Traceback Framework for Cooperating with Other Domains.

Geonlyang Kim † and Jungchan Na††,

Information Security Research Division
Electronics and Telecommunications Research Institute,
161 Gajeong-dong, Yuseong-gu, Daejeon City, Republic of Korea.

Summary
This paper describes a framework for tracing a cyber attack such as worm, virus, un-known attack in cooperation with several domains at the multiple domains environment. Many attackers are usually located in other domains and make an attack going through several domains. An administrative domain has to cooperate with other domains, otherwise it is difficult to trace a cyber attack even if the cyber attack is detected at an administrative domain. Therefore, a framework for tracing attack in cooperation with several domains as well as an administrative domain is needed. This paper is able to trace the location of an attacker and respond to the attack more quickly because of automation of tracing a cyber attack in cooperation with other domains.

Key words:
Traceback, Traceback Framework,

2. Introduction

The network security systems protect network systems within an administrative domain from incident or a cyber attack, but the response is carried out after a cyber attack, or it is blocking attack traffic or limiting the rate of attack traffic within an administrative domain. The response is passive. The active traceback for an attacker is requested because of legal responsibility of the damage of resource. Sharing traceback information among domains by constructing multiple domains environment is needed for securing the administrative network from a cyber attack actively or clearing the cause of a cyber attack exactly.

The several technologies for tracing a cyber attack have been studied since the past, but the general Traceback Framework that is independent on the specific trace technology has to be defined because the system that is dependent on the specific trace technology has the dangerousness where an attacker analyzes weakness and tries to attack it continuously. This paper describes the framework for tracing a cyber attack in cooperation with other domains as sharing trace information about the attack going through several domains, and defines the general framework that is independent on the specific trace technology for tracing a cyber attack.

Manuscript received October 5, 2008
Manuscript revised October 20, 2008

Figure 1 shows that it is a framework for sharing trace information among domains, and tracing the location of an attacker at the multiple domains environment when an attack occurs. The framework for tracing a cyber attack consists of Traceback System, Traceback Request System, Attack Response System, and Traceback Repository as shown in Figure 1. The functions of these components of a framework for tracing a cyber attack are described at the next section.

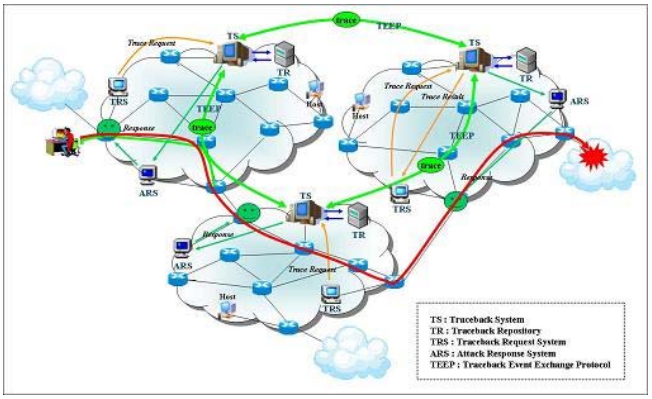

Figure 1. Traceback Framework

3. Components of Traceback Framework

3.1. Traceback Request System

Traceback Request System such as NMS(Network Management System), IDS(Intrusion Detection System), and so on requests a trace for the location of an attacker at Traceback System when attack traffic or abnormal traffic occurs within an administrative domain or the need for tracing the source of traffic occurs. Traceback Request System is able to be system having several functions such as network management, intrusion detection, security management, and so on. It is not system only requesting a trace the location of attackers.

3.2. Traceback System

Traceback System decides whether it executes a trace for an attack or not, and executes a trace for it. It receives a trace requests from Traceback System of other domains or Traceback Request System of an administrative domain, executes a trace for an attack in an administrative domain, and requests a trace to other domains when the attack didn't generate within an administrative domain. When Traceback System receives a trace request for an attack from other domain and the attack generates within an administrative domain, it executes a trace for the attack in an administrative domain and transmits the trace result to the domain that requests a trace. Traceback System has to have capability to deal with format and protocol for exchanging trace events such as a trace request, a trace result, and so on for communicating with Traceback Systems of other domains. When Traceback System receives a trace request from other domain, it needs capability to execute a trace after checking trace duplication for the same attack, and control that many traces aren't executed at the same time, because many resources are consumed for executing a trace of an attack

3.3. Attack Response System

Attack Response System takes response actions for an attack in an administrative domain when an attack occurs. When Traceback System finds out the location of an attacker by tracing in cooperation with other domains, it takes response actions that notify attack information or the location information of an attacker to an administrator, block attack traffic, or limit the rate of attack traffic for preventing the damage of an administrative domain.

3.4. Traceback Repository

Traceback Repository communicates with Traceback System and saves events related to tracing in cooperation with other domains or in an administrative domain. Traceback Repository saves trace events such as a trace request, a trace result, a trace progress in an administrative domain, and so on. Traceback Repository is needed for checking trace duplication for the same attack because many resources are consumed for tracing in cooperation with other domains. Traceback Repository locates usually in an administrative domain. And Traceback Repository that several domains share is useful because the check for trace duplication is easy. But retrieval speed of Traceback Repository is able to be slow. The LDIF(LDAP Data Interchange Format) is able to be use as the data format of Traceback Repository that several domains share for the improvement of retrieval speed, and LDAP (Lightweight Directory Access Protocol) is able to be use as the access protocol of it.

4. Communication among Components

Figure 2 shows the components of a framework for tracing a cyber attack at multiple domains environment. Traceback System communicates with Traceback Request System, Attack Response System, Traceback Repository within an administrative domain, and Traceback Systems of other domains.

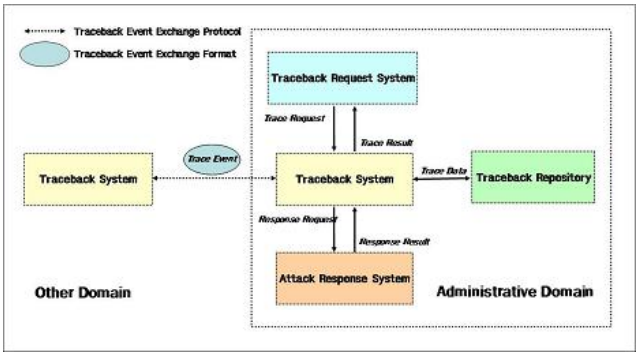

Figure 2. Communication among Components

When attack traffic is detected in an administrative domain and a trace request from Traceback Request System is generated, Traceback System executes a trace in an administrative domain, saves a trace result in Traceback Repository, and transmits it to Traceback Request System. When Traceback System in an administrative domain receives a trace request from other domain, it analyzes attack traffic. When the attack occurs within an administrative domain, it executes tracing the location of an attacker, and transmits a trace result to Traceback System of other domain requesting a trace. And when the attack occurs within other domain, it requests a trace to another domain that the trace wasn't executed for the same trace request. Traceback System has to use Traceback Event Exchange Format and Traceback Event Exchange Protocol when it requests a trace to other domains or transmits a trace result to other domains after it executes a trace, etc.

4.1. Traceback Event Exchange Protocol

When attack traffic occurs through several domains, cooperation of several domains is needed for tracing a cyber attack. Traceback Event Exchange Protocol is protocol for exchanging trace events between Traceback Systems when tracing the location of an attacker in

cooperation with domains. Domains intending to execute a trace in cooperation with other domains have to promise what protocol is used between domains in advance. Protocol for exchanging incidents and trace information between domains has been studied in INCH Working Group at IETF.

4.2. Traceback Event Exchange Format

Traceback Event Exchange Format as Traceback Event Exchange Protocol is a message format for sharing and exchanging trace events between domains when Traceback System executes a trace in cooperation with other domains. Domains intending to execute a trace in cooperation with other domains have to promise in advance what format is used between domains. IODEF(The Incident Object Description Exchange Format), RFC5070 of IETF is able to be referred to as the format for exchanging trace events between domains.

Traceback System has to be able to transform the Traceback Event Exchange Format into the local format of Traceback System, and the local format into the Traceback Event Exchange Format. Traceback System executes a trace after it checks trace duplication for the same attack. When it checks trace duplication, it uses trace information of Traceback Repository. When response for the attack is needed within an administrative domain, Traceback System transmits response request to Attack Response System.

5. Functions for Tracing a Cyber Attack

Traceback System has interfaces with Traceback Repository, Traceback Request System, and Attack Response System within an administrative domain as shown in Figure 3. Traceback System communicates with Traceback Request System when a trace request from IDS detecting attack traffic or specific host occurs. It communicates with Attack Response System when response action is needed after tracing the attack. It communicates with Traceback Repository for checking trace duplication for the same attack before tracing a cyber attack or saving trace information such as a trace result. And Traceback System communicates with Traceback Systems of other domains for exchanging trace information in cooperation with other domains for a cyber attack going through several domains. Figure 3 shows the structure of Traceback System, and the functions of system are as follows.

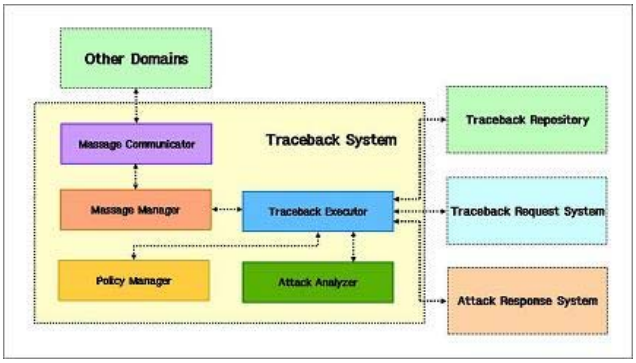

Figure 3. Traceback System

5.1. Deciding and Executing a Trace

Traceback Executor receives a trace request through Message Communicator and Message Manager when a trace request message is arrived from other domain. And it receives a trace request through Trace Request System when attack traffic is detected in an administrative domain and the need of trace occurs. If Traceback Executor receives a trace request, it decides whether execute a trace by checking policy information of an administrative domain, trace duplication, and so on. And it analyzes attack traffic through Attack Analyzer and executes a trace. When Traceback Executor isn't able to trace the location of an attacker within an administrative domain because an attacker exists within other domain, it make a trace request message through Message Manager, and requests a trace to adjacent other domain that attack traffic flows in.

When Traceback Executor receives a trace request from Traceback Request System of an administrative domain, it transmits result executing a trace to Traceback Request System. And when it receives a trace request from other domain, it transmits the result to other domain requesting a trace. When response action for attack traffic is needed within an administrative domain event if the attack occurs in other domain, Traceback Executor requests response action for attack to Attack Response System.

5.2. Analyzing an Attack

Attack Analyzer analyzes attack traffic to get data needed for executing a trace, and analyzing attack traffic is processed before executing a trace. When Traceback System requests a trace to other domain, Attack Analyzer extracts data needed for composing traceback request message because they include results analyzing attack traffic. The data needed for executing a trace and

analyzing attack traffic are able to be source IP address, source port, destination IP address, destination port, protocol, severity, confidence, the intermediate router IP address of attack traffic, and so on.

5.3. Managing a Policy

Policy Manager has function managing policy for traceback request message transmitting to other domain or traceback request message received from other domain. In other words, it has function managing policy such as policy accepting only a trace request transmitted from domain entering consortium, policy accepting only a trace request transmitted from the adjacent domain of domains entering consortium, policy accepting only the peer system, and so on. The policy is able to be applied to each component that composes trace messages according to the policy of each domain.

5.4. Managing a Message

Message Manager has functions decoding messages transmitted from other domains or encoding messages before transferring messages to other domains through Message Communicator, composing message by using trace data extracting for the message, requesting a trace by transferring a trace request from other domains to Traceback Executor, and managing message such as saving or deleting message. The IODEF is described by XML. So Message Manager has to have functions parsing XML of the IODEF for messages transmitted from other domains, and making XML of it for messages transferred to other domains.

5.5. Communicating by a Message

Message Communicator has functions communicating with Traceback Systems of other domains and exchanging messages. Domains exchanging messages have to enter a consortium for making a promise such as message transmission protocol or message data format exchanging for tracing a cyber attack in advance. Domains entering a consortium are able to communicate or cooperate with other domains of the consortium.

6. Conclusion

This paper describes Traceback Framework as a framework for tracing an attacker in cooperation with other domains when a cyber attack occurs at the multiple domains environment. Traceback Framework is able to trace and respond to attack traffic going through several domains more quickly by automation of tracing the location of an attacker in cooperation with other domains, and not only a vender but also all venders will be able to use it because it isn't dependent on the specific trace technology. This paper will provide network users with more secure and reliable network security service in cooperation with network security systems such as IDS, firewall, and so on. It is possible to trace the location of an attacker through Traceback Framework exchanging trace information in cooperation with other domains, and technology tracing the location of an attacker and scaring an attacker will provide network users with more secure network service through preventing a cyber attack.

References

[1] http://www.cert.org/ietf/inch/inch.html
[2] http://terena.org/activities/tf-csirt/
[3] J. Arvidsson, A. Cormack, Y. Demchenko, "TERENA'S Incident Object Description and Exchange Format Requrements", RFC3067 IETF, Febrary 2001.
[4] Glenn M Keeni, Roman Danyliw, Yuri Demchenko, "Requirements for the Format for Incident Information Exchange (FINE)", draft-ietf-inch-requirements-08.txt, IETF, June 25, 2006.
[5] R. Danyliw, J. Meijer, Y. Demchenko, "The Incidnet Object Description Exchange Format", RFC5070 IETF, December 2007.
[6] Kathleen M., "Real-time Inter-network Defense", draft-moriarty-post-inch-rid-06.txt, IETF, April 15, 2008.
[7] Kathleen M., Brian H., "IODEF/RID over SOAP", draft-moriarty-post-inch-rid-soap-05.txt, IETF, Febrary 25, 2008.

Geonlyang Kim received the B.S and M.S. degrees in Computer Science from Chonnam National University in 1999 and 2001, respectively. She has been a senior member of engineering staff at Electronics and Telecommunications Research Institute (ETRI) in Korea since 2001. Her research interest includes network security, and visualization of network security.

Jungchan Na received the B.S. degree from Chungnam University in 1986, the M.E. degree from Soongsil University in 1989, the Dr. degree in Computer Science from Chungnam University in 2004. He has been a principal member of engineering staff and the leader of managed security research team at Electronics and Telecommunications Research Institute(ETRI) in Korea since 1989. His research interest includes network security management, visualization of network security, and security situational awareness.