles/home-business--ecommerce-revenues-passes-the-trillion-dollar-mark.htm>

(7) <http://www.itfacts.biz/index.php?id=P1528>

(8) “Official (ISC)2 Guide To The CISSP Exam” Hansche, Susan; Berti, John; Hare, Chris. P. 161.

(9) <http://www.webopedia.com/TERM/p/phishing.html>

(10) [http://www.cio-today.com/story.xhtml?story\\_title=-----The-Year-of-Phishing&story\\_id=28868&category=cybercrime](http://www.cio-today.com/story.xhtml?story_title=-----The-Year-of-Phishing&story_id=28868&category=cybercrime)