https://doi.org/10.48009/2_iis_2009_88-94

A SECURITY VULNERABILITY AUDIT OF *FORTUNE 500* E-COMMERCE NETWORK SYSTEMS

Dr. Jensen J. Zhao, Ball State University, jzhao@bsu.edu
Dr. Allen D. Truell, Ball State University, atruell@bsu.edu
Dr. Melody W. Alexander, Ball State University, malexand@bsu.edu

ABSTRACT

This study examined the security vulnerability of the Fortune500 corporations' retail e-commerce network systems. The findings indicate that most e-commerce portals had their network information, such as network's IP address, physical address, and network range, publicly available on the Internet through the Google search. However, these e-commerce portals had their most ports closed, filtered, or behind firewalls with very few open ports. The Fortune 500 commercial banks' portals were most secure as none of their operating systems information was detectable. To further reduce the security vulnerability of the e-commerce network systems, this paper provided recommendations such as how to secure network information, how to hide portal's IP address, and how to secure operating systems.

Keywords: E-commerce, network systems, IP address, NAT, PAT, Port 80/tcp, Port 443/tcp, security, vulnerability, cyber intrusion, and hacker attack

INTRODUCTION

According to the U.S. Census Bureau's May 2008 E-Stats report [9], e-commerce activities in the U.S. have grown faster than total economic activities in all of the four major economic sectors of manufacturing industries, merchant wholesalers, retailers, and service industries. For instance, the U.S. Census Bureau announced that the estimate of U.S. retail (or B2C) e-commerce sales for the second quarter of 2008, adjusted for seasonal variation but not for price changes, was $34.6 billion, an increase of 2.9% from the first quarter of 2008. Compared with the second quarter of 2007, the second quarter 2008 retail e-commerce estimate increased 9.5%, while total retail sales increased 2.5% in the same period [10].

However, the increase of e-commerce activities has been accompanied by a similar rise in the number and type of cyber attacks against the security of e-commerce systems. Such attacks have impaired or even shut down e-commerce businesses by damages such as Web site defacement, denial of service, price manipulation, financial fraud, or systems and data breach [e.g., 3, 4, 5, 6].

For example, beginning in July 2005, the TJX Companies, Inc. experienced a massive intrusion into its computer network systems, resulting in the largest systems and data security breach in history. As a January 2007 report of *Computer World* revealed, at the time TJX disclosed the scope of its systems and data security breach, more than three dozen banks in Massachusetts alone reported that credit cards they issued have been compromised [11]. According to documents filed with the federal court in Boston, October 2007, this TJX systems and data security breach affected millions of consumers' private information, including about 29 million MasterCard victims and 65 Million Visa victims [7].

In addition, a 2006 survey of 214 bank Web sites [5] reported that 75% of the sites were vulnerable to hacking, with two big worrisome trends: (a) login boxes were placed on unencrypted Web (http) pages of a bank's Web site and (b) the use of third-party services transferred customers to insecure outside, third-party pages.

As Symantec's *July-December 2007 Internet Security Threat Report* [8] summarized, while Internet security administrators and end users adapted new measures to resolve security threats, attackers created new and innovative ways to attain their objectives. As a result, the threat landscape was constantly shifting. Based on the data collected over the last six months of 2007, Symantec observed that the security threat landscape was predominantly characterized by the following: (a) malicious activity becoming Web-based, (b) attackers targeting end users instead of computers, (c) underground economy being

consolidated and maturing, and (d) attackers adapting attack activities rapidly. Especially, Symantec observed that "the majority of effective malicious activities become Web-based: the Web is now the primary conduit for attack activity." (p. 2)

Since the Web is now the primary conduit for attack activity, it appears necessary to assess how secure the e-commerce Web portals are to block cyber intrusions and terrorist attacks. The problem addressed in this study was to assess the vulnerability status of the *Fortune 500* largest U.S. corporations' B2C e-commerce portals. To conduct the study, we raised the following three research questions:

1. What network information of the *Fortune 500* e-commerce portals is publicly available on the Internet?
2. How vulnerable are network systems of the *Fortune 500* e-commerce portals to cyber intrusions and attacks?
3. Are there any significant differences among industry groups of the *Fortune 500* e-commerce portals?

The primary purpose of the study was to provide the participating companies with the findings that they need to improve the security of their portals. Second, the findings would also enable students specialized in Internet security to identify opportunities for internships or jobs at the *Fortune 500* e-commerce portals that need to strengthen their Internet security.

METHODOLOGY

The population of this study consisted of the B2C e-commerce Web portals of the *Fortune 500* largest U.S. corporations. A thorough search of the *Fortune 500* corporate Web sites [2] identified 116 B2C e-commerce portals. These 116 portals were all used in the study according to the sample-size requirement [1]. Table 1 shows the demographic profile of these 116 portals.

Table 1
Demographic Profile of *Fortune 500* E-Commerce Portals (N=116)

Group	Type of Company Business	No. of Companies	Percentage
Group 1.	Airlines and Hospitality Services	13	11%
Group 2.	Apparel and Shoes	17	15%
Group 3.	Commercial Banks	12	10%
Group 4.	Computer/Telecommunication/Electronic Tools	29	25%
Group 5.	Food/Beverage/Drug/Personal Products	23	20%
Group 6.	General Merchandisers/Specialty Retailers	22	19%
	Total	116	100%

To find out what e-commerce network information of the *Fortune 500* corporations is publicly available on the Internet and how vulnerable their e-commerce portals are to cyber intrusion and attacks, we conducted Google search for related Web sites and auditing tools. We found three Web sites, *ZoneEdit.com*, *arin.net*, and *insecure.org*, offering the tools.

The *ZoneEdit.com* site is a leading Web site in DNS (Domain Name System) and domain management solutions. It provides a free DNS lookup utility tool, which enables any online user to enter a Web site domain name (e.g., yahoo.com) for searching its IP (Internet Protocol, e.g., 216.115.108.245) address (see at http://www.zoneedit.com/lookup.html).

The *arin.net* (American Registry of Internet Numbers) site provides a free database search service at *ws.arin.net*. The search service allows any online user to find a Web portal's registration information for resources registered with ARIN. The ARIN database contains IP addresses, autonomous system numbers, network name, type, and range, organizations or customers that are associated with these resources, and related points of contact. By entering a portal's IP address into the search tool, any person can get all the registered information of the

portal's network systems (see at http://www.arin.net/whois/).

The *insecure.org* site offers a free network mapping utility tool, *Nmap*, for network exploration and security auditing. *Nmap* uses raw IP packets to determine what hosts or ports are available on the network, what ports are open, filtered, or closed, what services (application name and version) those hosts are offering, what operating systems (OS) and OS versions they are running, what type of packet filters/firewalls are in use, and many other characteristics (see at http://insecure.org/).

Two research assistants were trained to use these three tools to measure the network vulnerability of each of the 116 corporate B2C e-commerce portals. All the searches and audits of the 116 portals were conducted in the fall of 2008. The results were saved in digital format, and data were recorded and coded. Frequency counts, percentage distributions, and cross-tabulations were prepared for data analysis. Pearson chi-square test was used to determine any significant differences at the .01 alpha level among industry groups in securing network systems.

RESULTS

Research Question 1 asked, "What network information of the *Fortune 500* e-commerce portals is publicly available on the Internet?" The Internet search at *ZoneEdit.com* and *ws.arin.net* identified the IP addresses and network information of the majority of the 116 *Fortune 500* corporate e-commerce portals. As Table 2 shows, 97% of e-commerce portals' IP addresses were publicly available on the Internet. As a consequence, with these publicly available IP addresses, any online users could go to *ws.arin.net* and enter the IP addresses for identifying a large amount of network information from a majority (74% - 97%) of the e-commerce portals, such as a portal's physical address; network range, name, handle, type, CIDR (classless inter-domain routing), and parent; organization name and ID; network registration date; servers' name; and registered tech handle, name, phone, and email (see Table 2).

Research Question 2 asked, "How vulnerable are network systems of the *Fortune 500* e-commerce portals to cyber intrusions and attacks?" Network systems connect to the Internet through computer ports. The ports of an Internet-connected computer are classified into the well-known ports, the registered ports, and the dynamic and/or private ports. The numbers of the well-known ports range from 0 to 1,023; those of the registered ports are from 1,024 through 49,151; and those of the dynamic or private ports range from 49,152 to 65,535. If the ports are open on the Internet without firewalls or filters, they are very vulnerable to cyber intrusions and attacks.

Table 2

Network Information Availability of Fortune 500 E-Commerce Sites (N=116)

Category	Frequency	Percentage
• IP address	113	97%
• Address (City, State/Province, Country)	113	97%
• Network Range	113	97%
• Network Name	113	97%
• Network Handle	113	97%
• Network Type	113	97%
• CIDR (Classless Inter-domain Routing)	113	97%
• Parent	108	93%
• Organization Name	103	89%
• Organization ID	103	89%
• Network Registration Date	102	88%
• Name of Server 1	88	76%
• Name of Server 2	88	76%
• Registered Tech Handle, Name, Phone, Email	86	74%

Among the 116 e-commerce portals scanned by using *Nmap*, 112 portals (97%) were detected of running 1,705 Internet ports. Only four portals (3%) were running a relatively smaller number of 1,680 ports. However, most of these detected ports were closed, filtered, or behind firewalls and only very few ports were detected as open. As Chart 1 shows, the majority of portals had only four or fewer open ports on the Internet, with 21 portals (18%) having only one open port, followed by 64 portals (55%) having two open ports and 15 portals (13%) having three open ports. By contrast, a tinny minority had 10 or more open ports on the Internet, with only one portal having 25 open ports.

Table 3 presents the network vulnerability information detected from the open ports of the e-commerce portals. The majority (97%) of the 116 portals had Port 80/tcp open for http (hypertext transfer protocol) or World Wide Web services. Web servers identified from Port 80/tcp were Apache, Microsoft IIS, and Netscape. Second, 79% of the portals also had Port 443/tcp open for encrypted https services such as personal and institutional Web accounts for business data transactions. Finally, nearly one-third of the e-commerce portals had their computer operating systems (OS) detected by the network scanner, Nmap, which revealed such OS information as running Windows NT/2K/XP/2003 Server, Sun Solaris 8, Linux 2.6x, and IBM AIX 4.x (see Table 3).

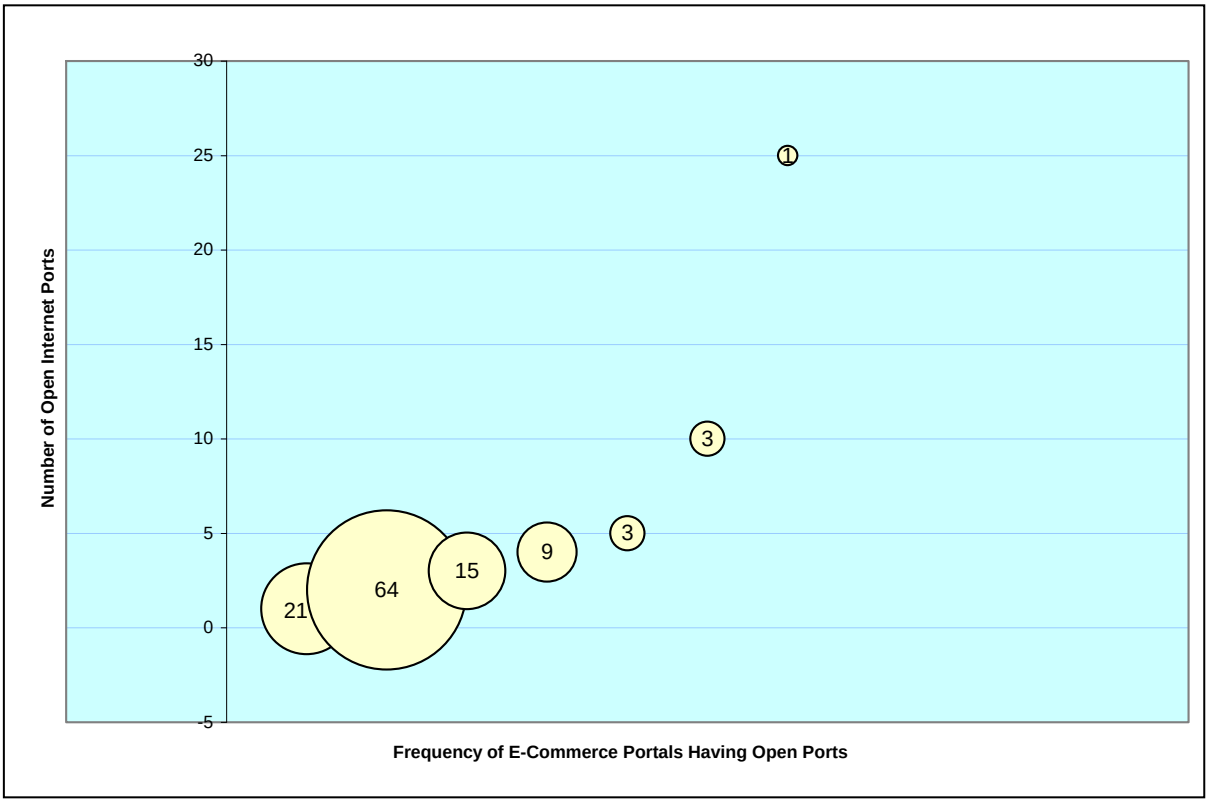

Chart 1. Number of Internet Ports Open at Fortune 500 E-Commerce Portals

Table 3

Network Vulnerability Status of *Fortune 500* E-Commerce Portals (N=116)

	Frequency	%

Category		
• Port 80/tcp open; service: http; common servers: Apache, IIS, Netscape	113	97%
• Port 443/tcp open; service: https; common servers: Apache, IIS, Netscape	92	79%
• OS information: e.g., Running: Windows NT/2K/XP, Sun Solaris 8, Linux 2.6x, IBM AIX 4.x	37	32%
• OS details: e.g., Windows IE7/XP/2003 Server, Sun Solaris 8, Linux 2.6.8 - 2.6.9, IBM AIX 4.3.2.0-4.3.3.0 on an IBM RS/*	31	27%

Research Question 3 asked, "Are there any significant differences among industry groups of the *Fortune 500* e-commerce portals?" Pearson chi-square test was used to determine whether any significant differences exist among the six industry groups on network information availability and vulnerability. To conserve space, Table 4 illustrates only the areas where significant differences existed among the industry groups. Regarding the portals' network operating systems (OS) information, significantly more portals in Group 1 (Airlines and Hospitality Services, 46%) and Group 2 (Apparel and Shoes, 53%) leaked their OS information in comparison with 32% of the *Fortune 500* 116 e-commerce portals. By contrast, no portal of Group 3 (Commercial Banks, 0%) was detected of any OS information while significantly fewer portals of Group 6 (General Merchandisers/Specialty Retailers, 9%) were detected of OS information. In addition, significantly more portals of Group 2 were also detected of their OS details, whereas no portal of Group 3 leaked any OS details and only 9% of Group 6 leaked their OS details (see Table 4).

Table 4

Significant Differences Among Industry Groups

Category	% of Fortune 500	vs	Industry Group	%	
OS information: e.g., Running: Windows NT/2K/XP, Sun Solaris 8, Linux 2.6x, IBM AIX 4.X	32%	vs	Group 2	53%	*
		vs	Group 1	46%	*
		vs	Group 6	9%	*
		vs	Group 3	0%	*
OS details: e.g., Windows IE7/XP/2003 Server, Sun Solaris 8, Linux 2.6.8 - 2.6.9, IBM AIX 4.3.2.0-4.3.3.0 on an IBM RS/*	27%	vs	Group 2	41%	*
		vs	Group 6	9%	*
		vs	Group 3	0%	*

* Significant at .01 level.

SUMMARY AND DISCUSSION

The findings of the study indicated that the majority of 116 Fortune 500 e-commerce portals' network information is publicly available on the Internet through the Google search. Such information includes networks' IP address and physical address; network range, name, handle, type, CIDR, and parent; organization name and ID; network registration date; servers' name; and registered tech handle, name, phone, and email address. The publicly available information of these e-commerce portals makes the portals vulnerable to cyber intrusions and hacker attacks. For example, searching for the IP address of a Web portal through its Web address (URL) is often the first step for cyber intruders to connect to the server of the portal. In addition, the network range and CIDR address reveal the total number of hosts the network posses and the network's higher-level and lower-level routing information. Having put these pieces of information together, a cyber intruder has a full picture of which parts of the network are vulnerable and easy to intrude.

However, the findings of the network vulnerability audit illustrated that the e-commerce portals had their most ports closed, filtered, or behind firewalls; only very few ports were detected as open. The majority (97%) of the portals had their Port 80/tcp open for http services and 79% of them also had Port 443/tcp open for encrypted https services. Although it is common to have Port 80/tcp and Port 443/tcp open for their respective services, such open status is vulnerable to cyber intrusions and attacks because open ports might leak networks server information and operating systems (OS) information. For instance, nearly one third of the e-commerce portals had their computer OS detected by the network scanner, which revealed such OS information as running Windows NT/2K/XP/2003 Server, Sun Solaris 8, Linux 2.6x, and IBM AIX 4.x. With such available information of open ports, network OS, and Web servers, hackers would be able to penetrate into the network to cause damages.

Moreover, the industry group comparison identified that the *Fortune 500* commercial banks' portals were most secure as none of their OS information could be detected. Following the commercial banks group was the group of general merchandisers and specialty retailers, of which only 9% leaked their OS information. However, the apparel and shoes companies need to further secure their portals and prevent their OS information from been detected by outside network scanners. Obviously, the finding of the commercial banks in this study did not support the 2006 survey results [5] that 75% of bank Web sites were vulnerable to hacking. This could mean that banks had made continuous improvement on the security of their Web sites.

CONCLUSIONS AND RECOMMENDATIONS

Based on the findings of the study, we conclude that the *Fortune 500* e-commerce portals were secured by keeping most of their ports closed, filtered, or behind firewalls. But this degree of security is not enough because the publicly available network information of their portals would attract cyber intruders and their few open ports still remain vulnerable to cyber intrusions and attacks.

To further strengthen the portals, we have the following recommendations for the *Fortune 500* e-commerce administrators and developers.

First, consider negotiating with American Registry of Internet Numbers on requiring username and password login for user identity management and access to a Web portal's registration information that contains sensitive data such as network's IP addresses and physical address, network name, type, and range. To make the negotiation successful, companies need form an alliance and conduct collective negotiation with American Registry of Internet Numbers.

Second, consider hiding e-commerce portals' IP addresses and port information by using the network address translation (NAT) and the port address translation (PAT) technologies. These two technologies are usually used together in coordination for two-way communication. Another more secure but more expensive alternative is to use the high anonymity proxy servers. These proxy servers not only hide the portals' original IP addresses but also not identify themselves as proxy servers, thereby making their portals anonymous on the Internet. Without knowing a portal's original IP address, cyber intruders have difficulties of getting the portal's network information.

Finally, the *Fortune 500* commercial banks' portals should serve as a security benchmark for other companies as none of these banks' OS information was detectable. These banks' portals appeared to firewall their open Port 80/tcp inbound access to all systems and also encrypted open Port 443/tcp for data transmission, thereby obscuring servers and operating systems from external scans.

REFERENCES

1. Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). New York: John Wiley and Sons.
2. Fortune. (2008, May). The *Fortune 500* largest U.S. corporations. *Fortune, 157*(9), F-34-60.
3. Greene, T. (2008, August). Business hacks reap money from e-commerce sites. *Network World, 25*(30). Retrieved August 10, 2008, from http://www.networkworld.com/news/2008/080808-business-hacks.html
4. Grow, B., Epstein, K., & Tschang, C. (2008, April 21). The new E-spionage threat. *Business Week*, 32-45.
5. Hovanesian, M. D. (2008, August 11). Security holes at the online bank. *Business Week*, 16.
6. Mookhey, K. K. (2004, April 26). Common security vulnerabilities in e-commerce systems. *Security Focus*. Retrieved October 5, 2008, from http://www.securityfocus.com/infocus/1775

7. Schuman, E. (2007, October 24). TJX breach more than twice as bad as reported. *eWeek*. Retrieved October 25, 2008, from http://www.eweek.com/print_article2/0,1217,a=217939,00.asp
8. Turner, D., Fossi, M., Johnson, E., Mack, T., Blackbird, J., Entwisle, S., et al. (2008, April). *Symantec Internet security threat report: Trends for July–December 2007* (Vol. 13). Retrieved October 10, 2008, from http://www.symantec.com/business/theme.jsp?themeid=threatreport
9. U.S. Census Bureau, (2008a, May 16). 2006 e-commerce multi-sector report. *E-Stats: Measuring the Electronic Economy*, U.S. Census Bureau. Retrieved October 5, 2008, from http://www.census.gov/eos/www/ebusiness614.htm
10. U.S. Census Bureau, (2008b, August 15). Quarterly retail e-commerce sales: 2nd quarter 2008. *E-Stats—Measuring the Electronic Economy*, U.S. Census Bureau. Retrieved October 5, 2008, from http://www.census.gov/mrts/www/ecomm.html
11. Vijayan, J. (2007, January 19). Breach at TJX shows IT security still lacking in retail industry. *Computer World*. Retrieved January 20, 2007, from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9008599