

Secure On-Line Transaction in Nigeria

Odabi I. Odabi

Department of Mathematics and Computer Science,
Benson Idahosa University, P. M. B. 1100,
Benin City, Nigeria.

Abstract

It may be simplest to contract with some other company, like electronic shop operator, Internet service Provider, or some other organization, to manage servers, orders, and content. However, that company itself must use some method or methods of accepting and processing orders. The simplest method of doing direct business on-line on the Internet is to set up a secure World Wide Web (WWW) Server, then create content pages and programme forms to take orders.

Keywords SSL, S-HTTP, Merchant, TCP/IP

INTRODUCTION

Nigeria is the most populous African nation and the large land area is increasing making it necessary for on-line business to have a place in the economy. It is becoming cumbersome to haul good from the West coast to the East coast and from North to South. The rail system is poor, the Air transportation is not developed to haul goods and the Road transportation does not provide the facility to effectively have efficient movement of human and materials.

At a point, Netscape Communications dominates the secure WWW server market, as it does the browser market, Netscape makes freely available evaluation copies of its software, and has been an active participant in the development of Internet standards for secure commerce. However, Web browsers and servers from any vendor are expected to interoperate with the servers and browsers of any other vendor – this is the whole point behind using Internet standards. A secure WWW server must, by definition, support some type of security protocol. At the moment, the two most important of these are the Secure Hypertext Transport Protocol (S-HTTP) and the Secure Socket Layer (SSL) which was initially developed by Netscape and offered to the Internet community as a proposed standard. One of their primary advantages is their relative unobtrusiveness to the consumer using SSL or S-HTTP enabled browser.

Secure Server Purchasing

The resulting browser/server interaction is, to the consumer, very closely mapped to the interaction that occurs when a consumer makes a purchase from a catalogue. The consumer browses through graphical and textual descriptions of the merchant's products, selects a purchase, and usually clicks on a button that says something like "BUY NOW" to make a purchase. If the consumer is using a secure browser

supported by the secure server, that button will produce a form on the consumer's screen, which the consumer must complete. Delivery and payment information will usually be required, and at some point after this information has been provided the product will be delivered. If the customer is using a browser that is not secure or that uses a protocol not supported by the server, then some other method must be employed to consummate the transaction.

Delivery information represents name, address, delivery address, e-mail address, and any other information necessary or desirable to deliver the product. If the product happens to be a physical item, then a physical destination, preferred shippers, and telephone number may be necessary. If the product is a digital item, then it may be transmitted directly to the consumer via the browser, by e-mail, or through some other applications like file transfer.

Secure Server Selling

Merchants want to make it economical, pleasant and easy for consumers to buy their products and doing so with a secure Web server is no different. There is a broad spectrum of options to choose from to balance price against a pleasing shopping experience. Ease of use is definitely a factor for the consumer using secure browser. First the merchant needs to publish product offerings on the Internet with a secure server. Servers are available that support (SSL) and S-HTTP and both. Because the Internet is an open network, based strictly on the proper and widespread implementation of standards, it does not make sense for merchants to limit their potential customers by using only one standard. By supporting both SSL and S-HTTP, they support transactions with consumers whose browser use either of those standards (Rosenblatt, 1995).

However the merchant must go beyond merely setting up the server. As with mail orders, there must be a mechanism for processing the information contained on an order form. The common Gateway Interface (CGI) is the first specification for this activity. WWW forms prompt the consumer for some kind of information and on receipt the form routes that information somewhere.

In the simplest case, the information provided by the consumer might be dumped into a data file to be manually processed later. The merchant would go through this file, processing credit card information and shipping the product off to the indicated delivery address. This may be an acceptable solution for low-volume applications – merchants who do not anticipate a large flow of on-line transactions, for instance. If the product is delivered immediately, there is no guarantee for the merchant that the payment information is correct, but waiting to ship the digital product may not be acceptable to the consumer who assumes immediate delivery. More often, the merchant will use interfaces of some type to automate transactions. For example, banks, credit card clearing organizations and credit card companies are all increasingly willing to authorize transactions executed over the Internet. Companies selling physical products over the Internet use e-mail confirmations and shipping notices to keep customers up to date on the status of orders and all merchants can use network applications to notify their internal organization of orders.

Required Facilities

The merchant must understand (and the educated consumer should understand) that purchasing products over the Internet requires a significant investment in software, hardware and services. Surprisingly, the software and hardware components are probably the smallest part of the investment, while the “services” can be acquired from any number of different providers.

The majority of Internet merchants will be unlikely to set up their own secure services, because doing so can be complicated for the Internet novice, and also because there are so many companies now offering such services. However, merchants who are aware of what their options are can be smarter consumers of these services, and customers who are aware of how their on-line orders are processed can be smarter on-line consumers.

Hardware

Technically, any computer that can run an implementation of TCP/IP (including a WWW server programme) and that can be connected to the Internet can be a WWW server. More realistically, the system should have a great deal of processing power to handle many simultaneous or near-simultaneous

requests for information. It should have a hard disk sufficiently large to store all the information to be published in the Web server as well as system software. It should have a sufficient fast Internet connection to support the maximum expected load on the system. And it should have security features sufficient to protect it from unauthorised access. Perhaps surprisingly, a graphical user interface, or any graphic capability, is not technically necessary on the server – it does not have to display information locally, but rather sends and receives data across the Internet (Hafner and Markoff, 1997)

In practice and at a minimum, this translates to a fast, current personal computer capable of running an operating system, using an Ethernet connection to an Internet router. A UNIX workstation or PC-architecture server system is preferred, though. The Internet connection itself should probably be at least a dedicated telephone line running 56 Kbps. Internet routers are often included in Internet service packages, but they are often simply fast personal workstations with special networking software and hardware. Some organizations using the Internet may prefer to simply get a server and an Internet connection and leave their internal networks out of the loop. However, those who do opt to connect their organizational networks to the Internet along with their Web server will almost certainly want to invest in some kind of firewall architecture to protect their network from intruders. This is likely to add to the cost of the hardware required for an Internet connection, but is necessary whether they are running Web server or not. Total cost depending on the systems selected, can be anywhere from a two million Naira or up. A typical implementation, using a low-end PC server/high-end personal workstation, should cost somewhere between N700,000.00 and N1,500,000.00, including router, network cards and cable.

Software

A TCP/IP implementation is necessary for the Web server. This may be built into the operating system, or it may be a part of the Web server package, but in any case it is necessary. Likewise, a Web server package is required. This is the Software that responds to requests from a browsers on the Internet and send out the desired information. Security, as mentioned before should be part of the operating system. Savvy system administrators make sure that there is no other software on Internet server. This guarantees that if an intruder should compromise that system, there is no software available to the intruder for further mischief. For example, network software installed and configured on a server allowing access to organizational data could be used by an intruder to access, modify or delete that information (Drake and Brown, 2000).

Services

The raw materials are relatively cheap, but the knowledge of how to put it all together is expensive. And there is quite a handful of different things that need to get done when setting up a server:

- Internet service.
- Administer Internet Link and servers.
- Create Web server content.
- Process transactions/

Internet service is simply the process of getting connected to the Internet, and keeping that access up and running. In some ways it is comparable to getting a telephone connection – the ISP simply offers connectivity, not content (Stern, 2003).

Some Internet service providers will also manage your link and your server hardware. This should mean they will keep the systems up and running and manage access to the systems. This often includes security and firewall services.

Creating and maintaining Web server content is critical and is a task often farmed out to consultants. While this approach may be effective for getting a website online quickly, maintaining and updating content must be ongoing task. Fortunately, there are many tools available to make Web authoring easy, and these will tend to drive down the cost of managing Web content.

Finally, transactions using debit/credit cards must be settled. The use of the “swipe” machines in stores where credit cards are accepted should be in shopping outlets. This transmit information about the transaction to a clearing company, which then provides an authorization code indicating whether the transaction will be processed. This same process can be linked to a secured Web server, for a price. This is just one of the services included in on-line commercial environment. The services of credit card is available, but Nigerians need to be properly sensitized on the its use and benefits

CONCLUSION

Setting up a Web site for buying and selling can be complicated and expensive. It is not for everyone, but some companies have been setting up electronic, virtual, or on-line malls. The shopping mall is a comfortable model for consumers and merchants, and it is relatively straightforward to simulate using the World Wide Web. Mall operators allow individual to “rent space” on the mall. The financial arrangement may vary, but generally include some kind of monthly charge, charges for storage space required, and also usually some charge for each transaction. As with other Internet Commerce service providers, digital malls provide a way for individual merchants to sell on-line without having to assemble all the parts themselves. The parts are still all there, and merchants investigating on-line commerce options should consider the systems and networking expertise

of the service provider as well as the commercial facilities. Building the infrastructures and services is very much achievable but Nigerian need to be better sensitized on the need to build credit.

REFERENCES

Drake, C. and Brown, K., (2000) Panic! Unix System Crash Dump Analysis, Prentice-Hall. 2000. Pp 91 - 94

Farmer D and Venem W., (2001): “Improving the Security of Your Site by Breaking Into it”

Hafner K., and Markoff J., (1997): “Cyberpunk”, Simon & Schuster, New York. Pp 74.

Libicki M., (2003): “What Is Information Warfare?” Institute for National Strategic Studies, USA.

Rosenblatt, K., (1995): High Technology Crime, KSK Publications San Jose, CA.

Spafford, E. H. and Weeber, S. A., (2001): Software Forensic: Can We Track Code to Its Authors? Purdue Technical Report CSD-TR 92 – 010

Stern D. L., (2003): “Preventing Computer Fraud”, McGraw-Hill. Pp 132.

“The New Processing Methodology,” (2001): User manual for Filter_I, New Technologies Inc.

BIOGRAPHY

Dr. Odabi I. Odabi is a currently the Head of Department of Mathematics/Computer Science at Benson Idahosa University, Benin City. He worked for Alameda County Government, California, U.S.A, where he rose to the post of IT Services Specialist before returning to his home country, Nigeria in 2004. Prior to this time he attended various institutions in United States of America including Golden Gate University, San Francisco CA. and earned M.Sc. (Telecommunication), M.Sc (Telecommunication Management), M.Sc. (Digital Security) and Ph.D. (Telecommunication). He is a certified IT Security professional.