Active Response Model and Scheme to Detect Unknown Attacks

Bonghan Kim, Sijung Kim, *Member, KIMICS*

Abstract—This study was conducted to investigate what to consider for active response in the intrusion detection system, how to implement active response, and 6-phase response models to respond actively, including the active response scheme to detect unknown attacks by using a traffic measuring engine and an anomaly detection engine.

Index Terms—Active response, anomaly detection, Intrusion detection, Unknown attack.

I. INTRODUCTION

The intrusion detection system is to monitor whether there is any suspicious action in such intrusion, and to detect and dispose the intrusion early. However the existing intrusion detection system has exposed many problems in network security so far. Thereby, the existing intrusion detection system using the passive response method must be first improved so that the system to protect a network more efficiently can be devised.

For this, a study of active response is being performed as a part of the active network security system based on IETF. Internationally, each governmental authority takes the initiative in studying the intrusion detection system with a new concept through next-generation network technology advices. Therefore this thesis was prepared to search how to solve problems in the existing intrusion detection system, and how to actively respond which is an important factor to lead technically. For this study, we investigated what to consider for active response in the intrusion detection system, how to implement active response, and 6-phase response models to respond actively, including the active response scheme to detect unknown attacks by using a traffic measuring engine and an anomaly detection engine.

II. RELAED WORK

ISO and U.S.A have steadily performed R&D for the intrusion detection system and so has comprehensive results for its model and prototype. Diverse projects are being performed under the auspice of DARPA/ ITO(Defense Advanced Research Projects Agency / Information Technology Office) anomaly event detection; analysis and response method for intrusion detection in a large-scale network; network intrusion detection; misuse intrusion detection technology; important resource allocation and intrusion response; and model-based real-time intrusion detection system. IETF defined the data format and exchange procedures to standardize the intrusion detection and response technologies and to share inter-system information. IETF IDWG(Intrusion Detection Working Group) announced IDMEF(Intrusion Detection Message Exchange Format) which specifies procedures to exchange information and format data required for intrusion detection systems and response management systems, and IDXP(Instruction Detection eXchange Protocol) which is a protocol to exchange data [1][2].

It is known that 60% of currently commercialized intrusion detection systems are based on the network and 70% of the intrusion judgment method applies the misuse detection technology. The commercial intrusion detection system is usually based on the network. However an integration model of the host-based system and the network-based system occupies a high market share. A hybrid model to improve the detection rate by adding the anomaly event detection function has recently increased.

The intrusion detection system market has been more and more expanded. It has been highlighted to integrate the security mechanism such as the intrusion prevention system or the private virtual network by inter-working among diverse intrusion response technologies.

III. ACTIVE RESPONSE APPROACH

A. Considerations for Active Response

Following 7 requirements for active response were considered [4].

1) Signature quality

The signature-based detection system must create a signature conforming to intrusion. It requires sensitivity and specificity to effectuate intrusion signature in filtering traffic.

Manuscript received April 21, 2008; revised August 12, 2008, Bong-Han Kim is with the Department of Computer and Information Engineering, Chongju University, Chongju, 360-764, Korea (Tel: +82-43-229-8495, Fax: +82-43-229-8486, Email: bhkim@cju.ac.kr)

2) Signature quantify and length

The system conforming to a flow payload responding to a signature must be compared with all signatures of which flows are known as IP protocol and port. A few signatures increase the matching speed. The cost of signatures under matching is in proportion to the length of signature. Accordingly the short signature is more efficient than the long signature.

3) Robustness against polymorphic worms

Polymorphic worms change their payloads while on attempting intrusion continuously. A signature sensitive to one worm payload may be insensitive to another worm payload. Thereby worms are allotted to match with the signature. If worms are polymorphic, each payload will not be included in any bite string. The polymorph will result in increasing the number of signatures required to match with worms.

4) Timeliness of detection

If a packet is not checked by patches or traffic filtering etc., port scanning worms will attack vulnerable hosts in geometric progression until infected hosts are saturated. So it is very important to patch infected hosts. Patching has to be completed before worms attack hosts actually according to the attack scenario. When the attack begins, signature-based filtering in attack traffic prevents worm propagation most efficiently.

5) Automation

The signature-based intrusion detection system should request an administrator to intervene in minimum real time. For instance, if the administrator examines signatures minutely to find specificity visually, it may be helpful to detect whether there are new attacks. However if he/she is absent, there is no response method. This should be considered together with the timeliness of signature detection.

6) Application neutrality

A knowledge of application protocols higher than TCP class(HTTP, NF RPC, etc.) may be useful when you identify worms and harmless traffics and produces sensitive and specific signatures. However learning the knowledge is not a prerequisite. That is why the applicability of the signature detection system is widening by all protocols higher than TCP class.

7) Bandwidth efficiency

If the signature detection system is dispersedly allocated, this traffic monitor will cooperate with other detection systems to check. Although an attack creates network activities greatly, communication must be scalable. That is to say, as attack activities increase, monitor-to-monitor cooperative communication must also increase.

B. Active Response Implementation Methods

Intrusion response is differently implemented in the system with a different operating system platform. The intrusion response system includes routers, firewalls, and hosts. To distribute response commands to each device, 2 approaches as follows must be considered [5]

1) Devising a specific protocol

A protocol functions to transfer commands between IDS and the intrusion response system. Once the intrusion response system receives a response command, it implements a response script or changes its own configuration. The typical type of this approach is IDIP. IDIP can transfer response commands and also cooperate for intrusion detection in all components of IDS.

2) Using an automatic interacting script

The script can log in the intrusion response system automatically and implement the intrusion response program or change the system configuration. In this approach, all commands in the script are similar to those in passive response. However the script is automatically implemented by a transducer. This approach is currently applied in the same area as IDS evaluation. It is a kind of automatic interacting script languages. It is dependent on the platform and not as complicated as a mobile agent.

Comparison of two approaches for response is described in a table 1.

Table 1 Comparison of two approaches for response

	Protocol Approach	Script Approach
Standardization	✓ Good ✓ Standard process used as information exchange method and information operation method	✓ Bed ✓ Monopolistic process used as information exchange method and information operation method
Interoperability	✓ Bed ✓ IDIP has already been embodied and it's in the stage of experiment. ✓ Some functions are required to improve themselves in the future. ✓ Every component is asked to be compatible with IDIP ✓ Impossible to integrate router used at present into framework	✓ Good ✓ Script is operated by converter without any support of response device. ✓ Present response device can be added to a response system easily.
Scal-ability	✓ Good ✓ Embedded inside, it is able to transmit intrusion response for powerful protocol and respond all kinds of requests at the stage of information exchange.	✓ Fine ✓ New intrusion response can be added to the response system by adding response script which responds to. ✓ When the system consumes, more cost is required because it's not standard.
Rollback assistance	✓ It doesn't support protocol at present.	✓ Good ✓ Intrusion Response Rollback Script can be made like intrusion response script.

C. Active Response Phases

As shown in Fig. 1, the active response consists of 6 phases: preparation, detection, containment, eradication, recovery, and follow-up [3].

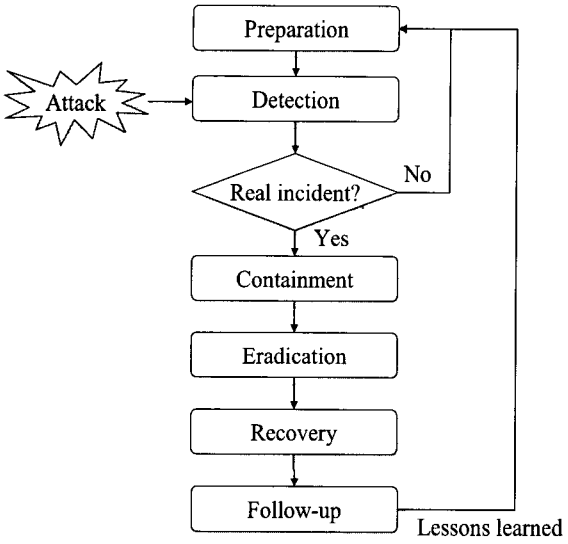

Fig. 1 Six-stage Active Response Model.

1) Preparation

The preparation phase is that the user considers how to respond to diverse attacks since information was collected. First of all, the user needs to collect as much information as possible for the network and the configured host. The network configuration diagram, IP list, previous vulnerability scanning records, each host's operating system, arpwatch or DHCP(Dynamic Host Configuration Protocol) data list are also included therein.

2) Detection

The detection phase occurs when there is any attack. The attack will be usually detected through log or IDS alert. Once this occurs, the intrusion detection system saves information for the attack's date, time, management, characteristics, and damage, etc. It is important to judge who is related to the attack and how the attack is performed. Therefore the user needs to decide the range of attack.

3) Containment

The containment phase requires the user's judgment and behavior about how to prevent and eradicate the attack causing much damage. This includes port shutdown in the firewall, disconnection from internet, stop using services and accounts, and system shutdown as well.

4) Eradication

Eradication is to remove backdoor, virus, vulnerabilities in the operating system, and attack route. Its procedures are set while an attacker can implement this phase in the preparation phase.

5) Recovery

The recovery phase has a backup copy for all systems with them kept online. The system backup is implemented on the assumption that eradication has been completed.

6) Follow-up

Follow-up is the phase which reviews previous phases and analyzes what has been exactly implemented and improved. When there is an attack again, follow-up is used to mitigate the attack.

IV. ACTIVE RESPONSE SCHEME TO DETECT UNKNOWN ATTACKS

Unknown attacks which are not detected in the signature-based intrusion detection system can be detected by the anomaly event detection technology. The most universal method for real-time detection are the traffic anomaly detection method to judge whether there is traffic congestion and protocol anomaly detection method to judge whether there is anomaly protocol.

A. Traffic Anomaly Detection

Therefore this thesis also uses the method to detect unknown attacks. To attack vulnerable systems or unspecific networks, Buffer Overflow Attack, Dos/DDos Attack, Worm Attack, Scan Attack, and Backdoor are generally used.

To detect traffic anomalies effectively, there should be a profile which informs you of normal operating characteristics with reference to Host/IP address, and virtual or physical LAN segments. The profile consists of a comprehensive list of parameters and values which are definitely set according to monitoring targets. The reliable profile should be stable and consistent when it monitors the normal function of target environment.

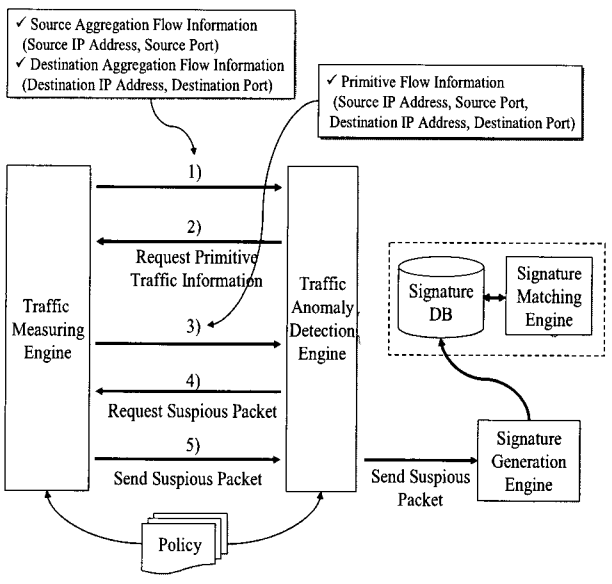

Fig. 2 Interaction of Traffic Measuring Engine Traffi c and Anomaly Detection Engine.

The profile for network traffic should have the adaptability and self-learning function as well as high reliability. The high-adaptive profile can check even normal changes in the network and so prevent wrong detection. The traffic statistics is very complex and changes dynamically. Thereby the administrator is limited in setting profiles manually. As a result, the self-learning function acts an important role to detect traffic anomalies successively.

As shown in Fig. 2, each attack can be detected in the signature-based intrusion detection engine. However, if there is no existing specific pattern, each attack can be detected in the anomaly detection engine irrespective of inexistence of specific patterns [6].

The definite inter-working between the traffic measuring engine and the traffic anomaly detection engine is as follows:

1) Providing aggregation flow information using the traffic measuring engine

The aggregation flow provides you with information for the source aggregation flow and the destination aggregation flow. The source aggregation flow provides the traffic anomaly detection engine with traffic collection information through the source IP address and the source port. The destination aggregation flow provides the traffic anomaly detection engine with traffic collection engine through the destination IP address and the destination port.

2) Requesting information for anomaly detection measurement and primitive traffic

The traffic anomaly detection engine judges whether there are traffic anomalies by using the aggregation flow information. The judgment criteria is dependent on whether there is any traffic exceeding the threshold value of BPS(Bits Per Second) and PPS(Packets Per Second) in various pairs of source IP addresses and source ports and various pairs of destination IP addresses and destination ports. The result is transmitted through the threshold value policy. If there is any flow exceeding threshold values, the flow requests the traffic measuring engine of primitive traffic information to get definite information for the relevant flow.

3) Providing primitive traffic information using the traffic measuring engine

The primitive traffic information transmitted from the traffic anomaly detection engine includes the traffic information of destination address and destination port in a pair of source IP address and source port, or the traffic information of source IP address and source port in a pair of destination address and destination port.

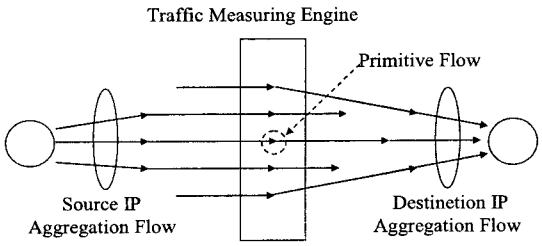

Fig. 3 Aggregation/Primitive Flow

Major modules of each engine for inter-working are as shown in Fig.4.

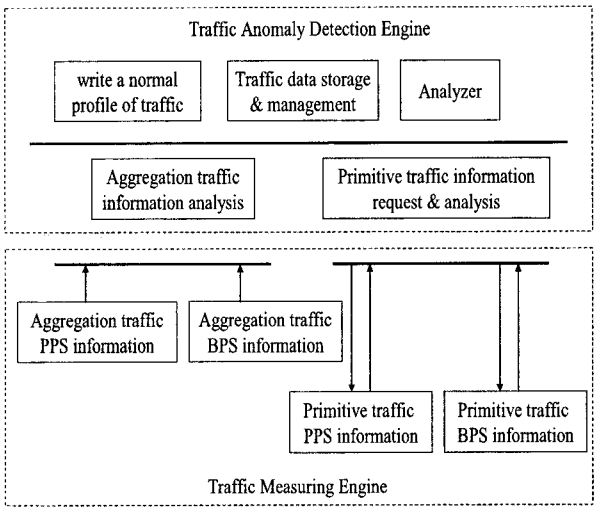

Fig. 4 Major modules of each engine for inter-working

4) Requesting to transfer anomaly detections and suspicious packets

The traffic anomaly detection engine receives definite primitive traffic information of the relevant aggregation flow and then judges whether it has an abnormal traffic. The judgment criteria is dependent on whether there is any traffic exceeding the threshold value of BPS(Bits Per Second) and PPS(Packets Per Second) in information for various destination IP addresses and destination traffics in a pair of relevant source IP address and source port, and in information for various source IP addresses and source traffics in a pair of relevant destination IP address and destination port. The traffic exceeding the threshold value requests the traffic measuring engine of raw packet information related to the flow.

5) Transmitting suspicious packets by the traffic measuring engine

The traffic measuring engine requested to transmit packet information related to the relevant flow transmits relevant packet in a packet buffer to the traffic anomaly detection engine.

B. Protocol Anomaly Detection

Protocol anomaly detection means exceptional protocol format and protocol actions related to Internet and standard use method. It also includes protocol anomaly in the layers of 3 and 4 of network, transmission layer, and the layers of 6~7 of application layer. In this case, basic TCP/IP stack action should be monitored from various sides. It can be done by the whole IP packet constructing, re-building TCP, and checking all anomaly conditions in the process. And in the case of inline IPS, at the end-host, it gets rid of possibility that the host would not interpret well. That is called Traffic Normalization. Anomaly detection that could happen in layers 3~4; IP Fragmentation Overlap, anomalous IP option, anomaly TCP Segmentation Overlap, inappropriate use of TCP option, and so on.

Buffer overflow intrusion detection using protocol anomaly detection engine can detect by analyzing length and composition of character of the value of field of application layer protocol from packets' data that attacker delivers to the system which he/she attacks.

Protocols that take most parts in network traffic at present are HTTP, SMTP, FTP, DNS, etc. and some fields that cause buffer overflow attack using the protocol are as followed.

Table 2 The field that generates a buffer overflow attack-HTTP

Inspection Field	The attack that is prevented
HTTP Client	
✓Limit maximum response header length ✓Prohibit binary characters in HTTP response headers ✓Validate HTTP response protocol compliance ✓Block user-defined URLs ✓URL filtering	✓Code Red worm & Mutations ✓Nimda worm & Mutations ✓HTR Overflow Worm & Mutations ✓MDAC Buffer Overflow & Mutations ✓Malicious URLs ✓User-Defined worms & mutations
HTTP Server	
✓Limit maximum URL length ✓Limit maximum number of response headers allowed ✓Limit maximum request header length ✓Limit maximum response header length ✓Specify header length, using regular expressions for header name and value ✓Restrict non-RFC HTTP methods	✓Encoding Attacks ✓User-Defined Worms & Mutations ✓Code Red Worm & Mutations ✓Nimda Worm & Mutations ✓HTR Overflow Worm & Mutations ✓Directory Traversal Attacks ✓MDAC Buffer Overflow & Mutations ✓Malicious URLs ✓Chunked Transfer Encoding Attacks

Table 3 The field that generates a buffer overflow attack-FTP

Inspection Field	The attack that is prevented
✓Analyze and restrict hazardous FTP commands ✓Block custom file types	✓Passive FTP Attacks ✓Client and Server Bounce Attacks ✓FTP Port Injection Attacks ✓Directory Traversal Attack ✓Firewall Traversal Attack ✓TCP Segmentation Attack

Table 4 The field that generates a buffer overflow attack-SMTP

Inspection Field	The attack that is prevented
✓Block multiple "content-type" headers ✓Block multiple "encoding headers" ✓Restrict unsafe SMTP commands ✓Strict enforcement of MAIL and RCPT syntax ✓Restrict mail from user-defined sender or domain ✓Restrict mail to user-defined recipients ✓Restrict mail to unknown domains ✓Enforce limits on the number of RCPT commands allowed per transaction	✓SMTP Mail Flooding ✓SMTP worm & Mutations ✓Command Verification Attack ✓SMTP Payload worm & Mutations ✓Worm Encoding ✓Firewall Traversal Attack ✓SMTP Error Denial-of-Service Attack ✓Mailbox Denial-of-Service Attack(excessive email size) ✓Address Spoofing ✓SMTP Buffer Overflow Attacks ✓MyDoom worm & Mutations

Table 5 The field that generates a buffer overflow attack-SMTP

Inspection Field	The attack that is prevented
✓Restrict DNS zone transfers ✓Restrict usage of DNS server as a public server ✓Provide separate DNS service for private vs. public domains ✓Enforce DNS over TCP protocol ✓Restrict domains on "not allowed" list ✓Provide cache protection ✓Restrict inbound requests ✓Restrict mismatched replies ✓Enforce DNS query format ✓Enforce DNS response format	✓Protect against DNS Cache positioning attacks ✓DNS Query Malformed Packet Attacks ✓DNS Answer Malformed Packet Attacks ✓DNS Query-Length Buffer Overflow ✓DNS Query Buffer Overflow-Unknown Request/Response ✓Man-in-the-Middle Attack

When IPS monitors application protocol, decoding that operates application protocol analysis can be done. Application protocol anomalies are such as illegal field value and association, anomalous use of instruction, anomalous length of field

Like in Fig 5, in order to confirm anomaly of field value, Field Length Calculation Engine which calculates the length of the field value and Character Distribution Analysis Engine which calculates character distribution that composes field value are needed.

1) Packet Preprocessing Engine

The functions of packet processing engine are to make sure that entering packet is what kind of protocol and play a role that extracts field value of field that needs analysis and sends it to Field Length Calculation Engine and Character Distribution Analysis Engine.

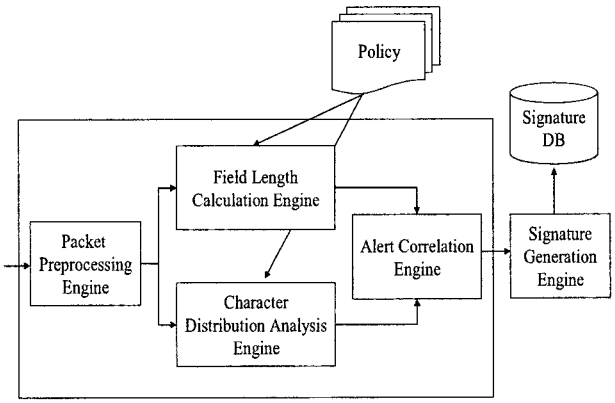

Fig. 5 Protocol Anomaly Detection Engine

2) Field Length Calculation Engine

Field Length Calculation Engine calculates the size of field value received, regards it as anomalous packet if the size is over the threshold of the field value, and transmits it to Alert Correlation Engine.

3) Character Distribution Analysis Engine

Character Distribution Analysis Engine analyzes character distribution of field value received and continuity of particular character. If they are over the threshold, it is regarded as an anomalous packet and transmitted to Alert Correlation.

4) Alert Correlation Engine

Alert Correlation Engine finally makes a decision whether the packet is legal or not by using information received from Field Length Calculation Engine and Character Distribution Analysis Engine and transmits Raw Packet to Signature Generation Engine if the packet is legal.

V. CONCLUSION

This thesis was prepared to search how to solve problems in the existing intrusion detection system, and how to actively respond which is an important factor to lead technically. For this study, we investigated what to consider for active response in the intrusion detection system, how to implement active response, and 6-phase response models to respond actively, including the active response scheme to detect unknown attacks by using the traffic measuring engine and the anomaly detection (traffic anomaly, protocol anomaly).

The active response scheme as aforementioned will be a cornerstone for diverse active response studies in future. If the active response intrusion detection system is implemented, it will be applicable to the security system to improve reliability and stability in the intrusion detection system, including devising active intrusion systems and information security systems in the financial field such as, fund transfer, electronic payment, and internet banking.

REFERENCES

[1] H. Debar, D. Curry, B. Feinstein, "The Intrusion Detection Message Exchange Format draft-ietf-idwg-idmef-xml-14", Internet-Draft, IETF, 2005

[2] Jinqiao Yu, Y. V. Ramana Reddy, Sentil Selliah, Srinivas Kankanahalli, Sumitra Reddy, Vijayanand Bharadwaj. "TRINETR: An Intrusion Detection Alert Management System," 13th IEEE (WETICE'04), pp.235-240, 2004.

[3] Carl Endorf, Eugene Schultz, Jim Mellander, "Intrusion Detection & Prevention", McGrawHill, 2004

[4] Kim, H.A. and Karp, B., "Autograph: Toward Automated, Distributed Worm Signature Detection", 13th Usenix Security Symposium (Security 2004), August, 2004

[5] Jian Zhang, Jian Gong and Yong Ding, "Research on automated rollbackability of intrusion response", Journal of Computer Security, Vol.12, No.5, pp.737-751, 2004

[6] Kai Hwang, Ying Chen, Hua Liu. "Defending Distributed Systems Against Malicious Intrusions and Network Anomalies" , IPDPS'05, 2005

Bong-Han Kim
received B.E. degree in Computer Science & Engineering, Chongju University, in 1994, M.E. degree in Computer Engineering, Hannam University in 1996 and Ph.D. degree in Computer Engineering, Hannam University, Korea in 2000. He is a professor in Dept. of Computer & Information Engineering, Chongju University. The author's major research are of network security, multicast security, P2P security.

Si-Jung Kim
Received B.E. degree in Computer Science, Hanbat National University, in 1990, Master. degree in Computer Education, Hannam University in 1995 and Ph.D. degree in Computer Engineering, Hannam University, Korea in 2002. She is an instructor in Dept. of Computer Science, Chungju University. The author's major researches are of computer education, protection of information, multimedia.