Winter 12-13-2018

EXPLORATIVE STUDY ON THE CYBER-ATTACK SOURCE TRACEBACK TECHNOLOGIES FOR BRIGHT INTERNET

Gyoo Gun Lim
Hanyang University

Hyun Gil Nam
Hanyang University

Il Woo Park
Hanyang University

EXPLORATIVE STUDY ON THE CYBER-ATTACK SOURCE TRACEBACK TECHNOLOGIES FOR BRIGHT INTERNET

Gyoo Gun Lim[1]
Business School, Hanyang University, Seoul, Korea
Hyun Gil Nam
Business School, Hanyang University, Seoul, Korea
Il Woo Park
Business School, Hanyang University, Seoul, Korea

ABSTRACT

In order to cope with the various types of cyber-attacks in the Internet, several methods of tracking the source of attack have been developed. However, until recently, most of them are defensive security methods rather than preventive one. In order to settle the Bright Internet, which is still in its early stage, it is necessary to establish a technical source tracking method. For this, a standard and evaluation criteria are needed to determine which technology would be appropriate for the Bright Internet requirements. In this paper, we classify cyber-attack source traceback technologies and derive some criteria for the evaluation of the technologies for the Bright Internet. Using the criteria, we can evaluate existing traceback technologies from the perspective of the Bright Internet. In this article, we try to evaluate SAVA, PPM, iTrace, Controlled flooding, Input Debugging, Central Track, IPSec, SPIE(Hash-based), and Marking+Logging methods. Based on this research, future research will require in-depth verification of traceback technologies that reflects all the principles of the Bright Internet in practice.

Keywords: Cyber-attack; Traceability; Source traceback; IP backtracking; Bright Internet; IP trace

[1] Corresponding author. gglim@hanyang.ac.kr +82-10-3301-0009

INTRODUCTION

According to the World Economic Forum (2016), one of the top ten risks likely to occur over the next decade is a cyber-attack. The analysis also suggests that cyber-crime will be more harmful in the era of the Fourth Industrial Revolution, where the world is connected via the Internet of Things and many intelligent technologies and applications are provided. In the era of the Fourth Industrial Revolution, an efficient cyber-attack sources tracking method should be provided for the social security. In particular, research on the tracking the source of cyber-attack has been carried out as a countermeasure or a tracking method for a specific attack such as DDoS(Distributed Denial of Service) by using the existing security technologies. As the scale and methods of cyber-attacks have been diversified, it becomes more difficult to track the source because attackers have been struggling to hide their locations by using various methods. Kim et al. (2014) defined the cyber-target attack tracing technology as a technology that can track the location of the actual hacker, that is, the origin of the attack, even if the location of the attacking system and the location of the hacker attempting to actually hack are different. Recently, it has evolved into a form of controlling a zombie PC by installing a proxy server or a server in a cloud environment where it is hard to track the exact source location. Therefore, techniques for tracking the location of an attacker have been actively researched and proposed.

Ultimately, the next generation of the Internet should be safer and more reliable not only high-speed (Lee, 2015). In order to realize this, the Bright Internet was suggested by AIS society to fundamentally suppress the cause of crime (Lee, 2016a). The five principles of the Bright Internet are: Principle of Origin Responsibility, Principle of Deliverer Responsibility, Principle of Identifiable Anonymity, Principle of Global Collaborative Search, and Principle of Privacy Protection. In this study, we focus on Principle of Origin Responsibility, Principle of Deliverer

Responsibility, and Principle of Identifiable Anonymity among five principles of the Bright Internet. In this study, we classify the traceback technologies and try to evaluate them from the Bright Internet point of view. Based on the evaluation, we can improve existing technologies by securing transparency and preventing cybercrime and the decision makers can develop cost-effective technology and applications.

This study, after describing the background of the research and the purpose of the research, Section 2 sets the goal of this study through previous research and literature reviews on existing cyber-attack source traceback technologies and the Bright Internet. And after classifying the existing traceback technology and classification criteria, we try to evaluate each technology from the Bright Internet viewpoint.

LITERATURE REVIEW

2.1. Traceback of Cyber-attack Source

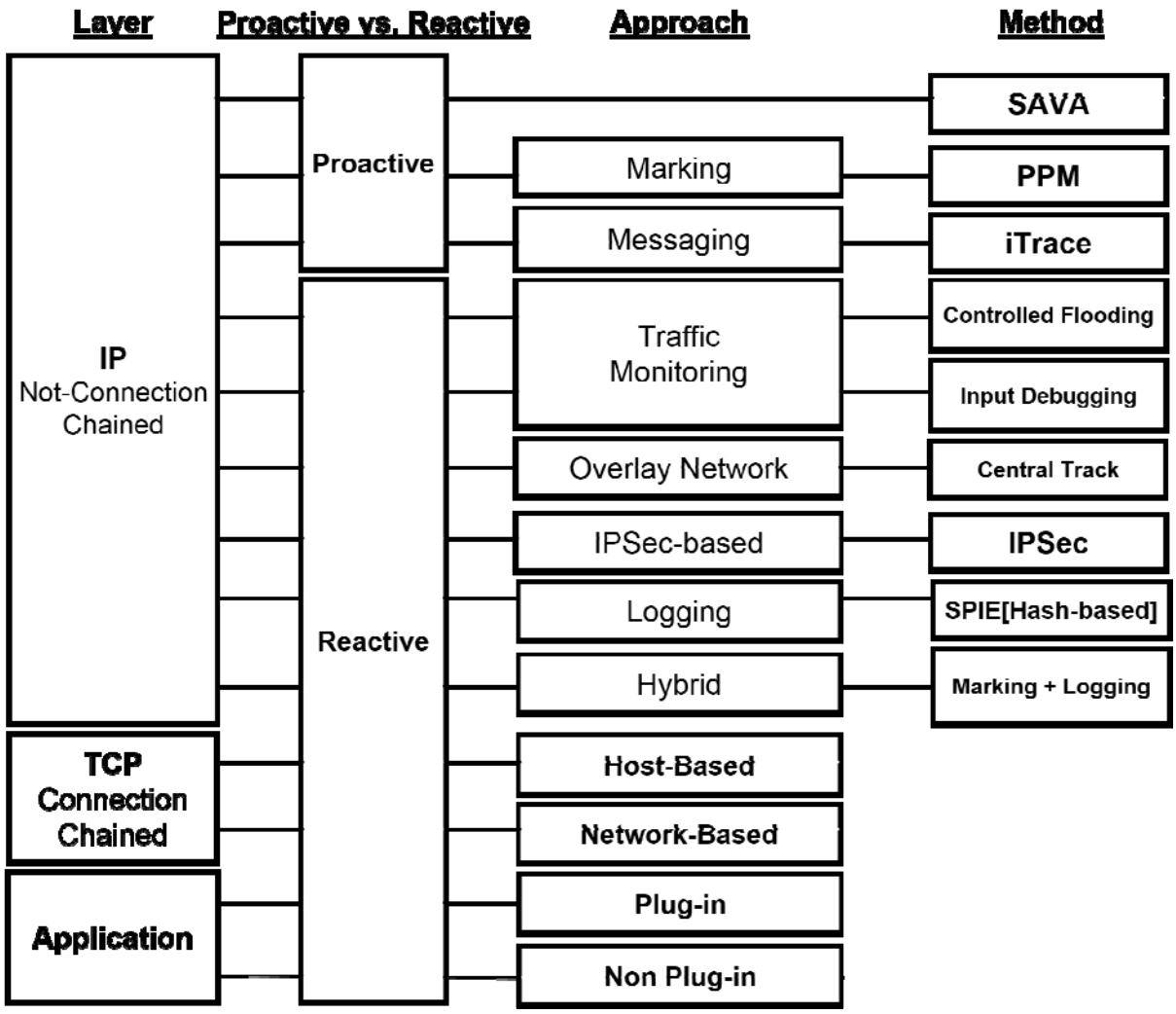
Savage (2000) evaluated each IP traceback technologies. This study evaluated the features of each traceback methods based on the overhead and basic functions of them. Murugesan (2014) also conducted a qualitative evaluation using the features of each technology using the IP traceback technologies to cope with DDoS attacks. This study provided more detailed reasons and evidences for the requirements of traceback. For the classification of the technolgies, Han (2008) classified the traceback technologies according to connection method, response method and application method. The connection method is divided into a TCP traceback method, which is a connection oriented communication method, and an IP traceback method, which is a non-

connection oriented communication method. The response method is classified into a passive traceback method that tracks the location of an attacker using traces left in the attacked victim system, and an active traceback method that actively restricts hacking attempts themselves. In addition, the network-based traceback method and the host-based traceback method are classified according to the location of the traceback module in the communication. Each method was broadly categorized based on technical commonalities. The detailed evaluation of each method is required. Huirong et al. (2008) evaluated whether it satisfies the agreement in ITU-T SG17 standardization meeting in 2008. They evaluated the strengths and weaknesses of each technology by using the common technical features of each method. The criteria of each item were classified in an overly detailed manner, and it evaluated them with narrow technical viewpoints.

In a broader perspective, an agreed study of cyber-attack source traceback was done by Kim et al. (2014). Classification of backtracking technology is largely divided into layer, IP, TCP and backtracking at application stage, and each technology is classified by the method using common technical breakpoints at each stage. It is similar to the previous study in that it uses technological commonality rather than a consistent classification, but it is more developed in that it classifies backtracking technologies into a wider range.

In addition, there are many cases in which the technical commonality of the layer and the case of preventive or countermeasures are distinguished in classification basically in domestic and foreign studies. For the evaluation items, the backtracking method was diversified, and the evaluation of each detail item by the preceding studies was performed, and the technologies were evaluated with relatively subdivided items. Most of the criteria were based on technical similarities and differences except for some items.

In Figure 1, we classified the traceback technologies into subdivided stages of classification, response, approach, and actual applications.



[Figure 1] Traceback technologies classification

2.2. Bright Internet

In the IoT era, where all things are connected by the Fourth Industrial Revolution, existing cyber problems will occur on a large and diverse scale, including human casualties.

Therefore, efforts to resolve the side effects in the Internet structure are necessary and a security paradigm with a preventive dimension has been proposed (Lee, 2015). Bright Internet preemptively reduces the origins of cyber security threats by having the ability to identify malicious sources and forwarders globally while maintaining the legitimate level of privacy for anonymous expression and innocent netizen. The Bright Internet presented five principles to realize the cause of provider responsibility: Principle of Origin Responsibility, Principle of Deliverer Responsibility, Principle of Identifiable Anonymity, Principle of Global Collaborative Search, and Principle of Privacy Protection. In a recent study by Shin et al. (2017) regarding the Bright Internet, it is said that it is difficult to prevent the threat of the state-led cyber terrorism, where the Internet is used as a weapon, only by the five principles of Bright Internet. In order to compensate this, The Internet Peace Principle is added. Lee et al. (2017) provided basic technology requirements for the implementation of the Bright Internet.

EVALUATION CRITERIA FROM THE BRIGHT INTERNET PERSPECTIVE

This study tries to evaluate each technology from the Bright Internet viewpoint. In this study, we selected three principles of ‘Origin Responsibility’, ‘Deliverer Responsibility’, ‘Identifiable Anonymity’ among the principles of the Bright Internet. We evaluate 'Source traceability', 'Waypoint traceability’, 'Possibility of identifiable anonymity' in order to evaluate the technology based on the three principles. There are costs and administrative considerations to actually use th e IP traceback technology for implementing the Bright Internet. Therefore, in this study, measures of the management aspect are introduced as 'ease of application', 'development cost', 'maintenance cost', and 'conversion cost'. In addition, the proactive of cyber-attacks or preventive

one is an important factor of the cyber-attack from the Bright Internet point of view. Based on the above, the evaluation results of existing technologies are shown as bellow;

(1) Source traceability (Origin Responsibility)

The criteria for source traceability were evaluated based on the principle of origin responsibility. This is most closely related to the traceback accuracy in the previous traceback technology evaluation researches and is described based on the previous studies.

(2) Waypoint traceability (Deliverer Responsibility)

It evaluates technologies on the basis of whether the accuracy of the confirmation of the waypoint of the attack is secured. It seems to be vulnerable if the information of each router is distorted when it constructs traceback using Central Track and IPSec(Internet Protocol Security) -based Tunnel. An Application-based traceback method has a big difference in the accuracy of checking the waypoint between the technologies.

The SPIE(Source Path Isolation Engine) has high accuracy of the waypoint checking because it is based on the Hash method. Controlled Flooding and Input Debugging traceback technologies are relatively reliable because they check the source while monitoring the traffic. In case of SAVA(Source Address Validation Architecture) method, because the validity of origin address is judged step by step, so it is easy to check the waypoint.

(3) Possibility of Identifiable Anonymity

An anonymity in the Bright Internet can be interpreted as a part about whether the original location and address can be confirmed at the time of traceback while ensuring the anonymity in

usual cases. In the case of iTrace and PPM among the traceback methods using the packet, it is difficult to control the intermediate stages because the traceback route can be reconfigured by gathering a plurality of packets. In addition, the application-based traceback method itself has difficulty in anonymizing the whole because it forms a path by using various information in addition to the IP packet information.

Since the SPIE traceback technology uses a single packet, the possibility of anonymity cannot be ruled out. In the case of IPSec, it is highly possible to implement the anonymity that can be verified when reconfiguring cases in a tunnel of routers within an IPSec connection. SAVA configures encryption with peer-to-peer when determining the validity of an address, thus it provides the identifiable anonymity.

(4) Ease of application

It might be required to install some hardware or software to apply the technology. An ideal technology might be implemented easily in ISP or etc. without change of the network structure. Except iTrace, the other traceback technologies cannot support packet display and logging in the current router. It is easy to apply because it uses ICMP (Internet Control Message Protocol). SAVA has low application possibility because it needs pre-negotiation between inter-AS. An overlay-based method can be applied only in a specific network. It cannot be applied in the general network environment where the structure of routers are changing dynamically.

(5) Development cost

Development costs are measured in terms of the initial costs incurred when building a new cyber-attack source traceback technology. It is necessary to consider the scalability of the

development cost during the technology introduction stage. In case of PPM with marking method, it is a simple technology among them. In addition, the PPM and iTrace traceback technologies are scalable because they require a traceback module for packet marking on routers in the network.

However, SAVA traceback technology requires a switch on the Access Network to be upgraded when applying a switch-based solution, and can be deployed between the host and the terminating router as a signature-based solution. It needs additional costs to insert and validate the signatures. It is also necessary to consider the additional costs and equipment costs of distributing and certifying the credentials.

(6) Maintenance cost

Maintenance cost is the expense to maintain it after introducing an traceback technology. Basically, the maintenance cost is high, which is high in management overhead. iTrace is characterized by low management overhead and stable message output in the event of a problem with intermediate routers.

In the case of PPM, the overhead of management is low, but when the number of attack packets increases, the cost for performance improvement may increase. It also has a lot of protection in backtracking compared to a logging-based approach. In addition, IPSec-based traceback technology might be expensive to manage communication tunnels.

Of the traceback technologies that take the traffic monitoring method, the Input Debugging has high management overhead for import and export, but the Controlled Flooding has relatively less overhead for management.

(7) Conversion cost

The conversion cost is measured in terms of the cost incurred when a new change is made in the existing cyber-attack prevention technology. iTrace and PPM traceback technology do not require ISP coordination. In the case of PPM, since it adopts the marking method, gradual installation may be possible.

Since the SPIE traceback method requires DGA (Data Generation Agents) to be installed on all routers for backtracking to build the system, the cost of switching increases relative to other approaches. The traceback technology of Traffic Monitoring method has a disadvantage that ISP cooperation should be established separately. In the case of SAVA traceback, cooperation with other authorities is also required for Inter-AS validation. And a new technology for address validation has a lot of work to do for many deployments. For example, all current technologies can be applied locally and independently.

ACKNOWLEDGEMENTS

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2018S1A5A2A01035729)

REFERENCES

Lee, J. K. (2015). Final Report for Bright Internet. IITP.

Savage, S., Wtherall, D., & Anderson, T. (2000). Practical Network Support for IP Traceback. Proc, Of ACM SIGCOMM 2000, 295-306.

Murugesan, V., Shalinie, M., & Neethimani, N. (2014). A Brief Survey of IP Traceback Methodologies. Acta Polytechnica Hungarica, 197-216.

Han, J., Kim, R., Ryu, J., & Yeom, H. (2008). Analyze traceback technology and security requirements. Information protection journal, 132-141.

Huirong, T., Brackney, R., & Youm, H. Y. (Sep. 2008). Draft text of Rec. X.tb-ucr: Traceback Use Cases and Capabilities. TD4158, ITU-T SG17.

Kim, J. T., Han, M. H., Lee, J. H., Kim, J. H., & Kim, I. K. (2014). Cyber attack traceback technology trend. Electronics and Telecommunications Trends, 93-103.

Lee, J. K. (2016a). Invited Commentary-Reflections on ICT-enabled Bright Society Research. Information Systems Research, 27 (1), 1-5.

Lee, J. K., Cho, D. G., & Lim, G. G. (2017). Design and Validation of the Bright Internet, Editorial Note, Journal of the Association for Information Systems, (2018) 19(2), 63-85

Shin, Y., & Lee, J., K., & Kim, M. (2017), Preventing State-led Cyberattacks by the Bright Internet and Internet Peace Principles. Journal of Association for Information Systems