International Journal of Engineering & Technology, 7 (2.33) (2018) 1156-1159

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Inter-Collaboration Design between ISP CERTs and Security Center for Effective Response of Large-Scale Cyber Attacks

Kyuil Kim[1], Buseung Cho[2*], Wonhyuk Lee[3], Dongkyun Kim[4], Hyungwoo Park[5]

[1]*Advanced KREONET Center, Korea Institute of Science Technology Information(KISTI), 245 Daehangno, Yuseong, Daejeon, 306-806, Korea*
[2,3,4]*KISTI, Advanced KREONET Center, 245 Daehanno, Yuseong, Daejeon, 306-806, Korea*
[5]*KISTI, Global Science experimental Data hub Center, 245 Daehanno, Yuseong, Daejeon, 306-806, Korea*
[*]*Corresponding author E-mail: bscho@kisti.re.kr*

Abstract:

Recently, cyber-threats have been increased every day with most of the information is transmitted by internet. Many institutions perform appropriate countermeasure against cyber crisis. However, they have been considered a partial solution to the problem. The current response for large-scale cyber-attacks is inadequate. Many institutions that provide main service and resource to the user are suffered by cyber-attacks. We propose the effective response method against their cyber threats. Our proposed mechanisms reduce the cyber threats through inter-collaboration design between ISP CERTs and security monitoring and response. While they perform the security monitoring for the only own circuit, the institution use the various networks such as main network and backup network etc. Among their network, ISP CERTs can exist or can't exist and security center can exist or can't exist too by the security service policy of ISP. Therefore, while institution reduces the cyber threat through them, the circuit that they don't exist significantly increases the security threat. And the institution not only hasn't the trust for the circuit but also increase in cyber threat because ISP optionally provides the security service. Therefore, we design the inter-collaboration mechanisms of them that rapidly and exactly response the cyber-attacks. We also implement inter-collaboration system based on the global threat management, global network control, RBL(Real-time Blocking List)

Keyword: *Cyber-attacks, Inter-Collaboration, ISP CERTs, Security Monitoring & Response, Hacking*

1. Introduction

These Days, internet has become the method used by many people. We carry out the task such as education, research, education and interest, etc. based on the own privacy information through the internet. However, cyber-attacks have been increased as their privacy information is transmitted by the internet. Internet always is not only exposed from cyber-attacks but also bring the critical damage from them. Currently, ISP CERTs and Security Center is working on countermeasures against cyber threats. But, they are situation that doesn't suitably answer to users not even already well-known attacks.

In this paper, we propose the effective response method against them. Especially, we propose inter-collaboration design between ISP CERTs and Security Center to defend cyber threats. Our design is systematic approach that promptly and correctly response cyber-attacks based on their role. It defines their role and has productive results to prevent the critical damage that cyber-attacks frequently occur. Also, our proposed mechanisms reduce the cyber threats through inter-collaboration design between ISP CERTs and security monitoring and response. While they perform the security monitoring for the only own circuit, the institution use the various networks such as main network and backup network etc. And the institution not only hasn't the trust for the circuit but also increase in cyber threat because ISP optionally provides the security service. Therefore, we design the inter-collaboration mechanisms of them that rapidly and exactly response the cyber-attacks.

2. Related Work

Recently, many studies such as Big data, IoT, and Session (C.L. Philip Chen and Chun-Yang Zhang, 2014), (Gandhi R., Sharma A., and Mahoney W., et al 2011), (M. Indu Masheswari, S. Revathy and R.Tamilarasi, 2016), (Narayanam Sri Prakash and N. Venkatram, 2016), (Sangjun Ko et al 2014), (S. Rahimi Moosavi et al 2015), (Teng Xu et al 2014) have been introduced the response technique for new cyber-attacks. Many people and institutions perform appropriate countermeasure for the cyber crisis through their studies. However, they always are being damaged by well-known cyber-attacks though have the various security devices and defensive measure. They have been considered a partial solution to the problem. We focus on not only the security techniques but also the overall security system based on inter-collaboration.

3Proposed Mechanism

3.1. Proposed Concept

In this section, we explain why proposed design is necessary. In left side of Fig1 show the security monitoring state for the arbitrary institutions and right side present proposed design based on inter-collaboration. Most of research and education institutions carry out large data transmission and collaboration task using the various networks. In their network, one use as main network and the others use as sub or backup networks. Among their network, ISP CERTs can exist or can’t exist and security center can exist or can’t exist too by the security service policy of ISP. Therefore, while institution reduces the cyber threat through them, the circuit that they don’t exist significantly increases the security threat. The institution not only easily is exposed by always cyber-attacks but also bring the problem to build the security policy and the appliances. We propose the inter-collaboration between ISP CERTs and security center to solve these problems. Our concept reduces the cyber threat level for the institution through the proposed design. As right side of this Fig1, the rapid and correct detection, analysis and response not only are possible but only can carry out the network control in case of the large scale attack through Inter-collaboration.

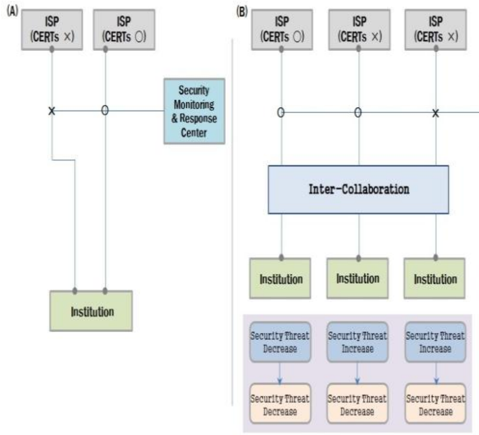

Fig. 1. Security Threat State of Institution

3.2. Proposed Model

In this section, we introduce the excellence of proposed model through existing and our model comparison. The upper of Fig.2 shows current security architecture. It consists of the circuit, monitoring and institution and the circuit is IX set (Internet eXchange IX = {IX_1, IX_2, ⋯, IX_i}) Monitoring field guards the threat traffic in ISP CERTs and security center. They mainly carry out the monitoring for assigned circuit to them. Institution provides the service and resource to the users and constructs the security system to protect own area. The root cause that many institutions don’t response the well-known cyber-attacks is the security countermeasure. First of all, DDoS attack absolutely performs the response in the institution though the security organization exists.

While institution uses multi-network such as main and backup network, etc. ISP CERTs and security center don’t realize the current situation because they monitors only own assigned circuit. Also, security organization doesn’t exist for the all circuits. Ether only ISP CERTs exist or only security center exist as their security and service policy in the IX. In the worst case, no one carry out the monitoring for the circuit. Therefore, when large-scale cyber-attack occurs institution doesn’t response the threat traffic received in the various and a lot of IP. After of all, they has the problem that don’t provide the user with their service though security device and manual exists.

We propose inter-collaboration model to solve this problem as the bottom of Fig1. Inter-collaboration stores and shares detected threat traffic in the each circuit. It carries out early response and the network control through shared information and notice the result to the institution. Institution sets the traffic threshold and different route through noticed result and share the task based on role. They not only can block the threat attack but also normally can provide main service to the user.

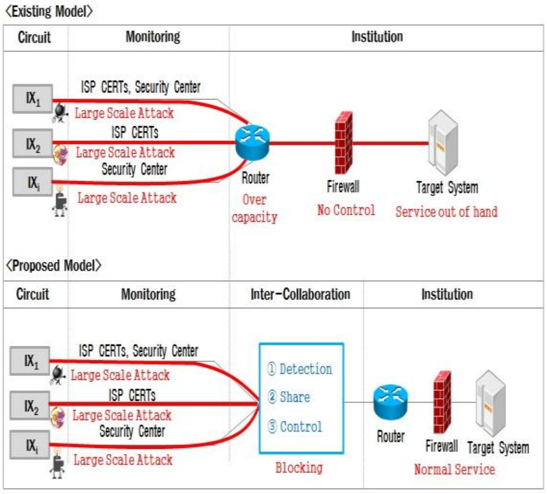

Fig. 2. Existing and proposed model comparison

3.3. Proposed Framework

We introduce inter-collaboration design to response as Fig3. Our design consists of global threat management, global network control, RBL, global inter-viewer and DB.

1. Global Threat Management: it classifies detected cyber-attacks (well-known and unknown) them to promptly response well-known attacks and raise detected accuracy. In the case of well-known attack, it receives and shares the detected attacks through their traffic threshold and detection pattern. The other way, unknown attacks perform the analysis sharing to verify false positive.

2. Global Network Control: it prevents the continuous damage and spread against cyber-attacks. It analysis the traffic of IP and determine the circuit blocking to perform the network control.

3. RBL (Real-time Blocking List): RBL denies IP and notices the result to the user when infected system sends the spam mail to the target system. User can’t access different circuits if is registered by RBL. Therefore, RBL must certainly be necessary for the inter-collaboration must quickly respond. We construct the RBL registration, measure and report to can carry out the quick response.

4. Global Inter-Viewer: it provides the intuitive screen for the real presentation of each module. Also, it enables one to extract and search the statistical data.

5. DB: it stores them after encrypts each the module information because security data is sensitive information.

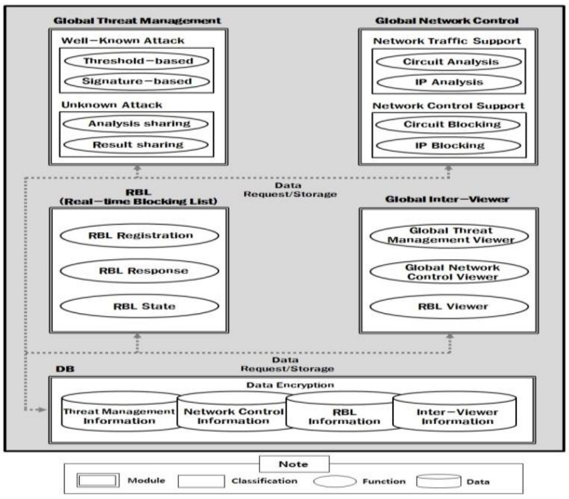

Fig. 3. Inter-collaboration framework against cyber threats

4. Process of Inter-Collaboration

4.1. Process of Global Threat Management

In this section, we describe the proposed process and effect of inter-collaboration system. Our design consists of three processes (global threat management, global network control and RBL (Real-time Blocking List). As the Fig4, global threat management is inter-collaboration between ISP CERTs and security center to promptly response the cyber-attacks.

Step 1~8 : ISP CERTs and security center register the threat traffic through proposed system when cyber-attack is detected. Inter-collaboration system classifies the cyber-attacks as unknown attack and well-known attack. Well-known attack divides by the signature-based and the threshold-based. The signature- based means cyber-attacks such as warm virus and web vulnerability etc. and threshold-based means large scale attacks alike DDoS attacks. Inter-collaboration system promptly notifies the technical solution to the institution through already analyzed data, if cyber-attack type is well-known. Otherwise, cyber-attack type is unknown, our system find the technical solution through the analysis sharing and notifies it to the institution because the analyzed data don't exist.

Step 9~13 : the institution returns the result after it response the cyber-attacks based on the technical solution from them. Our system performs the verification based the received result and notifies it to ISP CERTs and security center.

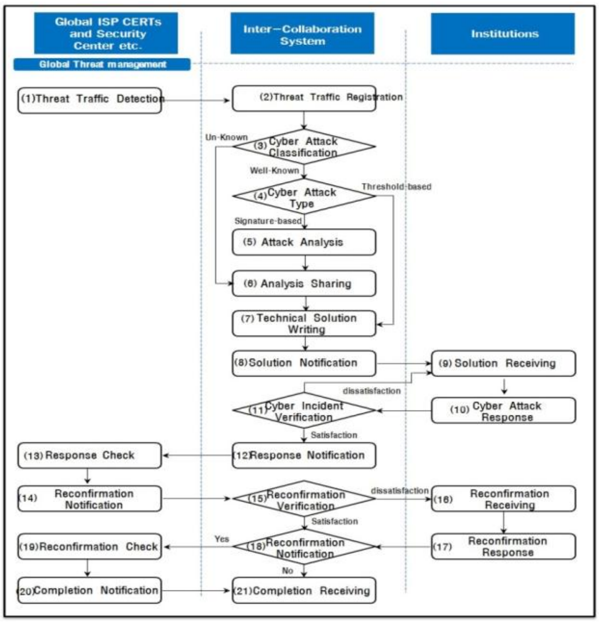
Global ISP CERTs and Security Center etc.
Inter–Collaboration System
Institutions
Global Threat management
(1)Threat Traffic Detection
(2)Threat Traffic Registration
Un-Known
(3) Cyber Attack Classification
Well-Known
(4) Cyber Attack Type
Threshold-based
Signature-based
(5) Attack Analysis
(6) Analysis Sharing
(7) Technical Solution Writing
(8) Solution Notification
(9) Solution Receiving
dissatisfaction
(11) Cyber Incident Verification
(10) Cyber Attack Response
Satisfaction
(13) Response Check
(12) Response Notification
(14) Reconfirmation Notification
(15) Reconfirmation Verification
dissatisfaction
(16) Reconfirmation Receiving
Satisfaction
(19) Reconfirmation Check
Yes
(18) Reconfirmation Notification
(17) Reconfirmation Response
No
(20) Completion Notification
(21) Completion Receiving

Fig. 4. Process of Global Threat Management

Step 14~21 : they check the response result and re-notifies for the reconfirmation to the inter-collaboration system if they don't satisfies the response result. Inter-collaboration system verifies the reconfirmation and it determines whether it carries out by myself or notifies the reconfirmation to the institution again. Received ISP and security center checks the re-response result and notifies to them.

4.2. Process of Global Network Control

As the Fig5, global network control performs the circuit supporting for the prevention of spread of damage during the certain period against the largescale cyber-attacks.

Step 1~6 : ISP CERTs and security center detects critical cyber-attacks in the networks and registers the inter-collaboration system. It classify as the large scale cyber-attacks and very large scale cyber-attacks. The large scale attack notifies the countermeasure through already standardization solution to the institution. Otherwise, Very large scale attack notifies the shared information to the institution after it comes up with the critical level of cyber-attacks through the analysis sharing.

Step 7~13 : Inter-collaboration system establishes the network control IP, control period and circuit name etc. And notifies ISP CERTs and security center after verifies the received response. They check the network control supporting and return the completion notification to our system.

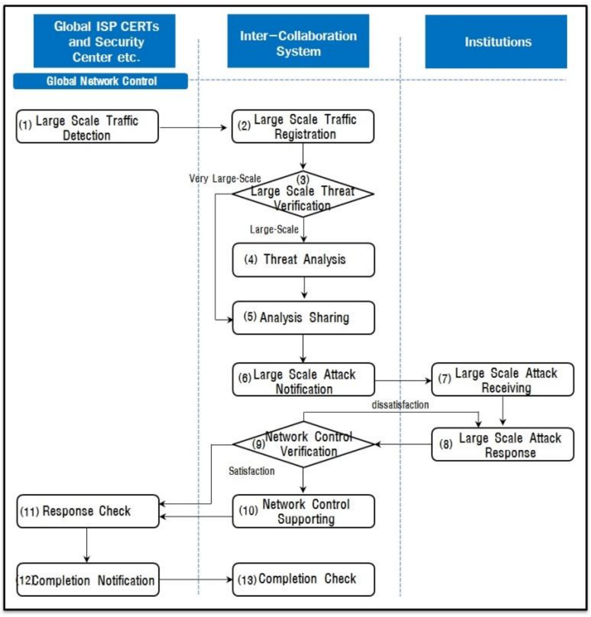
Global ISP CERTs and Security Center etc.
Inter–Collaboration System
Institutions
Global Network Control
(1) Large Scale Traffic Detection
(2) Large Scale Traffic Registration
Very Large-Scale
(3) Large Scale Threat Verification
Large-Scale
(4) Threat Analysis
(5) Analysis Sharing
(6) Large Scale Attack Notification
(7) Large Scale Attack Receiving
dissatisfaction
(9) Network Control Verification
(8) Large Scale Attack Response
Satisfaction
(11) Response Check
(10) Network Control Supporting
12 Completion Notification
(13) Completion Check

Fig. 5. Process Global Network Control

4.3. RBL (Real-time Blocking List) Process

As the Fig6, RBL(Real-time Blocking List) blocks the IP for the this system if arbitrary system is infected by the virus and the infected system transfers the spam mail from domestic and foreign networks. Blocked IP must promptly carry out the removal action because it can't connect another circuit. Therefore, our inter-collaboration system shows the process for RBL response and removal as follows.

Step 1~7 : Inter-collaboration system notifies RBL to the institution if RBL is registered by ISP CERTs and security center. Received institution returns the result to inter-collaboration system after it examines the infected system. It verifies this result and returns it to ISP CERTs and security center.

Step 9~12 : ISP CERTs and security notifies RBL removal to the institution after they check RBL response result.

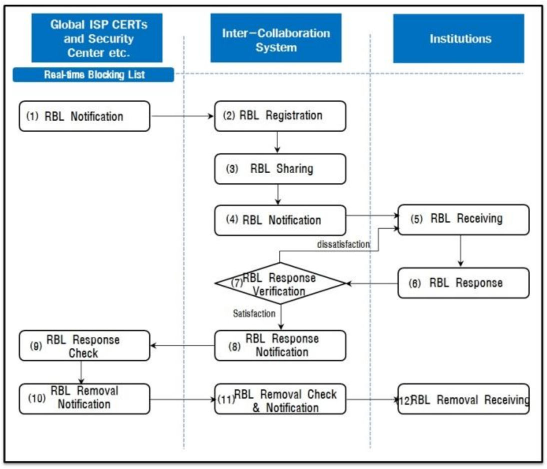

Fig. 6. RBL Process

4.4. Implementation

We implement the inter-collaboration system based on global threat management, global network control and RBL process. Our OS is Linux and it use JSP, HTML, Java script, CSS programming language. Also, development program applies ORACL 10, Apache Tomcat 6.0 and jquery 2.1 versions.

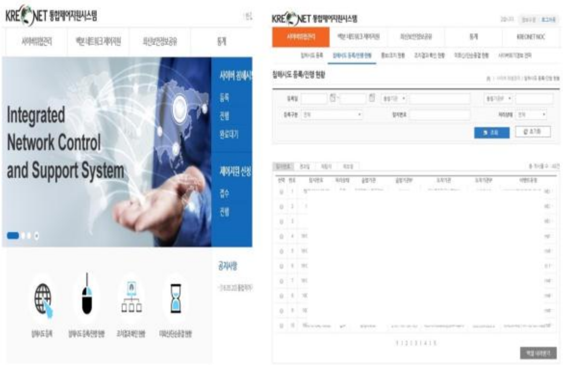

Fig. 7. Partial Screen of Inter-Collaboration System

Firstly, we constructed ORACL DBMS environment after built Apache Tomcat server. Secondly, we constructed actually DBMS using the SQL dump files. Finally, we uploaded developed web page, script files and style sheet etc. to the server. Fig7 shows one part of our system and we blinded the related items for the security.

5. Conclusion

We proposed inter-collaboration design between ISP CERTs and security center for effective response of well-known cyber-attacks. Also, we presented the false positive and inter-collaboration response for the unknown attack through our system. As a result, proposed system provided the users and institutions with the prompt and correct response for cyber threats.

Acknowledgment

This research was support by “Building and Services of Advanced KREONET Based on Software” Program funded by the Ministry of Science, ICT&Future Planning(K-17-L01-C04)

References

[1] C.L. Philip Chen and Chun-Yang Zhang, “Data-Intensive applications, challenges, techniques and technologies: A survey on Big Data,” Information Sciences Journal of Elsevier, vol. 275, pp.314-347, Aug. 2014.

[2] Gandhi R., Sharma A., and Mahoney W., et al., “Dimensions of Cyber-Attacks: Cultural, Social, Economic and Political,” IEEE Technology and Society Magazine, vol. 30(1), pp. 28-38, Mar. 2011.

[3] M. Indu Masheswari, S. Revathy and R.Tamilarasi, “ Secure Data Transmission For Multi-sharing in Big Data Storage,” Indian Journal of Science and Technology, vol. 9(21), DOI: 10.17485/ijst/2016/v9i21/95164, Jun. 2016.

[4] Narayanam Sri Prakash and N. Venkatram, “Establishing Efficient Security Scheme in Home IOT Devices through Biometric Finger Print Technique,” Indian Journal of Science and Technology, vol. 9(17), DOI: 10.17485/ijst/2016/v9i17/93039, May 2016.

[5] Sangjun Ko, Kyuil Kim, Yousu Lee and Jungsuk Song, “A Classification Method of Darknet Traffic for Advanced Security Monitoring and Response,” Lecture Notes in Computer Science, vol. 8836, pp 357-364, 2014.

[6] S. Rahimi Moosavi, T. Nguyen Gia, E. Nigussie, et al., “Session Resumption-Based End-to-End Security for Healthcare Internet-of-Things,” Proceeding of IEEE International Conference (CIT/IUCC/DASC/PICOM), DOI: 10.1109/CIT/IUCC/DASC/PICOM.2015.83, pp. 581-588, Oct. 2015.

[7] Teng Xu, James B. Wendt and Miodrag Potkonjak, “Security of IoT system: Design challenges and opportunities,” Proceedings of IEEE/ACM International Conference (ICCAD), DOI: 10.1109/ICCAD.2014.7001385, pp. 417-423, Nov. 2014.