Threat Intelligence Sharing Community: A countermeasure against Advanced Persistent Threat

Sonali Chandel[1], Mengdi Yan[1], Shaojun Chen[2], Huan Jiang[2], Tian-Yi Ni[3]
New York Institute of Technology, Nanjing, China [1, 2]
Arizona State University, Tempe, USA[3]
schandel@nyit.edu[1], myan04@nyit.edu[1], schen52@nyit.edu[2], hjiang09@nyit.edu[2], tianyin1@asu.edu[3]

Abstract

Advanced Persistent Threat (APT) having focused target along with advanced and persistent attacking skills under great concealment is a new trend followed for cyber-attacks. Threat intelligence helps in detecting and preventing APT by collecting a host of data and analyzing malicious behavior through efficient data sharing and guaranteeing the safety and quality of information exchange. For better protection, controlled access to intelligence information and a grading standard to revise the criteria in diagnosis for a security breach is needed. This paper analyses a threat intelligence sharing community model and proposes an improvement to increase the efficiency of sharing by rethinking the size and composition of a sharing community. Based on various external environment variables, it filters the low-quality shared intelligence by grading the trust level of a community member and the quality of a piece of intelligence. We hope that this research can fill in some security gaps to help organizations make a better decision in handling the ever-increasing and continually changing cyber-attacks.

Keywords: Threat Intelligence, Cyber Attack, Sharing Community, Advanced Persistent Threat, Data Sharing

1. Introduction

1.1. Overview

With the development of various internet technologies, information security has become one of the biggest concerns for every organization. Cyber threats and attacks are widely causing severe damages to the working environment and the reputation of all kinds of businesses. Many cybersecurity organizations provide many options for other organizations to detect and prevent the possible cyber threats and attacks, like data protection in the cloud service [1], virus scanners, firewalls, and some cybercrime detection systems with the purpose to reduce the economic, political and private information loss.

The collaborative sharing of these cyber threat information, which is also known as threat intelligence, among business organizations can effectively help defend or defeat these cyber-attacks. The attack actors in these cases can range from being an "inadvertent actor" with no malicious intent to the Advanced Persistent Threat (APT) [2].

APT, as a new class of cyber threat, has emerged recently. It was initially created to attack only military domains, but now it targets a wide range of industries [3]. APT is a multi-step cyber threat based on 'one-day exploits,' and typically the attack objectives can still be of service even after the critical systems have already been breached [4]. Finding a solution to cope with APTs are always very challenging because the current security methods are mainly focused on the known signature of cyber threats and attacks, while APTs targets unknown security loopholes [4]. This means that once the system is attacked, the damage and information loss that takes place is enormous.

Threat intelligence sharing is the open exchange of information and knowledge about threats, cybercrimes, vulnerabilities due to increasing need to protect companies' and government's systems against those security threats and issues [5]. Most of the available studies and research focuses on one factor claiming its effect on the overall performance of the sharing efficiency like insider threats or the quality of intelligence information.

Our contribution in this paper is a comprehensive analysis of the model of an intelligence sharing community platform that includes both aspects of community size and its composition [6]. As an improvement over the idea proposed in [6], we have defined the size of the community considering not only the information quantity but also the insider threat potentiality. Also, the composition of the community is based on the quality of intelligence sharing. This means that the lower quality of the sharing of intelligence implies less contribution from the community members — the threat intelligence sharing community model matters because this area still lacks a significant amount of exploration. An efficient and safe method for threat intelligence sharing will create a more powerful and instantaneous defense to the cyber-attacks.

There are five sections in this paper. Section 2 introduces the working principle of threat intelligence. Section 3 mentions the issues of threat intelligence. In section 4, we integrate a solution using a threat intelligence

978-1-7281-1198-8/19/$31.00 ©2019 IEEE
DOI 10.1109/MIPR.2019.00070

IEEE computer society

sharing community model for dealing with these issues. In section 5, we present the conclusion and shortcomings of our model along with the future of the threat intelligence sharing community.

1.2. Related work

Every year, security organizations, like the Escal Institute of Advanced Technologies (SANS Institute), McAfee and European Union Agency for Network and Information Security (ENISA) [7,8,9] publish their reports based on the analysis of many threat intelligence sharing platforms to predict some new trends of security issues, summarize the limitation of current platforms and also suggest the most powerful operations throughout the year. [3, 10] points that APTs are commonly targeted attacks and is typically a long-running campaign highly-focusing on a limited number of organizations. Based on the stages of APT attacks, the attack techniques and countermeasures vary [4, 11].

Many security experts propose that having a combination of several security techniques might reduce the likelihood of sensitive data being stolen. They also suggest that the individual and group security techniques should vary for organizations as people have different duties and the solutions to individuals cannot work in group settings. [12].

Also, there exist some commercial and open-source intelligence sharing community like the AlienVault Open Threat Exchange (OTX), which does not allow members to add new intelligence gathered themselves and the intelligence sharing between members is also limited [13].

This paper defines a community that approves sharing between members and adding new data sources by members themselves. We include both sharing intelligence quality and quantity as contributing factors of a member to the sharing community.

2. The working principle of threat intelligence

The rapid and exponential growth of targeted cyber-attacks has directly led to the evolution of threat intelligence services. The most important reason for the emergence of threat intelligence is to minimize security gaps as much as possible [14]. Threat intelligence is becoming ubiquitous in information security programs. According to Cybersecurity Insider's study in 2018, called "Threat Intelligence Report," 77% of organizations consider that threat intelligence is pivotal for achieving a robust security system [14, 15]. Threat intelligence sharing has been bringing abundant positive results in defending cyber-attacks all over the world. It not only focuses on detecting but also preventing threats.

Fig. 1 shows the threat intelligence lifecycle which can be divided into direction, collection, processing, analysis, dissemination, and feedback respectively.

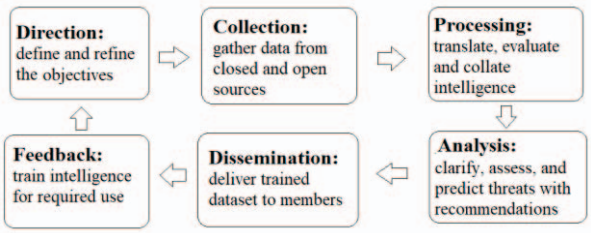

Figure 1. Threat intelligence life cycle

3. Threat intelligence issues

3.1. Threat intelligence sharing is underdeveloped and limited

Threat intelligence can help organizations in different regions working in different areas to obtain shared information from different locations at different times and improve their security and protection ability. However, due to multiple and diverse sources of information, the implementation of protocol conversion and product standardization is quite tricky. Also, due to competition and conflict of interest among different organizations, it is bound to form some specific technical barriers. As a result, sometimes it is quite difficult to fully comprehend the meaning of threat intelligence and share the analysis results [5].

3.2. Poorly-defined threat intelligence sharing community standards could lead to information quality defects

There is a considerable problem of information quality defects in the threat intelligence sharing community. Because of the limited resources and cooperation channels of massive data, the external source of the threat information is mostly dependent on the traditional tools. Since threat intelligence sharing community standards are not well defined, many times, an organization get into the sharing community for an opportunistic purpose such as non-sharing behavior or minimal contribution and make profits by using others' intelligence [16].

4. Solution to information leakage in threat intelligence

We place the sharing community in Quality of Indicators (QoI) system architecture shown in Fig. 2 [16], which was proposed by Al-Ibrahim et al. [16]. In the QoI system architecture, each pair of community members is connected in a P2P fashion. They transfer threat

intelligence to each other. The intelligence is sent to an assessor node for evaluating the quality of transferred information at the same time. In this paper, an evaluating model of the sharing community will be applied to the assessor node to help the member's organization prevent or counter-APT attacks.

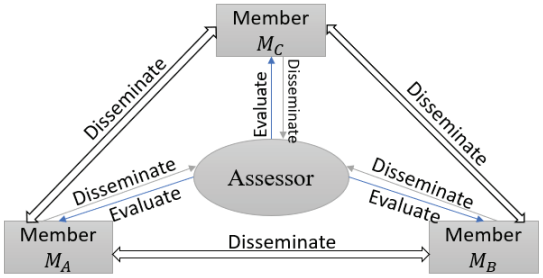

Figure 2. Threat Intelligence transfer architecture

For example, a member of the community M_A shares some intelligence information. Then this data will be disseminated not only to all the users but also to the assessor for evaluation. As APT is persistent, latent and hard to detect, a prompt information exchange platform is necessary for continuous countermeasure development and timely threat detection. More importantly, constructing a reasonable community organization would help a lot more on exchanging efficiency because the ones with low contribution will be removed.

4.1. Methodology: Define the sharing community

To improve the efficiency in sharing threat intelligence, we will redefine the sharing community by filtering the useless shared intelligence and members by grading both of them based on various indicators.

4.2. Study direction: size and composition of the community

To define the sharing community, we consider determining its two domains namely, size 'S' and community composition 'C.' Size (S) is decided by the quantity of sharing intelligence and the possibility of insider threats while composition (C) depends on who can offer valuable information that can be represented by scoring the quality of shared information.

If a member contributes a significant amount of intelligence, however, of little value, then the community should remove them, as it will affect the sharing quality of the whole community. For instance, a potential member would be willing to join the community when they see reliable and convincing data exchange instead of a community abounding inconsequential or irrelevant information.

Quality of data matters the most while the quality of intelligence leads to community composition. Therefore, the weight of 'C' is taken to be more than 50%, if we take 100 as a standard value comprised of 'S' and 'C' together.

The community size 'S' is decided by both sharing quantity and insider threats potentiality. As insider threat potentiality is comparatively important in a data sharing community and its effects on the community size, the weight of 'S' is chosen to be not much lower than 50% as well.

For this reason, 'a', which is the weight of size 'S' and 'b', which is the weight of composition 'C' is chosen to be around 40% (0.4) and 60% (0.6) respectively. This leads to the strategy for scoring a community with the following equation:

$$Community\ Score = a \times S + b \times C \quad (1)$$

Since the composition 'C' is decided by intelligence quality, several indicators have to be determined in scoring the quality. These are timeliness, authenticity, integrity, uniqueness, and effectiveness. The domains and indicators for defining the intelligence sharing community are shown in table1.

4.2.1. Size(S)

In a community, the inclusion of more members will bring more uncertainty. For such a threat intelligence sharing community focusing on cybersecurity, insider threats could cause devastating damage as well. At the same time, regardless of malicious users and infiltrators, there will be a rising probability of negligent users [17]. Two indicators including the quantity of threat intelligence and potentiality of insider threats are set to get the optimal size of a community and form the size criteria.

Table 1. Domains and Indicators for defining community

	Domain	Indicator
Community	**Size**	TI Quantity
		Insider Threat
	Composition	Timeliness
		Authenticity
		Integrity
		Uniqueness
		Effectiveness

4.2.1.1. Quantity

Usually, a more substantial amount of threat intelligence would be exchanged if more members were involved in a sharing community. Thus, we take the quantity of sharing intelligence as 'Q' and make it proportional to the number of community members 'M'

with reference to a linear constant 'k'. In this case, we give the relationship between Q and M as:

$$Q = k \times M \qquad (2)$$

4.2.1.2. Insider Threat Risks

According to Frank Brandenburg [18], with the increasing number of portable devices, remote controls, and cloud devices, the dynamics of allowing users' access to the network is more likely to create a significant percentage of potential insider threats very quickly. The potentiality of insider threats is obtained with an insider threat prediction model [6] as shown below:

$$T_i = M_i + O_i + C_i \qquad (3)$$

Where T_i stands for the threat that is caused by a member of the community. M_i is the motivation of a user. O_i is the chance of a user getting an opportunity for causing loss to the enterprise or organization and C_i is the capability of a user damaging the security of a sharing community.

The three parameters to assess threats are defined as below [6]:

$$M_i = f(V_i, S_i, P_i)$$
$$O_i = f(B_i, H_i, R_i)$$
$$C_i = f(D_i, U_i)$$

In general, the motive M_i for a member being an insider threat is evaluated by three variables:

- V_i stands for skill verification that helps to grade member's ability for bringing loss to the community
- S_i is the member's current stress level
- P_i is a predisposition to malicious behavior

Opportunity O_i found by a community member is marked by three indexes:

- B_i stands for changes of work behavior
- H_i stands for honeypot use (the degree of accessing the information forged for luring the insider attacks)
- R_i stands for system role (whether a member has the authority for advanced access to the system)

The member's capability C_i is defined by the following:

- D_i stands for demonstrated capability
- U_i stands for user sophistication attribute in the user taxonomy.

All the above variables are individually presented in table 2. The rubrics for grading the threat level T_i is shown in tables 3, 4, 5 and 6 where the three factors will receive an assessment of the following form: (1-2) low, (3-4) medium, and (5-6) high. [6]

Table 2. Symbols used in determining insider threat

Symbol	Meaning
T_i	Insider Threat Degree
M_i	Motivation
O_i	Opportunity
C_i	Capability
V_i	Skill Verification
S_i	Stress Level
P_i	Predisposition
B_i	Behavior Change
H_i	Honey Pot Use
R_i	System Role
D_i	Demonstrated Capability
U_i	User Sophistication

For example, according to table 3, if a member has no skill and a low-stress level, then their predisposition can be 1, 2 or 3. Next, as long as their predisposition is scored, their motive score is determined. If their predisposition of being an insider threat is above average, then their predisposition score is 3, which gives the total motive score as 3.

In the same way, the opportunity and capability score of this member can be obtained as well. Then, we can apply these three scores to get the results shown in table 6 and its footnote as the final score.

Table 3. Motive score

Skill Verification	*Stress Level*	*Predisposition*		
FALSE	*Low*	*1*	*2*	*3*
	Medium	*2*	*3*	*4*
	High	*3*	*4*	*5*

Table 4. Opportunity score

Demonstrated Capability	User Sophistication		
	Low	Medium	High
Low	1	2	3
Medium	2	3	4
High	3	4	5
Very High	4	5	6

Table 5. Capability score

Demonstrated Capability	User Sophistication		
	Low	Medium	High
Low	1	2	3
Medium	2	3	4
High	3	4	5
Very High	4	5	6

For instance, according to table 6, when a member's motive score is 3 (Medium), opportunity score is 5 (High), and capability score is 2 (Low), then its overall score for being an insider threat is 6. It can be seen that the overall score will range from 3 to 9.

Table 6. Overall Threat Score

Motive	Opportunity	Capability		
		Low	Medium	High
Low	Low	3	4	5
	Medium	4	5	6
	High	5	6	7
Medium	Low	4	5	6
	Medium	5	6	7
	High	6	7	8
High	Low	5	6	7
	Medium	6	7	8
	High	7	8	9

Note: According to Table 3, 4 & 5, the score computed above decides the level of motive, opportunity, and capability: Low (1-2), Medium (3-4), High (5-6)

Therefore, according to [6] danger level of the users which is the score of T_i is mapped from extremely high (9), top (7, 8), medium (5, 6) to low (3, 4).

We suggest that it is necessary for the community to pay more attention to the members with a high or extremely high score of T_i to restrain from the chances of insider threat attacks.

4.2.2. Composition(C)

The following conditions could limit the efficiency of threat intelligence sharing [19]:

- Members would choose to minimize the contribution to sharing intelligence when they become competitors in business or when it refers to their core secret in technology.
- The members would conceal some vital intelligence considering their business security.
- Organizations or companies get into the sharing community to make profits from processing the intelligence but showing a non-sharing behavior.

These considerations force the composition of a sharing community to be dynamic. It also helps to get rid of those members who may create unnecessary conflicts or neglect their duties. Whether a member is capable of staying in the community any longer has to be decided by regular scoring with their contribution of shared intelligence.

Grading a piece of threat intelligence requires analyzing five factors based on the principle of assessing information value [7]:

a) *Timeliness (t):* Being able to access and process the information timely is vital for people to make decisions. As soon as the right time has passed, the value of the intelligence would sharply decrease.
b) *Authenticity (a)*: Attackers may file false threat reports to mislead or overwhelm threat intelligence systems. If poorly handled, then data from legitimate sources can be tampered as well.
c) *Integrity (i):* Incomplete threat information may mislead the analysts causing a severe loss to the community considering the wasted time, money, and human resources.
d) *Uniqueness (u):* Only focusing on gathering and sharing more threat data would bring a risk that most of the information might be duplicate. It is necessary to capture and identify the essential structural elements of persistent attacks.
e) *Effectiveness (e):* The failure to identify relevant patterns and critical data points in threat data makes it impossible to turn data into intelligence and then into knowledge that can inform and direct security operations teams.

We apply the 'fuzzy synthetic evaluation method' for scoring and defining the 'Factors' set and 'Evaluation' set as follows [20]:

- Factors set (F) = {t, a, i, u, e}
- Evaluation set (E) = {1, 3, 5, 7, 9}

The specific numbers in the Evaluation set above correspond to {Equally Important (1), Slightly Important (3), Strongly Important (5), Very Strongly Important (7), and Extremely Important (9)}.

Analytic Hierarchy Process (AHP) is applied using MATLAB to calculate the following:

- The weight of the five factors shown in the evaluation set, E.
- The comparison matrix R, which contains comparisons of each two factors, is shown in table 7.

Analytic Hierarchy Process (AHP) is one of the multi-criteria decision-making methods that was initially developed by Prof. Thomas L. Saaty.

Table 7. The weight of factors for composition

Factor	*Timeliness*	*Authenticity*	*Integrity*	*Uniqueness*	*Effectiveness*	Weight
Timeliness	1	0.2	3	3	0.33	13 %
Authenticity	5	1	3	7	3	47 %
Integrity	0.33	0.33	1	1	0.2	7 %
Uniqueness	0.33	0.14	1	1	0.2	6 %
Effectiveness	3	0.33	5	5	1	27 %
Sum	9.67	2.01	17	17	4.73	100 %

More specifically, matrix R is shown as below:

$$\begin{pmatrix} 1.00 & 0.20 & 3.00 & 3.00 & 0.33 \\ 5.00 & 1.00 & 3.00 & 7.00 & 3.00 \\ 0.33 & 0.33 & 1.00 & 1.00 & 0.20 \\ 0.33 & 0.14 & 1.00 & 1.00 & 0.20 \\ 3.00 & 0.33 & 5.00 & 5.00 & 1.00 \end{pmatrix}$$

For example, from table 7 we can see that if 'Authenticity' is strongly more important than 'Timeliness,' then the score in the intersection of row 'Authenticity' and column 'Timeliness' will be 5. Equally, the score in the interception of row 'Timeliness' and column 'Authenticity' will be 1/5, i.e. 0.2.

To accept the result of the weight of these factors, it needs to be checked whether the value of 'Consistency Ratio' (CR) is ≤ 10%. CR can be calculated as follows [21]:

$$\mathrm{CR} = \frac{CI}{RI}$$

$$\mathrm{CI} = \frac{\lambda - n}{n - 1}$$

Where CI is the Consistency Index, λ is the maximum Eigenvalue of the matrix R, n is the number of factors, RI (Random Consistency Index) is decided by Saaty's random indexes as shown in table 8. In this case, we use n=5, which gives CR=7.6%, which meets the criteria of AHP. Hence, the weight of each factor is eligible [21].

Table 8. Saaty's Random Indexes

n	1	2	3	4	5
RI	0	0	0.58	0.90	1.12

Therefore, the composition score 'C' can be calculated from the column named weight in table 7:

$$C = t \times 0.13 + a \times 0.47 + i \times 0.07 + u \times 0.06 + e \times 0.27 \quad (4)$$

Where the coefficient of each factor represents the weight of each factor over the total value for a piece of information.

5. Conclusion and Future Work

In this paper, the present situation of the threat intelligence is introduced and analyzed. It also provides a new idea about how to define a threat intelligence sharing community that allows threat intelligence to be transferred and analyzed more effectively. The community not only enables members of the sharing community like different organizations to exchange their intelligence but also allows various companies and institutions to share threat intelligence in time. This can help in building a comprehensive cyber defense system. The key to this model is in its attention to the size and composition of the platform. Unlike the current existing platforms, the modified model in this paper over the model proposed by Kandias earlier, has very tight control over its internal members to avoid the deadly problems of insider threats.

If a community member does not upload their threat intelligence data for a long time or only upload low-quality data, they will be removed from the community by the security manager. This can help the sharing community get rid of those members who only ask for benefits without any contribution and encourage members to upload more high-quality threat intelligence as the voluminous low-quality intelligence is the main limitation of the existing threat intelligence platform.

This paper also considers the existence of insider threats when controlling the size of the community. The model prevents insider threats effectively via rating the threat value of community members according to the motives, opportunities, and abilities of community members. Those with higher scores will be cleared out of the community. The model also developed an excellent analytical standard for the value of threat intelligence.

The information evaluation model in this paper is elementary to understand as it is based on the 'fuzzy synthetic evaluation method,' depending on the timeliness, authenticity, integrity, uniqueness, and effectiveness of the intelligence. Also, the weight of each indicator is decided based on the comparison of a significant number of reports, which makes the model more reasonable.

All the evaluation of the threat intelligence and the detection of internal threats need professional skills for analysis, and this kind of capability is insufficient at the moment in the industry. This can impede the practical application of the model. Also, the threat intelligence collected from users has different data types and formats, which increases the difficulty of manual evaluation.

With the vast development of the artificial intelligence industry, deep learning methods have great potential to train neural networks that can analyze threat intelligence faster with higher efficiency. Use of AI can significantly improve the evaluation efficiency of our model and reduce labor costs. In the future, the threat intelligence community should also provide members with a uniform data type and format for uploading threat intelligence; then the intelligence can be better analyzed, evaluated, and utilized.

6. References

[1] Chandel, Sonali, Tian-Yi Ni, and Geng Yang. "Enterprise Cloud: Its Growth & Security Challenges in China." 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud

(EdgeCom). IEEE, 2018.
[2] IBM Global Business Services. 2016. "Securing the C-suite: Cybersecurity perspectives from the boardroom and C-suite," Managed Security Services, United States of America
[3] Chen, Ping, Lieven Desmet, and Christophe Huygens. "A study on advanced persistent threats." IFIP International Conference on Communications and Multimedia Security. Springer, Berlin, Heidelberg, 2014.
[4] Ghafir, Ibrahim, and Vaclav Prenosil. "Advanced persistent threat attack detection: an overview." Int J Adv Comput Netw Secur 4.4 (2014): 5054.
[5] Denise Anderson. The National Health Information Sharing & Analysis Center and the National Council of Information Sharing and Analysis Centers. 2017 [Online]. Available: https://docs.house.gov/meetings/IF/IF02/20170404/105831/HHRG-115-IF02-Wstate-AndersonD-20170404.pdf
[6] Kandias, Miltiadis, et al. "An insider threat prediction model." International Conference on Trust, Privacy and Security in Digital Business. Springer, Berlin, Heidelberg, 2010.
[7] "McAfee Labs Report Highlights Critical Challenges to Threat Intelligent Sharing," Mcafee.com, 2017. [Online]. Available: https://www.mcafee.com/enterprise/pt-br/about/newsroom/press-releases/press-release.html?news_id=20170405006423
[8] SANS Institute. CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/cti-security-operations-2018-cyber-threat-intelligence-survey-38285
[9] ENISA Institute. Exploring the opportunities and limitations of current Threat Intelligence Platforms, VERSION 1.0 DECEMBER 2017 [Online]. Available: https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms/at_download/fullReport
[10] Thonnard, O., Bilge, L., O'Gorman, G., Kiernan, S., Lee, M.: Industrial espionage and targeted attacks: Understanding the characteristics of an escalating threat. In: Balzarotti, D., Stolfo, S.J., Cova, M. (eds.) RAID 2012.
[11] Thomson, Gordon. "APTs: a poorly understood challenge." Network Security 2011.11 (2011): 9-11.
[12] Althebyan, Qutaibah, and Brajendra Panda. "A knowledge-based model for insider threat prediction." Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC. IEEE, 2007.
[13] M. Mutemwa, J. Mtsweni, and N. Mkhonto, "Developing a cyber threat intelligence sharing platform for South African organisations," 2017 Conference on Information Communication Technology and Society (ICTAS), Umhlanga, 2017, pp. 1-6.
[14] SANS Institute. The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing. [Online] Available: https://www.sans.org/reading-room/whitepapers/bestprac/state-cyber-threat-intelligence-survey-cti-important-maturing-37177
[15] Holger Schulze. Threat Intelligence Report. Cybersecurity Institute, 2018.
[16] O. Al-Ibrahim, A. Mohaisen, C. Kamhoua, K. Kwiat, L. Njilla, Beyond free riding: Quality of indicators for assessing participation in information sharing for threat intelligence, IEEE Symposium on Privacy-Aware Computing (PAC), 2017.
[17] Detex System, "2017 insider threat intelligence report", 2017. Available at https://www.thehaguesecuritydelta.com/media/com_hsd/report/154/document/2017-Insider-Threat-Intelligence-Report.pdf
[18] Barnum S. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™) [J]. Mitre Corporation, 2014.
[19] Zhou Jiuchang. On the Competitive Intelligence (CI) Sharing and Leak of Network Organizations[J]. Library and Information Service, 50(10):32-35, 2006. 2006, 50(10):32-35.
[20] Li, F., Wang, W., Shi, Y., & Jin, C. "Fuzzy synthetic evaluation model based on the knowledge system." International Journal of Innovative Computing, Information and Control 9.10 (2013): 4073-4084.
[21] CJCU. Analytic Hierarchy Process (What is AHP). [Online] Available: web.cjcu.edu.tw/~lcc/Courses/TUTORIAL/AHP%20Tutorial.doc