The Study of a Risk Assessment System based on PageRank

Cheng-Chung Kuo, Chia-Ling Hou, Chu-Sing Yang

Department of Electrical Engineering, National Cheng Kung University, Taiwan
jjguo@crypto.ee.ncku.edu.tw, {clhou, csyang}@mail.ncku.edu.tw

Abstract

In recent years, network technology has developed rapidly. However, the Internet has been subject to a variety of attacks. Several notable attack events have been reported, such as those involving the use of flooding flows on widely used message boards, installation of malware in an automated teller machine to steal more than 80 million, and use of WannaCry to encrypt users' files and request for ransoms. The majority of the attacks cannot be defended using single methods. Network-based intrusion detection systems (NIDSs) and host-based IDSs (HIDSs) can determine whether a system has been attacked. A NIDS alone cannot detect web-based attacks or system vulnerabilities. Thus, this paper proposes a risk assessment system (RAS) that integrates a NIDS and HIDS to detect suspicious behaviors and assess the risk value of Internet protocols (IPs). The RAS focuses on the analysis of attack or suspicious behaviors using the NIDS and HIDS. Furthermore, the system quantizes the influence of attackers in suspicious events by using PageRank. Finally, the RAS derives the risk value of every IP to warn users of an attack and protect hosts or devices from the attacks.

Keywords: Suspicious behavior, PageRank, Risk assessment

1 Introduction

Currently, network services not only enable people to select courses without location limitations but also assist people in paying bills anywhere. However, with advancements in network technology, the Internet is subject to a variety of attacks. Completely safety and security is not possible in this digital age. In 2017, WannaCry [1], which is a ransomware worm, rapidly spread across the globe. Attackers locked every file in victims' computers and demanded a ransom. If victims refused to accede to attackers' demands, the attackers did not relinquish the victims' files. Moreover, in 2016, the First Bank ATM heist astonished the world [2]. First, attackers permeated the telephone recording system of First Bank's London branch. The network security for this branch was relatively weak. After understanding the internal Internet topology in the London branch, hackers gained access to the delivery system. Finally, attackers remotely inserted malware in the ATM and embezzled more than 2 million dollars from an ATM network in Taiwan. Attackers can go to extreme lengths to achieve their goals. This poses a threat to every competent authority holding a position of responsibility.

In addition to the diversification of attack methods, attackers usually combine several principles to launch a new attack. Intrusion detection systems (IDSs) were developed to detect such attacks. A network-based IDS (NIDS) and host-based IDS (HIDS) can determine whether an attack has occurred. A NIDS can monitor packet payloads or flows to detect attacks. A HIDS can monitor logs, file changing conditions, and port opening actions to detect malicious behaviors in time and take appropriate actions to prevent attacks. However, the use of a NIDS or HIDS is no longer safe. Because of the limitation regarding network flow information, a NIDS cannot accurately detect web-based attacks such as structure query language injection, cross-site scripting, and phishing. These attacks can only be determined by using a HIDS to monitor logs such as apache logs. Consequently, network attacks cannot be defended by using a single solution or system. Thus, this study designed a risk assessment system (RAS) by combining two systems, namely a HIDS and NIDS. By managing the two systems, the RAS can divide data into two groups, namely attack Internet protocols (IPs) and suspicious IPs, and take appropriate actions for different groups, such as blacklisting attack IPs and calculating the risk of suspicious IPs to determine the degree of danger for users.

2 Background and Related Work

2.1 IDSs/Intrusion Prevention Systems

With the evolution of network technology, the Internet is subject to a variety attacks. Earlier, network managers could only intercept malicious connections and protect internal network environments by using a firewall [3] to set policies for malicious IPs and famous service ports. However, the majority of attacks target

*Corresponding Author: Cheng-Chung Kuo; E-mail: jjguo@crypto.ee.ncku.edu.tw
DOI: 10.3966/160792642019122007022

company and government agency network services through well-known ports [4] such as HTTP and TELNET. These attacks cannot be prevented by setting ports or IP policies; therefore, other information must be used to block attack behaviors.

Accordingly, an IDS [5] and intrusion prevention system [6] have been proposed. An IDS can warn managers of an attack or a high-risk event by detecting flow attack features and abnormal behaviors. Although an IDS and intrusion prevention system are similar, they differ in two aspects: First, an IDS does not function in inline mode, whereas an intrusion prevention system functions in real time [7]. Second, an intrusion prevention system is more active than an IDS, and this is because an intrusion prevention system can initiate timely actions such as blocking the connection and providing protection in case of an attack. Wireless communications also developed wireless IDS mechanisms [8-9].

Studies have indicated that an intrusion prevention system is a combination of an IDS and firewall [10]; however, the difference between an intrusion prevention system and IDS is whether the system performs the corresponding procedures or just warns users. According to [7, 11], and [12], an IDS is detailed in Figure 1. The IDS can be classified by data, detection, deployment (source), and response. The most prominent methods are deployment and detection, which have been introduced in sequence immediately.

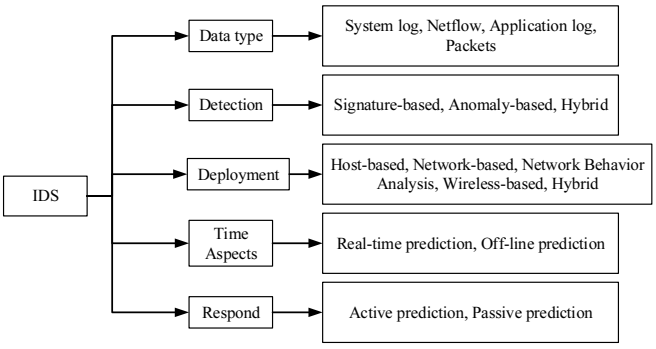

Figure 1. IDS classification

2.2 Risk Assessment

Risk assessment is a crucial procedure for confirming the security of a system. According to ISO 31000:2018 [13], risk assessment can involve many different risk assessment methods through risk identification, risk analysis, and risk evaluation. Risk identification involves determining the target value in the environment. A system has different procedures to evaluate risk. Moreover, risk analysis involves observing an influence variable, and a system uses methods, such as event replaying, to confirm the variety. Finally, risk evaluation involves executing the analysis solution for protecting the environment.

The common vulnerability scoring system (CVSS) [14] is a standard that can capture and translate vulnerabilities into a numerical score to represent the danger degree. The CVSS was established by the US government and manufacturers in the world. The score can be applied to not only calculate the danger but also translate the danger level (namely, low, high, and medium) to help users gauge the circumstance. In summary, the CVSS provide standardized vulnerability scores, an open framework to generate the scores objectively, and a prioritized risk mechanism to help users understand the priority of a threat. The CVSS consists of three metric groups (Figure 2).

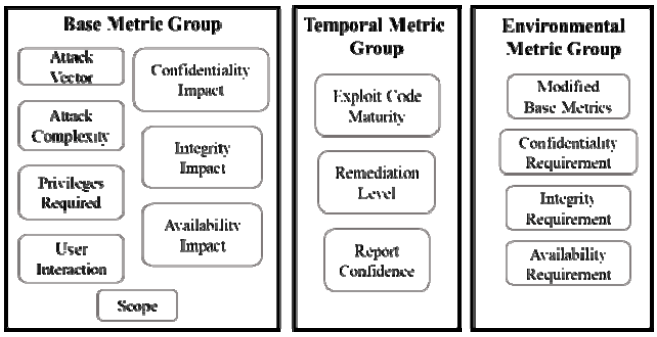

Figure 2. CVSS metric groups

The base metric group indicates the internal characteristics of a vulnerability that are constant over time and across user environments. The temporal metric group represents the features of a vulnerability that may change over time but not across user environments. For example, a sample using a vulnerability that occurs after the software update time can increase the CVSS score. Finally, the environmental metric group reflects the patterns of a vulnerability that are relevant and unique to a particular user environment. Because scenarios involving the temporal and environmental metric groups do not occur frequently, this study focused on the base metric group method to achieve risk estimation by combining NIDS and HIDS results.

2.3 Link Analysis

In social networks, link analysis is a crucial method to understand link information. Link analysis can address various social network problems, such as website relation, and calculate the popularity of a website. For example, prominent bloggers can introduce popular shops or restaurants in their blog articles and include the hyperlinks of the websites of such shops or restaurants in the articles. The relationship between a blogger's website and a cited website is closer than that between the blogger's website and a noncited website. Link analysis can be used to transform this citation relation into a degree. A study [15] demonstrated that link analysis can determine elements that affect social network operation. Link information can be used to demonstrate the degree of closeness among social networks. Moreover, link analysis can be used to improve concept location

techniques. Link analysis can be used to manage a web document to obtain high performance. Readers can refer to [16] for more details. The most prominent link analysis method used by Google is PageRank, which is introduced in the following text.

The increasing convenience of social networks has prompted interest in the relation and importance among different websites. PageRank was proposed to address this interest. Research [17] indicated that PageRank results can be used to measure human interest and attention. PageRank is actually a method that quantifies the citation relation, which is called a devoting value, among websites. If website A cites website B, then this relationship can be regarded as A devoting to B in PageRank calculation. After determining every citation relation among websites, PageRank summarizes the devoting value of all the websites. The websites can only obtain the value when someone cites them. However, for a website that is not cited, the value of the website is one of the total number but not zero. Because the value should not be gauged only through citation, the website is assigned a score to represent its value.

The system proposed in this study applies PageRank to estimate the IP relation because the citing and being cited behavior is like IP connecting and being connected relation. PageRank is used to determine the close relationship among IPs and to monitor those IPs to prevent potential malicious behavior. Therefore, if IP A launches an attack on IP B, the devoting value of IP B is expected to be higher than that of others, as determined through PageRank calculation. Subsequently, the IP B user can be notified to inspect their machine.

3 System Design

This study proposes a RAS to manage data from a NIDS [18] and HIDS [19] and assess IP risk. The proposed system divides data into attack and suspicious IPs.

Figure 3 presents the RAS architecture. The HIDS analyzes abnormal machine behavior. Port monitoring, log analysis, and file monitoring constitute the monitoring component. The result is uploaded to an open-source platform, namely Elasticsearch, Logstash, and Kibana (ELK) [20]. In addition, the router transforms flows into netflows, and the NIDS analyzes these netflows by using a supervised learning method. After analysis, the NIDS provides a corresponding label to each flow to distinguish different connection types. The system provides five label types: normal, horizontal scan, vertical scan, flooding flows, and brute force. The system also appends the result of the traditional NIDS [21], which monitors different patterns, such as the threshold, to estimate the event type. Finally, the result is uploaded to the ELK platform. The components of the ELK platform are described as follows: Elasticsearch is a Json-based and distributed search engine that can upload self-defined data. Logstash is a host-side data collection pipeline. Kibana can visualize Elasticsearch data through charts and graphs.

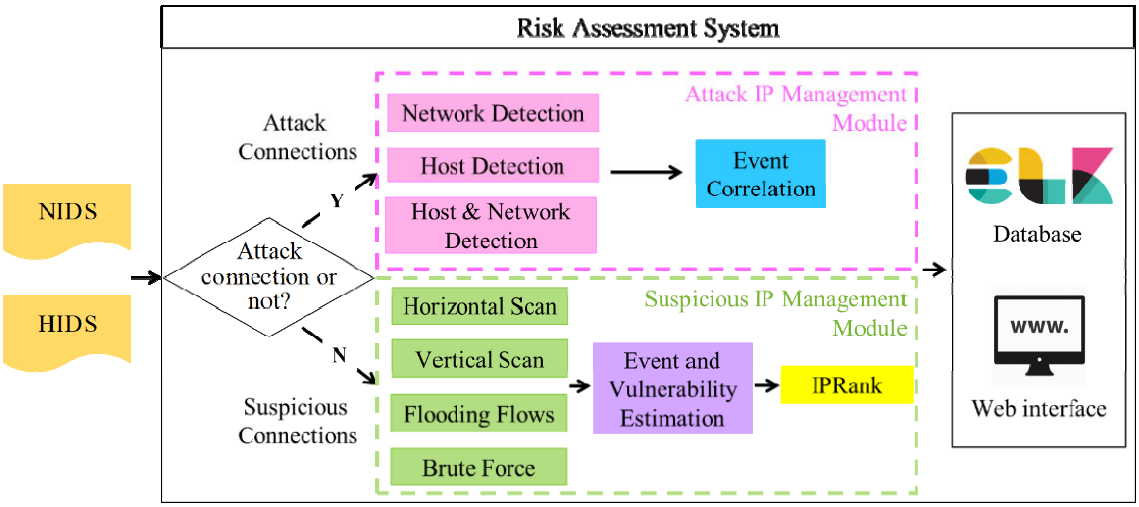

Figure 3. System architecture

Currently, attacks cannot be defended using a single solution approach. Attacks usually combine two or more methods to compromise victims. For example, web-based attacks can only be detected from a web server HIDS because the apache log records visitor information. However, because of limitations in flow detection, a NIDS views web-based attacks as normal connections. The flow information of some attacks, such as web-based attacks, is perceived as normal behavior in a NIDS. The attack footprint can only be detected using logs. Therefore, the proposed RAS solves the aforementioned difficulty and estimates the IP behavior risk, as presented in Figure 4. The RAS first reads HIDS and NIDS data from the ELK platform, after which it compares NIDS labels obtained from supervised learning with those obtained from

pattern monitoring to determine whether the labels are the same. If the labels are the same, then the flow is certainly an attack. If they are not, then the flow is defined as a suspicious connection. The proposed system establishes distinct mechanisms to manage attack and suspicious connections. The attack IP management module analyzes the attack connections and HIDS attack data, and the suspicious IP management module manages the suspicious connections. Both management modules use an IP visualization algorithm to generate an IP relation graph.

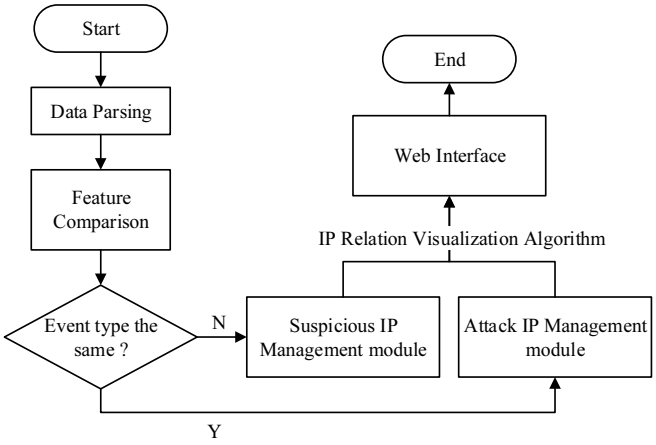

Figure 4. RAS flowchart

3.1 Attack IP Management Module

Figure 5 presents a flowchart of the attack IP management module. This module blacklists attack IPs and manages the blacklist. The module collects the data of NIDS labels that are determined to be the same. Subsequently, this module executes IP comparisons to compare attack IPs in the HIDS and appends the missing-attack IPs into the blacklisted IPs. The module also includes an event correlation algorithm, which is represented by the flowchart enclosed within the dark-blue dotted box in Figure 5. This algorithm correlates different machine events from the same attack IP, different machine events with distinct data sources from the same attack IP, and different time period machine events from the same attack IP. The reason for this algorithm is described as follows. Consider, for example, a scenario in which an attacker intends to quietly launch attacks and compromise hosts. The attacker is discreet and first scans host A. Subsequently, the attacker may attack host B with flooding flow and subject host C to brute force simultaneously. These attacks may appear less severe and distinct. However, when correlated, the coordinated attack becomes apparent. Therefore, the attack IP management module accumulates information of various events, such as duration and packets, after event correlation. Furthermore, the module appends the latest occurring time of the IP. The blacklisted data are also delivered to the ELK, and a blacklist relation graph is generated by using the IP relation visualization algorithm. The module also scans all the blacklisted data in the ELK platform to confirm their immediacy. If the final update time of a blacklisted IP is determined to be a month ago, the module deletes this IP from the blacklist. Because the IP ism not detected by the system in the current month, MARS must release the resource for other events.

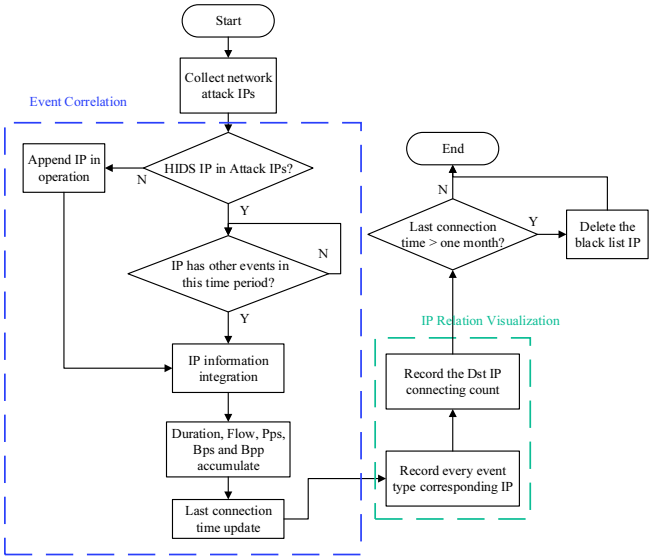

Figure 5. Attack IP management module flowchart

3.2 Suspicious IP Management Module

Figure 6 presents the suspicious IP management module. This module collects a suspicious IP that has a different event type label from the two NIDS labels. Moreover, the module compares the suspicious IP with the blacklisted IP. If the suspicious IP matches the blacklisted IP, which is used to discover the attack behaviors, then this suspicious IP is not analyzed in this step. In the next step, the possible risk that the suspicious IP may transform into an attack IP is estimated. The module applies a behavior estimation algorithm to quantify the degree of danger of the suspicious IP. The algorithm estimates the danger of the suspicious IP according to its event type, namely horizontal scan, vertical scan, flooding flows, and brute force. These four event types are clarified by using source IP, destination IP, destination port, and different methods to define the danger degree. For example, the degree of danger associated with the horizontal scan event type can equal the affected extent, and it can be calculated by using the destination IP count and port count. If a suspicious IP consist of an event flow that includes three event types, the danger degree is estimated using different methods because each event type has distinct features. Furthermore, the algorithm uses a target port to determine whether the suspicious connection targets a specific service port. Attackers can easily execute an attack or intrusion by using these target ports. Therefore, the algorithm assigns a high value to the IP for describing the risk if the suspicious

connection uses the target port to connect with the destination IP. Moreover, the suspicious IP records are used to estimate the risk. If a suspicious IP has appeared in the suspicious IP record, then this IP is more dangerous than others in this field. Additionally, if the host uses a HIDS [17] to transfer attack details to the proposed system, the proposed system can immediately detect the attack and warn users to protect the host in time. The host that deploys the HIDS is usually the critical server in the environment. Therefore, the risks of these servers are higher than those of other machines.

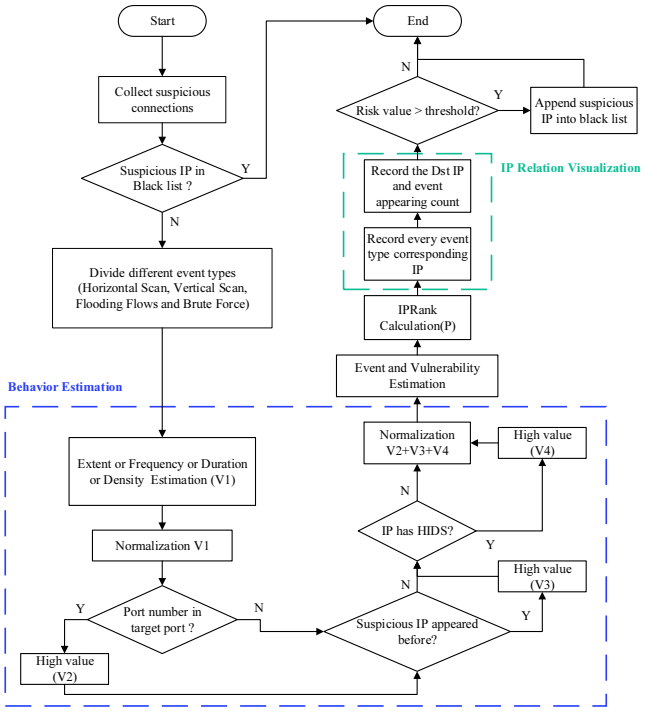

Figure 6. Suspicious IP management module flowchart

Some compromised victims have some irregular connections such as scanning, but users do not notice the connections because attackers usually erase their footprints to avoid detection. Therefore, the relation among IPs is essential to prove the abnormal behavior of suspicious IPs. The module in the proposed system uses IPRank to quantify IP relations in a time interval to detect unusual behaviors. IPRank is implemented by using the traditional PageRank algorithm to complete the relation quantification. The traditional PageRank algorithm is used to gauge the importance of every website through the citation relation in the social network. The value of each website is calculated using its being-cited number. The citation relation functions as the IP connection in the environment. Therefore, the citation relation is used to calculate the IP relation through IPRank.

$$C_{ab} = \begin{cases} 1, \text{ if } a \text{ connects to } b \\ 0, \text{if } a \text{ does't connect to } b \end{cases}, \quad (1)$$

$$H = \left[C_1\ C_2 \cdots C_i\right], \forall i > 0 \wedge i \in N, \quad (2)$$

$$\text{Impact} = \begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_i \end{bmatrix} * w, \begin{cases} w = 1.5, \text{if } srcip \cap dstip \neq Null \\ w = 1, \text{if } srcip \cap dstip = Null \end{cases}, \quad (3)$$

$$\text{IPRank} = H * \text{Impact}, \forall t > 0. \quad (4)$$

IPRank has the same procedure as that of the traditional PageRank algorithm. The IP relation is transformed into a matrix H by using formulas (1) and (2). Here, C is the relation of all IPs and i is the total number of suspicious destination IPs. Additionally, the value of each IP is calculated using the being-connected relation in IPRank and the traditional PageRank algorithm. In the traditional PageRank algorithm, the value of the website is not only determined by the being-cited number but also determined by the original value to represent the website in the environment. However, in IPRank, the importance of every IP is displayed. The value of each IP is calculated by using being-connected information. The only difference between the traditional PageRank algorithm and IPRank is the original value. If all destination IPs are being attacked (i.e., they are being compromised), then IPRank increases the impact by revising w to a higher value. However, the impact of the attack remains the same. Because the IP and website circumstances are different, the original values of all IPs cannot be the same. Accordingly, the IPRank value of every IP is initialized, as revealed by formula (3), which determines the impact of every destination IP in a specific period. The connection count of every source IP to each destination IP is used to calculate the impact. Moreover, the algorithm determines whether the source IPs appear in the destination IP list (being an attacker). If the source IPs appear in the list, w is set to 1.5, indicating that the impact of the attack is higher than that of others. Subsequently, formula (4) is used to determine the IPRank value. In formula (4), the H matrix and impact matrix are multiplied to calculate the total impact of the source IPs on the destination IPs in this environment. Finally, the IPRank value is derived, representing the importance of each IP in the environment. A high value indicates that the IP launches as many suspicious events as possible; thus, this IP can be considered to be more important than an IP with a low IPRank value.

The use of public risk estimation can increase the reliability of the system. Accordingly, CVSS-based event and vulnerability estimation algorithms [12] can be used to determine the potential risk of each IP. Event and vulnerability estimation terms can be separated into three categories, namely exploitability metrics, temporal tracing metrics, and impact metrics. The exploitability metrics comprise an attack service

vector (ASV), attack complexity (AC), and privileges required (PR). The ASV reflects the distance of the attacker's location and specific services such as secure shell and remote desk protocol. AC indicates the complexity degree of various vulnerability exploitations. PR reflects the level of privilege that attackers can successfully exploit vulnerability. Specifically, PR is the authorization level of the host. The temporal tracing metrics only evaluate history records (HRs). They are used to examine whether the IP has previously appeared in the suspicious list. Furthermore, distinct situations in the following formula involve different calculations. Impact metrics focus on the damage impact when a system's vulnerability has been successfully exploited. Confidentiality impact (C) indicates the confidentiality of the information resources when a system's vulnerability has been successfully exploited. Integrity impact (I) denotes the trustworthiness and veracity of information in a situation in which system vulnerability has been successfully exploited. Availability impact (A) represents the availability of the impacted component that results from a successful exploitation of system vulnerability.

If the degree of danger of a suspicious IP is not within a predefined range, the tracing algorithm (blue dotted rectangle in the figure) blacklists the IP. The tracing algorithm scans the suspicious IP data and determines the high-risk IP in this time section. After scanning, the algorithm appends all the high-risk suspicious IP into blacklist and deletes them from the suspicious IP data.

In the flowcharts illustrated in Figure 5 and Figure 6, the procedures enclosed in the green dotted rectangles involve collecting detailed information regarding suspicious and attack IPs, which includes the number of times source IPs have attacked destination IPs (connection count) and the number of horizontal scans (event type IPs). This information can help the IP relation visualization algorithm to determine the relationship among these suspicious/attack IPs. The algorithm first records how many suspicious/attack IPs occur and then uses the event type IP and connection count to list the relations between IPs. However, because the suspicious relation is highly complex, the algorithm only displays the campus suspicious/attack IP graph to warn users.

3.3 Web Interface

The system is equipped with a web interface to display the condition of the network environment to the user. The interface can be divided into two parts. One of the parts displays relation graphs for three circumstances. Specifically, the part presents relations between attack IPs (Figure 7) and suspicious IPs (Figure 8). The node size indicates the number of attacks the IPs launch. Therefore, a bigger node indicates that an IP executes more attacks. The arrows represent the direction of the attack. These graphs can conveniently display the attack and suspicious IP connection.

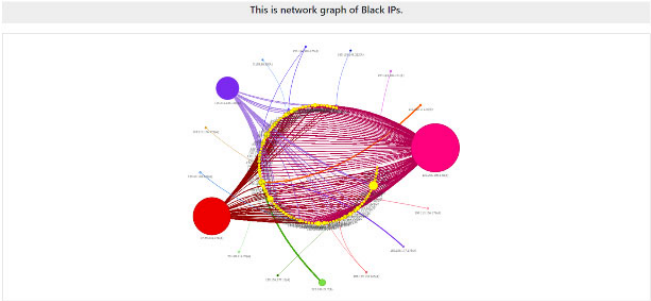

Figure 7. Blacklist relation graph

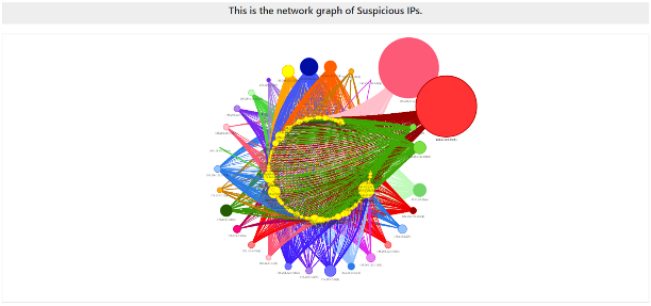

Figure 8. Suspicious IP relation graph

To ensure that network users are aware of the condition of the entire network, the interface also provides detailed daily information comprising the time data of blacklisted and suspicious IPs. Figure 9 and Figure 10 present detailed information indicating activities that have occurred in a particular period. Each data section has a drop-down icon that can be clicked to display detailed information such as destination IPs and ports.

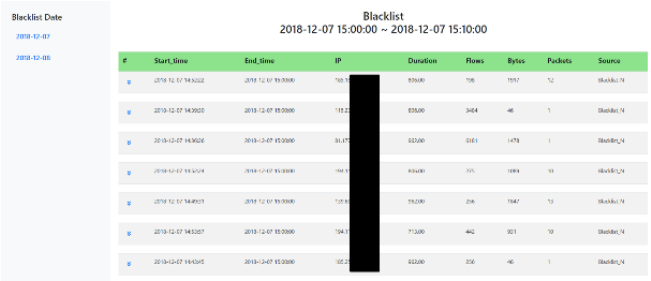

Figure 9. Daily blacklist detail

Figure 10. Daily suspicious IPs detail

The web interface uses the ELK dashboard to display a summary of blacklisted IPs (Figure 11) and suspicious IPs (Figure 12). Figure 11 shows that the blacklist consists of 31 blacklisted IPs, and the pie chart displays the percentage of IP sources (suspicious IPs or only blacklisted IPs). The table below the pie chart shows blacklisted IP information such as duration, flows, bytes, and time. Additionally, Figure 12 shows that the number of suspicious IPs is 18, and the table provides details about the suspicious IPs, such as ranking and risk value.

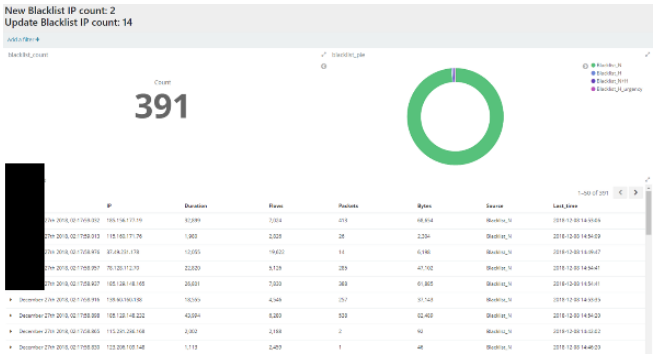

Figure 11. Blacklist ELK dashboard

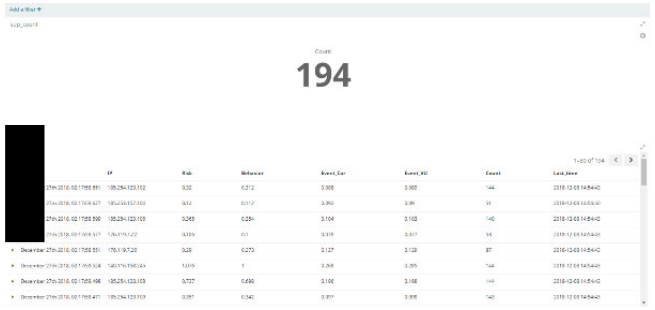

Figure 12. Suspicious IP ELK dashboard

4 Experiment

The proposed RAS was deployed in the campus network. Figure 13 depicts the campus environment. The RAS focuses on analyzing a local network router and combines the HIDS attack information to comprehensively protect users. The router exports every connection into the netflow and passes the data (red arrows) to storage. The NIDS then shares the storage and request for the latest data. The data pass through the router for switching and delivery to the NIDS, and the NIDS analyzes the results. Thus, the router does not directly deliver data to the NIDS. After NIDS analysis, the results are uploaded from the local network (blue arrows) to the normal network, and the RAS then obtains data from the ELK to execute the services.

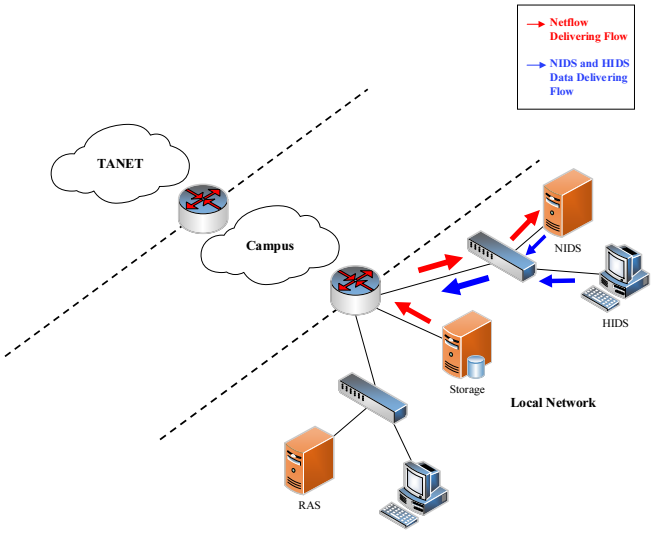

Figure 13. Campus network environment

The HIDS in Figure 13 is developed on a host. The HIDS monitors every service and log to gauge whether an attack has occurred. Once an attack occurs, the HIDS delivers results to the ELK (blue arrows) by switching to the EE router. When the data pass to the EE router, the router delivers the data to the NOC router, which then passes them into TANET to be uploaded to the ELK platform. The RAS then obtains the HIDS and NIDS results from the ELK platform (green arrows) and combines all the data into the blacklist and analyzes suspicious IPs.

The study conducted an experiment to demonstrate the proposed RAS. In the campus network, the operating center releases only in-to-out attacks. However, external attacks are more prevalent than in-to-out attacks. The internal host is usually compromised by external attacks and then transforms into a springboard. Therefore, recording external attacks is crucial. In the executed experiment, a time interval was used for NIDS analysis.

The time interval used in the experiment was as follows: December 7, 2018, 15:00:00 to December 8, 2018, 15:00:00.

In this experiment, the RAS detected 386 attack IPs. These IPs could be divided into three types, namely network-based detection, network- and host-based detection, and host-based detection. Network-based detection was determined to involve attacks such as horizontal scans, vertical scans, flooding flows, and brute force. Host-based detection was determined to involve attacks attempting to exploit vulnerable components, execute command injection, and perform directory traversal. In host-based detection, an attacker does not generate sufficient flows. Therefore, the NIDS does not classify the attack as an attack. However, its behavior suggests an attack; therefore, the HIDS classifies it as suspicious connections. Network- and host-based detection was determined to involve attacks that have been captured by the HIDS and NIDS attack IPs. In host-based detection, attacks are not detected in

suspicious IPs but in the HIDS. Such attacks are more dangerous than others. Figure 14 indicates that network-based detection is the most prevalent. This is because network attacks occur every day. Furthermore, the NIDS and HIDS were determined to have detected two times the normal attacks in this period. Host-based detection was determined to have three records.

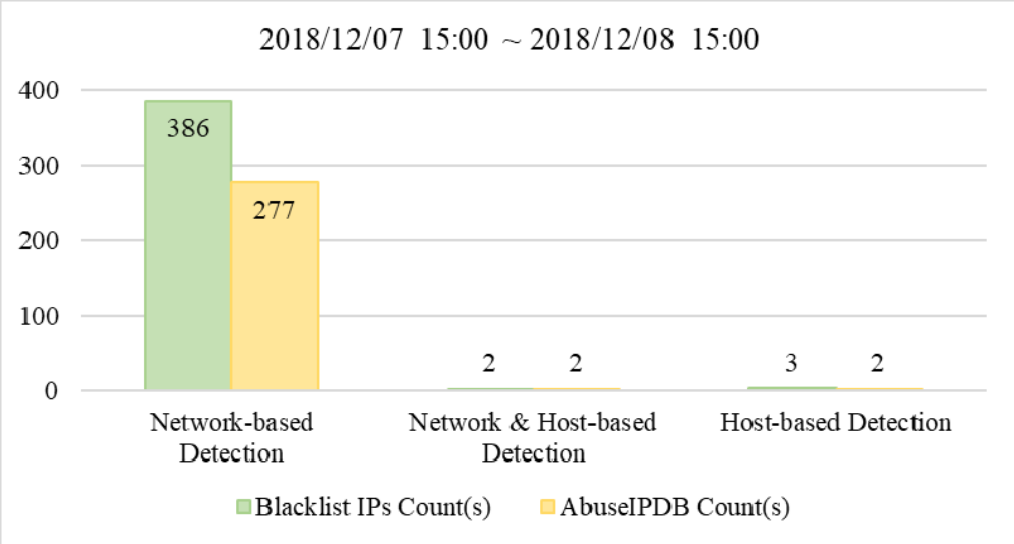

Figure 14. Blacklist detection result

The yellow bar in Figure 14 is the number of blacklisted IPs in AbuseIPDB [22]. AbuseIPDB is a global blacklist database, which can receive reports of global blacklisted IPs. Because this database includes global blacklists, we used it to verify the experimental results. In this study, 109 blacklisted IPs were not present in AbuseIPDB. To determine the information of these IPs, we used Whois to confirm each IP usage. Whois [23] is a global database that includes every public domain. Therefore, Whois records the official authority domain or application domain of the world. The Whois database confirmed that most of the IPs corresponded to Internet service providers (ISPs) or cloud services (Table 1). These IPs generate numerous connections to deliver data or provide services. Therefore, their behaviors resemble an attack condition.

Table 1. External blacklisted Ips

Src IP Addr	Dst Port	Src Owner
58.152.66.0/25	53413	Hong Kong Telecommunications (HKT) Limited Mass Internet
50.117.47.0/24	1080	United States EGIHosting
120.192.0.0/11	22	China Mobile Communications Corporation
92.53.90.0/24	3389	Selectel Ltd (Russian Internet hosting provider)

However, some IPs that were not observed in AbuseIPDB were identified as attackers in organizations such as city governments and famous web IP blocklists. Furthermore, several attack IPs were observed in the campus. For example, three IPs were identified as attacks because they established several connections to Internet services such as Amazon or queried to foreign ISP and broadcast packets in this period (Table 2).

Table 2. Internal blacklisted IP

Src IP Addr	Dst IP Addr	Dst Port	Dst Owners
140.116.216.**	13.35.*.*	80	Amazon
140.116.221.**	140.114.*.*	80	NTHU
140.116.85.**	140.116. *.0/24	123	NCKU

Figure 15 shows suspicious detection results in the specified period. In this experiment, the number of total suspicious events was 155. As indicated in the figure, horizontal scans were the most prevalent suspicious events. Therefore, attackers usually use horizontal scans. In addition, attacks such as vertical scans, flooding flows, and brute force were observed. First, attackers use horizontal scans to confirm that hosts are open, and they then use vertical scans to determine available services. Finally, they use flooding flows or brute force to compromise hosts. Because attackers wish to avoid detection, they launch their

attacks at low frequency and strength. Therefore, such attacks cannot be confirmed as real attacks. The system decides to identify such attacks as suspicious events to track and display the risk of these IPs to the users. Users are warned of these IPs and can take remedial actions through the management interface and block these IPs if them turns black.

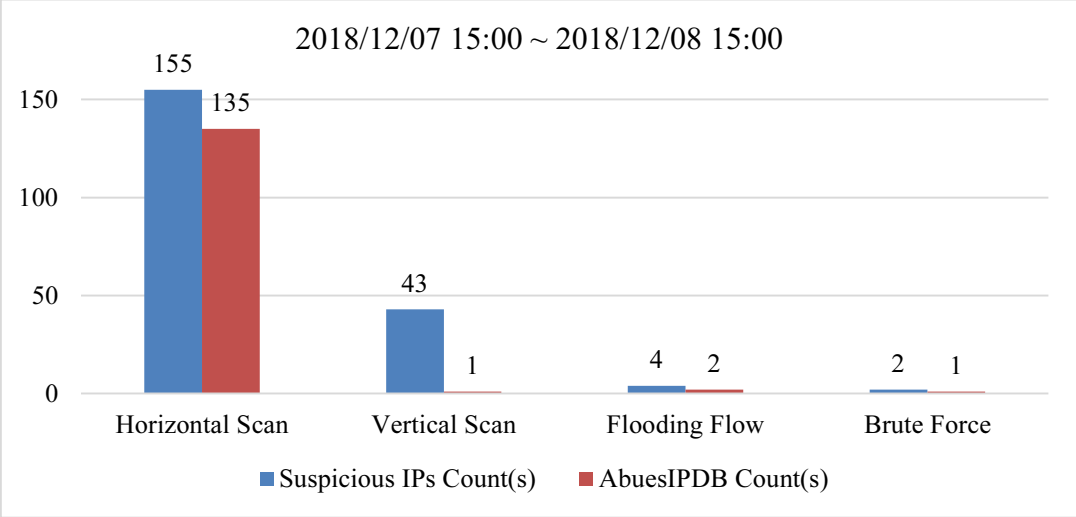

Figure 15. Suspicious IP detection result

The red bar in Figure 15 represents the number of blacklisted IPs in AbuseIPDB (comprising 155 suspicious IPs but missing 20 IPs). Figure 15 indicates the existence of brute force attacks in AbuseIPDB. Such attacks attempt to gauge the host service information and discretely compromise it. Five campus IPs were present in the remaining non-AduseIPDB IPs (Table 3), and Whois was used to confirm the information of each IP. The first IP in the table was used for conducting the security experiment in the campus. The destination IPs consisted of hacker recruiting and unsecure websites. Similarly, the fourth IP was used to research destination IPs. The destination IPs consisted of particular colleges in Korea and Malaysia. The second and third IPs were the most prevalent in the remaining 20 IPs. Because the behavior and amount of querying or response from prominent cloud computing services and ISP were similar to the attacks, the RAS identified these behaviors as suspicious IPs to track such conditions and provide warnings about real attacks. The last IP in the table generated considerable flows to the subnet 192.168.250.0/21. Because 192.168.XX.XX were in private IP range, these situations were recognized as environmental configuration setting errors.

5 Conclusions

This paper proposes a RAS for analyzing attack and risk levels in a campus environment. First, the system compares the threshold monitoring NIDS and supervised learning NIDS and separates the attack IP and suspicious IP connections. Subsequently, the attack IP management module blacklists the attack IPs. The attack IPs are compared with the HIDS attack record, and the missing-attack IPs are appended into the blacklist to warn users.

The suspicious IP management module divides suspicious flows into three event types by using the behavior estimation algorithm. Moreover, to gauge the relation among suspicious IPs, the module used the event correlation algorithm based on IPRank to calculate the relation of every IP. The highest rank indicates that the attack launches as many suspicious connections as possible. The proposed RAS combines two systems, namely the HIDS and NIDS, to identify most of the attacks. However, the limitation of the aforementioned systems is that they cannot precisely detect zero-day attacks. In the future, the RAS can be integrated with other data sources such as honeypot and DPI to improve detection accuracy and risk assessment. Besides, with the advance of machine learning technology, the behaviors of network and hosts can be improved. This will be the next step this study needs to accomplish.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This work was supported in part by the Ministry of Science and Technology of Taiwan, under Contracts MOST 108-2218-E-006-035 and 108-3116-F-006-008-CC2.

References

[1] J. M. Ehrenfeld, Wannacry, Cybersecurity and Health

Information Technology: A Time to Act, *Journal of Medical Systems*, Vol. 41, No. 7, p. 104, July, 2017.

[2] M. L. Hsieh, S. Y. K. Wang, Routine Activities in a Virtual Space: A Taiwanese Case of an ATM Hacking Spree, *International Journal of Cyber Criminology*, Vol. 12, No. 1, pp. 333-352, January-June, 2018.

[3] K. Ingham, S. Forrest, *A History and Survey of Network Firewalls*, University of New Mexico, Technical Report 2002-37, January, 2002.

[4] A. W. Moore, K. Papagiannaki, Toward the Accurate Identification of Network Applications, *International Workshop on Passive and Active Network Measurement*, Boston, MA, USA, 2005, pp. 41-54.

[5] F. Sabahi, A. Movaghar, Intrusion Detection: A Survey, *2008 Third International Conference on Systems and Networks Communications*, Sliema, Malta, 2008, pp. 23-26.

[6] Z. Wang, X. Li, Intrusion Prevention System Design, in: Z. Zhong (Ed.), *Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012*, Springer-Verlag London, 2013, pp. 375-382.

[7] P. S. Kenkre, A. Pai, L. Colaco, Real Time Intrusion Detection and Prevention System, in: S. Satapathy, B. Biswal, S. Udgata, J. Mandal (Eds.), *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, Springer, 2015, pp. 405-411.

[8] S. C. Sethuraman, S. Dhamodaran, V. Vijayakumar, Intrusion Detection System for Detecting Wireless Attacks in IEEE 802.11 Networks, *IET Networks*, Vol. 8. No. 4, pp. 219-232, July, 2019.

[9] S. Liu, L. Wang, J. Qin, Y. Guo, H. Zuo, An Intrusion Detection Model Based on IPSO-SVM Algorithm in Wireless Sensor Network, *Journal of Internet Technology*, Vol. 19 No. 7, pp. 2125-2134, December, 2018.

[10] M. Guimaraes, M. Murray, Overview of Intrusion Detection and Intrusion Prevention, *Proceedings of the 5th Annual Conference on Information Security Curriculum Development,* Kennesaw, GA, USA, 2008, pp. 44-46.

[11] A. Lazarevic, V. Kumar, J. Srivastava, Intrusion Detection: A Survey, *Managing Cyber Threats*, Springer, 2005, pp. 19-78.

[12] H. J. Liao, C. H. R. Lin, Y. C. Lin, and K. Y. Tung, Intrusion Detection System: A Comprehensive Review, *Journal of Network and Computer Applications*, Vol. 36, No. 1, pp. 16-24, January, 2013.

[13] Iso.Org, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, 2019.

[14] CVSS V3.0 Specification Document, *FIRST: Forum Of Incident Response and Security Teams*, https://www.first.org/cvss/specification-document#n4, 2019.

[15] G. Beigi, J. Tang, H. Liu, Signed Link Analysis in Social Media Networks, *Tenth International AAAI Conference on Web and Social Media*, Cologne, Germany, 2016, pp. 539-542.

[16] G. Scanniello, A. Marcus, D. Pascale, Link Analysis Algorithms for static Concept Location: An Empirical Assessment, *Empirical Software Engineering*, Vol. 20, No. 6, pp. 1666-1720, December, 2015.

[17] L. Page, S. Brin, R. Motwani, T. Winograd, *The PageRank Citation Ranking: Bringing Order to the Web*, Stanford InfoLab, Tech. Rep., January, 1998.

[18] D. K. Tseng, C. S. Yang, *A NetFlow Based Malicious Traffic Detection Research using XGBoost*, Master Thesis, National Cheng Kung University, Tainan, Taiwan, 2018.

[19] S. H. Yao, C. S. Yang, *Detection and Handling of Web Attack on Linux Web Server using Signature-based Approach: A Study of Cryptojackin*g, Master Thesis, National Cheng Kung University, Tainan, Taiwan, 2018.

[20] ELK, https://www.elastic.co/cn/elk-stack, 2019.

[21] C. Y. Kuo, C. S. Yang, *Design and Implementation of a Network Intrusion Detection System Based on NetFlow*, Master Thesis, National Cheng Kung University, Tainan, Taiwan, 2015.

[22] Abuseipdb.Com, *Abuseipdb - IP Address Abuse Reports - Making The Internet Safer, One IP At A Time*, https://www.abuseipdb.com/, 2019.

[23] Global WHOIS Inquiry, *Whois365.Com*, https://www.whois365.com/tw/, 2019.

Biographies

Cheng-Chung Kuo received the B.S. degree in Computer Science Engineering from National Sun-Yat Sen University (NSYSU) and the M.S. degree in Computer Science and Information Engineering from Chang Gang University, Taiwan. His research interests include network security, malware analysis and network management.

Chia-Ling Hou received the B.S. degree in Department of Electrical Engineering from National Changhua University of Education and the M.S. degree in Computer and Communication Engineering from National Cheng Kung University. Her research interests include network monitoring and network security

Chu-Sing Yang is a Professor of Electrical Engineering in the Institute of Computer and Communication Engineering at National Cheng Kung University (NCKU). He joined the faculty of the Department of Electrical Engineering at NCKU in 2006. His research interests include software-defined networking, network management, cloud computing, and cyber-security.