モバイルネットワークセキュリティ情報提供フレームワーク

川口 信隆[1] 東 雄介[1] 田原 慎也[2] 塩澤 秀和[1] 重野 寛[1] 岡田 謙一[1]

モバイルネットワークにおける問題点の１つに，エンドユーザが利用前にネットワークのセキュリティ状態を知ることが難しいことがある．この問題を解決するために我々はCMSF(Cooperative Mobile Network Security Information Frame Work)を提案する．CMSFでは，実際にモバイルネットワーク内の端末に備わっているIDSからのログをCMSFサーバで集約，解析することでモバイルネットワークのセキュリティ状態を求める．CSMFをベースとしたワーム検知システムの評価により，CMSFの有効性を確認した．

Cooperative Mobile Network Security Information Distribution Framework

Nobutaka KAWAGUCHI[1] Yusuke AZUMA[1] Shinya TAHARA [1] Hidekazu SHIOZAWA[2]
Hiroshi SHIGENO[1] Kenichi OKADA[1]

One of the problems with mobile networks is the lack of security information of the networks. Different from organization and home networks, the security measures and conditions of mobile networks are usually unknown to the end users. To tackle these issues, in this paper, we propose CMSF: Cooperative Mobile Network Security Information Distribution Framework. In CMSF, the CMSF server analyzes logs received by IDS, which are equipped with hosts in mobile networks, and computes the security conditions of the mobile networks. By the preliminary experiments of CMSF based worm detection system, we have confirmed the effectiveness of our framework.

1 Introduction

Today, mobile networks that enable mobile users to connect to the Internet with high-speed has become popular. Many organizations and facilities provide the mobile network services in various locations such as stations, shops, restaurants, airports and so on.

However, different from organization and home networks, users usually do not know the security and management condition of the networks. For example, whether security facilities such as firewalls and IDS are properly managed and whether attacks occur in the networks are unknown to the end users before entering the networks. This is because administrators of the mobile networks usually do not announce the information of the security condition of the networks in real-time.Even if they do, the credibility of such informaion can not be necessarily authenticated for end users. Then, users may enter a network filled with attacks without any prior protections and suffer serious damages.

To tackle the issues, we propose a framework which provides the information of the security conditions of the mobile networks by the cooperation of mobile users. We name this framework CMSF (Cooperative Mobile Network Security Distribution Framework) [1]. the CMSF does not rely on the official announcements from the administrators to obtain the security conditions. Instead, the CMSF accumulates security logs from the personal security modules of end users who actually use the networks, and analyzes the security condition from the logs. Today, due to the improvements of computation powers of PCs, many mobile devices are equipped with the personal security modules such as IDS, anti-virus softwares and personal firewalls. The CMSF utilize the modules and make it possible to track security condition of the networks in real-time. The analyzed results are distributed to users who want to know which networks are secure. The CMSF takes the difference between personal security modules and network IDS managed by administrators into the consideration to compute the reliable results. Using the CMSF, a mobile user can know the security condition of mobile networks and choose the most appropriate network for the user.

As an application of CMSF, we show the CMSF based detection method of network worms that propagate in the mobile networks. Through the computer simulation experiments, the effectiveness of this method is confirmed.

The following sections are organized as follows. In section 2, we introduce related works about Distributed IDS and worms. We propose CMSF in section 3. In section 4, we describe the CMSF based worm detection method. We evaluate the performance of this method in section 5. Section 6 concludes this paper.

2 Related Works

2.1 Distributed IDS

Distributed IDS is a IDS composed of heterogeneous IDS which monitor various points of interest such as networks and hosts. The CMSF is a kind of Distributed IDS since

[1]慶應義塾大学 理工学部 情報工学科
Department of Instrumentation(Information), Faculty of Science and Technology, Keio University

[2]玉川大学 工学部
Department of Faculty and Technology, Tamagawa University

various mobile devices cooperate to evaluate the security condition of mobile networks. Stuart Staniford, et.al. stated the need of aggregation and analysis of the logs from many IDS positioned in various networks for the measurement of the network anomalies and detection of distributed attacks at an early stage [2]. Since then, there have been many works that have modeled the decentralization and cooperation framework of firewall, IDS and any security facilities. DOMINO [3] is a distributed intrusion detection system that enables fast portscan detection by gathering packet logs from various domains. S.Stolfo, et.al. proposed a cooperative distributed intrusion detection system [4].

The most of these works have focused on the cooperation of IDS or firewalls which are managed by administrators of domains. As long as we know, the CMSF is the first work that focuses on the cooperation of personal security modules of end users to analyze the security statuses of mobile networks.

2.2 Worm Detection

Cooperation of detection systems will achieve fast detection and effective containment of worms. Kostas G.Anagnostalis, et.al. proposed a worm immunization framework [5] in which each worm detection agent starts scans only when threat level of worm propagation exceeds a threshold. Jayanthkumar Kannan, et.al. proposed collaborative firewall framework [6] to contain worms in early stage of the propagation.

As mentioned above, these works use the large scale detection systems managed by domain administrators and are different from our work in this point. In addition, although many works [7] [8] have modeled and simulated the propagation of network worms in various environments such as the Internet, enterprise networks and ad-hoc networks, as long as we know, this paper is the first work that focuses on the propagation of worms in the mobile networks.

3 Cooperative Mobile Network Security Information Distribution Framework

3.1 Overview

The objective of the CMSF is to provide mobile users with security conditions of mobile networks by collecting security logs from mobile devices and analyzing them in real-time. We assume mobile networks which are managed by various providers such as HostSpots. The CMSF does not rely on the official announcements from administrators of the mobile networks. This is because the administrators unusually open the information to end users. In addition, the ability of network managements of the administrators are not necessarily reliable. Moreover, in the worst case they themselves might be malicious. Instead, the CMSF obtains logs from users who actually use the networks. Therefore, the CMSF can analyze the condition of the mobile networks independent of the policies and the abilities of the administrators.

In addition, since various users including users who have infected devices enter and leave the mobile networks in turn, the conditions of the networks will change by minutes. Therefore real-time tracking of the conditions is required.

Figure 1 shows the overview of the CMSF. The CMSF has the following three steps.

1. First, personal security modules of user devices in the mobile networks periodically send the security logs to the CMSF Server. The CMSF Server is a server responsible for collecting, analyzing and distributing the results to end user. The CMSF Server is provided and managed by the organizers of the CMSF.

2. Second, On receiving the logs, the CMSF Server analyzes them and computes the security conditions of the mobile networks.

3. Third, users who want to know the security conditions of mobile networks access to the CMSF Server. The CMSF Server returns the analysis results and judges whether the user can use the networks safely by comparing the status of users devices with the attacks detected in the networks.

We will describe the details of each steps in the later sections.

3.2 Generation and Transmission of Security Logs

The first step is the generation and transmission of security logs. Mobile devices equipped with security modules periodically send the security logs that may show the existence of worms, port scans, malicious packets to the CMSF Server. The CMSF Server receives the logs from many users and conducts security analysis.

So, the CMSF needs cooperation of end users. Due to the recent improvements of computation power, many mobile PCs have personal firewall and IDS modules. Users who join the CMSF install the agent program that obtains security logs from the modules and sends them periodically to the CMSF server. Since users use various security modules, the formats of logs will be different for each other. Therefore the agent should convert the formats so that the CMSF server can deal with them. Here, we call a mobile device that joins the CMSF and sends logs as *CMD (CMSF Mobile Device)* and a personal security module run on CMD as *PSM.*

Different from network IDS managed by network administrators, there are the following issues about the reliability and performance of CMD and PSM.

- PSM run on the CMD on which various user applications are active. Some of the applications and services may have vulnerabilities. So, CMD themselves can be the targets of attacks. If CMD is compromised, CMD may send forge logs to the CMSF server to defeat the framework.

- PSM is active only when its CMD is in the network. Therefore, when there is no CMD in a network, security log about the network are not transmitted and the security condition of the network is uncertain.

- The source data that a PSM can use for attack detection are limited since a CMD is usually able to capture only the unicast packets destined for the CMD and broadcast packets and therefore, the detection capability of PSM may be lower than that of network IDS managed by network administrators.

How to deal with these issues is important to make the CMSF robust and reliable. We will show some examples of the solutions in later sections.

In each transmission interval T_{trans}, logs are transmitted from CMD to the CMSF server. The selection of T_{trans} is a tradeoff between the network overhead and quality of real-time analysis. As T_{trans} increases, the network overhead decreases but the false positive rate and the false negative rate will increase. If many logs are generated in a short time period, logs should be compressed and only the summary is transmitted. For example Tang,et.al. proposed an effective log compression method [9].

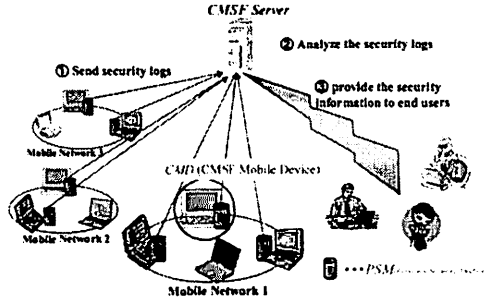

Figure 1: Overview of CMSF

3.3 Analysis of Security Logs

The second step is the analysis of security logs. The CMSF server analyzes the logs received from CMD to detect attacks in mobile networks. However, as mentioned above, the logs are not always reliable. Some of them may be already tampered by attackers. Or, malicious CMD may send forged logs. So, there are cases where some CMD says that an attack occurs in a network while the other CMD says that there is no attack in the network.

Therefore, the CMSF server uses a threshold-based scheme to estimate whether attacks really occur. Assume, at time T the Server receives logs from N CMD in a network and, each CMD sends one log. Each log shows whether an attack occurs or not in the network at time T. N_p of N logs show the occurrence of the attack and the other $N_n (= N - N_p)$ logs show the non-occurrence of the attack.

In this case, the CMSF server determine whether an attack occurs as follows.

1. If $N_p \geq TH_p$, the server estimates that the attack really occurs.

2. If $N_p < TH_p$ and $N_n \geq TH_n$, the server estimates that the attack does not occur.

3. If $N_p < TH_p$ and $N_n < TH_n$, the occurrence of the attack is unknown to the server. In this case, the estimation at time $T-1$ is used again. For example, if the server estimated an attack occurs at time $T-1$, the server estimates that the attack still continues at time T.

TH_p and TH_n are the thresholds of log analysis. As N_p increases, the false positive rate increases and the false negative rate decreases. Also, as N_n increases, false negative rate decreases and false positive rate increases.

3.4 Distribution of Analyzed Results

The third step is the distribution of the analyzed results to the mobile users who would like to know the security conditions of mobile networks. We assume the request users devices are not always equipped with any PSM. This is because, some users cannot intall PSM in their mobile devices for various reasons but want the information of security conditions of mobile networks. Whether the CMSF server accepts the users who do not send logs and contribute to the framework depends on the policy of this server.

Which Networks conditions a user wants to know will depend on the location of the user. For example, if a user is in a railway station, the user will want to know the conditions of networks near the station. When an attack occurs in a network, whether the attack is really harmful to a user may depend on the status of the user's mobile devices since most attacks exploit the vulnerabilities of specified operating systems, applications and network services. Then, the CMSF server should show the customized security condition for each user according to the devices status. As there are more serious attacks that exploit the vulnerabilities of a user device, the security condition of the network for the user should be worse.

The communication between the CMSF server and a mobile user U is as follows.

1. When U wants to know the security conditions of mobile networks which are at location L, U accesses the CMSF server and sends the position information of L. In addition, U also sends the status of U's mobile devices S to the server. S should contain the attribute of the device such as settings of the OS, installed applications, active services, update logs and so on.

2. On receiving the information from U, the CMSF server retrieves the analyzed results of mobile networks located at L from databases. Then, the server uses S to assess the vulnerabilities of Us device and compares the vulnerabilities with the attacks in the networks. Finally the server computes the security condition of each network and returns to U.

3. Using the results, U will enter the most secure one among the networks in L or just refrain from entering any network when there is not enough secure network to U.

To obtain the information from the CMSF server, U must join any networks to connect to the Internet. Therefore, if U joins the network filled with attacks, the Us device may be compromised before U obtains the information and customizes the security level of the device to an appropriciate level or leaves the network. Therefore U should take the following three ways to prevent such situations.

1. U is at L and sets the security level of the device to highest level where the most network ports are closed, the network services are down and the communication with any host other than CMSF server is not allowed. Next, U enters a mobile network at L and obtains security condition. Finally, U sets the security level to the appropriate one or leaves for the more secure networks at L according to the information from the CMSF Server.

2. U is at L and obtains information by some means other than the use of mobile networks. For example, if U has a mobile phone that can connect to the Internet, uses the phone to access the CMSF Server.

3. U preliminarily obtains the information when U is at the location L' other than L and uses a trusted network such as an organization network or home network at L'. Then, U goes to L and enters the most secure mobile network at L.

With the first way, U can obtain the latest information without any other network devices or equipments. The second way needs means to connect to the Internet securely and the additional cost can be high. The third way may lack the real-time information of mobile networks since while U moves from L' to L, the security condition might be greatly changed. Therefore, if U needs real-time information, the first and second way are appropriate. If U wants to know only the long-term conditions of the networks, the third way may be reasonable.

In addition, since end users may be unfamiliar with network security issues, visualization of the security condition is one of the requirements to make the CMSF serviceable. We are now developing a visualization tool [10] [11] that overlays the security conditions and location of mobile networks to a digital map.

4 CMSF based worm detection method in the mobile networks

In this section, we will show a worm detection method in mobile networks based on CMSF.

Most of network worms exploit one or some vulnerabilities of the network applications and services. Assume one host, which is already infected by a worm, enters a mobile network. If many hosts in the network have the vulnerabilities the worm can exploit, the worm will infect the hosts and stay in the network for long time after original infected host leaves the network. On the other hand, if the portion of vulnerable hosts in the network is enough small, the worm can not infect other hosts and will vanish from the network when the original infected host leaves the network. It is therefore not easy to estimate whether worms exist in a mobile network at a moment. The precision of estimation will depend on the percentage of vulnerable hosts, the number of hosts in the network and the infection speed.

Infected hosts usually conduct aggressive and discriminate address scanning to find vulnerable hosts. The most worms conduct local subnet scans that target on the local address space as well as global address scans [7]. Many of existing detection methods use the behaviours to detect the existence of worms. Since CMD is able to capture only the packets destined for itself and broadcast packets, PSM will use the ARP request packets to detect the address scanning. The ARP request packet is a broadcast packet used to resolve a given IP address (target address) to a MAC address.

When an infected host scans local address space, many ARP requests that try to resolve unused IP addresses will be broadcasted. Then, when the target address is unused, the packet will be retransmitted several times. Therefore PSM can detect the scanning hosts by finding hosts that send many ARP requests for the same address in a short time interval.

Since various CMD may install various PSM, the probability $P_{scan}(s,t)$ that a PSM detects a scanning host that sends s ARP request packets per second when t seconds passes since the start of scansis as follows.

$$X(s) = \frac{min(s,m)}{m} \cdot \frac{A-H}{A} \tag{1}$$

$$P_{scan}(s,t) = X(s) \cdot \prod_{1}^{t-1}(1.0 - X(s)) \tag{2}$$

A is the size of address space of a network and H is the size of the used address space. m is a threshold of the scanning rate. For example, when $s > m$ and $H << A$, the scan will be detected after about 1 second on average. Also, when $s = 1$, $m = 10$ and $H << A$, the scan will be detected after about 10 seconds on average.

Notice, in general, a scanning host is not always an infected host. The host may just scan the network for other reasons. However, if some hosts in a network conduct scans in a time period W_d, worms will exist in the network. Therefore most of PSM will detect the existence of worm when the number of scanning hosts N_{scan} in W_d exceeds a threshold TH_{worm}.

In each T_{trans}, CMD sends whether worms exist in the network to the CMSF server. Also, if CMD itself has been attacked directly, some information about the features of the worms such as the target ports and services are sent at the same time. Then, the CMSF server estimates the existence of the worms according to the threshold-based scheme described in Section 3.

5 Evaluation Experiments

In this section, we will show the effectiveness of the CMSF based worm detection method by computer simulation experiments.

5.1 Evaluation Condition

In this experiments we assume one mobile network. Various hosts including CMD, infected hosts enter and leave the network in turn. In this simulation, the condition of the network takes one of the two statuses; the worms exist or no worm exists.

Table 1 shows the parameters and initial values. Most of the parameters take the default values in all simulations and some parameters are varied according to each simulation condition.

We assume a C class network and then the address space allocated to mobile devices is 250. At the start of simulations, we assume there are 20 hosts in the network. Since R_{enter} and R_{leave} take the same value, the average number of hosts in the network is 20. Each host stays in the network for 2000 sec on average. R_{cmd} is the percentage of the mobile users who join to the CMSF. R_{worm} is the percentage of hosts which are already infected when entering the network. Also we assume CMD does not send forge logs unless the CMD is infected by the worms.

In this simulation, we have evaluated, Matching Rate, False Positive Rate (FP Rate) and False Negative Rate (FN Rate). Matching Rate means the percentage of time that the analyzed results by the CMSF server match the actual condition of the network. For example, when a simulation time is 100 sec and the total time where the analyzed results match the real condition is 70 sec, Matching Rate is 0.7(=70/100). FP Rate is the rate of the time the CMSF server estimates that worms will exist although no worm exists in the network in fact. Also, FN rate is the rate of the time the CMSF server estimates that worm does not exist but algthough there worms exist in fact. False positive estimate can happen when all CMD, which detect the existence of worms, leave the network, and then all infected hosts leave the network before new CMD enters. In this case, the number of CMD will be under TH_n and the CMSF server keeps on estimating that worms still exist in the network. False negative estimate can happen when the number of detected scanners does not exceed TH_{worm} or CMD is infected before detection and send forged logs which assert there is no worm in the network.

In the experiments, we have conducted 2 types of simulations by varying R_{cmd} and R_{vul}. The simulation time is 100000 sec.

5.2 Simulation Results

5.2.1 The effect of R_{cmd}

Figure 2 and Figure 3 show the Matching Rate and FP/FN Rates with various R_{cmd} respectively. The Matching Rate increases as R_{cmd} increases. Next, FN Rate decrease as R_{cmd} increases. To contrary, FP Rate increases when R_{cmd} is between 0.0 and about 0.04, and after R_{cmd} passes 0.04, FP Rate decreases as FN Rate. When R_{cmd} is 0.1, the FN Rate is about 0.2. In this case, since the R_{vul} is 0.2, when the CMSF server announces there is no worm in a network and a user enters the network, the probability the users device is infected by worms is up to 0.04 ($= 0.2 \cdot 0.2$). Therefore, it can be said CMSF is successful in preventing hosts from being infected by worms with small R_{cmd}.

5.2.2 The effect of R_{vul}

Figure 4 and Figure 5 show the Matching Rate and FP/FN Rates with various R_{vul} respectively. As R_{vul} increases the Matching rate increases and the FN Rate decreases. This is because, as R_{vul} increases, the number of infected hosts increases, and then the probability that the number of detected infected host by PSM exceeds TH_{worm} becomes higher as a result. Therefore, it can be said the CMSF is effective against worms that exploit the vulnerabilities of major network services and applications, such as the Windows RPC Service vulnerability exploited by MSBlast and Sasser.

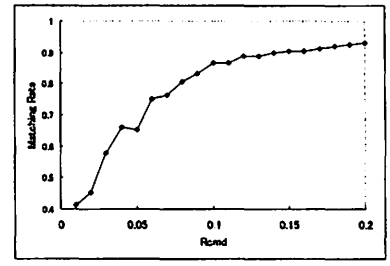

Figure 2: Matching Rate with various R_{cmd}

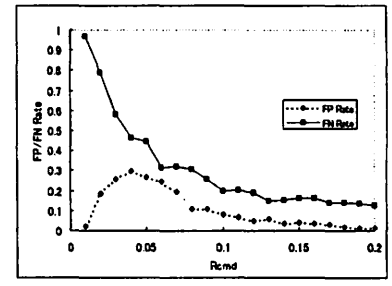

Figure 3: FP/FN Rate with various R_{cmd}

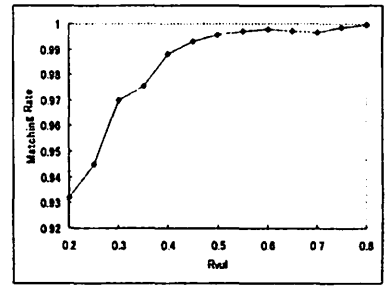

Figure 4: Matching Rate with various R_{vul}

Table 1: The parameters and default values

Parameter	Explanation	default value
N_h	the number of hosts in the network at the start of simulations	20 hosts
R_{enter}	the probability that 1 host enters the network per each second	0.01 / sec
R_{leave}	the probability that 1 host leaves the network per each second	0.01 / sec
R_{cmd}	the ratio of CMD to the all mobile devices	0.1
R_{worm}	the probability that an entering host is already infected	0.01
R_{vul}	the ratio of vulnerable hosts to the all mobile devices	0.2
A	entire address space in the network	250
T_{trans}	the interval to send logs to the CMSF server	1 sec
TH_p / TH_n	the thresholds of log analysis	3 / 3
w	the threshold of scan detection	10
TH_{worm}	the threshold of worm detection	2
W_d	the window of worm detection	10 sec
s	the number of scans per second	1

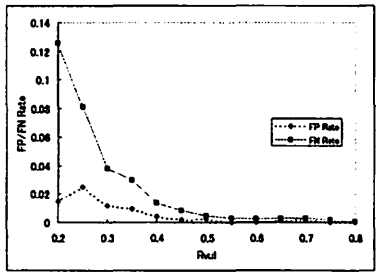

Figure 5: FP/FN Rate with vairous R_{vul}

6 Conclusion and Future works

In this paper, we have proposed CMSF: Cooperative Mobile Network Security Information Distribution Framework. In this framework the CMSF server obtains security information of networks from users who actually use the networks and have mobile devices equipped with personal security modules. Then the server analyzes the condition of networks from the information and distributes the results to users who want the knowledge of which networks are secure. Also, we have described the CMSF based worm detection method. Through simulation experiments, the effectiveness of the CMSF have been presented.

Acknowledgement

This work is supported in part by a special grant from the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research(C),2006,1850063, a Grant in Aid for the 21st century Center Of Excellence for Optical and Electronic Device Technology for Access Network from the Ministry of Education, Culture, Sport, Science, and Technology in Japan and ASF, Advanced Security Forum.

REFERENCES

[1] N.Kawaguchi,et.al.,CMSF:Cooperative Mobile Network Security Distribution Framework, in Proc. of The Third International Conference on Mobile Computing and Ubiquitous Networking , pp.99-106, 2006.

[2] S. Staniford ,et.al., How to Own the Internet in Your Spare Time, in Proceeding of 11th USENIX Security Symposium, August 2002.

[3] V.Yegeswaran,et.al., Global Intrusion Detection in the DOMINO Overlay System, in Procof NDSS'04, 2004.

[4] M. Locasto,et.al., Collaborative Distributed Intrusion Detection. Tech Report CUCS-012-04, 2004.

[5] K. G. Anagnostakis,et.al., A Cooperative Immunization System for an Untrusting Internet, in Proc of the 11th IEEE ICCN,2003.

[6] J.Kannan,et.al., Analyzing Cooperative Containment of Fast Scanning Worms, in Proceedings of USENIX SRUTI 2005 Workshop,2005.

[7] C.C.Zou,et.al., Code Red Worm Propagation Modeling and Analysis, in Proc. of ACM CCS 2002.

[8] Syed A.Khayam,et.al., A Topologically-Aware Worm Propagation Model for Wireless Sensor Networks, in Proceedings of ICDCS-Workshop, 2005.

[9] Y.Tang,et.al., A Simple Framework for Distributed Forensics, in Procc of the 2nd International Workshop on Security in Distributed Computing Systems, 2005.

[10] Y. Azuma,et.al.,Providing Security Information of Mobile Networks using Personal IDS, FIT2005 Information Technology Letters, pp.281-282, 2005.

[11] S.Tahara,et.al., Visualizing Security Information of Mobile Network considering Geographical Location, Technical Report 2006-GN-61, pp.23-28,2006.