Internet Security As An E-commerce Enabler

Víctor R. González, PE, MCP
Student of Masters of Engineering Management
Polytechnic University of Puerto Rico
vgonzal@janpr.jnj.com

Alfredo Cruz, PhD.
Associate Professor
Polytechnic University of Puerto Rico
across@coqui.net

ABSTRACT

In the words of futurist Joel Arthur Barker "when the paradigms shift, everything starts from ground zero".

The digital revolution is swiftly reshaping all aspects of life in society "in ways and forms we cannot fully appreciate". These "new digitally-based economic arrangements are changing how people work together and alone, communicate and relate, consume and relax" [1]. The economic system based on direct contact between merchants and customers is giving way to an electronic, human independent system we know as e-commerce. The immense advantages of the new system (product availability, time and cost reductions, lack of geographical barriers) provide savings that are passed on to customers. On the other hand, there are disadvantages, such as lack of human interaction, privacy and security issues and the opportunity for scam artists to take advantage of the system's anonymity to commit their crimes.

Security and privacy are the most prominent concerns mentioned by users. The purpose of this paper is to present the different enabling factors and obstacles to e-commerce, focusing on the security alternatives available to facilitate digital commerce.

SINOPSIS

De acuerdo al futurólogo Joel Arthur Baker "cuando el paradigma cambia, todo comienza desde cero".

La revolución digital está cambiando todos los aspectos sociales "de maneras y formas que no podemos apreciar completamente". Estos "nuevos arreglos basados en una economía digital están cambiando la forma en que las personas trabajan solas o en conjunto, se comunican y se relacionan, consumen y se relajan" [1]. El sistema económico basado en el contacto directo entre los comerciantes y sus clientes está dando paso al sistema electrónico, independiente de contacto humano que conocemos como comercio electrónico. Las grandes ventajas del nuevo sistema (disponibilidad de productos, reducciones en costo y tiempo, eliminación de barreras geográficas) resultan en ahorros a los consumidores. Por otro lado, existen desventajas, tales como la ausencia de relaciones interpersonales, falta de privacidad y seguridad y la oportunidad para que criminales astutos aprovechen la anonimidad del sistema para cometer sus crímenes.

La falta de seguridad y privacidad son la preocupaciones mayores mencionadas por los usuarios. El propósito de este artículo es presentar los distintos factores que estimulan y aquellos que obstaculizan el desarrollo del comercio electrónico, enfatizando en alternativas para mejorar la seguridad del comercio electrónico.

I- INTRODUCTION

The digital revolution started as the Internet opened up to the world. Up to that moment, military, research and education objectives were the main Internet drivers. Soon enough, the availability of graphical tools and the creation of the World Wide Web (WWW) consolidated the unlikely union of business and the Internet, thus giving birth to electronic commerce. Many privacy advocates, nervous with the possibility of Big Brother controlling our lives through the Net, voiced their disapproval. In spite of those concerns, e-commerce exploded. Industry experts have tried to estimate its growth, only to find that their most optimistic projections have fallen short. In 1997, private analysts forecasted that retail sales would reach $7 billion by 2000. By the end of 1998, Internet generated retail business probably reached $15 billion. As with all new technology, obtaining real data is still very challenging. Forecasters are now estimating business to consumer sales between

$40 and $80 billion for 2003. Business to business e-commerce is expected to reach $1.3 trillion in 2003.

II- FACTORS AFFECTING E-COMMERCE GROWTH

In the meantime, most of the people are waiting for technology to become more robust and reliable. Consumers, as well as businesses, are looking for tried and true methods to safely exchange economic information through the Internet. The most current research identifies three factors affecting Internet based business growth:

A- INTERNET ACCESS COST

Market forces (offer and demand) will control this factor. Although the issue has three aspects, namely, the **cost of the access device**, typically a PC, the Internet Service Provider **(ISP) cost** and the **telephone line access cost**, situations vary by country. Some ISP's in Europe are offering free access. Some US based companies offer low cost PC's in exchange for a long-term ISP contract. Other companies are developing alternate devices, such as Web-TV. Telephone connection charges and fees continue to decline, promoting Internet access growth. Dial-up access over regular telephone lines is very slow, in the order of 28-56 Kbps. There are options under development to provide faster and better access, namely, broadband cable modems (up to 1 Mbps, depending on the number of users in the segment), ISDN (Integrated Services Digital Network, 64-128 Kbps) and DSL (Digital Subscriber Line, 128 Kbps-1Mbps).

B- POLITICAL AND REGULATORY ISSUES

As the world becomes an interconnected entity, countries and institutions start to understand and realize the benefits of instant communications as set forth by the Internet. Countries will enact laws to promote Internet growth or amend those that hinder its development.

C- CONCERNS ABOUT PRIVACY AND SECURITY OF CREDIT CARD PURCHASES

The third aspect is the most complex, since the Internet is an open system in constant change. There are different motivations for technological advances, and not all forces are positive. The ever-growing virus list, the blatant advertising of pornographic material, the illegal access to secure sites (Pentagon, White House) by unauthorized users and the damages to public domain sites send a message to the general public that the Internet is full of perils.

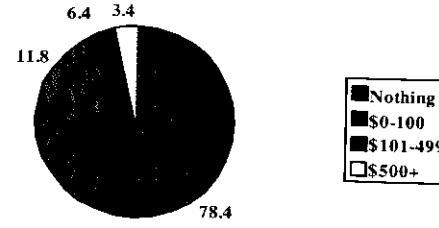
III- E-COMMERCE TRANSACTIONS

Customers have several options to complete a transaction: 1) research online and finalize their purchase offline, usually at the merchant's brick and mortar facility, 2) research and order online, but process payment offline, usually by phone, or, 3) research, order and pay online, via credit card.

The Internet is mainly used as a research tool. It provides for fast gathering of data, product feature analysis, cost comparison and evaluation from independent sources, all in a relaxed atmosphere. For example, the number of people shopping for books was estimated at 12.6 million in 1998. The number of people looking for cars or car parts was estimated at 18.2 million in the same period. Anyone who has visited a car dealership can attest the uneasy feelings produced by high-pressure sales tactics, as opposed to the accurate facts and figures obtained online from reliable sources in the comfort of the prospective client's home. Although cars cannot be purchased online, the opportunity to conduct a more rational research provides great advantages to consumers.

E-commerce has grown enormously on small ticket items like books and CD's, intangible products, such as vacation packages and investment products, mainly because customers do not need to physically inspect them, prices (therefore risks) are manageable and delivery, if needed, is fast and cheap [2, 3]. Figure 1 illustrates the distribution of online sales based on traffic and spending. The largest portion corresponds to users who buy nothing (78.4%). As the sales amount increases, the percentage of those who buy online decreases.

Online spending distribution



Source: Harris Interactive

Figure 1: *Online spending values*

IV- SECURITY AND PRIVACY ISSUES

A study by the Boston Consulting Group identified security concerns as the principal obstacle for Internet growth [4].

Throughout history, merchants have gathered personal information about their customers to better understand how to serve their needs and wants.

This information is often distributed to other businesses. With the advent of the digital era, customers perceive that online businesses have better tools to collect personal information and act upon it. One example is the use of cookies. According to Netscape, cookies are small pieces of code that server side connections use to store and retrieve information on the client side of the connection [5, 6]. Cookies were created to extend the capabilities of web-based client/server applications. The problem with them is that they work in the background, without the user's knowledge or consent, gathering and broadcasting personal information such as sites visited, pages accessed, username and password combinations for secured sites, etc.

To further affect the lack of privacy perception, many sites ask for users to provide detailed personal information that the user does not consider pertinent to the web merchant. Users also know that this information is frequently sold or made available online to other businesses. For this reason, many users have adopted aliases and nicknames in an effort to protect their private lives from possible misuse or abuse of this information.

Internet users fear that they may be exposing themselves by providing sensitive information to unscrupulous individuals. Criminals may obtain physical addresses by pretending to represent honest e-commerce sites. This information could later be used to commit crimes against their unsuspecting victims.

To summarize, customers lack the ability to assess the qualities of e-commerce sites as they use to evaluate brick and mortar merchants. Security cues available in the real world to assess vendor reliability, honesty and trust are not available to the virtual commerce customer.

V- ENCRYPTION: THE SECURE ALTERNATIVE

Encryption is the art and science of protecting data transmitted through an open, insecure medium. It is as old as the written word. Roman generals used encryption mechanisms to prevent sharing important messages with the enemy in the event the messenger carrying it was intercepted. Modern encryption uses algorithms to change the original message (plain text) into a form that hides its contents to the open world (cipher text). The ciphering and deciphering processes are accomplished by using a key.

There are two types of key-based algorithms: symmetric (private key) and asymmetric (public key). Figures 2 and 3 illustrate both concepts.

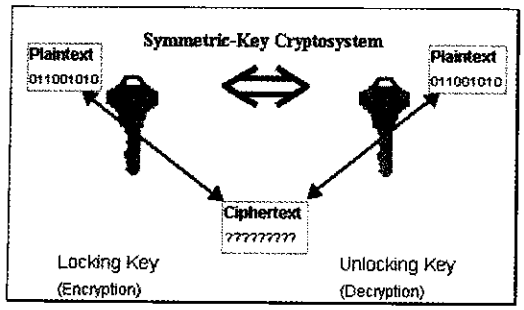


Figure 2: *Symmetric key encryption*

On the first one, both the encryption and decryption processes use the same key.

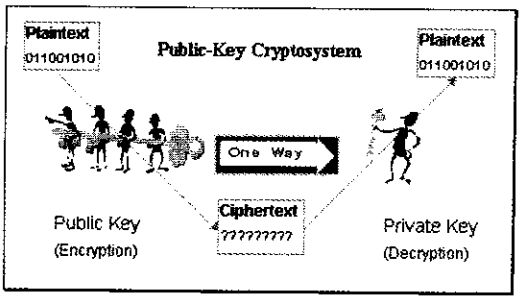


Figure 3: *Asymmetric key encryption*

On the second, the encryption process uses one (public) key and the decryption process uses a private (secret) key.

In practice, both systems are used together to improve security of transmitted data [7]. Well known encryption algorithms publicly available are:

DES – Data Encryption Standard (symmetric)
RSA – Rivest-Sharmir-Adelman (asymmetric)
SET – Secure Electronic Transaction; a standard to process secure credit card transactions online
SSL – Secure Sockets Layer; a Netscape developed standard to process secure transactions

These methods are as strong as the length of the keys used for their encryption. Any home computer is capable of breaking a 32-bit length code by trying each of the 2^{32} possible keys in sequence. As the number of bits in the key increases, the computational power required to break the code by testing all possible values increases exponentially. DES, for example, uses 56-bit keys [9]. Military security relies on 1024 and 2048-bit encryption keys.

VI- CONCLUSION

E-commerce customers must learn to identify secure sites and the use of encryption while processing transactions. Secure connections are identified by the closed padlock at the bottom of the browser page and the use of S-HTTP (secure hypertext transfer protocol) in the URL line.

The perception that the Internet is an insecure system must be dispelled through an education campaign to users and prospective customers.

Merchants must increase user awareness on the amount of security features in their sites. With increased confidence, they can invite users to complete the research, order and payment cycle online by providing incentives or discounts. Finally, the process must be easy to follow and should end by reassuring the client that the order was processed as specified, including delivery information. Users must develop a new set of rules to evaluate the dependability of e-commerce sites. These will become the standard for client/merchant relationships until paradigms shift again.

VII- REFERENCES

[1] P. Buckley, "The Emerging Digital Economy II", U.S. Department of Commerce, 1999.

[2] J. Berst, "The Big e-commerce bang", ZDNetAnchorDesk, www.anchordesk.com, September 1999.

[3] M. Kane, "E-commerce: It's still anybody's game", www.zdnet.com/zdnn/stories/news/0,4586,2281787,00.html, June 24, 1999.

[4] M. Kleeman, et al, "eTrust Internet Privacy Study", The Boston Consulting Group, March, 1997.

[5] M. Slayton, "An Introduction to Cookies", www.hotwired.com, 1996.

[6] V. Meyer-Schonberger, "The Internet and Privacy Legislation: Cookies for a treat?", www.wvjolt.wvu.edu/wvjolt/current/issue1/article/mayer/mayer.htm, 1998.

[7] ECC white paper, "An Introduction to Information Security", www.certicom.com/ecc/wecc1.htm, March 1997.

[8] SSH white paper, "Cryptography A-Z – Introduction to Cryptography", www.ssh.fi/tech/crypto/intro.html, 1998.