Dynamic Security Policy Control for Protecting LAN from Attacks by Insecure Internal Network Devices

Yutaka Juba
Ritsumeikan University
1-1-1, Noji-Higashi, Kusatsu,
Shiga 525-8577, JAPAN
yutaka@
coms.ics.ritsumei.ac.jp

Hung-Hsuan Huang
Ritsumeikan University
1-1-1, Noji-Higashi, Kusatsu,
Shiga 525-8577, JAPAN
huang@fc.ritsumei.ac.jp

Kyoji Kawagoe
Ritsumeikan University
1-1-1, Noji-Higashi, Kusatsu,
Shiga 525-8577, JAPAN
kawagoe@is.risumei.ac.jp

1. INTRODUCTION AND MOTIVATION

There are varieties of network devices, recently used at home by connecting to the Internet, including printers, cameras, TVs, Network access storage in addition to the indispensable devices, such as network routers. These devices are mainly developed based on existing OS and middle-wares. For example, Linux, ITRON, and Windows are the top three operating systems used in embedded software incorporated in the network devices. It was reported by MITI Japan in 2010 that 60% of the network protocol implementations used in such devices were developed based on existing middleware components. Therefore, network devices strongly depend on existing softwares developed by other software vendors.

There is one crucial problem on network devices caused by use of other dependent software components, which is its vulnerability of the software in network devices [1]. A network devices containing vulnerability is easily attacked and is controllable by an attacker, which means that the attacker can use it as a springboard to attack another computer within the same network. The vulnerability problem occurs easily because they tend not to be updated frequently.

Juba et al. proposed the architecture for solving the vulnerability problem by introducing OpenFlow based network configuration reconstruction and several security policies [2]. Their points on the proposed architecture and method are 1) isolating an insecure network device, soon after the device can be detected as insecure one and 2) introducing five kinds of security policies. All the intra-LAN transmissions are monitored and checked by IDS (Intrusion Detection System). Once an insecure network device is identified with the IDS, the device can be isolated from the LAN immediately. The rapid isolation of such a device is important to keep the network secure from further attack. Security policies are proposed to enable a network administrators to specify a balance between the network performance and the security level.

In their proposed architecture and method, there is one important problem, which is that the network administrator is difficult to specify a balance between the performance and the security level. The administrator needs to specify the policy by himself/herself, judging from the current LAN traffic condition. When the administrator selects an inappropriate security policy, either network performance or the security level significantly deteriorates. For example, if an administrator selects a performance oriented policy, it was measured that the time necessary for isolation of an insecure device is 565.2msec at most. In this policy, the maximum network speed reaches 95.0Mbps in 100Mbps LAN. On the contrary, if the administrator selects a secure oriented policy, the time necessary for device isolation decreased to 66.0% (373.0msec at most) of the speed in the high performance policy. The maximum network speed also decreased to 68.4% (65.0Mbos).

Therefore, it is very difficult for a network administrator to select an appropriate security policy. He/she may consider to keep the LAN secure at the cost of performance deterioration while the current LAN may be in a situation when no attacks are observed. There is a possible situation when a DDoS attack within LAN happens in the high-performance policy, because many attacks can be done within the longer time period from an insecure device attack to the device isolation.

2. CONTRIBUTION

In this paper, we propose a method to dynamically control security policies for protecting LAN from attacks by insecure network devices, based on the architecture proposed by Juba et al.[2]. In our proposed method, the network condition is taken into considerations based on the amount of LAN traffic and alerts from IDS. Depending on the current network condition, the most appropriate security policy can be selected and adapted. With our proposed method, both the time to the network device isolation and loss of throughput can be reduced.

The main contributions of this paper are 1) we propose a novel method to dynamically control security policies using score-based and rule-based algorithms, and 2) a better balance of security quality level and network performance overhead is attained compared with those in manual selection of the security policy [2].

The dynamic control of security policies is to dynamically change the security policy by recognizing the conditions of both network devices and LAN from security stand points. The statistical information from the OpenFlow Protocol or by alerts from the IDS are used to estimate the conditions. We introduce two control algorithms methods: score-based and rule-based algorithms to realize the dynamic security policy control.

In the score-based algorithms, a score is calculated as a function of amount of transferred data for each network device. The score is defined as the amount of transferred data. If the score becomes less than a thresholds, then the high-performance policy is selected. On the contrary, if the score becomes greater than another thresholds, the high-secured policy is selected. Improvement in network performance can be obtained by this score-based algorithm.

In the rule-based algorithm, alerts from IDS are used to control policies. Rules can be prepared beforehand constructed from pairs of critical levels and types of alerts, using a machine learning method. When a new alert from the IDS is received, then rules are evaluated, followed by changing

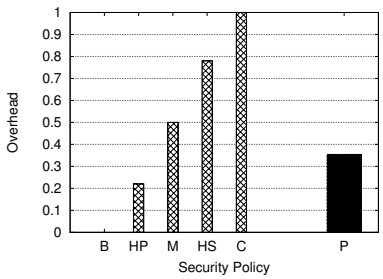

Figure 1: Overhead for various policies and our dynamic control method (right).

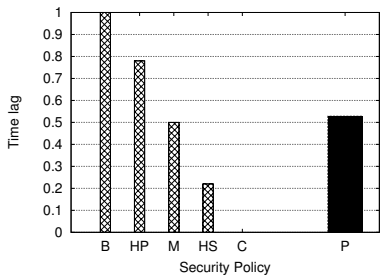

Figure 2: Time lag for various policies and our dynamic control method (right).

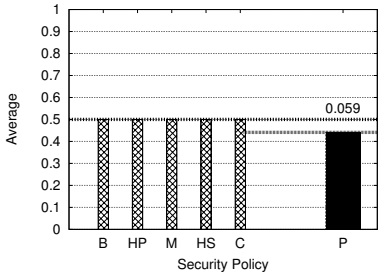

Figure 3: Average of harmonic means of overhead and time lag results for various policies and our dynamic control method (right).

Figure 4: Results. (B: BASIC, HP: HIGH PERFORMANCE, M: MEDIUM, HS: HIGH SECURED, C: COMPLETE, P: the proposed method)

policies depending on the result of rule evaluations.

We can continuously and strictly monitor LAN throughput. Therefore attacks by insecure network devices can be early detected using the score-based algorithm. Early detection of attacks by network devices should be necessary, because we can quickly isolate the detected devices from LAN. Because information from the IDS is also important to keep the LAN secure, the rule-based algorithm can be effective in dynamically changing the LAN from performance orientation to secure orientation, and vice versa.

Both algorithms can be processed in parallel. In the score-based algorithm, policies can be regularly changed, while the rule-based algorithm can modify policies every time having alerts. In a secured situation, the score-based algorithm can enhance throughput rate, although the rule-based algorithm can better enhance keeping secured in a critical situation.

We conducted experiments to verify relationships between LAN performance and security policies including our dynamic security control method.

3. PRELIMINARY EVALUATIONS

We set up experiment environment as follow: 1) Open vSwitch is used as a software-based virtual network switch. 2) Debian GNU/Linux 6.0 is run on an HP ML110G7 (Xeon R31220 3.1GHz, 8GB of memory). KVM is used to conduct our experiments in virtual environment. Twenty virtual machines were initiated, including four virtual machines for IDSs. The LAN speed is set to 100Mbps. 3) Snort, an open source intrusion prevention and detection system is used as IDS. Although Snort supports the state-full inspection capability, any other IDS can be used instead of Snort. The IDS is used only as a function of sending all the received packets to it and receiving alerts from it. 4) OpenFlow Controller is used to change network configuration. The POX library is used for OpenFlow Controller development. 5) Our experimental system is written in Python. 6) In the score-based algorithm, $W = 0.7$. 7) In the rule-based algorithm, a set of rules are constructed using Naïve Bayes. 8) Used security polices (in order of security oriented): COMPLETE, HIGH SECURED, MEDIUM, HIGH PERFORMANCE and BASIC[2].

The basic measures for evaluation are 1) packet inspection overhead, 2) time lag between the detection of the attack and the system performance. Our experiments use iperf to carry out simulated attacks, and to calculate differences in two cases: the security policy is fixed, and security policy is modified dynamically. In our experiments, tests with total 32 patterns were conducted, which consist of variations on traffic throughput and attack timings. The harmonic mean of the results of the 32 patterns, after normalized by the result in the case of BASIC policy overhead, is calculated.

The results are shown in Fig.2 Fig2.(a) shows the overhead for the proposed control and the static controls. From this figure, our dynamic security policy control overhead is almost in the center between the cases of MEDIUM and HIGH PERFORMANCE. Fig2.(b) shows the time lag for the proposed control and the static controls. From this figure, the time lag of our method is smaller than the cases of BASIC and HIGH PERFORMANCE. Fig2.(c) shows the average value of the harmonic means of the time-lag and the overhead, for the proposed control and the static control cases. It can be seen that the average values of the proposed method was 0.059 smaller than those of all the static control methods. Form these results, it can be confirmed that we achieved smaller time lag and overhead on average, comparing with the cases of the static policies.

4. CONCLUSION AND FUTURE WORK

In this paper, we propose a method of dynamic security policy control for protecting the LAN from attacks by insecure network devices. The points of our contribution on the proposed method are 1) we propose a novel method to dynamically control security policies using score-based and rule-based algorithms, and 2) a better balance of security quality level and network performance overhead is attained compared with those in manual selection of the security policy [2]. From the experiments, it is confirmed that our dynamic policy control works better than manually specified policy control. Our future work includes implementation of the proposed method and evaluation by field experiments.

5. REFERENCES

[1] IPA, Reporting Status of Vulnerability-related Information about Software Products and Websites. http://www.ipa.go.jp/files/000018135.pdf

[2] Y. Juba et al. 2013, Dynamic Isolation of Network Devices Using OpenFlow for Keeping LAN Secure from Intra-LAN Attack, KES2013, Sept., 2013.