Proposal of a detection method for SSH attack based on SYN packets transmission interval

Tomoya Kotone[1] Naomi Nakamoto[2] Minoru Ikebe[2] Kazuyuki Yoshida[3]

Abstract: A dictionary attack against SSH service is a common security threat. Detecting these attacks is a crucial activity. We have been developed a SSH password cracking detection system called "*SCRAD*." *SCRAD* detects attackers based on packet counts per connection using all SSH packets. However, *SCRAD* has two issues. At first, *SCRAD* becomes heavy workload due to check all SSH packets. Second, *SCRAD* failed to detect attacker in some cases. The causes of false negative were the difference of authentication times and the kinds of sender's OS. Therefore, we propose a new lightweight SSH password cracking detection system called "*SCRAD-LW*." *SCRAD-LW* detects attackers based on SYN packets transmission interval. In this paper, we consider two parameters "*T*" and "*k*" for detection thresholds. "*T*" is a period time and "*k*" is a number of SYN packets within *T* seconds. *SCRAD-LW* calculates the variance of SYN packet transmission interval when SYN packets are over *k* times within *T* seconds. We evaluate DR (Detected Rate), FPR (False Positive Rate) and FNR (False Negative Rate) in each parameter value. As a result, *SCRAD-LW* can detect in the data amount of one tenth of *SCRAD*. Therefore, *SCRAD-LW* is more light workload than *SCRAD*. And, *SCRAD-LW* detects all attackers which *SCRAD* fails to detect.

Keywords: SSH, password cracking, SYN packet, transmission interval

1. Introduction

A lot of information is handled on the network with spread of the Internet. We use various services as E-commerce, E-mail services and administrative proceedings on the Internet. Therefore, the Internet is important role in our life. But, there are many anomalous communications in the Internet. For example, scan attack is the process of identifying active hosts and listening ports on target network. Therefore, we have been developing a "intrusion detection system"[1]. Our IDS system detects many scan attacks to port 3389(RDP), 1433(SQL over TCP) and 22(SSH). Attackers discover hosts to serve the above-mentioned ports. However, the attackers perform SSH brute force attacks or denial-of-service (DoS) attacks with SSH hosts. Our campus network denies the inbound packets of RDP and SQL over TCP by firewall. On the other hand, our network allows SSH packets from the Internet for the convenience. However, if an attacker took the password of a SSH server by SSH brute force, the attacker abuses the SSH server. In fact, we observed the scan attacks and the password cracking attacks to SSH servers in Oita University. For the above reasons, it is important to defend the SSH servers from scan attacks and password cracking attacks.

The SSH protocol supports some authentication methods. The typical authentication method is "password authentication" and "public key authentication." The password authentication method is the simplest one. The user specifies the username and corresponding password. Such authentication lets the user have only one set of credentials necessary for authentication. Thus, the public key authentication method uses public key and private key of the client. This authentication method is better safe. But, default authentication method is password authentication. And, normal users tend to use default setting.

In addition, if a host infected with a bot in the campus network, the host tries to crack the password to the other host in inside and outside network. Thus, it is important to detect the attackers in the inside and the outside of the network.

Therefore, we have been developing SSH password cracking detection system called "*SCRAD*(SSH password CRacking Attack Detection system)[2]." *SCRAD* detects attackers based on SSH packet counts per connection.

However, *SCRAD* has two issues. At first, *SCRAD* becomes a heavy workload due to check all SSH packets. Second, *SCRAD* failed to detect attacker in some cases. Therefore, we propose a new lightweight SSH password cracking detection system called "*SCRAD-LW*." *SCRAD-LW* detects attackers based on SYN packets transmission interval.

In the remainder of this paper, we describe related work about detection SSH dictionary attacks in Section2. Section3 describes the overview of *SCRAD-LW* and a detection algorithm. And, we describe two thresholds for detection of attackers. In Section 4, we evaluate DR(Detected Rate), FPR(False Positive Rate) and FNR(False Negative Rate) in our proposed system. Section 5 summarizes this paper and describes future works.

2. Related work

SSH password cracking attacks have been detected in two ba-

[1] Course of Computer Science and Intelligent Systems, Graduate School of Engineering, Oita University
[2] Department of Computer Science and Intelligent Systems, Faculty of Engineering, Oita University
[3] Center for Academic Information and Library Services, Oita University

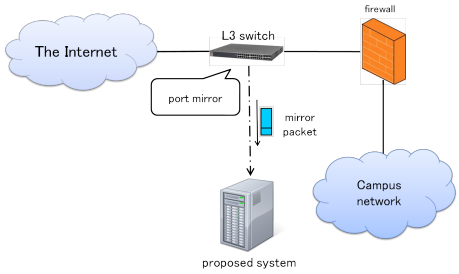

Fig. 1 SCLAD-LW system overview

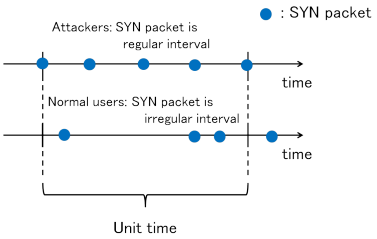

Fig. 2 Transmission interval about SYN packet of normal user and attacker

sic ways that rely on either log files or network traffic.

One of approaches, Takemori et al.[3] proposed a detection method based watching DNS queries log. The system detects attackers who appear many times per unit time in DNS queries log. However, the system is difficult to detect attackers immediately.

The other approach, Sato et al.[4] proposed a detection method based on network traffic. They focused on "existence of a connection protocol" and "difference in the inter-arrival time of an authentication-packet." The system is able to detect individual attacks and distinguish between success and failure of attack. And, the system can detect attackers existing in/out the LAN. However, the workload of the system is heavy. Because, the system has to check state of SSH connection flow from SSH packets excepting control packets which have no payload.

3. Proposed system

We propose a lightweight SSH password cracking detection system called "*SCRAD-LW*." *SCRAD-LW* detects attackers based on the transmission interval of SYN packets.

3.1 Problems of *SCRAD*

We have been developed a SSH password cracking detection system called "*SCRAD*[2][5]." *SCRAD* uses patricia tree[6] to store sender's information. And, *SCRAD* detects attackers based on SSH packet counts per connection. The detection threshold value is less than 45 packets per connection. A detection rate of *SCRAD* is approximately 87%.

However, *SCRAD* has two issues.

(1) Heavy workload.
SCRAD detects attackers based on SSH packet counts per connection. Then, *SCRAD* has to check all kinds of SSH packets for TCP flags (FIN, SYN, RST, PSH, ACK, URG) and update state and packet count in patricia tree every time. Therefore, packet-handling process is heavy.

(2) False negative in some cases
In some cases, the number of attacker's packets was exceeded the threshold for *SCRAD* slightly [5]. We investigated these attackers. As a result, authentication time of these attacker is more than default times. Therefore, the number of packet is more than we had expected.

3.2 Overview

SCRAD-LW collects SSH packets from border layer-3 switch that is outside of firewall in campus network (Figure1). In addition, our system collects only SYN packet of SSH using tcpdump[7] from mirroring packets and uses patricia tree to store sender's information. *SCRAD-LW* has to update inter-arrival time and packet count in patricia tree when the system observes a SYN packet.

3.3 Detecting Algorithm

We focus on the difference in SYN packet transmission interval between the attackers and normal users (Figure2). We suppose that the attackers performs the attacks (e.g. scan attacks and brute force attacks) to SSH server periodically using programs. Thus, transmission interval of SYN packets from attackers becomes uniform. Moreover, if password authentication is failed, the attacker reconnects to the SSH server repeatedly. Thus, the attackers sent a large number of SYN packets.

On the other hand, transmission interval of SYN packets from the normal users becomes not uniform. Because, normal user connect to SSH server when they needed. And, the normal user tends a few number of SYN packets.

The SYN packets transmission interval of automated task through SSH (e.g. SCP) becomes uniform. We compared the number of SYN packets of automated tasks through SSH with attackers. The number of SYN packets of automated tasks through SSH was less than the number of SYN packet of attackers. Therefore, our system can distinguish between the automated tasks through SSH and the attackers.

We investigated the packet data of the attackers detected by *SCRAD* as a preliminary experiment. And, we calculated the variance of the transmission interval of the each attacker and normal user. An investigation period is 18 days from July 4th to July 21st, 2013.

We define t_i $(i = 0,1,...,n)$ which is a receiving time of i th SYN packet received from each sender. Then, the transmission interval (x_i) expresses $t_i - t_{i-1} (i = 1,2,...,n)$ (sec). We calculated the variance of the transmission interval of the SYN packets per sender (V).

Figure 3 shows the variance of SYN packet arrival interval from each attacker. The variance values of below 73 were 70% of the all attackers. Moreover, we observed attackers who variance value is over 73. The attacker had sent SYN packets for some time (Figure 4). We confirmed interregnum between the attack and the attack in the attackers. Therefore, we investigated the above attacker's variance at one attack. The variance was below 73 at once attack.

Figure 5 shows the variance of SYN packet arrival interval from each normal users. As a result, the variance of each normal users greatly exceeded 73. Thereby, we were able to distinguish

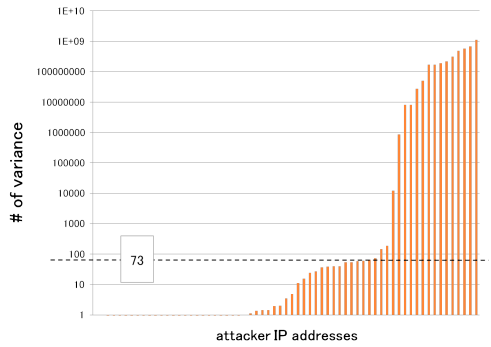

Fig. 3 The variance of transmission interval of SYN packet received from each attacker

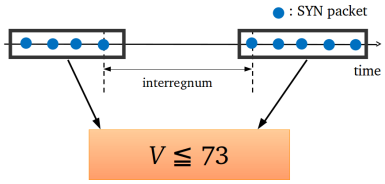

Fig. 4 Interregnum between attack and attack

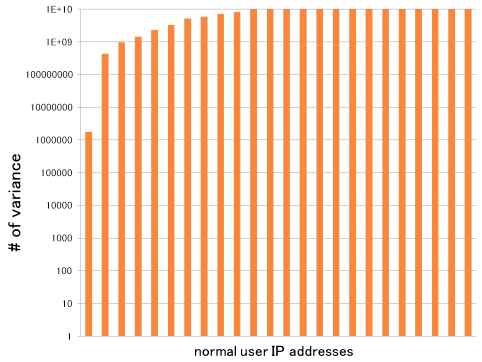

Fig. 5 The variance of transmission interval of SYN packet received from each normal user

Table 1 Operational result of a number of attackers and normal users

	attackers	normal users
SCRAD	21	29
real value	24	26

attackers and normal users using the difference of SYN packets transmission interval.

We decide our detection algorithm (Figure 6). *SCRAD-LW* calculates the variance of SYN packet transmission interval when SYN packets are over k within T sec. If the variance is less than 73, *SCRAD-LW* detects that host as an attacker.

3.4 Features of *SCRAD-LW*

Three benefits of *SCRAD-LW* are as follows.

(1) *SCRAD-LW* collects both incoming and outgoing SSH packets from border layer-3 switch. Thus, *SCRAD-LW* can detect attackers existing in/out the LAN.
(2) *SCRAD-LW* can detect attackers immediately.
(3) *SCRAD-LW* is more light workload than *SCRAD*.
(4) *SCRAD-LW* independents from authentication times and kind of OS.

```
P_Tree source, attacker;

void analyze(char *packet){
 long ctime = current_time();
 P_Tree *N = getNode(getSrcIP(packet), source);
 if(N==null) N=addNode(getSrcIP(packet), source);

 N->cnt++; N->sum += ctime - N->lasttime;
 N->ssum += pow((ctime - N->lasttime), 2.0);
 N->lasttime=ctime;
 if(N->cnt >= k && varriance(N) <= 73) detect(N, attacker);
}
/*_____________________________________________________*/
/* alarm_handler startup every 60 seconds */
void alarm_handler(){ checkTimeOut(attacker); }

void checkTimeOut(P_Tree *N){
 if(N != null){
   checkTimeOut(N->left); checkTimeOut(N->right);
   if(current_time() - N->lasttime >= T){ delete(N); }
 }
}
```

Fig. 6 Algorithm of SCRAD-LW using pesudo code

4. Evaluation

4.1 Packet data

We capture whole SSH packets from border layer-3 switch in campus network (figure1). Collecting period is 7 days from July 22nd to July 28th, 2013. The whole SSH packets was 22,379,631 packets. SYN packets was 2,256,289 packets out of the whole SSH packets. *SCRAD* uses the whole SSH packets for detection. However, *SCRAD-LW* can detect attackers using only SYN packets. Therefore, *SCRAD-LW* is one tenth of the amount of data in *SCRAD*. Consequently, the number of update for patricia tree declined one tenth than SCRAD's one.

4.2 Operational results

In this experiment, *SCRAD-LW* used the above packet data while setting each detecting parameter (T and k). T (sec) is a period time and k is a number of SYN packets within T. We calculates variance of each host. Table 1 shows a number of attackers and normal users that detected by *SCRAD* during 7 days. *SCRAD* distinguished 3 hosts as normal users. However, these hosts connected to SSH server repeatedly in a short term[5]. The behavior of these hosts is similar to the behavior of attackers. Then, we judged these hosts as attackers. After that, we compared real value with the table 1.

4.2.1 Evaluation metrics

In this paper, we evaluate each threshold using three metrics (Detection rate, False positive rate and False negative rate). Table 2 shows a relationship between a number of attackers and normal users in *SCRAD* and *SCRAD-LW*.

Table 2 A relationship between a number of attackers and normal users in two systems

		SCRAD-LW	
		attackers	normal users
real value	attacker	TP (Correct result)	FN (Unexpected result)
	normal user	FP (Missing result)	TN (Correct absence of result)

Table 3 experimental result

(a) detection result of each threshold

		the number of SYN packet : k			
		5	7	10	12
detection period : T(sec)	75	1.00	0.86	0.62	0.62
		0.02	0.00	0.00	0.00
		0.00	0.14	0.38	0.38
	150	1.00	0.90	0.71	0.67
		0.02	0.00	0.00	0.00
		0.00	0.10	0.29	0.33
	225	1.00	0.90	0.71	0.67
		0.02	0.00	0.00	0.00
		0.00	0.10	0.29	0.33
	300	1.00	0.90	0.71	0.67
		0.02	0.00	0.00	0.00
		0.00	0.10	0.29	0.33

(b) table format

	the number of SYN packet : k
detection period : T(sec)	Detection rate (DR) False positive rate(FPR) False negative rate(FNR)

$$DR = \frac{TP}{TP+FN}\ ,\ FPR = \frac{FP}{TP+FP}\ ,\ FNR = \frac{FN}{TP+FN}$$

- Detection Rate (DR) – DR is a rate of detected attackers on *SCRAD-LW* among the total number of attacker.
- False Positive Rate (FPR) – FPR is a rate of detected normal users as attackers on *SCRAD-LW* incorrectly among a number of hosts detected on *SCRAD-LW*.
- False Negative Rate (FNR) – FNR is a rate of not detected attackers on *SCRAD-LW* among the total number of attacker.

4.3 Evaluation result

In this experiment, we use T with 75, 150, 225, 300 seconds in a period time. And, we use k with 5, 7, 10, 12 in each T.

Table 3(a) shows detection result of each threshold. And, table 3(b) shows a format of Table 3(a). Detection rate is shown at the top of the frame. And, false positive rate and false negative rate are shown center and below of the frame respectively.

4.4 Discussion

4.4.1 Detection rate

The detection rate does not appear the difference in T is 150, 225 and 300 sec. However, the detection rate in 75 sec was lower than the others. We describe cause of failure detection later.

The detection rate decreases with increasing k. In the case of $k = 5$, *SCRAD-LW* was able to detect all attackers who failed to detect by *SCRAD*. *SCRAD-LW* focused on the arrival interval of SYN packet from SSH client. Therefore, *SCRAD-LW* does not depend on the difference of authentication times and the kind of OS of attackers.

4.4.2 False positive

In the case of $k = 5$, the false positive occurred regardless of T. Then, we investigated log files of *SCRAD-LW*. The all connections of false positives were same source IP address. Moreover, the above host had sent some SYN packets from our campus network. We extracted the above host's packets from whole SSH packets. As a result, the host sent 6 SYN packets in a short term. The above host communicated relay server of VPN (Virtual Private Network). We are currently investigating the behavior of the above host.

4.4.3 False negative

We found false negative in $T = 75$ and $k = 7$. The attacker transmitted a SYN packet to target host every 13 seconds. The attacker sent 23 SYN packets in total. Then, *SCRAD-LW* observed 5 SYN packets within 75 seconds. Therefore, the behavior of attacker do not satisfied *SCRAD-LW*'s detection threshold in $T = 75$ and $k = 7$.

In addition, we found false negative in $T = 300$ and $k = 10$. *SCRAD-LW* observed 7 SYN packets from the attacker at 18:00 on July 28. After that, *SCRAD-LW* observed 7 SYN packets again at 9:00 on July 29. The attacker sent only 7 SYN packets within 300 sec. Therefore, *SCRAD-LW* failed to detect this attacker.

4.5 Validation

In this experiment, *SCRAD-LW* does not appear the difference of the detection rate in T is 150, 225 and 300 sec. However, the detection rate in 75 seconds was lower than the others. Thus, we decide 150 seconds for the detection term.

In addition, the false negative rate declines when k is decreased. Then the false positive rate is rising. In fact, the false positive occurred in *SCRAD-LW* when k was 5. Thus, we decided 7 SYN packets within 150 for detection parameter.

5. Conclusion

In this paper, we proposed a lightweight method to detect SSH password cracking attacks based on SYN packets transmission interval. *SCRAD-LW* improves the two issues of *SCRAD*. We decided two parameters (T and k) for detection thresholds. We evaluate DR, FPR and FNR in each parameter. As a result, *SCRAD-LW* can detect in the data amount of one tenth of *SCRAD*. And, *SCRAD-LW* detects all attackers who false negative of *SCRAD*. However, there are wrong detection in some cases.

In our future work, we operate *SCRAD-LW* in the long term with decided parameters in this paper. Moreover, it is necessary to block the attacker whom *SCRAD-LW* detected.

References

[1] Kotone, T., Amamoto, D., Ono, Y., Arima, T., Ikebe, M. and Yoshida, K.: Study for the behavior of detected host using the scan attack detection system (In Japanese), *The 65th Joint Conference of Electrical and Electronics Engineers in Kyushu*, pp. 278–278 (2012).

[2] Kotone, T., Amamoto, D., Ikebe, M. and Yoshida, K.: Development of a detection system for the SSH password crack attacks and its operational results (In Japanese), *Multimedia, Distributed, Cooperative and Mobile Symposium(DICOMO) 2013*, pp. 742–748 (2013).

[3] Takemori, K., Romana, D.A.L., Kubota, S., Sugitani, K. and Musashi, Y.: Detection of NS Resource Record DNS Resolution Traffic, Host Search, and SSH Dictionary Attack Activities, *International Journal of Intelligent Engineering and Systems*, Vol. 2, No. 4, pp. 35–42 (2009).

[4] Satoh, A., Nakamura, Y. and Ikenaga, T.: SSH Dictionary Attack Detection based on Flow Analysis, *2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet*, pp. 51–59 (2012).

[5] Nakamoto, N., Kotone, T., Ikebe, M. and Yoshida, K.: Improvement for detection threshold of SSH password crack attacks (In Japanese), *The 66th Joint Conference of Electrical and Electronics Engineers in Kyushu*, pp. 441–441 (2013).

[6] D. R. Morrison: PATRICIA–Practical Algorithm To Retrieve Information Coded in Alphanumeric, *Journal of the Association for Computing Machinery*, Vol. 15, No. 4, pp. 514–534 (1968).

[7] tcpdump: http://www.tcpdump.org/.