

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

### *Overview of Previous Article*

Our last article was the first in this E-Commerce Security track series. In the last article, we examined the dominant role E-Commerce has and will play into the near term and the future. A formal definition of E-Commerce was provided, as well as the importance of taking a proactive stance on security issues. The specific threats against E-Commerce Servers were also examined, which included:

- The Human Element;
- Viruses and Worms;
- Trojan Horses;
- Logic Bombs;
- Denial Of Service Attacks;
- Ping Of Death;
- SYN Flooding;
- Phishing Attacks;
- Data Packet Sniffing;
- IP Spoofing;
- Port Scanning;
- Trapdoors and Backdoors

This article, Part II, will examine the various tools and methods that are available to protect your E-Commerce Server from the above mentioned threats as well as other threats.

This article is divided into the following sections:

#### (1) Solutions To Threats From A Wireless Perspective:

- \*A Technical Discussion Of The Data Packet
- \* Threats from Wireless: Social Engineering and Man In the Middle Attacks
- \*A Solution: Authentication-The Use of Secure Sockets Layer
- \*A Solution: Encryption-The Use of Secure Shell
- \*A Solution: Tunneling-The Use of Virtual Private Networks

#### (2) Solutions To Threats From A Hard Wired Perspective:

- \*A Solution: The Use of Firewalls
- \*A Solution: The Use of Routers
- \*A Solution: The Use of Network Intrusion Devices

## *Solutions To Threats From A Wireless Perspective*

The threats to E-Commerce Servers described in the last article can be initiated from both a hard wired source as well as a wireless source. Although wireless security will be covered in much more detail in a subsequent article, this section will describe in some detail the implications of threats to E-Commerce Servers from wireless, and solutions to those threats. Wireless applications are certainly making their mark in today's E-Commerce world. In fact, these applications even has its own term, known as "Mobility Commerce" or simply, "M-commerce." M-Commerce is expected to make a big splash, especially in wireless entertainment services, generating more than \$27 billion and having a customer base of 2.5 billion by 2008 (Source: 1). But, M-Commerce poses one of the greatest threats to E-Commerce Servers today. This is so because when your customer connects to your website to place an order, for example, at a "Wi-Fi" or "Hot Spot", from a Starbuck's café, the data packets are leaving the confines of your customer's laptop computer to the point of Internet access. Since this is a wireless connection, the data packets are literally flying in the air (as opposed to a hard wired connection, where the data packets travel in the confines of the network cable). It is at this point a hacker can intercept the data packets and cause havoc to your E-Commerce Server. As an E-Commerce business owner, you need to consider the risks posed by wireless.

However, before we go any further, a detailed and technical discussion of what a data packet is warranted at this point. The data packet will be a central core in subsequent E-Commerce articles, therefore an understanding of what it really is is important.

### **The Data Packet**

All of the information we send over the Internet, whether it is e-mail or transferring files from one computer to the other, tend to be very large chunks of data. These large chunks of data are broken down into much smaller chunks, known as "data packets." So for example, the e-mail you send is actually broken down into much smaller chunks, which are the data packets. You may be asking at this point, "Why is my e-mail being broken down into so many smaller chunks of data?" Well, it is these small chunks of data that allow for the instantaneous sending of e-mail to your recipient, such as your big E-Commerce customer. If you were to have sent this e-mail as one massive chunk, it would take a very long time for your customer to receive your e-mail. And as business owners, we are all very familiar with the adage "time is money."

A data packet (the small chunks of data) consist of primarily three things:

- A) A Header section;
- B) A Data section;
- C) A Trailer section

The Header section consists of the source address, and the destination address. The source address identifies your computer as the sender, and the destination address

identifies the computer where the data is supposed to go (the recipient). In this case of sending e-mail, the destination address is the computer of your E-Commerce customer. The Header also contains clock information, in order to synchronize the exact transmission times.

The Data section consists of the actual data-for example, the content of the message of the e-mail you are sending to your E-Commerce customer.

The Trailer section consists of a mathematical algorithm, specifically called the Cyclical Redundancy Check, or CRC. The CRC helps to make sure that the data sent in the data packet remains intact. So, when your big E-Commerce customer receives your e-mail, it is the CRC which has insured that the message remained intact when you sent it. Essentially, the CRC generates a number on the data packet when it leaves the source computer. When the data packet reaches the destination computer, which is your E-Commerce customer, this number is calculated again by the CRC. If the number remains the same, it means the data has arrived in a stable state, and intact. However, if the results are different, it means that the data was altered or changed in some manner during transmission. In this case, the altered data packet is then sent back to the source computer for retransmission. A data packet is diagrammed in Diagram #1.

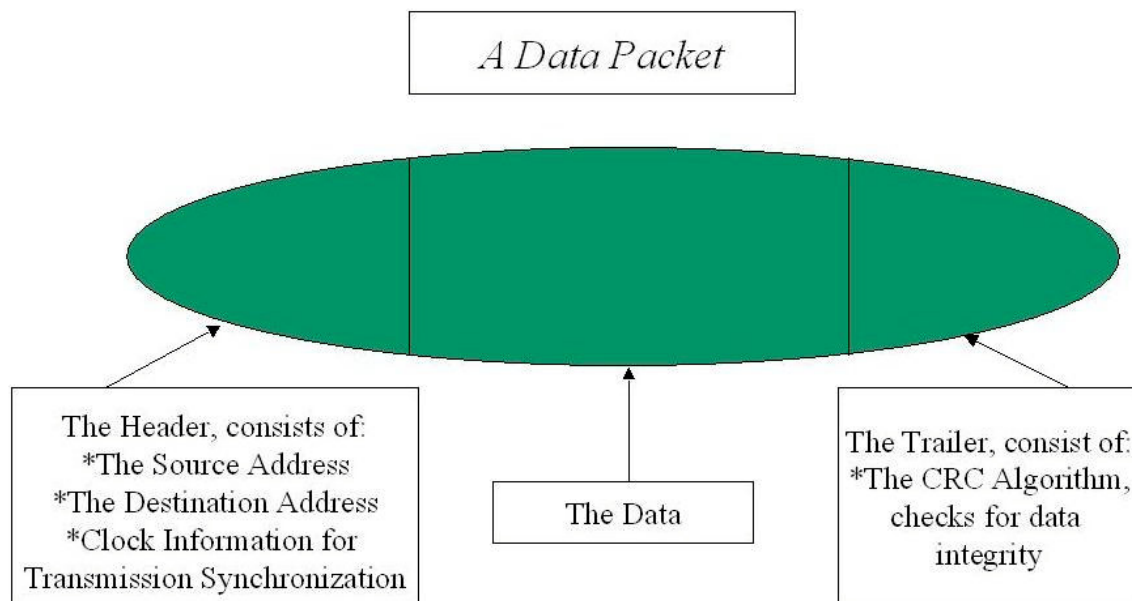


DIAGRAM 1

### Threats from Wireless-Social Engineering and Man In the Middle Attacks

Protection from wireless threats depends a lot upon the place which provides the wireless connection, in the example we have been using, Starbuck's. It would primarily be the responsibility of each café to make sure that they have implemented reasonable security

protocols. However, as an E-Commerce business owner, there are proactive steps you can take to make your customers aware of how they can take steps to help protect themselves, and your E-Commerce Server. The first thing you can do is to tell your customers to be aware of the surroundings and the people in which they use wireless access. This touches onto an area called “Social Engineering.” Social Engineering can be defined as the: “Successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, or unauthorized disclosure of an information system, a network or data” (Source: 2). For example, your customer could be sitting in a Starbucks’s café, accessing your E-Commerce site via a wireless connection on their laptop computer. Well, the person sitting next them could very well be a hacker, and try to strike up a friendly conversation with your customer in order to disguise themselves, and not to create any suspicion. At the same time, while your customer is having this friendly conversation with the hacker, the hacker could very well be using a data sniffer to intercept and analyze the data packets that are being sent from your customer’s laptop computer to the wireless access point. With the information collected from the data packets, the hacker can create havoc not only to your customer’s computer, but also to your E-Commerce Server. Also, this same hacker who is having the friendly conversation with your customer could potentially even steal the login session from your customer, and claim that they are a legitimate customer, and as a result, have full access to your E-Commerce site like any real and legitimate customer would have. This is known as a “Man In The Middle Attack”. Thus, it is very important that you tell your customers to be aware of what is around them when they use wireless access, and to use wireless access when they are at a reasonable distance away from people.

### **A Solution: Authentication-The Use of Secure Sockets Layer**

The “Man In The Middle Attack” directly relates to an area of network security called “Authentication”. It can be defined as “. . . verification who the user is and whether the user is allowed access to the network” (Source: 3). In the case of your customer logging into your E-Commerce site, they want to be sure that they are logging into a legitimate site, and from your standpoint as the E-Commerce site owner, you want to make sure that your customer’s login session cannot be hijacked by an illegitimate user, as described above. There is a tool for this exact purpose, and it is called “Secure Sockets Layer”, or SSL for short. The basic essence of SSL is that, digital certificates are shared and transmitted between your customer’s computer and your E-Commerce Server. SSL was developed by Netscape Communications and RSA Security. How do you know if you are at a website that is using SSL? The answer is simple: If you see “https” (which stands for Hypertext Transfer Protocol-Secure) instead of the usual “http” in the web address bar, and also you will notice a locked padlock image in the lower right hand of your browser (the latest versions of Netscape and Internet Explorer show this same image). Secure Sockets layer should be used on an E-Commerce site wherever your customer has to submit their Username and Password, and where they have to submit Credit Card Information in order to purchase your products and services.

## **A Solution: Encryption-The Use of Secure Shell**

Apart from authentication, you want to be sure that the connection between your customer's computer and your E-Commerce Server (and vice versa) is private to the outside world, and encrypted. Encryption is “. . . a method of scrambling or encoding data to prevent unauthorized users from reading or tampering with the data” (Source: 4).

There is a tool for this also, and it is called “Secure Shell”, also known as SSH. It is a method that provides for an encrypted login connection to a server, for example, your E-Commerce Server. In this case, your customer's Username and Password, which would normally be sent as plain text over an insecure Internet connection, would be scrambled into an undecipherable format. For more information about Secure Shell and downloads, please visit [www.openssh.org](http://www.openssh.org).

## **A Solution: Tunneling-The Use of Virtual Private Networks**

Unless you are using either Secure Sockets Layer or Secure Shell, whenever you connect to the Internet, any information you transmit (such as a Username/Password, Credit Card Number) is sent as what is known as “cleartext”. This means that any information transmitted is very readable as well as easily accessible when the data packets are intercepted. Although Secure Sockets Layer and Secure Shell will do a good job in protecting the information your customer sends to your E-Commerce Server and vice versa, there is one more tool that is available in order to provide further protection: Virtual Private Networks, or also known as VPN's. Virtual Private Networks not only offer encryption, but they also use the concept of “tunneling” for the added protection. The concept of “tunneling” means that the original data packet which contains the confidential information (such as the Username/Password, Credit Card Number) is placed inside another data packet for the extra layer of protection. An example of “tunneling” can be seen in Diagram #2.

There are currently three major network protocols which support the use of Virtual Private Networks:

- Point To Point Tunneling Protocol, also known as PPTP: This can be considered to be an older protocol, comes with Windows NT. Essentially, this is a more secure form of the Point to Point Protocol, which is the protocol used for accessing the Internet via a dial up modem.
- Internet Protocol Security, also known as IPSec: This type of protocol offers more security features, such as ensuring the confidentiality and authenticity of the data packets. This protocol makes use of advanced encryption techniques, such as Digital Signatures and Digital Certificates.
- Layer 2 Tunneling Protocol, also known as L2TP: This type of protocol is a combination of Microsoft's Point to Point Tunneling Protocol and Cisco Systems Layer 2 Forwarding Protocol. The primary advantage of L2TP is that it can support other protocols such as Internetwork Packet Exchange (also called IPX, this is the

protocol used by Novell Netware) and AppleTalk (this is the protocol used by Apple computers).

The use of a Virtual Private Network offers a number of advantages such as cost savings; quick and easy network set up and configuration (scales easily); network topology simplification; improves Internet security; and extends geographic connectivity, especially for your E-Commerce customers that could be thousands of miles away from you physically.

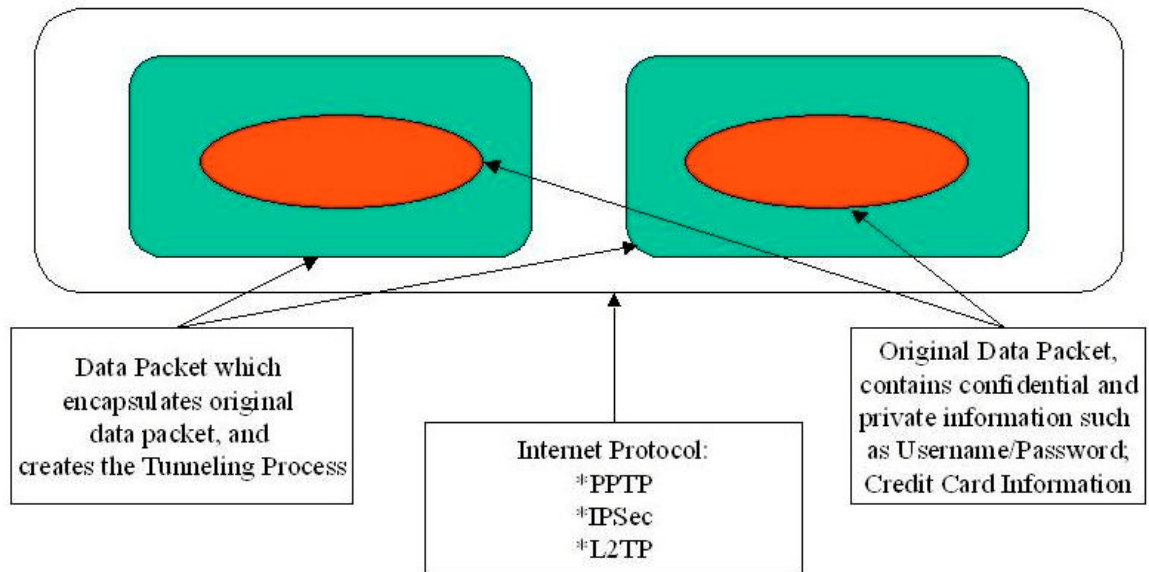


DIAGRAM 2

Currently, there are no standards for creating and implementing a Virtual Private Network. Therefore, the configuration is often dictated by the needs and demands of the business. When deciding upon the technology to be used in a Virtual Private Network, as the E-Commerce business owner, you want to go with a brand leader. In this regard, Cisco Systems, Inc. is a leader, and they offer a wide range of technological solutions for Virtual Private Networks. One of their leading products is the “Cisco VPN 3000 Concentrator”.

### *Solutions To Threats From A Hard Wired Perspective*

We have just reviewed solutions to threats posed to your E-Commerce Server from a Wireless Perspective. In this section, we will review solutions to threats posed to your E-Commerce Server from a “Hard Wired Perspective”. What do we mean by a “Hard Wired Perspective?” We mean a computer that is linked to and can access the Internet via a network cable (whether it be a telephone line, an Ethernet Cable, etc), and launch attacks to your E-Commerce Server. In other words, the data packets do not flow in the air, they flow in the physical confines of the network cable. There are a number of

solutions, in particular, we will be examining the use of Firewalls, Routers, and Network Intrusion Devices.

### **A Solution: The Use of Firewalls**

A Firewall can be considered to be the fortress, or protection zone, which protects your E-Commerce Server and the network it resides upon from the outside world (see Diagram #3). More specifically, a firewall can be defined as “a network configuration, usually both hardware and software, that forms a fortress between networked computers within an organization and those outside the organization” (Source: 5). Essentially, the concept of the Firewall is to examine, or filter, the incoming data packets from the outside world and determine if they are to be allowed into the network which houses your E-Commerce Server. In order to filter out the data packets, certain conditions need to be first established as to what the Firewall needs to look out for when examining the data packets. The following are examples as to what conditions can be set up in the Firewall:

- **The IP Address:** Every computer or server on a network contains a unique IP address which identifies it from the other computers and servers. For example, the IP address of the server on which the website of HTG Solutions resides on is 64.78.54.76. So, you could set up a condition in the firewall which would block all data packets coming from this IP address. Also, you can establish a condition which blocks data packets from domain names. So again, you could set up a condition which blocks data packets coming from www.htgsolutions.com. In fact, when you open up a Web Browser, and type in a domain name in order to access a certain website, that domain is actually broken down into the IP address. So for example, when you type in www.htgsolutions.com, the domain name gets broken down into its IP address of 64.78.54.76. This happens via the Domain Name Server, or DNS. You could even type in the IP address directly and that will take you to the website as well. In fact, the primary reason why we use domain names is that it is far easier to remember a name than a series of numbers.
- **The Network Protocol:** You can set up a condition so that the network on which your E-Commerce Server resides upon will only communicate with other computers via only certain kinds of protocols. In other words, you can restrict the type of protocol your E-Commerce Server will communicate with. Examples of network protocols which can be restricted in the firewall:

\*HTTP: Hyper Text Transfer Protocol, the network protocol used to access Web sites;

\*FTP: File Transfer Protocol, the network protocol used to transfer files from one computer to another;

\*SMTP: Simple Mail Transfer Protocol, the network protocol used to send and receive e-mail;

\*Telnet: The network protocol used to access remote computers.

- **Specific Words and Phrases:** You can include a condition in the firewall which examines the incoming data packets for certain words or phrases. If the firewall determines that a data packet contains the same keyword or phrase that is also established as a condition, the data packet is discarded. The key point to remember here is that there has to be an exact match. For example, if a condition was set up in the firewall to block all data packets containing the name “htgsolutions”, and there was one data packet which had “htg-solutions” instead, that data packet would be allowed to enter the network.

Also, a Firewall can act as a “Proxy Server”. For example, if you have to use your E-Commerce Server to access other Web sites on the Internet, the Firewall will act as the intermediary between your E-Commerce Server and the Internet. The security advantage here is that your E-Commerce Server really never interfaces with the outside world. All of the data packets that come from the Internet is first received by the Firewall, and are inspected. After inspection, they are then directed to your E-Commerce Server.

Another security method you can use for a Firewall is called “Stateful Inspection”. With this, only key parts of the data packet are examined, not the entire contents. For example, information in the data packets that is sent to the outside world from your E-Commerce sever is compared to the information in the inbound data packets that are received by the Firewall which protects your E-Commerce Server. If there is a reasonable match in the information, the data packets are then allowed to enter the network which houses your E-Commerce Server. This is also known as “Dynamic Packet Filtering”, vs. “Static Packet Filtering”, which is the establishing of conditions mentioned previously.

An advantage of a Firewall is that it can act as a central “choke point”, or central point of administration, where security rules and audit procedures can be implemented. The Firewall can also provide valuable information to the Systems Administrator, such as the types and amount of data packet traffic, number of attempted network break ins, etc. The security level to be established on the Firewall depends upon the level of security you want to implement to protect your E-Commerce Server. For example, you can implement very minimal security, or go all the way and implement maximum security, which in this case, would block all communications to and from your E-Commerce Server. You could start out first by implementing maximum security, then work backwards, and decide the kinds of network connections you want to allow.

However, the key thing to remember about a Firewall is that while it is a means of excellent protection of your E-Commerce Server to the outside world, it cannot protect against threats and attacks from within the network in which your E-Commerce Server resides. In this regard, the best form of protection is to implement and monitor the Firewall as part of the overall security policy.

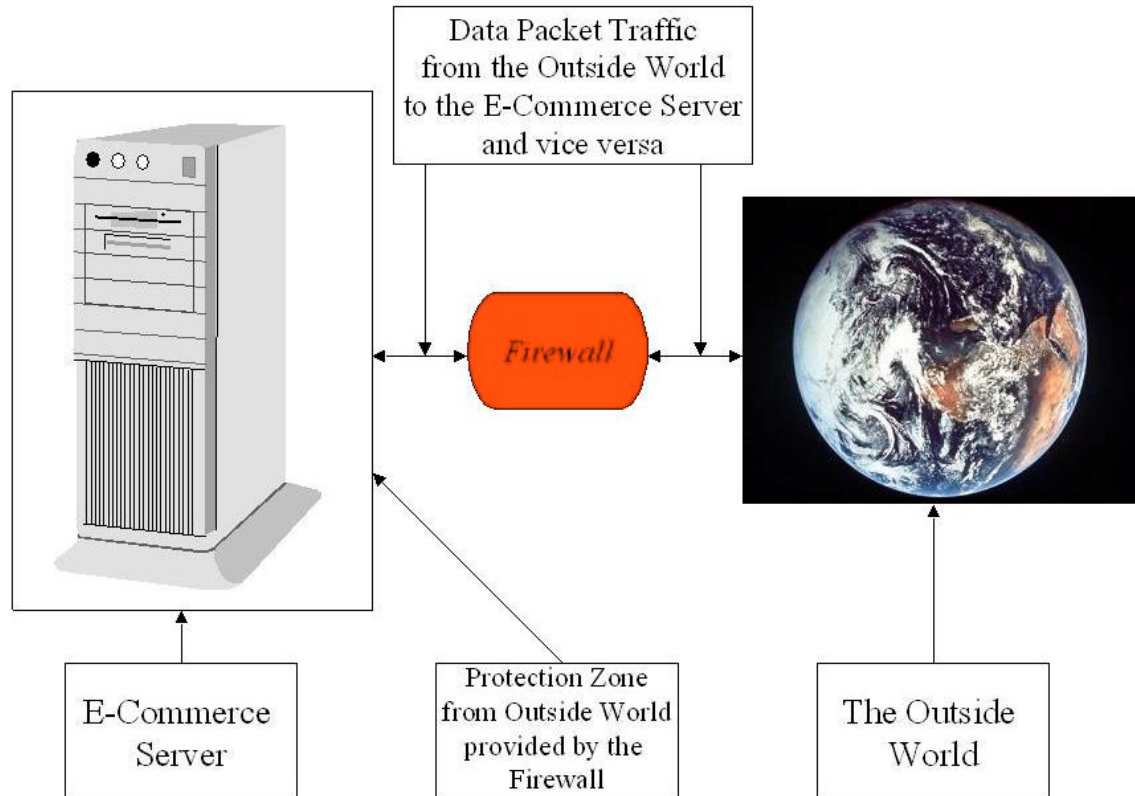


DIAGRAM 3

### A Solution: The Use of Routers

A firewall can either come in the form of a software package or a hardware package. When it comes as the latter, it is called a “Router”. In a network, there is typically more than one computer or server, associated with lots of network cabling. Usually, the cabling at some points in the network come to a central place where there are further distributed. These central points are called “Hubs”. The Hub usually has a number of ports, or slots, in which the network cabling connects into. The Router offers two advantages over the Hub: (1) It is a Firewall, so it protects the network and the E-Commerce Servers, and (2) Routers insure that data packets do not go where there are not intended to, and make sure that they arrive where there are intended to. In this regard, the Router actually determines the best or most efficient path in the network for the data packets to travel. It should also be noted that the Router consists of ports also, just like the Hub, in which the network cabling can connect into.

In terms of Firewall capability, Routers follow the same principles and concepts as described in the previous section. However, routers also add another layer of protection to your E-Commerce Server, and it is known as Network Address Translation, or NAT. Essentially, the TCP/IP address of your E-Commerce Server is masked to the outside world. Only the TCP/IP address of the router is visible. This can also mean cost savings

for the E-Commerce business owner. Depending upon who is your Internet Service Provider, you typically have to pay an extra fee if you want connect multiple servers or computers to the network (basically, you are just paying for extra TCP/IP addresses). But with NAT, you can use one TCP/IP address for multiple computers or servers, without extra charge.

With respect in determining the most efficient path for a data packet to take in a network, at the heart of the Router is a “Configuration Table”, also known as a “Routing Table”. This table consists of: (1) Information on the network connections that leads to certain groups of TCP/IP addresses in the network; (2) The priority for which connections to be used; and (3) The rules on how handle the network traffic (which is the flow of the data packets). To help determine the optimal path for the data packet to take, mathematical algorithms are used, and they are grouped in two categories: (1) Global Routing Algorithms: Each router has information about every other router on the network, as well as the traffic status of the network; and (2) Decentralized Routing Algorithms (also known as Distance-Vector algorithms): The router only has information about another router it is directly connect to; the router does not possess information about the entire network. A key point to remember here is that as the size of the network and data packet traffic increases, so does the size of the Configuration Table. And as the size of this increases, the efficiency of the router in directing the data packet traffic consequently degrades.

Routers provide a cost effective means for protecting your E-Commerce Server and the network it resides in. There are many vendors who develop routers, but among the most popular are Linksys, Netgear, and Cisco Systems. Routers are now pretty much “Plug and Play”, meaning that they require minimal installation efforts. Routers come in both hard wired and wireless types. A picture of a Router can be seen in Diagram #4.



DIAGRAM 4

## **A Solution: The Use of Network Intrusion Devices**

While Firewalls do a good job of protecting your E-Commerce Server network, they only take a defensive role. In this regard, Intrusion Devices (also known as an “IDS”) provide an offensive role, in that they not only defend your E-Commerce network, but they also actively look for threats that take place both outside and inside of the network, and alert the Security Administrator of the threat. In certain cases, the IDS will even block the threat, by blocking the TCP/IP address of the source causing the threat.

In order for the IDS to detect threats, it must have an audit trail in its system in order to conduct comparisons. The data that is used to create an audit trail is called Audit Data. The Audit Data consists of:

- “Internet Connection Event Data:
  - \*Username
  - \*Host Name
  - \*Source/destination IP address
  - \*Timestamp
  
- System Level Event Data:
  - \*Logon attempts (successful/unsuccessful)
  - \*Date and Time of each logon and logoff
  - \*Devices used
  - \*Functions performed
  
- Application Level Event Data:
  - \*Data files opened and closed
  - \*Specific actions (read, edit, delete, print)
  
- User Level Event Data:
  - \*User initiated commands
  - \*Identification and authentication attempts
  - \*Files and resources accessed”

(SOURCE: 6)

The actual hardware of the IDS is composed of three components: (1) The sensor (which captures the data); (2) The analyzer (determines in an actual intrusion into the network has taken place); and (3) The user interface (which displays the results coming from the analyzer).

Today, there are two types of Intrusion Detection Devices available: (1) A Network Based Intrusion Detection Device (also known as a “NIDS”); and (2) A Host Based Intrusion Detection Device (also known as a “HIDS”). With the former, the NIDS are placed in strategic locations throughout the E-Commerce network. They examine the data packet traffic in real time. The advantage here is that the data packets are examined before they enter into the E-Commerce network. The NIDS are primarily looking for data packets which can launch Denial of Service Attacks against your E-Commerce Server, or those that carry malicious code in them. Scalability is an issue with NIDS. As the E-Commerce network grows in size as well as the flow of data packet traffic, the NIDS must be able to support this growth. Also, the use of encryption technology may not work well with NIDS, in other words, it may not be able to decipher the encryption of the data packets, and thus let them enter. With the latter, an Intrusion Device resides on a single server or computer. Thus, intrusion detection is only done for that single server or computer. NIDS can be viewed as global protection for the E-Commerce network, and HIDS can be viewed as local protection.

In order for the Intrusion Detection Device to actually detect an attack, it has to analyze and make comparisons to the audit data it has been given to what is happening on the E-Commerce network in real time. In order to make these comparisons, the Intrusion Detection Device uses what is known as an “Analysis Engine”. There are three types of Analysis Engines:

- Rule Based Analysis Engine:

The pattern of user activities is analyzed. There are two methodologies utilized here, a state based methodology and a model based methodology. With the former, network intrusion attempts are classified as a pattern of changes in system states. An example of a change in a system state would be a user accessing a file containing executable code, modifying the code, and saving it. With the latter, the pattern of user activity is created into a model.

- Statistical Based Analysis Engine:

Statistical profiles are created to compare any deviations to what would be considered as normal behavior on part of the users accessing the E-Commerce network. Examples of deviations or suspicious network behavior include:

- “\*Multiple, failed logon attempts
- \*Users logging in at strange hours
- \*Unexplained changes to system clocks
- \*Unusual error messages
- \*Unexplained system shutdowns or restarts”

(Source: 7)

- Signature Based Analysis Engine:

Under this system, the information in the data packet coming into the E-Commerce network is compared against a database of information or “signatures” of known network attacks.

### *Conclusions*

In summary, we have looked at solutions to threats posed to your E-Commerce Server. We have examined threats from the wireless perspective and the hard wired perspective. With respect to wireless, the use of Secure Sockets Layer, Secure Shell, and Virtual Private Networks was examined. In terms of hard wired, the use of Firewalls, Routers, and Intrusion Detection Devices were also examined.

It is important to keep in mind that while each of these security measures described do afford a good sense of protection, you should not just use only one of them as your means of defense from threats and attacks. As I said in the last article, you must use a multi-tiered security system in order to have the best layer of security possible. For example, you should use a combination of the six security measures described. But above all, the key is to remain proactive, and be aware of the threats that are imminent and could happen. As discussed previously in the article, Firewalls do a good protecting the E-Commerce network from the outside, but they cannot defend against threats and attacks from within the E-Commerce network. Thus, it is up you, to take the proactive stance to make sure that these internal threats and attacks do not occur.

### **Preview Into the Next Article**

Given the explosion of E-Commerce threats and attacks, there has been a move in the business community towards using what is known as Open Source Software in E-Commerce applications. This type of software has proven to be much more stable, robust, scalable, and most importantly, more secure than what the other alternatives are. The most popular Open Source Software systems are Linux (as the Operating System), Apache (as the Web Server), and variations of Structured Query Language (also, known as SQL, for the Database), which include PostGRE SQL and My SQL. . Our next article, entitled “The Trend Towards the Use of Open Source Software in E-Commerce: Technical and Business Implications” will examine and review the technical and business aspects of Linux, Apache, and SQL.

### **SOURCES:**

- (1) <http://www.rocsearch.com/samples/Mobile%20E-Commerce%20-%20Applications%20and%20Business%20Opportunities.pdf>
- (2) “Official Guide To The CISSP Exam”, Hansche, et al., 2004, p. 58
- (3) “Official Guide To The CISSP Exam”, Hansche, et al., 2004, p. 184

(4) <http://securityresponse.symantec.com/avcenter/refa.html>

(5) [http://docsrv.sco.com/INT\\_Proxy/glossary.htm](http://docsrv.sco.com/INT_Proxy/glossary.htm)

(6) “Official Guide To The CISSP Exam”, Hansche, et al., 2004, p. 212

(7) “Official Guide To The CISSP Exam”, Hansche, et al., 2004, p. 209