Experiment on repetitive router exchanging for router metabolism

Yuya SUGA[†], ***Nonmember***, **Rei ISHIOKA**[††], ***Student Member***, ***and*** **Junichi MURAYAMA**[††], ***Member***

SUMMARY In the near future, undetectable malware programs may infect routers. Even such programs can be removed by initializing routers. However, packet forwarding needs to be suspended during the initialization. To solve this problem, we have been studying a metabolic router. This hardware router comprises multiple virtual routers redundantly. The master virtual router is exchanged periodically with the initialized backup one. Despite malware is undetectable or not, this exchange removes the infected malware from the hardware router. This paper evaluates this exchanging scheme through experiments. The results are as follows: (1) VRRP can exchange virtual routers within 1 millisecond. (2) This exchange can be repeated semi-permanently by periodically decreasing the priority levels of the exchanged virtual routers. (3) This exchange removes malware from the hardware router. Consequently, it is expected that the router metabolism can mitigate malware infection damage.

key words: *virtual router, hitless exchanging, repetitive exchanging, malware, metabolism*

1. Introduction

Recently, cyberattacks such as Distributed Denial of Service (DDoS) attacks or phishing scams have frequently occurred [1] [2] [3]. These attacks use malicious software called malware. It infected hosts or servers. In the near future, malware may also infect routers in networks [4].

A basic countermeasure against such attacks is to detect and remove malware. A malware program can be detected by searching a computer file containing malware's signature information [5]. A detected program file is removed immediately from the system. However, signature obfuscation technology is advancing, and thus malware detection is becoming difficult [6]. Accordingly, how to remove undetectable malware programs becomes an important issue.

A basic solution for this issue is to initialize router software. If a router is initialized periodically, damage caused by malware will be mitigated. On the other hand, during the initialization, the router stops packet forwarding. This is serious for business use.

In order to solve this problem, router redundancy technology seems attractive. In this approach, the master router forwards packets. It is continued even when the backup router is initialized. After this initialization, the master router can be exchanged with the initialized backup one in a hitless manner. Consequently, the whole router system can continue packet forwarding without interruption. According to such backgrounds, we have been studying this router mechanism as a metabolic router shown in Fig.1.

As a router-exchanging scheme, the Virtual Router Redundancy Protocol (VRRP) [7] is familiar. In VRRP, hitless router-exchanging can be done by means of increasing the exchanging-priority level of the backup router higher than that of the master one. However, if this exchanging is repeated simply, the priority level increases gradually, and it will reach the upper limit. Thus, this exchange cannot be repeated semi-permanently.

In order to solve this problem, we have proposed a dynamic priority control scheme [8]. This paper evaluates this scheme by experiment. The evaluation comprises the following three experiments: hitless router-exchanging, repetitive router-exchanging, and malware deletion through router-exchanging. In the first experiment, a VRRP scheme achieved hitless router-exchanging. In the next one, our priority-control scheme enabled semi-permanent repetition of router-exchanging. In the final one, router-exchanging removed a malware program from the hardware router. Consequently, we can say that our metabolic router concept is promising as one of the countermeasures against malware.

The rest of this paper is organized as follows: Sect.2 shows an overview of our repetitive router-exchanging scheme. Then, Sect.3 evaluates our scheme by experiment. Finally, Sect.4 shows the conclusion of this paper.

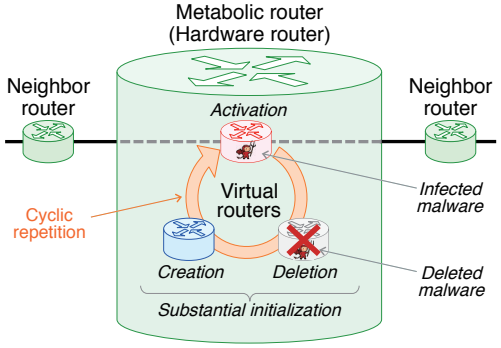

Fig. 1 Metabolic router concept

2. Repetitive router-exchanging

This section presents our repetitive router-exchanging scheme. A configuration of our scheme is depicted in Fig.2. A hardware router comprises two virtual routers

[†]The authors are with Tokai University, Minato-ku, Tokyo, 108-8619 Japan.

[††]The authors are with the graduate school of Tokai University, Minato-ku, Tokyo, 108-8619 Japan.

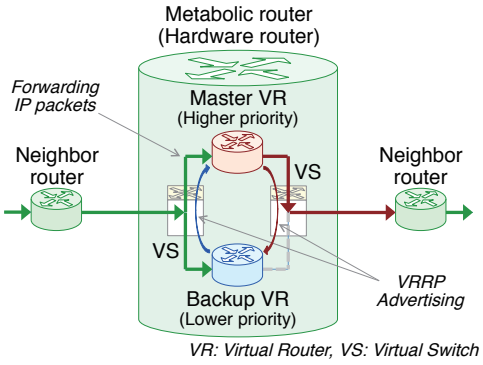

Fig. 2 Router-exchanging scheme

(VRs) achieved using virtual machine technology. These VRs are combined redundantly so as to conform to VRRP.

A procedure of system operation is summarized in Fig.3. In the initial stage, the system comprises only the master VR. Then, a backup VR is added to this system (Fig.3 (1)). Next, each VR sends and receives VRRP advertisement messages (Fig.3 (2)). Each VR compares the advertised VRRP priority level with its own level (Fig.3 (3)). Here, the backup VR's priority level has been set higher than the master VR's level. Accordingly, the current master VR stops forwarding the packet, while the backup one starts it (Fig.3 .(4)). This exchange is done simultaneously, and thus it can be said hitless substantially. After this exchange, the old master and the old backup become the new backup and the new master, respectively. In addition, the new backup router is disconnected from the system (Fig.3 (5)).

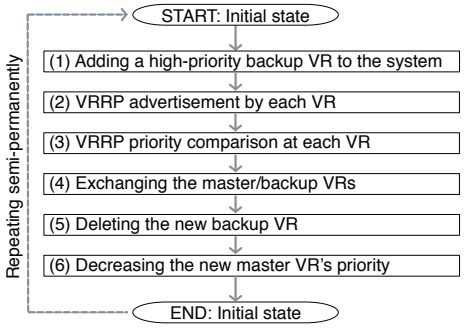

Fig. 3 Router-exchanging procedure

In this stage, the new master VR's priority level is higher than the old master VR's one. If this procedure is repeated simply, the priority level will increase gradually, and it will reach the upper limit. In order to solve this problem, our proposed scheme is required. Namely, after the disconnection, the master VR's priority level is decreased to the system's initial level (Fig.3 (6)). Typically, the priority level is changed from outside the VR using SSH remote control.

In this stage, the system returns to the initial state completely. Consequently, the same procedure can be repeated any number of times.

3. Experiment

Our proposed router-exchanging scheme was evaluated by the following three experiments: hitless router-exchanging, repetitive router-exchanging, and malware deletion. They are presented in this section.

3.1 Hitless router-exchanging

The router-exchanging period was measured using an experiment system. A system configuration is depicted in Fig.4. The hardware specifications of Host1, Host2, and Host3 in the figure are summarized in Table 1. In addition, that of Host1 as a web client is summarized in Table 2. Each virtual router was assigned hardware resources shown in Table 3.

As the software specification, the hardware and virtual routers employed Linux Ubuntu version 20.04 and VyOS version 1.1.8 [10], respectively. In addition, the virtual switch employed bridge-utils [11].

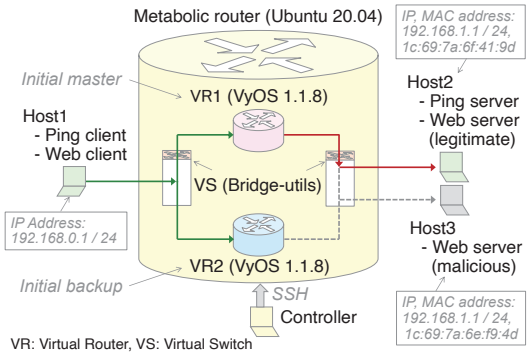

Fig. 4 Experiment system configuration

Table 1 Hardware specification of Host1, Host2 and Host3

CPU	Intel Core i7-10710U
Memory	64GB
SSD	1TB

Table 2 Hardware specification of web client

CPU	Intel Core i7-8559U
Memory	64GB
SSD	2TB

Table 3 Hardware resources allocated to each virtual router

CPU	4 virtual cores
Memory	1GB
Disk space	10GB

In Fig.4, VR1 and VR2 are located in the upper center and the lower center, respectively. In addition, Host1 and Host2 are on the left and on the right, respectively. In the first stage, the VRRP priority levels of VR1 and VR2 were set to 254 and 253, respectively. Then, Host1 and Host2 communicated with each other using Linux's ping command. Here, the payload length of each IP packet was set to 84 bytes, and the packet transmission interval was set to 1 millisecond. The packet length was set shorter in order to measure router-exchanging latency rather than packet forwarding throughput. In this condition, VR1 acted as the master VR and forwarded all packets without packet loss.

In the second stage, during the ping communication, the VR2's priority level was changed from 253 to 255. Accordingly, the master router was changed from VR1 to VR2. Here, all ping packets were forwarded without loss. As shown in the bottom center of Fig.4, VR's priority level was changed using the Secure Shell (SSH) [12] outside the VR.

From those results, we can conclude that the master and backup routers can be exchanged with each other within 1 millisecond using VRRP.

3.2 Repetitive router-exchanging

The limitation of the number of VR exchanging times was also measured using the system described above. When the backup VR's priority level becomes higher than the master VR's level, those VRs are exchanged immediately. The highest priority level is limited to 255 due to the VRRP specification.

In the conventional VR exchange scheme, the priority level increases every time VRs exchange, and it will reach the upper limit. In the experiment, the priority levels of VR1 (master) and VR2 (backup) were initially set to 255 and 254, respectively. Continuously, the VR2's priority level was changed from 254 to 255. The results are summarized in Table 4. This table shows that VRs were exchanged in some cases, while they were not in other cases. Namely, VR exchanging became unstable when VR's priority levels reached the upper limit. Consequently, the conventional scheme is insufficient for repeating VR exchanging semi-permanently.

On the other hand, in our proposed scheme, VRs' priority levels are reduced periodically. Thus, they will not reach the limit. The procedure and results of the experiment of our proposed scheme are summarized in Table 5.

In the first stage, priority levels of VR1 (master) and VR2 (backup) were initially set to 254 and 253, respectively (Step1 in Table 5). Accordingly, VR1 forwarded packets, while VR2 did not.

In the second stage, the VR2's priority level was increased from 253 to 255 (Step2 in Table 5), and VRs were exchanged immediately. After the exchange, the VR1's priority level was decreased from 254 to 253 (Step3 in Table 5). Continuously, the VR2's priority level was also decreased from 255 to 254 (Step4 in Table 5).

In the third stage, the VR1's priority level was increased from 253 to 255 (Step5 in Table 5), and VRs were exchanged again. After the exchange, the VR2's priority level was decreased from 254 to 253 (Step6 in Table 5). Continuously, the VR1's priority level was also decreased from 255 to 254 (Step7 in Table 5).

In this final stage, the VRs' states were returned to the initial states (Step1 in Table 5). This means that, in our proposed scheme, priority level can be suppressed below the upper limit, and hitless VR-exchanging will be repeated semi-permanently.

3.3 Malware deletion

The effect of malware deletion was measured using the experiment system shown in Fig.4. The specification of the hardware router is the same as that in the experiment described above. We also implemented a web client (Firefox 85.0.1) on Host1 and a web server (Apache 2.4.41) on Host2 and Host3. Here, Host2 and Host3 acted as a legitimate and spoofed web servers, respectively. In VR1, a dummy malware-program and a dummy malicious-route were added to the initial programs and the initial forwarding routes, respectively. On the other hand, VR2 was configured clean without such dummies.

Host2 and Host3 were assigned the same IP address (192.168.1.1/255.255.255.0), while their MAC addresses are different from each other (1c:69:7a:6e:f9:4d and 1c:69:7a:6f:41:9d). The forwarding tables of VR1 (tainted) and VR2 (clean) were configured statically to resolve 1c:69:7a:6f:41:9d (Host3: the spoofed web server) and 1c:69:7a:6e:f9:4d (Host2: the legitimate web server) from 192.168.1.1, respectively.

In the first stage, VR1 and VR2 acted as the master and backup, respectively. In this initial state, Host1 (the web client, 192.168.0.1) intended to access Host2 (the legitimate web server, 192.168.1.1). However, it actually accessed actually Host3 (the spoofed web server, 192.168.1.1). This is because the forwarding table of VR1 (the current master VR) has been tampered with due to the emulation of malware infection. In this stage, a dummy malware-program file and a dummy forwarding-route (from 192.168.1.1 to 1c:69:7a:6f:41:9d) were detected by means of SSH access to the hardware router.

In the second stage, the master VR1 and backup VR2 were exchanged with each other. Accordingly, Host1 (the web client, 192.168.0.1) accessed Host2 (the legitimate web server, 192.168.1.1) as intended. In this stage, either a dummy malware-program file or a dummy forwarding-route is not detected. On the other hand, the legitimate forwarding route (from 192.168.1.1 to 1c:69:7a:6e:f9:4d) was detected. This is because the master router was initialized by the VR exchanging, and its forwarding table had not yet been tampered with malware.

After completing VR exchanging, by means of disconnecting VR1 (the new backup router) from the system, the dummy malware-program and the dummy forwarding route can be completely removed from the system. The discon-

Table 4 Experiment of the conventional scheme

Step	Operation		Result		Comment
	VR1	VR2	VR1	VR2	
1	Setting priority level: 255	Setting priority level: 254	Master	Backup	The initial state
2	-	Changing priority level: from 254 to 255	Backup	Master	Unstable VR exchanging
			Master	Backup	

Table 5 Experiment of the proposed scheme

Step	Operation		Result		Comment
	VR1	VR2	VR1	VR2	
1	Setting priority level: 254	Setting priority level: 253	Master	Backup	The initial state
2	-	Changing priority level: from 253 to 255	Backup	Master	Stable VR exchanging
3	Changing priority level: from 254 to 253	-	-	-	Emulating VR1 initialization
4	-	Changing priority level: from 255 to 254	-	-	Preparation for repetition
5	Changing priority level: from 253 to 255	-	Master	Backup	Stable VR exchanging
6	-	Changing priority level: from 254 to 253	-	-	Emulating VR2 initialization
7	Changing priority level: from 255 to 254	-	-	-	Returning to the initial state

nected VR1 should be initialized immediately. In place of this initialization, a newly created VR can be added as a new backup router.

Immediately after a malware infection, a web client may access the spoofed web server unintentionally. In order to mitigate this damage, the interval of VR exchanging should be shortened. However, a too short interval may increase the processor's load and thus decrease packet-forwarding throughput. Consequently, optimizing this interval is our important issue. Regardless of this optimization, our scheme still needs to be used together with the conventional malware detection approaches.

In addition, our basic exchanging scheme does not inherit dynamic forwarding routes generated by the routing protocol from the old master router. In order to solve this problem, we have also proposed an additional routing processing function [13]. Its experimental evaluation is also our important issue.

4. Conclusion

In this paper, for achieving router metabolism, we evaluated our repetitive router-exchanging scheme through three experiments. In the first experiment, the master virtual router was exchanged with the backup one. They were exchanged within 1 millisecond by means of the VRRP's priority control. By using this exchanging, a hardware router can be initialized almost in a hitless manner. In the second experiment, the router's priority level was suppressed below the upper limited level through the periodical priority control. This means that the hitless initialization of a hardware router can be repeated semi-permanently. In the third experiment, by means of exchanging virtual routers those composing the hardware router, both the dummy malware-program and the dummy forwarding route were removed practically from the router. This effect can also be expected even for undetectable malware programs. As the results of those three experiments, we can say that router metabolism is promising as one of the countermeasures against malware.

Acknowledgement

The experiments were assisted by Yu Tamura of Tokai University. This work was supported by JSPS KAKENHI Grant Number JP19K11948.

References

[1] A. Sood et al., "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," IEEE Security & Privacy, vol.11, no.1, pp.54-61, Jan. 2013.
[2] N. An et al., "Behavioral anomaly detection of malware on home routers," 2017 12th International Conference on Malicious and Unwanted Software (MALWARE), pp.47-54, Oct. 2017.
[3] A. Stasinopoulos et al., "The weakest link on the network: Exploiting ADSL routers to perform cyber-attacks," IEEE International Symposium on Signal Processing and Information Technology, pp.000135-000139, Dec. 2013.
[4] K. Gajera et al., "A Novel Approach to Detect Phishing Attack Using Artificial Neural Networks Combined with Pharming Detection," 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), pp.196-200, Jun. 2019.
[5] P. O'Kane et al., "Obfuscation: The Hidden Malware," IEEE Security & Privacy, vol.9, no.5, pp.41-47, Sep. 2011.
[6] E. M. Rudd, et al., "A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions," IEEE Communications Surveys & Tutorials, vol.19, no.2, pp.1145-1172, Apr. 2017.
[7] U. Anwar et al., "Performance Analysis and Functionality Comparison of FHRP Protocols," ICCSN 2019, pp.111-115, Jun. 2019.
[8] Y. Miyaoka et al., "A repetitive router-switching scheme for achieving a metabolic router," ICETC 2020, D1-2, Dec. 2020.
[9] M. Rosenblum et al., "Virtual machine monitors: current technology and future trends," IEEE Comp. Mag., vol.38, no.5, pp.39-47, May. 2005.
[10] "VyOS - Open source router and firewall platform," https://vyos.io/, Jan. 23, 2021.
[11] "IEEE 802.1d ethernet bridging - Browse Files at SourceForge.net," https://sourceforge.net/projects/bridge/files/, Jan. 23, 2021.
[12] T. Ylonen et al., "The secure shell (SSH) protocol architecture," IETF RFC 4251, Jan. 2006.
[13] Y. Tamura et al., "A route inheriting scheme for maintaining dynamic routes cleanly in a metabolic router," ICETC 2020, D1-3, Dec. 2020.