A VULNERABILITY AUDIT OF THE U.S. STATE E-GOVERNMENT 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
Dr. Rod Davis, Ball State University, rdavis2@bsu.edu

ABSTRACT

This study investigated the network vulnerability status of the e-government service portals of the 50 U.S. states and Washington, D.C. The findings indicate that most state e-government portals had their network information, such as portal's IP address, CIDR, and network range, publicly available on the Internet through the Google search. However, the state e-government portals had their most ports filtered or behind firewalls with very few open ports—
Port 80/tcp and Port 443/tcp. To further reduce the vulnerability of state e-government network systems, this paper recommended how to hide portal's IP address and how to secure open ports.

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

INTRODUCTION

Many states and nations view e-government as a strategic player for economic competitiveness and growth in the Internet era. While the European Commission referred to e-government as a key element of Europe's competitiveness agenda [5], the U.S. federal government committed to expand e-government to be the best one in the world [6]. As government officials [e.g., 1, 11] claimed, e-government portals enable businesses and citizens to easily find the information or service they need and to complete business transactions electronically, thereby strengthening their economic competitiveness and growth. The high efficiency of and easy access to the e-government services makes the government more transparent and efficient [10].

A survey of e-government services prepared for the European Commission found that European Union (EU) citizens saved seven million hours a year on the time they spent for their income tax returns, and EU firms saved about €10 per transaction with the government when doing it online. Moreover, the potential for further savings would be still huge [5]. Chevallerau's study [2] identified that e-government provides its users and government agencies with seven tangible benefits: (a) improved quality of information supply, (b) reduced work-process time, (c) fewer administrative burdens, (d) reduced operational cost, (e) improved service level, (f) increased work efficiency, and (g) increased customer satisfaction.

Unfortunately, the growing popularity of e-government services on the Internet also raised security issues. E-government portals are likely targets for terrorists. Cyber intrusions into e-government portals and computer network systems could impair e-government services any time if the e-government portals are not secure [8]. A 2005 study by a team of Norwegian researchers [9] reported that 82% of the e-government portals around the world were vulnerable to common Web-application attacks such as Cross Site Scripting and Structured Query Language (SQL) injection. Specifically, 90% of the European e-government portals and 76% of the North American (U.S. and Canada) e-government portals were vulnerable to common Web-application attacks, respectively.

According to a 2008 in-depth report of *Business Week* [7], in response to the new espionage threat to government networks, the U.S. federal government launched a cyber initiative to overhaul U.S. cyber defenses. One goal in the initiative was that by June 2008 all federal government agencies must cut the number of communication ports, through which their networks connect to the Internet, from more than 4,000 to fewer than 100.

With governments' increased awareness of Internet security issues, it appears necessary to examine how secure e-government portals are now to block cyber intrusions and terrorist attacks.

The problem addressed in this study was to investigate the network vulnerability status of the U.S. state e-government portals. To conduct the study, we raised the following two research questions:

1. What e-government network information is publicly available on the Internet?
2. How vulnerable are network systems of state e-government portals to cyber intrusions and attacks?

The purpose of the study was to provide the state e-government administrators with the findings that they need to secure their portals. In addition, the findings would also enable our students specialized in Internet security to identify opportunities for internships or jobs at the e-government portals that need to strengthen their Internet security.

METHODOLOGY

The population of this study was the official e-government portals of the 50 U.S. states and Washington, D.C. These 51 portals were all used in the study according to the sample-size requirement [3]. To find out what e-government network information is publicly available on the Internet and how vulnerable state e-government 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 51 e-government portals. All the searches and audits of the 51 portals were conducted in the fall of 2007. The results were saved in digital format, and data were recorded and coded for statistical analysis.

RESULTS

Research Question 1 asked, "What e-government network information is publicly available on the Internet?" The Internet search at *ZoneEdit.com* and *ws.arin.net* identified the IP addresses and network information of most state e-government portals. As Table 1 shows, 98% of state e-government portals' IP addresses were publicly available on the Internet. As a consequence, the portals' IP addresses enabled any online users at *ws.arin.net* to identify a lot of network information from most (84% - 96%) e-government portals, such as organization name, ID, and address; CIDR (classless inter-domain routing) address; network range, name, handle, parent, and type; servers' name, registration date, and updated date; and registered tech handle, name, phone, and email (see Table 1).

Table 1
Network Information Availability of State E-Government Portals (N = 51)

Category	Frequency	Percentage
IP addresses	50	98%
Organization Name	49	96%
Organization ID	45	88%
Address (City, State/Province, Country)	45	88%
Network Range	44	86%
CIDR (Classless Inter-domain Routing)	44	86%
Network Name	44	86%
Network Handle	44	86%
Parent	44	86%
Network Type	44	86%
Name of Server 1	44	86%
Registration Date	44	86%
Updated	44	86%
Registered Tech Handle, Name, Phone, Email	44	86%
Name of Server 2	43	84%

Research Question 2 asked, "How vulnerable are network systems of state e-government 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 1023; those of the registered ports are from 1024 through 49151; and those of the dynamic and/or private ports range from 49152 to 65535. If the ports are open on the Internet without firewalls or filters, they are very vulnerable to cyber intrusions and attacks.

Of the 51 e-government portals scanned by using *Nmap*, 41 portals (80%) were detected of running large numbers of Internet ports (i.e., between 1,669 and 1,671 ports). The remaining 20% of the e-government portals were running relatively smaller numbers of ports ranging from 1,631 up to 1,668 ports. However, most of these detected ports were filtered or behind firewalls and only very few ports were detected as open. As Chart 1 shows, one state e-government portal had 265 ports open on the Internet. By contrast, 17 portals (33%) had only one open port, 25 portals (49%) had two open ports, and the remaining eight portals had several open ports ranging from 3 through 29.

Table 2 presents the network vulnerability information of the e-government portals. All the 51 e-government portals had Port 80/tcp open for http (hypertext transfer protocol) or World Wide Web services.

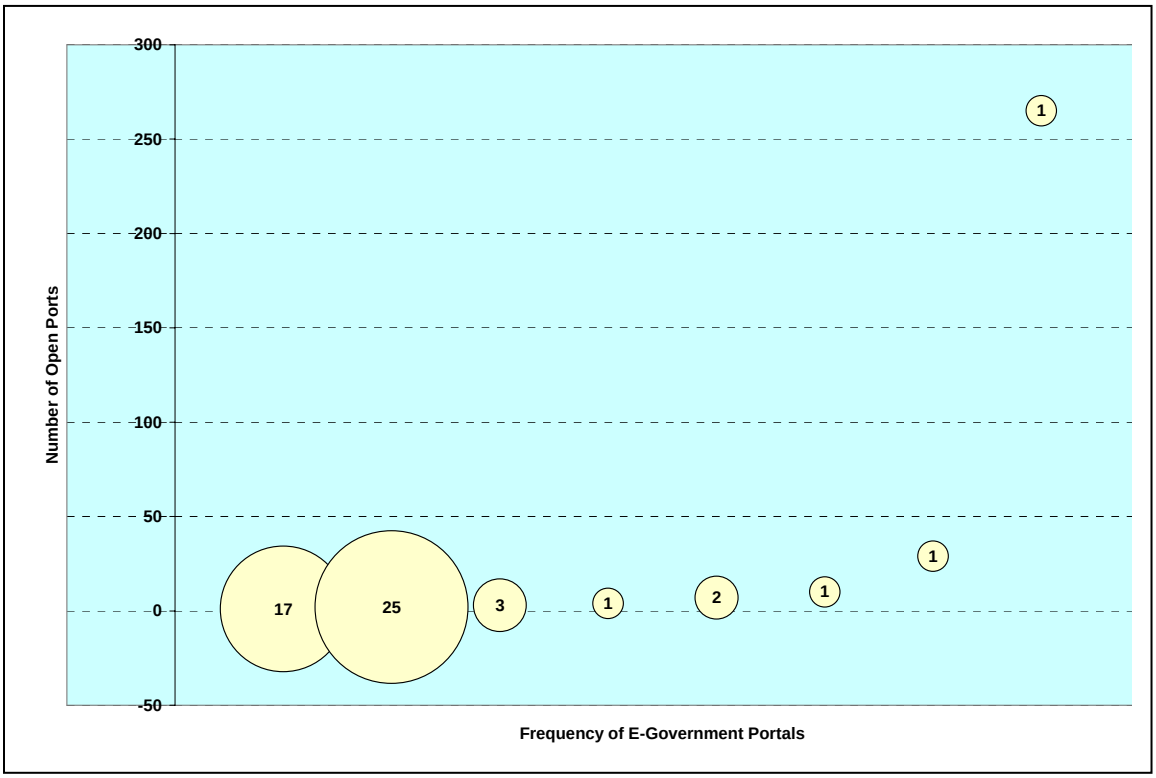

Chart 1: Number of Open Ports at E-Government Portals

Table 2
Systems Vulnerability Status of State E-Government Portals (N = 51)

Category	Frequency	Percentage
Port 80/tcp open; service: http; servers: Apache, IIS, Netscape…	51	100%
Port 443/tcp open; service: encrypted https; servers: Apache, IIS…	31	61%
OS information: e.g., Running: Windows 95/98/ME/NT/XP	17	33%
OS details: e.g., Windows XP SP2/2003 Server	16	31%
My Accounts: encrypted with SSL (secure sockets layer) protocol	50	98%

Web servers identified from Port 80/tcp were Apache, Microsoft IIS, and Netscape. Second, 61% of the e-government portals had Port 443/tcp open for encrypted https services such as personal and institutional Web accounts for business data transactions. Third, around one-third of the e-government portals had their computer operation systems (OS) detected by the network scanner, Nmap, which revealed such OS information as running Windows 95, 98, ME, NT, XP, and 2003 Server. Finally, an additional audit showed that 98% of the e-government portals offered personal and business data transaction services for online users at *My Account* links, all of which were encrypted with SSL protocol (see Table 2).

SUMMARY, DISCUSSION, AND CONCLUSIONS

First, the findings indicate that most state e-government portals' network information is publicly available on the Internet through the Google search.

Such information includes networks' IP address; CIDR address; networks' range, name, handle, parent, and type; servers' name, registration date, and updated date; and registered tech handle, name, phone, and email address.

Such publicly available information of the state e-government portals makes these 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 high-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.

Second, the findings of the network vulnerability audit report that the state e-government portals had their most ports filtered or behind firewalls with very few open ports. While all the e-government portals had their Port 80/tcp open for the http services, 61% of them had Port 443/tcp open for encrypted https services. These open ports revealed server information as well as operation systems information. 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.

However, the additional audit showed that all the *My Account* services were encrypted with SSL protocol for personal and business data transactions. This finding indicates that the state e-governments' encrypted transactional services were not vulnerable to common Web-application attacks such as Cross Site Scripting and Structured Query Language (SQL) injection. This is an obvious improvement compared with the findings of a 2005 survey that 76% of the North American (U.S. and Canada) e-government portals were vulnerable to common Web-application attacks [9].

In conclusion, even though the state e-government portals have all their *My Account* services encrypted with SSL protocol and their most ports filtered or behind firewalls, the portals are still not secure enough because (a) their publicly available network information would attract cyber intruders and (b) their few open ports still remain vulnerable to cyber intrusions and attacks.

RECOMMENDATIONS

Based on the findings and conclusions, we have the following recommendations for the state e-government administrators and developers.

First, consider hiding e-government 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.

NAT is a technique of transceiving network traffic through a router that involves rewriting the source or destination IP addresses and the port numbers of IP packets as they pass through the NAT-enabled router. Therefore, NAT can prevent malicious activity initiated by outside hosts from reaching those local hosts as it disguises the internal network's structure through rewriting and the traffic appears to outside parties as if it originates from the gateway machine. However, using NAT complicates the Internet tunneling protocols because NAT modifies values in the headers which interfere with the integrity checks done by tunneling protocols.

PAT is a device to translate all communications between internal hosts on a private network and external hosts on the Internet. With PAT installed, all communications sent to or from external hosts contain only the IP address and port information of the PAT device instead of internal host IP addresses or port numbers. PAT translates or replaces IP addresses and ports of its internal hosts; therefore, it effectively hides the true endpoint IP address and port of the internal hosts. External hosts are only aware of the IP address of the PAT device and the particular port being used to communicate on behalf of specific internal hosts. A disadvantage of PAT is that, if many internal hosts on the private network make many connections to the Internet, the PAT device may not have sufficient room in its internal table to keep track of the connections or it may simply run out of unused ports.

Second, a more secure and also 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.

Third, firewall Port 80/tcp inbound access to all systems, firewall outbound access to the port, and only allow known proxy servers to access the Internet, thereby forcing clients to use the proxy servers as well as obscuring servers and operation systems from external scans. When proxy servers and firewall are not used to protect Port 80/tcp, portal administrators have to monitor the port traffic cautiously and detect hackers' fingerprints used in exploitation of Web servers and applications. Regarding the open Port 443/tcp for encrypted https services, user IDs and passwords must be required to grant access to the port and outgoing access to the port from servers should be restricted.

REFERENCES

1. Brush, M. (2007). MoEIS increases accuracy and efficiency of e-government solutions. *Tier News*. Retrieved January 10, 2007, from http://www.tier.com/news/pf.cfm?id=166
2. Chevallerau, F. (2005). The impact of e-government on competitiveness, growth, and jobs. *The IDABC eGovernment Observatory of European Communities*. Retrieved January 9, 2007, from http://europa.eu.int/idabc/egovo
3. Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). New York: John Wiley and Sons.
4. European Commission. (2005, January 14). E-government services yield real benefits for EU citizens and businesses. Retrieved October 2, 2005, from http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/41&format=HTML&aged=0&language=EN&guiLanguage=en
5. European Communities. (2005, February 14). E-government and competitiveness: Identifying the connection. *eGovernment News*. Retrieved October 2, 2005, from http://europa.eu.int/idabc/jsps/documents/dspshowPrinterDocument.jsp?docID=3863&lg=en
6. Executive Office of the President of USA. (2004). Expanding e-government: Partnering for a results-oriented government. Retrieved May 1, 2005, from http://www.egov.gov/
7. Grow, B., Epstein, K., & Tschang, C. (2008, April 21). The new E-spionage threat. *Business Week*, 32-45.
8. Halcnin, L. E. (2004). Electronic government: Government capability and terrorist resources. *Government Information Quarterly*, *21*(4), 406-419.
9. Moen, V., Klingsheim, A. N., Simonsen, K. F., & Hole, K. J. (2007). Vulnerabilities in e-governments. *International Journal of Electronic Security and Digital Forensics*, *1*(1), 89-100. Retrieved October 20, 2007, from: http://www.inderscience.com/storage/f110978361112425.pdf
10. The Digital Task Force. (2004). The Danish e-government strategy 2004-2006. Retrieved October 20, 2007, from: http://e.gov.dk/uploads/media/strategy_pixi.pdf. Accessed 26 October 2005
11. State of Nebraska. (2001). E-government to business initiative: Business portal action plan. Retrieved January 9, 2007, from http://www.nitc.state.ne.us/sgc/workgroups/businessportal/documments/Business_Portal_Action_Pland.pdf