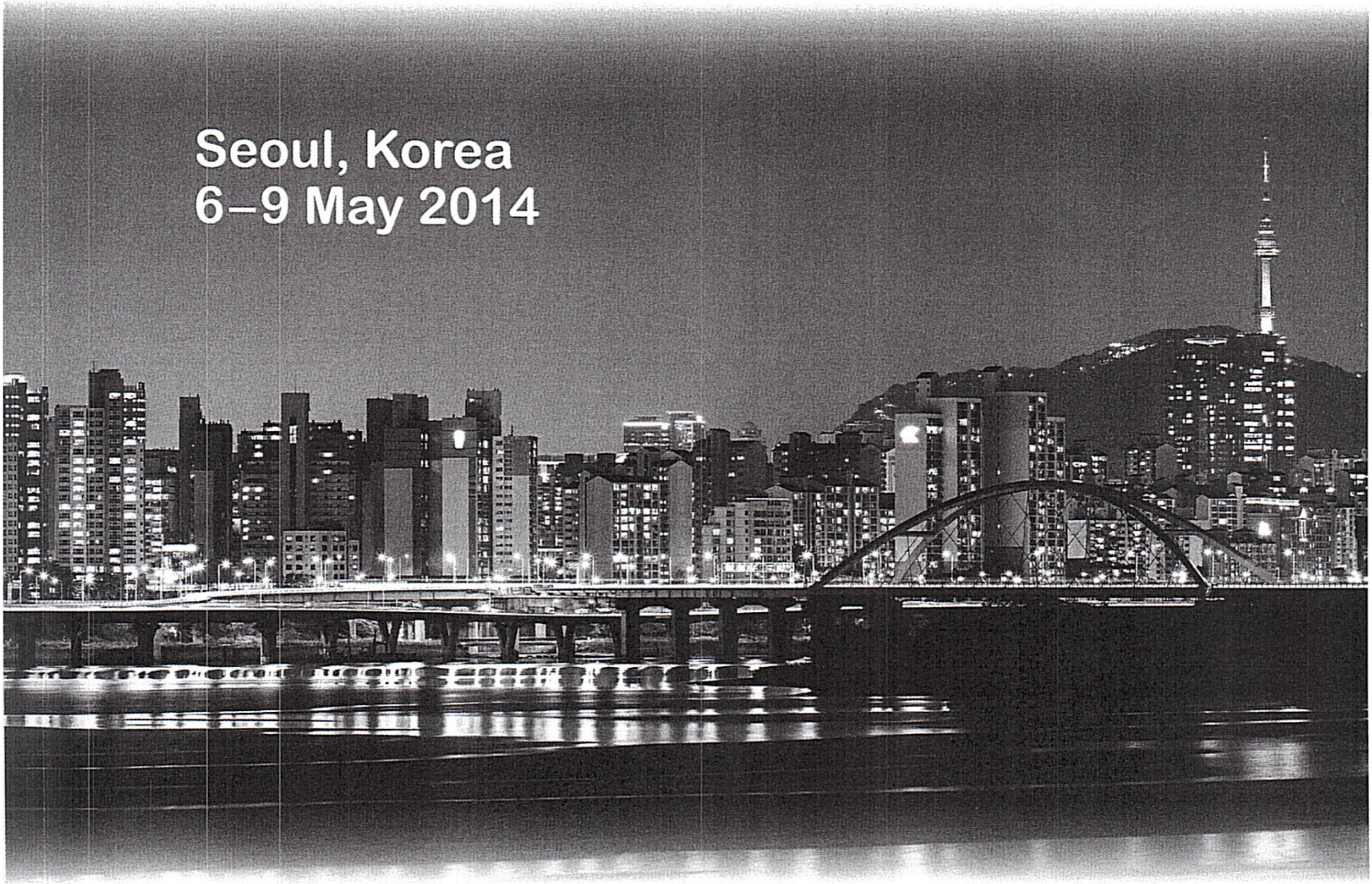
2014 Fifth International Conference on Information Science and Applications

ICISA 2014

Technically Co-Sponsored by IEEE Computer Society


Seoul, Korea
6–9 May 2014

Technically Co-Sponsored by

IEEE

IEEE computer society

Track 12: SATA Workshop

A Study on Preventative Measures for Ninja Hacking

Byungho PARK
Dept. of CIC, Hongik University, Sejong Campus, 339-701
Korea
sunsonbob@hongik.ac.kr

R. Young Chul Kim
Dept. of Computer & Information Communication, Hongik
University, Sejong Campus, 339-701
Korea
bob@selab.hongik.ac.kr

Young B. PARK
Dept. of Computer Science, Dankook University, 330-714
Korea
ybpark@dankook.ac.kr

Abstract— **Anonymous declared that it would hack North Korea, the world-wide closing country on June 25 in 2013, using internal supporters, but it is not known to have succeeded in hacking concretely. However, our previous study suggested hacking with Ninja gate, not with the existing method by connected routing. As a result of this study, we mentioned that even though it is a closing network, it will need a separate measure. This study suggests a countermeasure against Ninja Hacking.**

Keywords— Ninja router; anonymous; backdoor; closing network

I. Introduction

Anonymous, International Hacker Group, invaded a website operated by North Korea's Government-controlled Cho-sun central Communication and declared individual information of site members in April, 2013. Also, they declared that they would hack Gwangmyung, North Korea's network, on June 25 in 2013 in order to celebrate the initiation of Korean War[5,6]. The cause why it is noticed is that North Korea is a very closing country so that its ordinary population cannot use the Internet, but the special-level people can use it very limitedly.

Especially, Gwangmyung, the public network used inside North Korea, is the solely closed network, and it is very difficult to hack though the Internet.

Anonymous declared that it would hack it with Ninja gateway and internal supporters, but the specification about the concrete Ninja gateway was not known. Several hacking methods have been noticed using network devices, and US-CERT of US Government announced that there existed backdoors in D-Link routers recently in October, 2013[7]. D-Link has a problem that if an operator uses the remote control function and starts attacking the establishment of router may be changed, and an error may be made. The previous study suggested the only outline by possible hacking methods, using backdoors for the router itself in the environment of the Internet connected to the network [1-3][8].

We specified the Ninja gateway method by router hacking through backdoors in the network unconnected physically with the application of a method [1]. Also, in this paper, we suggested that we should not think that a typical national closed network such as national ministry networks are not safe which are operated separately by it, and we should need independent preventative measures.

This study proposes a countermeasure against hacking with Ninja gateway, and it is composed of 4 chapters.

Chapter 2 describes the related studies, Chapter 3 suggests a preventative measure against Ninja gateway hacking, and Chapter 4 is the conclusion of this study.

II. PREVIOUS STUDY

Generally, the connection of networks is made by the link between routers.

Router is a network device which sets a route between networks and connects traffic with the fastest path, and apparatus which establishes an optimal route. It connects the separate networks, using the same transport protocol and links each network layer with one another. It is a device which extracts the location of a packet directing the best route for it, and then it transports the data packet to the next router device along this path. Figure 1 describes a typical role of the router.

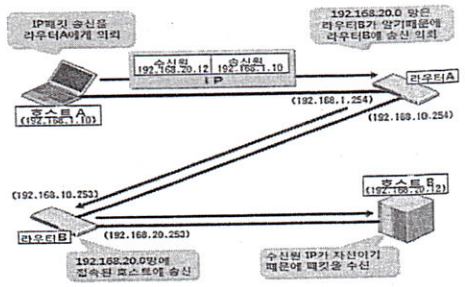


Fig. 1. An example of Network Configuration Using Multi Router

978-1-4799-4441-5/14/$31.00 ©2014 IEEE

Router decides a node within different networks or its own, depending on place cards in addition to the functions of a bridge. Like a switch which can transport a packet to a destination based on the MAC address, Router has routing software and a routing table within itself and provides a routing service with a routing table corresponding to an address table. Then routing software examines a destination address of the received datagram and transfers it properly via one of the output ports with reference to a routing table established in the memory about this address. More precisely, Router counts on a routing table thoroughly and does routing. Therefore, the role of a router, managing the routing table, occupies more than half of the specific gravity, and it is possible to find the optimal route depending on how to configure and manage this routing table.

Ninja router can build any router on a mediocre and common desktop as well as a router, and it just needs not to look like a router.

We show an example of Ninja router in Figure 2.

Fig. 2. (Left) Ordinary Router & (Right) Ninja Gateway Using Desktop PC

Only, the basic structure of a router has CPU, a general processing unit like that of a general computer and each memory just needs to hold the operating system of a router, the information for establishing environments, and the routing information, and to input and output the traffic through the network interface[13].

III. Preventative Measures for Ninja Hacking

The Internet is a network to connect servers and exchange various information, and it can be divided into two kinds: the public network which is connected and used by most common people around the world, and the internal intranet which is used as a military, a police, and an administration network. In particular, each country thinks that those internal closed networks are separated from the Internet physically, and they are absolutely safe. However, Anonymous, international hacking group, is surprising enough to get much attention for hacking Gwangmyung, the intranet of North Korea, a closed network, but it did not specify which tool and method it would use, or how it would hack Gwangmuyng as its actual attribute. It is just known that it used the term of Ninja, an unknown warrior who appeared and did his task covertly in a Japanese legend, As a result, it can be inferred that it will be an illegal router or a routing operation method.

In our previous study, we suggested the concept of a ninja router technique.

Figure 3 shows the mechanism of the routing table hacking.

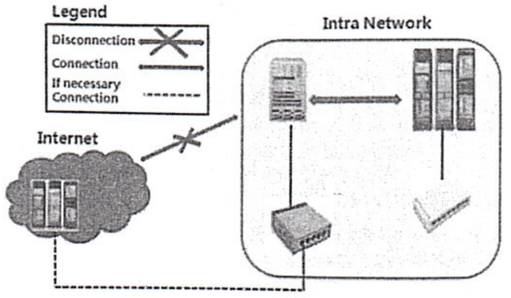


Fig. 3. The Configuration of Ninja Gateway using Backdoor(swiching hub)

How can we prevent a method about hacking Ninja gateway in advance?

First, if an abnormal routing IP is detected in the routing table, it means that an unauthorized routing is established there. As a solution, an identification method is suggested to prepare an authorized separate routing table, delete the hacked one, and then replace it with the existing allowed routing IP through comparison if a new routing IP is added. Also, this study is expected to be able to trace back where it is hacked, and blockade it.

IV. CONCLUSION

The Internet has been a living apparatus which is directly and indirectly important in people's life around the world.

Especially, national security, bank, and administration networks are separated from the Internet and used as an essential element in the population's life and the nation's management. However, Anonymous' declaration about hacking Gwangmyoung, the Internet of North Korea, the typical closing country in the world, gives us many suggestions.

Our previous study proposed a bottom-up connection method through a backdoor in a network which is not linked physically, and especially, specified problems about a separated network considered secure by routing table hacking.

Therefore, in this study, we suggested various hacking examples about routing table hacking, and countermeasures against them.

Acknowledgment

This work was supported by the IT R&D Program of MKE/KEIT [10035708, "The Development of CPS(Cyber-Physical Systems) Core Technologies for High Confidential Autonomic Control Software"] and Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2013R1A1A2011601)

REFERENCES

[1] B. Park, D. Shin, H. Na, A Study on Ninja Gateway Routing Using Backdoor Method, Journal of Security Engeering.(2014), Vol. 11, No. 1, pp115-121.

[2] A. T. Mizrak, S. Savage and K. Marzullo, Detecting Malicious Packet Losses. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS. (2009), VOL. 20, NO. 2, pp.191-206.

[3] J. S. Sung, A Study on the Prevention Plan of Security Incident. Journal of Security Engineering. (2012), Vol. 9, No.6, pp.513-526.

[4] A. S. Tanenbaum, Computer Networks (4th ed.), Prentice Hall PTR, NJ 2003)

[5] http://mickhartley.typepad.com/blog/2013/06/ninja-gateway.html, Jun 28 (2013).

[6] http://www.nknews.org/2013/06/anonymous-claims-secret-north-korean-military-documents, Jun 20 (2013).

[7] http://www.us-cert.gov/ncas/current-activity/2013/10/18/Reports-D-Link-Router-Backdoor, Oct 18 (2013).

[8] http://www.cs.rutgers.edu/~iftode/citadel.pdf, Sep 26 (2005).

[9] http://www.terms.co.kr/router.htm, Jun 22 (1999).

[10] http://ko.wikipedia.org/wiki/ %router%, Sep 24 (2013).

[11] http://songsunghan.tistory.com/12, Jul 11 (2007)

[12] http://docstore.mik.ua/orelly/networking/tcpip/ch02_05.htm, Dec 1 (1999).

[13] http://www.linuxjournal.com/article/5826, Aug 5 (2010).

ICISA 2014

Technically Co-Sponsored by IEEE Computer Society

Technically Co-Sponsored by

IEEE

IEEE computer society