LL-004

Providing Security Information of Mobile Networks using Personal IDS

Yusuke Azuma† Naohiro Obata† Nobutaka Kawaguchi†
Hidekazu Shiozawa‡ Hiroshi Shigeno† Kenichi Okada†

1. Introduction

In mobile network services such as hot spot services, many anonymous users including malicious ones share a network and it may cause security threats.

The security information of the mobile networks (*e.g.* the information about the existing attacks and worms in the networks) is the important factor to find the networks the users can access to safely. However most networks do not provide such information to the users.

Therefore in this paper, we propose a security information provider service of mobile networks. Our service provides security information by collecting and analyzing logs from Personal IDS connected to the networks. As a result our service enables to find the safe networks without relying on official information from the networks.

2. Background

Staniford *et. al.* stated the need of gathering and analyzing the logs from IDS positioned in various networks to measure the anomalies of networks and detect the propagation of worms at an early stage [1]. Log Analyzing System for IDS [2] computes the anomaly of logs for short time interval by comparing them to the logs for long time interval. And logs from an analyzed network are also compared to the logs from the other networks to compute the anomaly. We analyze logs using a similar algorithm to compute the degree of safety of the mobile networks.

3. Security Information Provider Service

3.1 Concept

In this section, we propose a service that provides security information for users by collecting and analyzing logs from Personal IDS. Since there are a few mobile networks that provide the security information to users, it is difficult to verify the degree of safety of most networks until the users actually access to them. We address the problem by gathering the logs from Personal IDS installed in client hosts in various mobile networks and analyze them. Today, many users use personal security softwares that include an IDS module for personal use and we use the IDS to get the information without relying on the official information from the mobile networks.

Our service provides the following two security information to the users.

- The safe mobile networks positioned near the user
- The security conditions required to connect to a network safely

We define an *anomaly score* as the degree of safety of each network. As the score is higher, the safety of network is considered to be lower. We also define a *vulnerability matching* as the matching between the existing attacks in each network and the vulnerabilities of users hosts to provide the information about the attacks exploiting the vulnerabilities and the way to prevent the attacks to the users.

The details of anomaly score and vulnerability matching are described in later sections.

3.2 Service Protocol

Figure 1 shows the protocol used in our service.

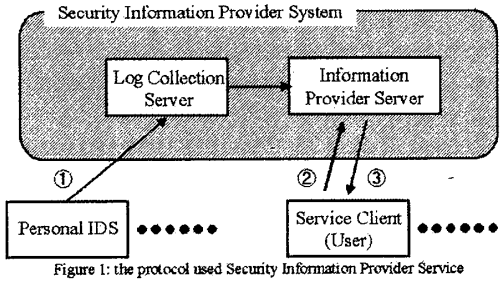

Figure 1: The protocol used in Security Information Provider Service

1. Each Personal IDS periodically sends its logs and the identity of the network it resides to, to the Log Collection Server. The Log Collection Server, which receives the logs from IDS connected to various mobile networks, analyzes those logs and computes the anomaly score of the networks.
2. The Information Provider Server is accessed from the Clients. The Client sends its location and attributes such as the OS version and settings. The Server performs the vulnerability matching using the information.
3. The Information Provider Server returns the anomaly score and the result of vulnerability matching to the Client. The Client finds the safe networks near the client or changes the security level using the information to connect to a network safely.

†Faculty of Science and Technology, Keio University
‡Faculty of Technology, Tamagawa University

3.3 Anomaly Score

The Log Collection Server computes the anomaly score of each network. There are two kinds of anomaly scores; a *network − line based anomaly score* and *time − line based anomaly score*.

First, a network-line based anomaly score shows the anomaly of the logs from the analyzed network by comparing to the logs from the other networks. Second, a time-line based anomaly score shows the anomaly of the logs of a network generated in the most recent time interval by comparing to the logs generated in the long time interval.

Network-line based anomaly score

E_{mk} is the number of time that the attack k is detected in the network m, N_{mk} is the number of IDS that send logs of attack k in the network m, and l_k is the threat level of the attack k. The threat level of network m, L_{net_m} is

$$L_{net_m} = \sum_k \left(\frac{E_{mk}}{N_{mk}} \times l_k \right) \quad (1)$$

then, the network-line based anomaly score of network m W_m is

$$W_m = \frac{L_{net_m}}{\left(\sum_l^n L_{net_l}\right)/n} \quad (2)$$

where n is the number of all the networks except the analyzed network m.

Time-line based anomaly score

Network m is the analyzed network. t_{short} is the analyzed short time interval, and t_{long} is the compared long time interval. E_{tmk} is the number of times that the attack k is detected in the time interval t, N_{tmk} is the number of IDS that sends logs of attack k, l_k is the threat level of the attack k. The threat level in time t interval, L_{t_m} is

$$L_{tm} = \sum_k \left(\frac{E_{tmk}}{N_{tmk}} \times l_k \right) \quad (3)$$

then the time-line based anomaly score $T_{t_{short}m}$ is

$$T_{t_{short}m} = \frac{L_{t_{short}m}}{\left(L_{t_{long}m}\right) / \left(\frac{t_{long}-t_{short}}{t_{short}}\right)} \quad (4)$$

3.4 Vulnerability matching

The Information Provider Server matches the existing attacks in each network with the vulnerabilities of the client inferred from its attributes such as the OS version and settings with the existing attacks in each network.

Then, the result of the matching shows the networks, in which the attacks exploiting the vulnerability exist, and the security conditions required to connect to the networks safely such as OS updates and packet filtering.

4. Evaluation

We implemented a prototype system of our service and ran experiments to show the validity of the proposed service.

There are 3 networks (NW 1,2,3) used for the experiments. In each network, 2 hosts with Personal IDS exist. Using the port scan tool *nmap*, we ran TCP stealth scan and UDP scan against the networks, and the network-line based anomaly score and response time are measured.

Result 1 in Figure 2 shows the network-line based anomaly score when only TCP stealth scan is run against the all networks. Result 2 in Figure 2 shows the network-line based anomaly score when UDP scan is run against NW 1 as well as TCP stealth scan.

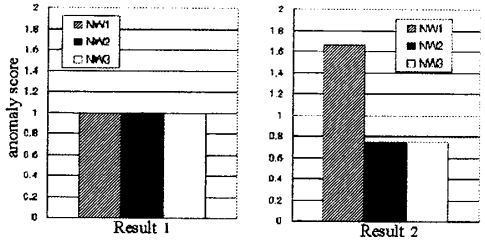

Figure 2: The network-line based anomaly score

The anomaly score of NW 1 becomes bigger than that of the other networks since the number of scans against NW 1 is larger than the number of scans against the other networks. So, we conlude that the network-line based anomaly score appropriately reflects the change of attacks.

Next, the response time of processing user's request is 220 msecs and this should be considered as acceptable.

5. Conclusion

In this paper, we have proposed a security information provider service of mobile network using Personal IDS logs from mobile hosts connected to the networks. Using our service, the users can access to the mobile networks safely without relying on official information from the networks. We showed the validity of our proposed service through the experiments.

Acknowlegment

This work is supported in part by the Applied Security Forum.

References

[1] Stuart Staniford,Vern Paxson,Nicholas Weaver: How to Own the Internet in Your Spare Time,Proceeding of the 11th USENIX Security Symposium(2002).

[2] Keisuke Takemori, Yutaka Miyake, Kouji Nakao, Fumiaki Sugaya, Iwao Sasase: A Support System for Analyzing Log Information of Security Devices Applied to Wide Area Monitoring, Computer Security Symposium, pp. 397–402 (2003).