Security Information Sharing Platform over Multiple Services

Bo Hu and Yuuichi Murata
NTT Secure Platform Laboratories
3-9-11 Midori-cho, Musashino-shi, Tokyo, Japan
Email: hu.bo@lab.ntt.co.jp

Junichi Murayama
School of Information and Telecommunication Engineering
Tokai University
2-3-23 Takanawa, Minato-ku, Tokyo, 108-8619, Japan

***Abstract*—It is necessary to protect services and users from diversified sources of cyber attacks even in complexly interconnected systems and networks. If a large number of smartphones in a mobile network are controlled by malware, they may be exploited to attack an application service in a fixed network. In this case, the conventional approach, which only protects the ingress and egress of services, cannot trace and identify those attacking smartphones in another network and the malware. To solve this problem, we propose a platform to share security information over multiple service infrastructures such as a fixed network, mobile network, and smartphone application market.**

Keywords—security information; multiple services; smartphone; malware

I. INTRODUCTION

Due to the diversification of networks, terminals, and services, the interconnection of service offering systems and networks has recently become highly complicated [1], and securing users and services over interconnected ICT environment is becoming a big challenge. Application services on the Internet are protected by Internet service providers (ISPs) or application service providers (ASPs) from layer 2 to 7 with various security appliances such as intrusion prevention systems (IPSs) and firewalls (FWs). However, only the ingress and egress of services, where there is a termination point of the cyber attack, can be protected by such an approach [2]-[6].

For example, if a large number of smartphones in a mobile network are controlled by malware, they may be exploited as tools of a distributed denial of service (DDoS) attack to an application service in fixed networks. In this case, the conventional approach in the ingress and egress of the service only can detect the increasing traffic and estimate the attacking IP source addresses. Unfortunately, since these IP source addresses belong to the mobile network, the conventional approach cannot trace and identify the specific attacking smartphones and malware. Due to the lack of an efficient strategy and solution to identify attacking terminals through complexly interconnected systems and networks, DDoS attacks remain, and both fixed and mobile networks have the burden of unnecessary traffic load. Moreover, the smartphone malware remain a potential threat on a smartphone application market. Therefore, an approach to fill the gap of security information among different actors in a cyber attack is necessary.

For solving this problem, we propose a platform to share security information over multiple service infrastructures such as fixed networks, mobile networks, and smartphone application markets. Section II describes the conventional methods that only protect the ingress and egress of the services. Section III describes the concept and framework of our security information sharing platform and our algorithm to identify smartphone malware based on the shared information. Section IV concludes the paper.

II. NETWORK MODEL AND DDOS ATTACKING MODEL

A. Network Model

Figure 1 gives an example of the interconnected relationship of systems and networks for offering services. Users can launch various applications on smartphone. These applications use the 3rd Generation (3G) or Long Term Evolution (LTE) mobile network to access the servers on the Internet. The above sequence of user actions involves multiple providers. Smartphone applications are provided in a smartphone application market, the 3G or LTE network is provided by a mobile carrier, and the application in the Internet is provided by an ISP or an ASP who contracted with the ISP for Internet reachability. These providers interconnect with each other for offering services.

B. DDoS Attacking Model

Following a real-world service model, smartphone applications are developed and released by different application developers. Since the market has to test and manage thousands of applications, it is possible to disguise and release malware as a normal application. If the malware spreads widely, a large number of terminals may be exploited for a large-scale DDoS attack which critically damages the services on the Internet. In this DDoS attacking model, the root cause is the malware which follows the remote commands from attackers, user terminals and mobile carrier networks are exploited as attacking tools, and the application services in the ISP are victims of the attack.

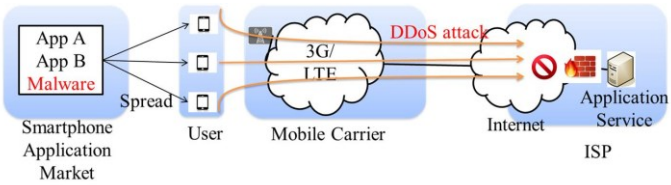

Fig. 1. Interconnected systems and networks

III. Security Information Sharing Platform

In this section, we first introduce conventional defense approach within a network and pointed out its inefficiency. And then we propose the basic concept, architectural framework and the algorithm of the proposed security information sharing platform.

A. Defense within a Network

As a conventional approach, Internet service providers or ASPs monitor and protect networks and services from layer 2 to layer 7 by using various security appliances such as IPSs and FWs. Figure 2 gives an example of an ISP protecting an application within a FW within its network. If the service suffers a DDoS attack, the FW will reduce the damage from the attack by estimating and blocking specified attacking IP addresses or protocols. Several studies have been conducted to enhance the effectiveness of this defense [2]-[6]. However, since the packets will be still sent from the attacking sources, obviously, this defense approach is passive and not efficient for resource utilization.

On the other hand, since the mobile carrier has no specific security information of DDoS attacks in another network, even though the traffic is increasing, it is difficult to check all the packets transferred in the network to find and block the attacking traffic. This means the mobile carrier also has to endure unnecessary abnormal traffic.

Moreover, for the application market, since it is difficult to perform a completely accurate check to detect malware from thousands of regular applications, once the malware was released to the market, it may spread widely. Without any feedback, this spread cannot be stopped.

Therefore, it is necessary to apply a more efficient method to identify and block cyber attacks from the sources in this attacking model which involves multiple networks.

B. Defense between Networks

Sections III.A showed the defense approach within a network and pointed out its inefficiency. This is due to a lack of information sharing between networks. Therefore, we propose a new defense approach by sharing security information between networks. The basic concept is shown in Fig. 2. To fill the gap of security information to detect the cyber attacks occurring in another network and system, it is necessary to transfer the appropriate information from the attacked termination to the appropriate network or system where this cyber attack originated. Especially in the case of defense between mobile and fixed carrier, since mobile carrier will check the internal private IP address with international mobile subscriber identity (IMSI), it is different to spoof IP address inside the mobile carrier network even though the attack use connectionless protocol such as UDP flood. Therefore, the information sharing for tracing attackers will be effective in this case.

This sub-section describes the basic thinking and elementary actions of this proposal to show how and what kind of security information is shared step by step with the use case shown in Fig.1.

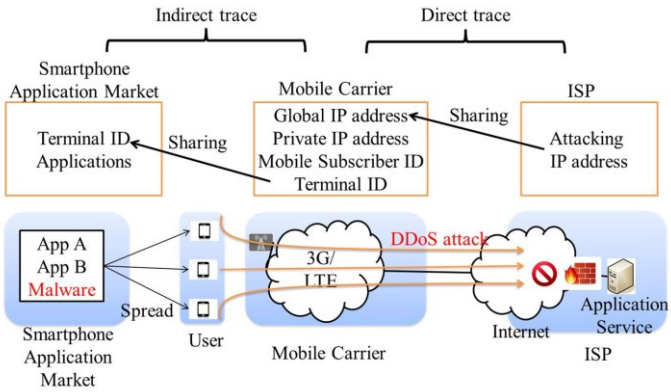

Fig. 2. Concept of security information sharing

As shown in Fig. 3, from the viewpoint of an ISP, when a cyber attack occurs, the ISP will analyze the abnormal accesses and estimate the IP source address of the attack. Since these attacking IP addresses belong to another provider, the ISP needs to collaborate with that provider to block the attacking traffic from the source. In this case, the appropriate information needs to be shared is the attacking IP addresses. The appropriate destination is the mobile carrier whose network interconnects with the ISP network in the IP layer and covers these attacking IP addresses.

From the viewpoint of a mobile carrier, after receiving the attacking IP addresses from the ISP, this mobile carrier can analyze the attacking user terminals (e.g., smartphones). If this mobile carrier translates private IP addresses to global ones for the Internet access, it should trace the private IP addresses by referring to access logs and detection date information [7]. However, since the root cause controlling these smartphones is the malware, a cross-layer trace from the network layer to application layer is also required. The appropriate information to be shared is the terminal identification data (ID) such as international mobile equipment identity (IMEI) or IMSI which can identify terminals. The appropriate destination should be the market delivering and managing applications for terminals.

Finally, from the viewpoint of an application market, the applications in every terminal can be listed within the terminal ID. Only focusing on one of those terminals, the market may find dozens or hundreds of applications. However, by comparing the applications downloaded in different attacking terminals, the common applications can be extracted. After excluding the well-known regular applications in these common applications, the ones which are unusual but exist in all the attacking terminals will be left. It will be easier to test these limited applications to find the malware for the market.

In the case described above, tracing attacking IP addresses and terminals between the ISP and mobile carrier can be categorized as direct trace, since the tracing target generated attacking traffic. On the other hand, tracing malware between the mobile carrier and application market can be categorized as indirect trace, since malware is not detectable from the viewpoint of attacked services but indirectly exploit terminals.

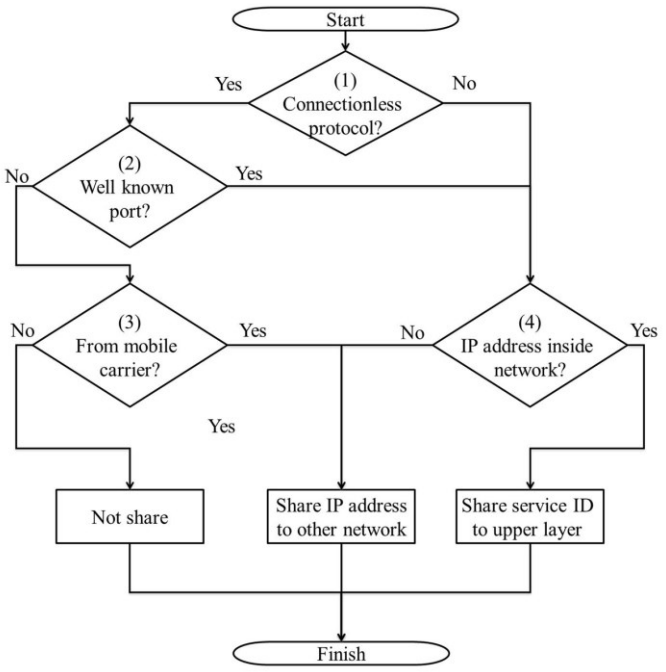

Fig. 3. Algorithm for security information sharing

C. *Algorithm for security information sharing*

For achieving the proposed defense between networks, we also propose an algorithm to decide whether and what kind of information should be shared between networks. The flow chart of proposed algorithm for security information sharing is shown in Fig.3.

The first step of all is to check the transport layer protocol which is shown as step (1) in Fig.3. Since the attacking IP address may be spoofed in the case of connectionless protocol such as UDP. If the protocol is connectionless type, the next step is to confirm transport layer port number for more information to check the authenticity of the addresses. If the protocol is connection oriented, detected IP addresses are real addresses available on the network, and the next step is to check the network of attacking IP addresses.

The step of confirming transport layer port number is shown as step (2) in Fig.3. Since attackers may exploit open DNS or NTP servers on the Internet for a large scale reflection DoS attacks, the port number of attacking packets will be useful judgement information. If the port number is a well known number used for DNS or NTP responses such as 53 or 123, the attacking addresses are possibly real ones of the exploited open DNS or NTP servers, and those addresses should be shared to another network. If the port numbers are not well known ones, the next step is to check whether those addresses are from mobile carriers.

The step of checking whether attacking addresses belong to mobile carriers is shown as step (3) in Fig.3. As mentioned in section III.A, since mobile carriers will identify internal terminals and users, it is difficult to spoof addresses for attackers who exploit the user terminals. Namely, if those attacking addresses are from mobile carriers, the address information will be credible and should be shared to another network for tracing the attacking terminals. On the other hand, if those addresses are not from mobiles carriers, they may be spoofed ones and not worth to be shared to another network.

The step of checking the network of attacking addresses is shown as step (4) in Fig.3. By referring to address ranges of different providers, we can find out whether those addresses are inside the network or in other interconnected networks. If attacking addresses are inside the network, it is easy to identify the terminals and users. Since the root cause is the upper layer application running on the terminals, the mobile carrier should share the service information to upper layer providers. In the case shown in Fig.2, after checking the addresses, the mobile carrier can identify terminals and users, and then specify operating systems of terminals and contracted application markets of users. And then the mobile carrier should share IMEI (or IMSI) to appropriate application markets for tracing the malware. On the other hand, if those IP addresses are from other network, it is necessary to share them to the appropriate for tracing the attacking terminals.

IV. CONCLUSION

We proposed a approach to share security information over multiple service infrastructures such as fixed networks, mobile networks, and smartphone application markets for achieving defense between networks. For achieving this kind of defense, we also Based on the proposal, we can expect to rapidly identify the attacking terminals and malware managed by different providers to keep the damage from DDoS attacks to a minimum.

REFERENCES

[1] Herbert G. Thompson Jr., and Christopher Garbacz, “Mobile, fixed line and Internet service effects on global productive efficiency,” Information Economics and Policy 19 (2007) 189–214

[2] Jelena MirkovicG, Peter Reiher, and I.N. Sneddon, “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms,” ACM SIGCOMM Computer Communications Review, vol. 34, No. 2, April 2004

[3] Jelena Mirkovic, Gregory Prier, and Peter Reiher, “Attacking DDoS at the Source,” Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP’02), 2002

[4] Yonghua You, Mohammad Zulkernine, and Anwar Haque, “Detecting Flooding-Based DDoS Attacks,” ICC '07. IEEE International Conference on Communications, June 2007

[5] Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao, “Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring,” IFIP International Federation for Information Processing, 2004

[6] Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao, “Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems,” ACM Computing Surveys, Vol. 39, No. 1, Article 3, April 2007.

[7] Klaus Doppler, Mika Rinne, Carl Wijting, Cássio B. Ribeiro, and Klaus Hugl, “Device-to-Device Communication as an Underlay to LTE-Advanced Networks,” IEEE Communications Magazine, December 2009