Journal of Engineering and Applied Sciences 13 (Special Issue 12): 9491-9496, 2018
ISSN: 1816-949X

A Study on the Management and Security for a Web-Server System in the Same Area Using the Back-Door Type Private Network

[1]Keun-Young Choi, [2]Hyun-Chang Lee and [2]Kyu-Tae Lee
[1]Department of Information and Communication Engineering, Graduate School,
[2]Division of Information and Communication Engineering, Kongju National University,
31080 Choong-Nam, Cheon-An, Korea

Abstract: In this study, a back-door type private network to web-server management is proposed. The proposed method shows excellent security performance among computers located in the same area. The features of the back-door type private network and the virtual host function of the http daemon were investigated for the proposed method. When an administrator in the same area manages a web-server by combining back-door type private network and virtual host function of http daemon, they can get excellent security performance without special security system. In addition, they can be provided with convenient web-based and Windows-based management environment. In order to verify the performance of proposed method an experimental test web-server with back-door type private network and http daemon were set. Then, the test web-document was installed after the public network and the private network were combined with corresponding web-documents. When an administrator belonging to the private network accesses the experimental web-server both public web-documents and secured web-documents are appeared normally. In contrast when a public user belonging to the public network accesses it, only public web-documents are shown and secured web-documents are unreachable. Consequently, the proposed method can manage the web-server in the web-based environment without any exposure to the public network. It also allows unsecured protocols to be used without installation of a secured protocol.

Key words: Backdoor, LAN, network, private network, security, web-documents

INTRODUCTION

The internet has expanded the range of applications and users due to the development of the web that provides a convenient service for the public. Especially, the development of smart-phones has further expanded the application of the internet. In recent years, appearance of not only IP-TV (Internet Protocol Television), IP-phone but also IoT (Internet of Things) has been increasingly influential for public. The internet is a large-scale system that combines various elements and technologies and a server is required for the application of the internet. The largest number of servers that make up the internet is the web-server. It provides various contents for smart-phone as well as web-page and e-mail service used by personal computer. In addition, the IP-TV requires a server to provide contents and the IP-phone requires a server to relay from general telephone or wireless cellular-phone. As the number of servers increases, the number of hackers who occupy the server or seek important information is also increasing which makes computer system security problem more important. One of the recommended methods for computer system security is to build a fire-wall system that blocks unnecessary access to the daemon and allows transmitting selected internal network data which is the best option in respect of security (Cheswick and Bellovin, 1994; Peterson and Dacie, 1996). However, since, the fire-wall system for protecting the web-server must be always in operation with the web-server, there is a financial burden to operate another server. Also, it is difficult to secure the ability to operate the fire-wall system optimally which is a lot of difficulty for the individual to use. For this reason, security issues are becoming more serious in smaller systems that operate on individual rather than large systems with specialized equipment and professional staff. Another risk factor in the operation of the web-server is the tool for communicating various control commands, files and data necessary for server operation. In telnet or FTP (File Transfer Protocol), the account and password used for user authentication are not encrypted. Therefore, this information can be easily acquired by

Corresponding Author: Hyun-Chang Lee, Division of Informmation and Communication Engineering, Kongju National University, 31080 Cheon-An, Korea

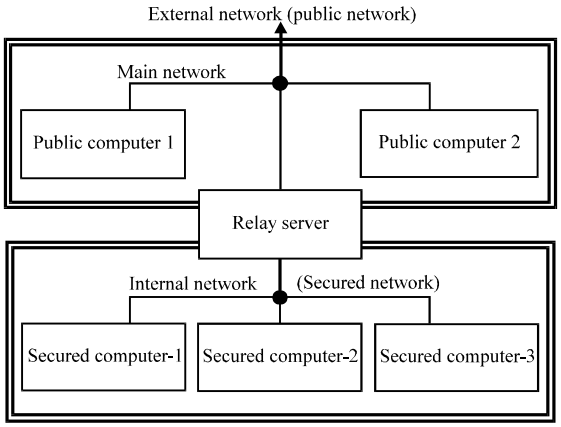

Fig. 1: Security by separated networks

packet tapping in the same network (Braden, 1988). An alternative way to enforce the security is SSL (Secured Socket Layer) that secured telnet and secured FTP are used (Kaufman *et al*., 1995). There is a drawback that the daemon is installed on the server and an overflow attack is possible on the port through port scan. For the security of personal information transmission, a separate network configured as shown in Fig. 1. DMZ (Demilitarized Zone) method and screened network method (Yong-Joon *et al*., 1998) have been investigated that systems are separated from public and internal networks by constructing a separate network and establishing a relay system.

These methods are very effective for security and can use programs or protocols that are vulnerable to security between internal networks. However, when a relay server is exposed to hacking, all internal networks are exposed to hacking. Therefore, there is a need for highly specialized experts who can operate the relay server at an optimal state at all times. For this reason it can be used in a comparatively large-scale network and it is difficult for an individual to utilize economically and operationally. To overcome such security vulnerabilities, BDP network (Back-Door type Private network) (Lee and Lee, 2006) was proposed that can securely communicate data between computers located in the same area without network knowledge. Also, a method for effectively communicating data in a Back-Door type private network was proposed.

In this study, the BDP network which has excellent network security performance among the computers in the same area is applied to web-server management to solve various problems that occur during operation of web-server. The following topics are introduced in this study: the BDP network and configuration of a web-server are discussed, the BDP network is designed for web-server management and the proposed method is implemented in the system and is verified by experiments.

MATERIALS AND METHODS

The BDP network and web-server

Principle of the BDP network: The BDP network has two NICs (Network Interface Cards) installed in each computer as shown in Fig. 2. one NIC (eth0) connects to the existing main network and the other NIC (eth1) internally constitutes a private network (Lee and Lee, 2006).

Each computer determines the device (eth0 or eth1) to which data will be input or output by the setting of the routing table (Narten, 1989). The private network uses an IP-address that is not used in the main network (i.e., the private IP-address class regulated by RFC-1918) (Rekhter *et al*., 1996). And if it is detected as an IP-address class by net-mask it communicates via the eth1. If all other IP-addresses are set to the default gateway eth0, then the public data is accessed via. the default gateway to the main network and the private data is communicated via. the private network to the corresponding computer.

The BDP network has the following properties: the BDP network can be easily installed and operated without affecting the existing main network topology, since, private data passes through a separate network without going through the main network information is not leaked to the outside. Therefore, the BDP network does not require a daemon installation for a secured protocol which enhances security. The load on the main network is reduced and the BDP network can communicate at the full speed of the private network. Since, the BDP network does not receive account and password analogy attack, packet tapping or daemon overflow attack, existing telnet and FTP can be used without security feature. In a Windows-based system, since shared directory information is not leaked to the outside but only appears on the private network, file sharing is possible with security. The BDP network requires a NIC per station, so it can be installed economically and without expertise. If a dynamic IP-address is used in the main-network it can be applied by configuring the class differently due to the private IP-address.

Virtual host: The virtual host function is provided by most http daemons and is used to build two or more web-sites on a single web-server. Each web-site can be distinguished by IP-address or domain name as shown in

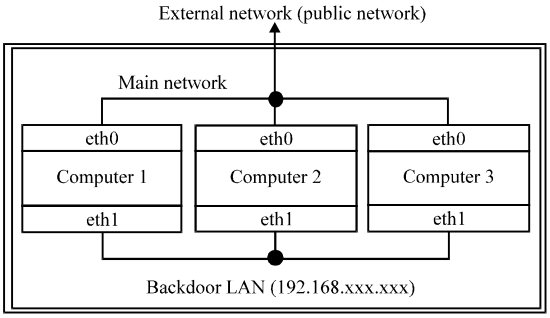

Fig. 2: Structure of the BDP network

Algorithm 1. Algorithm 1 is a part of Apache http daemon's httpd.conf file and other daemons have a similar structure. Is the place to record IP-address and port-number responded by the http daemon. When multiple listen addresses are recorded, the http daemon responds to them. The root directory of the main web-site is recorded at where the configured directory is the root directory of the public web-site. Is a configuration for a virtual host. When two or more web-sites operate on a single web-server it configures the IP-address, port-number and root-directory of the additional web-site.

Algorithm 1; Example of http daemon configuration for virtual host:

```
                ⋮
(a)   Listen main IP-address
      Listen secured IP-address
                ⋮
(b)   DocumentRoot main root dictionary
                ⋮
(c)   NameVirtualHost secured IP-address
        <VirtualHost secured IP-address>
          DocumentRoot secured root
          ServerName secured IP-address
        </VirtualHost>
```

RESULTS AND DISCUSSION

Combine with the BDP network: The BDP network provides another route and IP-address that can access the web-server. Therefore, when the BDP network is combined with the virtual host function of the http daemon a separate site can be operated on the main network and the private network. The "abc" directory is specified as the web-site root of the main network and the "bcd" directory is designated as the web-site root of the private network as shown in Fig. 3a. If the directory tree that the "abc" directory and the "bcd" directory have the same rank topology is configured as shown in Fig. 3 b, the web-sites in the main and private networks are completely separated. If the topology is configured as

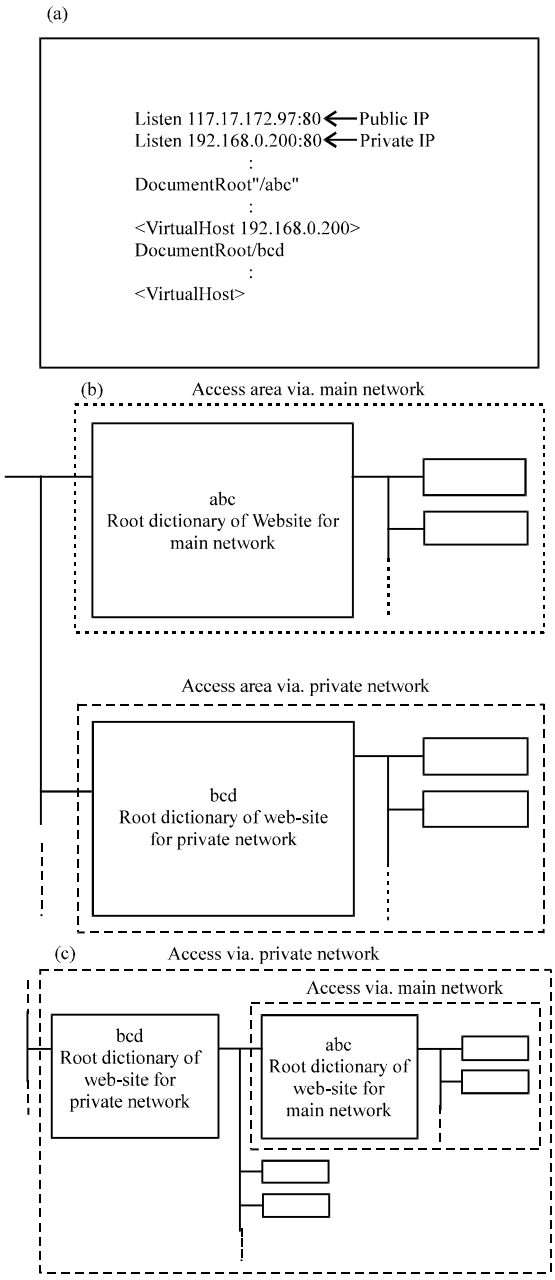

Fig. 3: Example of dualized web-directory area: a) Configuration; b) The same rank topology and c) Subordinate topology

shown in Fig. 3c, the web-site directory of the main network can be treated as one of the sub-directories of the web-site directory of the private network.

As a result, both the topology in Fig. 3b and the topology in Fig. 3c can manage the web-contents provided through the main network and the web-contents provided through the private network in a separate directory tree within the server. Therefore, web-contents

development, modification and management can be performed on the web-page for the private network. When all the work is completed, this can be copied to the web-directory for the main network. The data is not exposed to the outside due to the characteristics of the BDP network. In addition when a shadow server (test server) is used it is only possible to access through private network. The security problem can also be solved when data is sent from the shadow server to the main server. When the web-page is managed in proposed method, a separate log-in process is unnecessary and encryption is not required. Moreover, in contrast that text-based UNIX should be managed by console; Windows-based management is possible through a browser on a PC on the same private network. If the Windows system such as X-Windows or Solaris is installed on UNIX for Windows-based management (i.e., only for administrator), the storage capacity and task load of server is increased.

Experiments and considerations: In order to verify the performance of the proposed BDP network and virtual host, the BDP network and the Apache http daemon were installed on a test web-server and the "httpd.conf" file was configured as shown in Fig. 4a.

When a user connects to the web-server via. ok.kongju.ac.kr" domain using the public IP-address of 117.17.172.94, web-page root directory becomes "/home/secured/public". When the user accesses the web-server via. the private IP-address of 192.168.153.200, "/home/secured" becomes the web-page root directory. And the directory tree is configured as shown in Fig. 4b. After installing test web-documents in each root directory, an administrator located in the same area connects to the server as shown in Fig. 5.

Figure 5 a shows a web-page accessed via. the domain name (i.e., access to web-server via. the public IP-address) and the public web-page is displayed. Figure 4b shows a web-page accessed via. the private IP-address, although, the user connects to the same server, a web-page for the administrator is displayed. If a public web-document is linked to the web-page for the administrator and accessed, a public web-document appears as shown in Fig. 5c). The URL (Uniform Resource Locator) shown in the address window is treated as one of the sub-directories of the private web-page.

Figure 6 shows screen-shots of accessing the experimental web-server from a public user belonging to another network. Figure 6 a shows that, the user accesses the web-server via. domain name and public web-page is displayed. However, when accessing is attempted with a

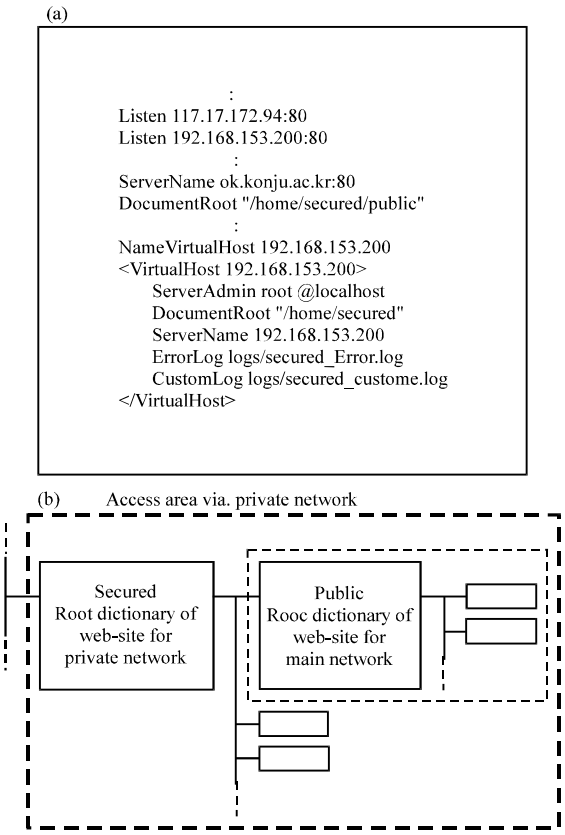

Fig. 4: Http daemon and directory tree configuration for experiment: a) Http Daemon (Apache) configuration and b) Directory tree

private IP-address, there is no IP-address in the public network. Consequently, an unreachable message appears as shown in Fig. 6b.

Since, the private network does not appear in the public network, hacking is fundamentally blocked. Therefore it is possible to use data transfer, server management, unsecured telnet and unsecured FTP on internal network (i.e., private network) without special security system.

Note that, the proposed method was verified following effectiveness against cyber-attack (Kolichtchak, 2001; Ansari *et al*., 2002; Wang *et al*., 2010).

Packet tapping: Since, all of the private data in the proposed method communicate via. the private network, no packet appears in the public network.

Port scanning: In the public network, the attack path is reduced because 80 or 8080 for the http daemon port are detected and the other port is not open. The required telnet port 23 or FTP port 21 exists only on the private network.

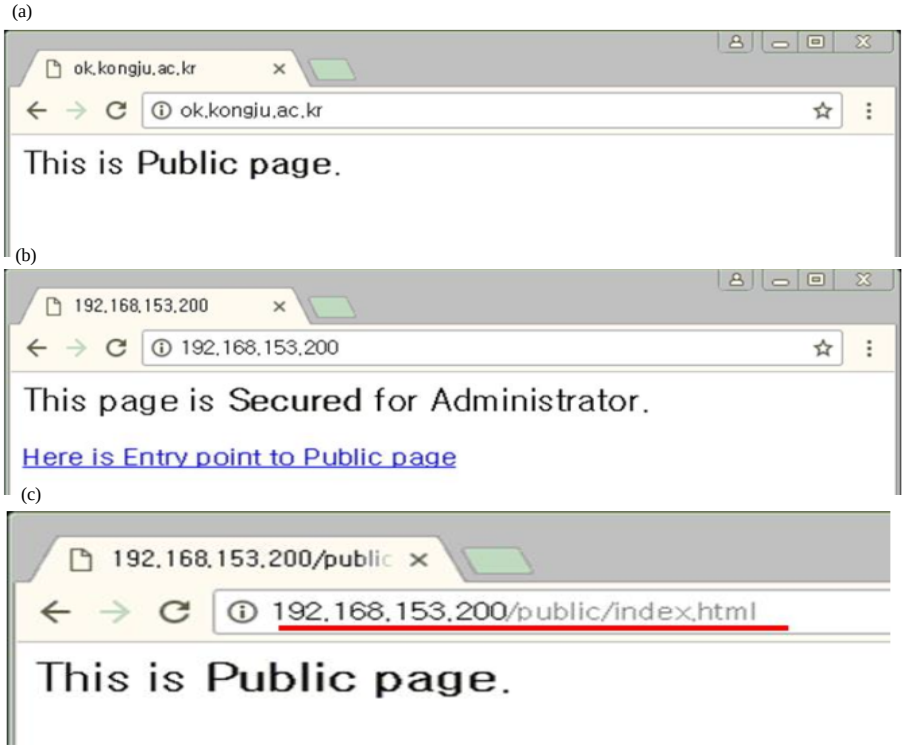

Fig. 5: Experimental results of accessing by an administrator: a) Accessing via. the public IP-address (domain name); b) Accessing via the private IP-address and c) Accessing public page via. the private IP-address

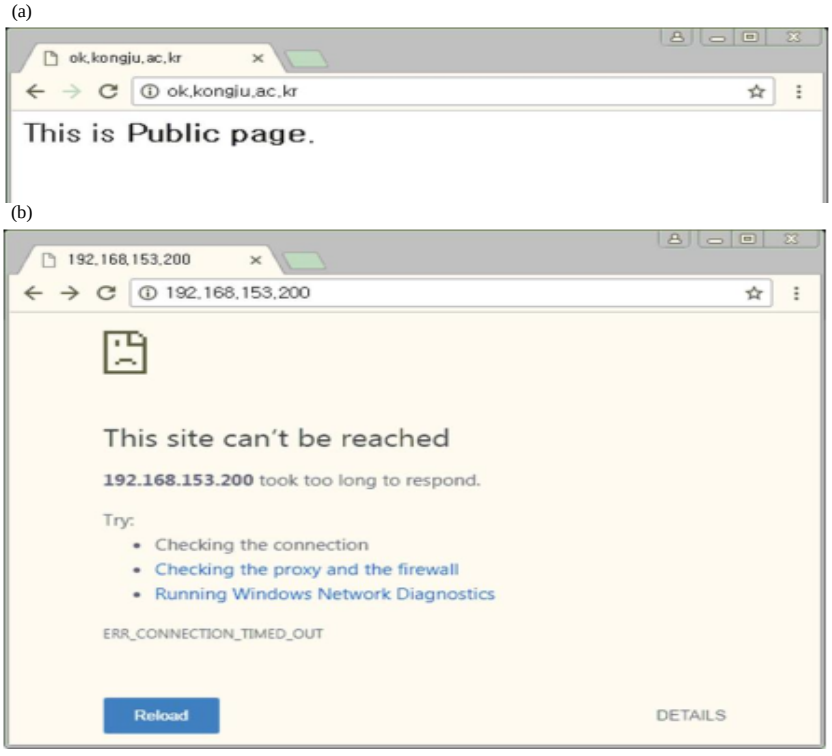

Fig. 6: Experimental results of accessing by a public user: a) Accessing via. the public IP-address and b) Accessing via. the private IP-address

Daemon stack overflow: In the private network, since, only the http Daemon is open, security can be focused on it which is advantageous for management.

Account and password analogy: This attack is impossible because there is no need separate log-in process.

Browser exploit: This is not a network problem but a server management problem. If Daemon Version and Operating System (OS) version do not appear it can be defended.

DoS (Denial of Service), DdoS (Distributed DoS) attack: Even if a DoS or DDoS situation occurs it becomes a public network and it is independent of the private network. Therefore, an administrator can easily take action via the private network.

IP-spoofing attack: Even if a spoofing attack is attempted with an IP-address for a private network via. the public network, the NIC connected to the public network does not recognize the IP-address for the private network. Therefore, there is no need for such an end-point authentication.

CONCLUSION

In this study, a back-door type private network to web-server management is proposed. The proposed method shows excellent security performance among computers located in the same area. When an administrator in the same area manages a web-server by combining back-door type private network and virtual host function of http daemon, they can get excellent security performance without special security system. In addition, they can be provided with a convenient web-based management environment. The proposed method was verified by test web-server with back-door type private network and http daemon. Then, the test web-document was installed after the public network and the private network were combined with corresponding web-documents. When an administrator belonging to the private network accesses the experimental web-server both public web-documents and secured web-documents are appeared normally. In contrast when a public user belonging to the public network accesses it only public web-documents are shown and 2018 secured web-documents are unreachable. Therefore, the proposed method can manage the web-server in web-based and Windows-based environment without any exposure to the public network. It also allows unsecured protocols to be used without installation of a secured protocol.

REFERENCES

Ansari, S., S.G. Rajeev and H.S. Chandrashekar, 2002. Packet sniffing: A brief introduction. IEEE. Potentials, 21: 17-19.

Braden, R.T., 1988. A pseudo-machine for packet monitoring and statistics. Proceedings of the ACM SIGCOMM International Conference on Computer Communication Review Vol. 18, August 16-18, 1988, ACM, New York, USA., pp: 200-209.

Cheswick, W.R. and M.S. Bellovin, 1994. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, Boston, Massachusetts, USA., ISBN:9780201633573, Pages: 306.

Kaufman, C., R. Perlman and M. Speciner, 1995. Network Security: Private Communication in a Public World. Prentice Hall, Upper Saddle River, New Jersey, USA., ISBN:9780130614667, Pages: 504.

Kolichtchak, A., 2001. Buffer overflow attack detection and suppression. New Haven, Connecticut.

Lee, H.C. and J.E. Lee, 2006. A study on the improving operation efficiency of the back-door type private network. J. Korean Inst. Commun. Inf. Sci., 31: 199-206.

Narten, T., 1989. Internet routing. Proceedings of the ACM SIGCOMM International Conference on Computer Communication Review Vol. 19, September 25-27, 1989, ACM, New York, USA., pp: 271-282.

Peterson, L.L. and S.B. Dacie, 1996. Computer Networks: A Systems Approach. 3rd Edn., Morgan Kaufmann Publishers, Burlington, Massachusetts, USA., ISBN:9781558603684, Pages: 552.

Rekhter, Y., B. Moskowitz, D. Karrenberg, D.G.J. Groot and E. Lear, 1996. Address allocation for private internets. Network Working Group, 1: 1-9.

Wang, X., C.C. Pan, P. Liu and S. Zhu, 2010. SigFree: A signature-free buffer overflow attack blocker. IEEE Trans. Dependable Secure Comput., 7: 65-79.

Yong-Joon, L., K. Chang-Goo, P. Sung-Yul and R. Keun-Ho, 1998. Design and implementation of the wall and walls firewall system. J. KISS. C. Comput. Practices, 4: 575-587.