The application of E-commerce in Business Application: Their Problems and Prospects

Partha Sarathi Bhattacharjee
Research Scholar, Dept. of Comp. Sc. .
Assam University, Silchar,
Assam, India - 788011

Anish Kumar Saha
Asstt. Professor, CSE Dept
NIT, Agartala
Agartala , Tripura(W)

Shahin Ara Begum
Phd,Reader , Dept. of Comp.Sc
Assam University, Silchar
Assam , India - 788011

ABSTRACT

The paper outlines the reality of global e-commerce, pointing out inherent risk areas that could threaten the system. This paper investigates the relationship between globalization, ecommerce adoption or acceptance that lead to business performance and effectiveness. In this paper, we will discuss how globalization impact on e-commerce in business with policy implementation, pro and cons of e-commerce enhancement in the increase to business. It will outline the framework of the new policies and regulations needed by e-commerce. There will be future research and conclusion based on what we believe globalization of e-commerce will lead to growth in business.

The World Wide Web has become an environment for distributed applications of all kinds. The originally intended use of the Web as distributed system for knowledge-interchange seems to disappear, compared to the increasing number of Electronic Commerce Web applications. Organizations offer products and services in the Web, and use the Web as a means to integrate their heterogeneous business application systems. Offering Web-based products requires combining services of different application systems, which were build on the coarse-grained Web implementation model. Reusing the respective fine-grained services and application systems respectively integrating these cross-platform application systems increases quality and reduces costs of the new product. The Web as a global point of sale seems to be very promising but obviously suffers from its heritage - the coarse-grained implementation model.

E-Commerce, an electronic medium that generates revenue on demand, can be demanding in maintaining security administration and management. Ensuring a desktop PC, or a server on the LAN can provide moderate challenges in securing the device, securing a device in an E-Commerce environment can prove most challenging. Whether Consumer or Business, E-Commerce provides extraordinary challenges in that our organization uses this revenue generating medium to provide a service which is highly accessible publicly and privately and usually requires undesirable communication to be opened to these devices. The criticality of E-Data poses additional security measures, sensitive data pertaining to customers and business partners traversing private to public networks requires proactive measures to insure a secure environment.

In the problem area, we will describe some attacks in business applications by unauthorized access of business software and their related protocols and in the prospect area, we will conclude some detection methods for the attacks and their prospective prevention methods.

Keywords

Globalization, E-commerce, network attacks, IDS

1. INTRODUCTION

Globalization refers mainly to the expansion of trade, investment, and other business interactions among the countries of the world. It also refers to the growing standardization of culture around the world. The process of globalization has been an integral part of the recent economic progress made by India. Globalization has played a major role in export-led growth, leading to the enlargement of the job market in India. One of the major forces of globalization in India has been in the growth of outsourced IT and business process outsourcing (BPO) services. The last few years have seen an increase in the number of skilled professionals in India employed by both local and foreign companies to service customers in the US and Europe in particular. Taking advantage of India's lower cost but educated and English-speaking work force, and utilizing global communications technologies such as voice-over IP (VOIP), email and the internet, international enterprises have been able to lower their cost base by establishing outsourced knowledge-worker operations in India. As a new Indian middle class has developed around the wealth that the IT and BPO industries have brought to the country, a new consumer base has developed. International companies are also expanding their operations in India to service this massive growth opportunity.

2. LITERATURE SURVEY

In the ensuing decade the use of the World-Wide Web has moved far beyond of its originally anticipated scope and changed from a distributed system for knowledge interchange towards a new application environment [9]. This yields to a dramatic and rapid growth of the Web, more recently triggered by organizations offering Web-based products and services and thus asking for e-commerce applications. A more general definition defines e-commerce as "any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact". The scope of e-commerce reaches from simple Web presence to shared business processes connecting different organizations. E-commerce can be divided into four categories: business to business e-commerce, business to consumer ecommerce, business to administration e-commerce, and consumer to administration ecommerce. From these categories, business to business e-commerce, which covers all transactions between companies, has been well established. Business to administration e-commerce and consumer to administration e-commerce have not yet emerged broadly. The Business to consumer e-commerce expands with benefit from the distribution of Web browsers for universal, cross-platform access and offers opportunities for new products, e. g. the integration of a rapidly increasing number of Web-based services provided by different business units to a single point of access [6]. This often requires that services of different business application systems, e. g. systems for order management, inventory management, or procurement, are combined to a new product, which hides the respective services and application systems from the customer. This may be achieved by introducing integration layers, thus integrating the respective application systems.

The importance of electronic information systems is obvious to all participants in the modern economy [2]. When information fails to circulate, whole sectors of the economy are vulnerable. Finance, wholesale and retail trade, transportation, much of manufacturing, and many service industries would slow to a crawl without computers. Vital public services – utilities, national defense, and medicine – are equally dependent. Information security – the safeguarding of computer systems and the integrity, confidentiality, and availability of the data they contain – has long been recognized as a critical national policy issue. Two current trends indicate that its importance is growing. First, the integration of computers into more and more aspects of modern life continues. Second, cyber-attacks, or breaches of information security, appear to be increasing in frequency, and few observers are willing to ignore the possibility that future attacks could have much more severe consequences than what has been observed to date.

The core issue, in both public and private sectors, is whether we are devoting enough resources to information security. Part of the answer must come from economic analysis. What are the costs, both historical and potential, of security breaches? How frequently can attacks be expected? Can these factors be quantified precisely, so that business firms and other organizations can determine the optimal amount to spend on information security and measure the effectiveness of that spending?

3. SECURITY OVERVIEW

In the software industry, security has two different perspectives. In the software development community, it describes the security features of a system. Common security features are ensuring passwords that are at least six characters long and encryption of sensitive data. For software consumers, it is protection against attacks rather than specific features of the system. Security is not a number of features, but a system process. The weakest link in the chain determines the security of the system. In this paper, we focus on possible attack scenarios in an e-Commerce system and provide preventive strategies, including security features that we can implement. In a typical e-Commerce experience, a shopper proceeds to a Web site to browse a catalog and make a purchase. This simple activity illustrates the four major players in e-Commerce security. One player is the shopper who uses his browser to locate the site. The site is usually operated by a merchant, also a player, whose business is to sell merchandise to make a profit. As the merchant business is selling goods and services, not building software, he usually purchases most of the software to run his site from third-party software vendors. The software vendor is the last of the three legitimate players. The attacker is the player whose goal is to exploit the other three players for illegitimate gains. The attacker can besiege the players and their resources with various damaging or benign schemes that result in system exploitation. Threats and vulnerabilities are classified under confidentiality, integrity, and availability. A threat is a possible attack against a system. It does not necessarily mean that the system is vulnerable to the attack.

4. THE CRIMINAL INCENTIVE

Attacks against e-Commerce Web sites are so alarming that they follow right after violent crimes in the news. Practically in every month, there is an announcement of an attack on a major Web site where sensitive information is obtained. Why is e-Commerce vulnerable? Is e-Commerce software more insecure compared to other software? Did the number of criminals in the world increase? The developers producing e-Commerce software are pulled from the same pool of developers as those who work on other software. In fact, this relatively new field is an attraction for top talent. Therefore, the quality of software being produced is relatively the same compared to other products. The criminal population did not undergo a sudden explosion, but the incentives of an e-Commerce exploit are a bargain compared to other illegal opportunities. Compared to robbing a bank, the tools necessary to perform an attack on the Internet is fairly cheap. The criminal only needs access to a computer and an Internet connection. On the other hand, a bank robbery may require firearms, a getaway car, and tools to crack a safe, but these may still not be enough. Hence, the low cost of entry to an e-Commerce site attracts the broader criminal population. The payoff of a successful attack is unimaginable. If we were to take a penny from every account at any one of the major banks, it easily amounts to several million dollars. The local bank robber optimistically expects a windfall in the tens of thousands of dollars. Bank branches do not keep a lot of cash on hand. The majority is represented in bits and bytes sitting on a hard disk or zipping through a network. While the local bank robber is restricted to the several branches in his region, his online counterpart can choose from the thousands of banks with an online operation. The online bank robber can rob a bank in another country, taking advantage of non-existent extradition rules between the country where the attack originated, and the country where the attack is destined. An attack on a bank branch requires careful planning and precautions to ensure that the criminal does not leave a trail. He ensures the getaway car is not easily identifiable after the robbery. He cannot leave fingerprints or have his face captured on the surveillance cameras. If he performs his actions on the Internet, he can easily make himself anonymous and the source of the attack untraceable. The local bank robber obtains detailed building maps and city maps of his target. His online counterpart easily and freely finds information on hacking and cracking. He uses different sets of tools and techniques everyday to target an online bank.

An e-Commerce system with several points that the attacker can target:

- Shopper
- Shopper' computer
- Network connection between shopper and Web site's server
- Web site's server
- Software vendor

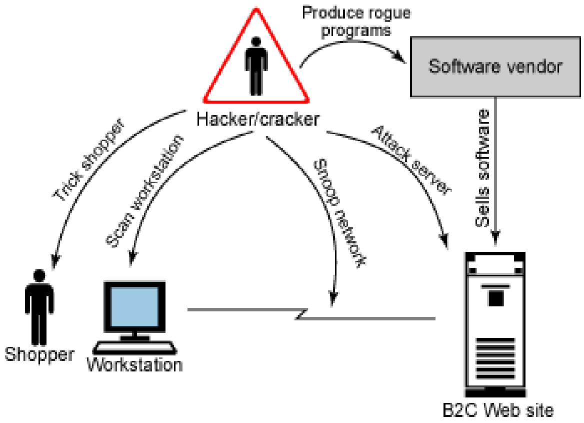

Fig 1: The Points, attacker can target
Source : Microsoft Technet Library

5. TYPES OF ATTACKS

Various types of attacks were identified during business applications and a variety of such methods have been described in the literature in recent years [5,7,10,11].

5.1 Tricking The Shopper

Some of the easiest and most profitable attacks are based on tricking the shopper, also known as social engineering techniques. These attacks involve surveillance of the shopper's behavior, gathering information to use against the shopper. For example, a mother's maiden name is a common challenge question used by numerous sites. If one of these sites is tricked into giving away a password once the challenge question is provided, then not only has this site been compromised, but it is also likely that the shopper used the same logon ID and password on other sites. A common scenario is that the attacker calls the shopper, pretending to be a representative from a site visited, and extracts information. The attacker then calls a customer service representative at the site, posing as the shopper and providing personal information. The attacker then asks for the password to be reset to a specific value. Another common form of social engineering attacks are phishing schemes. Typo pirates play on the names of famous sites to collect authentication and registration information. For example, http://www.ibm.com/shop is registered by the attacker as www.ibn.com/shop. A shopper mistypes and enters the illegitimate site and provides confidential information. Alternatively, the attacker sends emails spoofed to look like they came from legitimate sites. The link inside the email maps to a rogue site that collects the information.

5.2 Snooping the Shopper's Computer

Millions of computers are added to the Internet every month. Most users' knowledge of security vulnerabilities of their systems is vague at best. Additionally, software and hardware vendors, in their quest to ensure that their products are easy to install, will ship products with security features disabled. In most cases, enabling security features requires a non-technical user to read manuals written for the technologist. The confused user does not attempt to enable the security features. This creates a treasure trove for attackers. A popular technique for gaining entry into the shopper's system is to use a tool, such as SATAN, to perform port scans on a computer that detect entry points into the machine. Based on the opened ports found, the attacker can use various techniques to gain entry into the user's system. Upon entry, they scan file system for personal information, such as passwords. While software and hardware security solutions available protect the public's systems, they are not silver bullets. A user that purchases firewall software to protect his computer may find there are conflicts with other software on his system. To resolve the conflict, the user disables enough capabilities to render the firewall software useless.

5.3 Sniffing the Network

In this scheme, the attacker monitors the data between the shopper's computer and the server. He collects data about the shopper or steals personal information, such as credit card numbers. There are points in the network where this attack is more practical than others. If the attacker sits in the middle of the network, then within the scope of the Internet, this attack becomes impractical. A request from the client to the server computer is broken up into small pieces known as packets as it leaves the client's computer and is reconstructed at the server. The packets of a request are sent through different routes. The attacker cannot access all the packets of a request and cannot decipher what message was sent.

5.4 Guessing Passwords

Another common attack is to guess a user's password. This style of attack is manual or automated. Manual attacks are laborious, and only successful if the attacker knows something about the shopper.

5.5 Using Denial of Service Attacks

The denial of service attack is one of the best examples of impacting site availability. It involves getting the server to perform a large number of mundane tasks, exceeding the capacity of the server to cope with any other task. For example, if everyone in a large meeting asks us our name all at once, and every time we answer, they ask us again. We have experienced a personal denial of service attack. To ask a computer its name, we use ping. We can use ping to build an effective DoS attack. The smart hacker gets the server to use more computational resources in processing the request than the adversary does in generating the request. In Distributed DoS attack, the hacker infects computers on the Internet via a virus or other means. The infected computer becomes slaves to the hacker. The hacker controls them at a predetermined time to bombard the target server with useless, but intensive resource consuming requests. This attack not only causes the target site to experience problems, but also the entire Internet as the number of packets is routed via many different paths to the target.

5.6 Using Known Server Bugs

The attacker analyzes the site to find what types of software are used on the site. He then proceeds to find what patches were issued for the software. Additionally, he searches on how to exploit a system without the patch. He proceeds to try each of the exploits. The sophisticated attacker finds a weakness in a similar type of software, and tries to use that to exploit the system. This is a simple, but effective attack. With millions of servers online, what is the probability that a system administrator forgot to apply a patch?

5.7 Using Server Root Exploits

Root exploits refer to techniques that gain super user access to the server. This is the most coveted type of exploit because the possibilities are limitless. When we attack a shopper or his computer, we can only affect one individual. With a root exploit, we gain control of the merchants and all the shoppers' information on the site. There are two main types of root exploits: buffer overflow attacks and executing scripts against a server.

In a buffer overflow attack, the hacker takes advantage of specific type of computer program bug that involves the allocation of storage during program execution. The technique involves tricking the server into execute code written by the attacker.

Of the roughly 1.8 million connections containing attacks in the DARPA dataset, 1.7 million of those are from the denial of service attacks, which is to be expected given the nature of such attacks. A visual examination of the ROC curve (line with "star" points in figure 2) shows three distinct segments: those rules which have an excellent detection rate with barely any false positives resulting the initial spike, followed by a slow climb for the large number of rules that provided some detections with many false positives, and finally our extrapolation from the last rule to (1,1) [12].

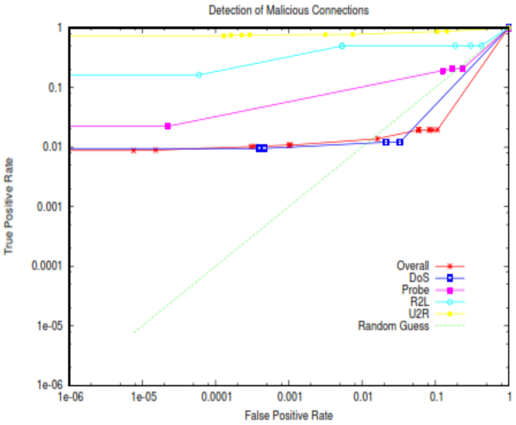

Fig 2: Receiver Operating Characteristic Curves in log, log scale. Y-axis is percentage of malicious connections detected. X-axis is percentage of alerts produced not corresponding to an attack.

6. PROTECTION MECHANISMS AGAINST ATTACKS

Despite the existence of hackers and crackers, e-Commerce remains a safe and secure activity. The resources available to large companies involved in e-Commerce are enormous. These companies will pursue every legal route to protect their customers. Figure 3 shows a high-level illustration of defenses available against attacks

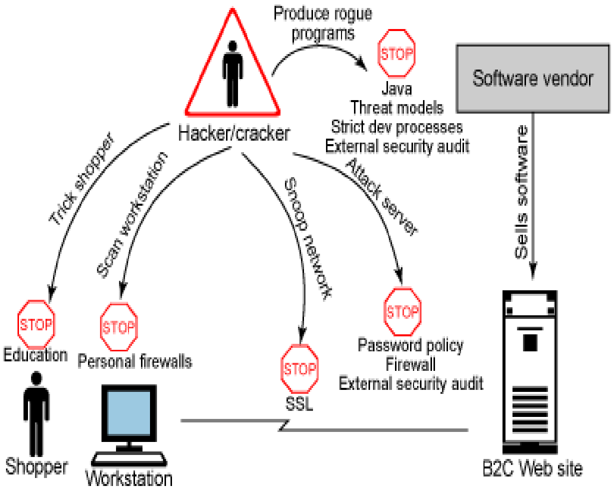

Fig 3: Attacks and their defenses
Source: Microsoft Technet Library

At the end of the day, our system is only as secure as the people who use it. Education is the best way to ensure that our customers take appropriate precautions:

- Install personal firewalls for the client machines.
- Store confidential information in encrypted form.
- Encrypt the stream using the Secure Socket Layer (SSL) protocol to protect information flowing between the client and the e-Commerce Web site.
- Use appropriate password policies, firewalls, and routine external security audits.
- Use threat model analysis, strict development policies, and external security audits to protect ISV software running the Web site.

7. CONCLUSION

Firewalls don't prevent attacks; they simply reduce the likelihood of a break-in. When we deploy a firewall, we'll still get just as many attacks as we always did—we just won't have to worry about them as much. All firewalls provide some capability for logging these attacks for later, manual review. This allows administrators to watch for attacks that are out-of-the-ordinary. It's also useful for forensics purposes. If an attacker does manage to defeat our firewall, we can refer to the firewall's log and gather information to determine how the attacker carried out the attack.

Intrusion detection is an advanced firewall feature, and many firewalls (such as ICF) lack this feature. Intrusion detection systems (IDSs) can identify attack signatures or patterns, generate alarms to alert the operations staff, and cause the routers to terminate the connection with the hostile sources. These systems can also prevent DoS attacks. A DoS attack occurs when a user sends fragments of TCP requests, masked as legitimate TCP requests, or sends requests from a bad IP source. The server can't handle so many requests and displays a DoS message to legitimate site users. IDSs provide real-time monitoring of network traffic and implement the "prevent, detect, and react" approach to security.

Although IDSs are necessary to meet security requirements for many businesses and some home users, their use has downsides that we should take into account:

- IDSs are processing-intensive and can affect the performance of our site.
- IDSs are expensive.
- IDSs can sometimes mistake normal network traffic for a hostile attack and cause unnecessary alarms. These unnecessary alarms can be so frequent that they cause operational staff to ignore genuine alarms.

There are a number of third-party tools available for intrusion detection. For example, we can use Cisco's Intrusion Detection System (IDS) or ISS's Real Secure for real-time network traffic monitoring. IDSs are still in the process of being enhanced and developed and as the attack is uncertain, so the IDS is also not fixed and it is being changed according to the change of method of attacks.

8. REFERENCES

[1] Bamogo, D. et.al, (1996), "The Impact of new Communication and Information Technologies in Developing Countries: A Case study of Burkina Faso", international workshop on Information Technology for Development UNU/INTECH, Maastricht, The Netherlands

[2] Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel (2004) ,"CRS Report for Congress-The Economic Impact of Cyber-Attacks"

[3] Eddie Powell, (2000), "Network Intrusion Detection for the E-Commerce Environment"

[4] ECOM (ed), (1998), "Electronic Commerce – An Introduction, http://ecom.fov.uni-mb.si/center/"

[5] Freeman, C. (1994a) "The Diffusion of Information and Communication Technology in the World"

[6] H.W. Gellersen and M. Gaedke ,(1999), "Object-Oriented Web Application Development", IEEE Internet Computing 1, pp. 60-68

[7] Howell D.,(2002) "hackers often choose their corporate targets", Investors Business Daily

[8] M. Gaedke, H.-W. Gellersen, A. Schmidt, U. Stegemüller and W. Kurr,(1999), "Object-oriented Web Engineering for Large-scale Web Service Management", 32nd Annual Hawaii International Conference On System Sciences (HICSS-32).

[9] M. Gaedke and K. Turowski, (2000), "Integrating Web-based E-Commerce Applications with Business Application Systems", Netnomics Journal 2, pp. 117-138

[10] Mann D. E. and Christey S. M.,(1999), "Towards a Common Enumeration of Vulnerabilities", 2nd Workshop on Research with Security Vulnerability Databases, Purdue University, West Lafayette, Indiana

[11] Ptacek T.H. and Newsham T.N.,(1998) "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection"

[12] S Terry Brugger and Jedadiah Chow,(2005) "An Assessment of the DARPA IDS Evaluation Dataset Using Snort"