International Journal of Advanced Science and Technology
Vol. 4, March, 2009

A VoIP Traffic Monitoring System based on NetFlow v9

Chang-Yong Lee* , Hwan-Kuk Kim, Kyoung-Hee Ko, Jeong-Wook Kim, Hyun-Cheol Jeong
Korea Information Security Agency, Seoul, Korea
{chylee, rinyfeel, khko, kjw, hcjung}@kisa.or.kr

Abstract

With the development of VoIP (Voice over IP) service, new security threats are expected to be appeared. However, existing IP network security solutions can not detect new VoIP specified network threats because they can not reflect characteristics of VoIP. In this paper, we propose a novel system that can monitor VoIP service and detect VoIP network threats practically. The proposed system collects attributes of VoIP traffic based on NetFlow, and executes monitoring and detecting based on statistic and behavior.

1. Introduction

VoIP allows users to perform voice communication using IP network. With some advantages, low cost and providing various extra services, VoIP service has become so popular, and is considered as a business with good prospects. Worldwide VoIP market is expected to be extended over 5 times from current scale until 2012. With this development, VoIP is considered to be the alternation for current PSTN (Public Switched Telephone Network) in the near future.

However, new security threats are expected to be appeared with the new service. Basically, it is implemented over IP network, and it inherits every security threats of IP network. In addition, appearance of new security threats specified by VoIP characteristic is forecasted. Currently, most of VoIP service use SIP (Session Initiation Protocol) [1] for call set up, and use RTP (Real-time Transport Protocol) [2] for media transportation. Therefore, various security threats using characteristics of SIP and RTP are prospected to be appeared.

DoS, scan and some other existing IP based network attacks can be detected and prevented by the existing network security solutions (e.g. firewall, IPS (Intrusion Prevention System)). Generally, they use 5-tuple information (source IP/port, destination IP/port, protocol) inside of IP headers. However, this way of measure is not appropriate to VoIP's case. SIP protocol uses an additional identifier, URI (uniform resource identifier), for user identification and application header is located in a payload of IP packet. Therefore, with existing solutions that check only IP headers, it is impossible to account SIP/RTP traffic.

Therefore, a new system is required to recognize, measure and analyze SIP/RTP traffic. In this paper, we propose a structure of a system for monitoring, analyzing and detecting SIP-based VoIP service traffic anomaly. The proposed system collects SIP/RTP traffic information based on NetFlow, executes monitoring VoIP traffic and detects VoIP abnormal traffic by analyzing collected information.

*Corresponding author
This work was supported by the IT R&D program of MKE/IITA.
[2008-S-028-01, The Development of SIP-Aware Intrusion Prevention Technique for protecting SIP-base application Services]

The remainder of this paper is organized as follow. In Section 2, we give related work. In Section 3, we describe VoIP network threat model. In Section 4 and 5, we describe the proposed system and rules for detection. We conclude the paper in Section 6.

2. Related Work

2.1 NetFlow

IP flow is defined as a union of IP packets those have same source IP address/port, destination IP address/port, protocol information. If new arrival packet's attribute is not found from a flow table, a new flow will be generated. On the other hand, if it is found, only corresponding flow's attribute (e.g. packets count, bytes, last update time, etc.) will be updated. With this process, only a flow table is maintained until time out, and after the time out, the flows in the table are sent to a flow collector. Due to it doesn't have to maintain whole packets, it can save disk space and system resource. So, a lot of network devices use flow based traffic account to monitor and manage their networks.

Cisco NetFlow [3] is the most popular IP flow format to account IP traffic. Currently, NetFlow version 9 has been released and NetFlow version 5 is used by most of network management devices and network security devices. Actually, it is not too much to say that NetFlow is a industrial standard for traffic measuring.

However, NetFlow version 5 is not appropriate to VoIP. It supports a fixed template, flow size and metrics, and an user is not able to configure anything to the format of the flow. Cisco released NetFlow vsersion 9 that has an extended header idea.

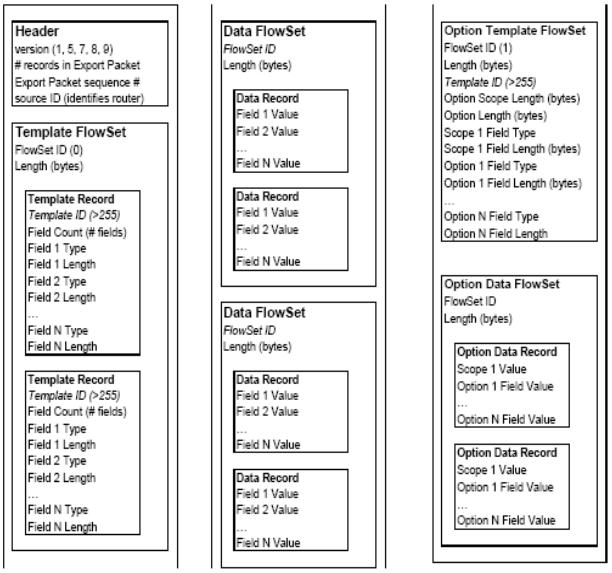

Figure 1. A format of NetFlow version 9 packet

In NetFlow version 9's case, packet header is same as NetFlow version 5. However, the most important change of the NetFlow Version 9 format is that it is template based. Templates provide a flexible design to the record format, a feature that should allow future

enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format[4].

2.2. nProbe

VoIP abnormal traffic detecting product never has been released, yet. Only nPorbe [5] supports some metrics to measure SIP/RTP traffic since it's version 4.0. nProbe is an open source NetFlow probe. It supports to generate NetFlow version 5, 9 and IPFIX flow. Especially, it supports to generate Netflow version 9 including extended flow header. Since its version 4.0, SIP/RTP plugin is added and it is able to measure VoIP traffic metrics that can be used by netflow collectors for building accurate analysis applications. Table 1 shows VoIP metrics that can be measured by nProbe.

Table 1. VoIP metrics that can be measured by nProbe

SIP	RTP
SIP_CALL_ID	RTP_FIRST_SSRC
SIP_CALLING_PARTY	RTP_FIRST_TS
SIP_CALLED_PARTY	RTP_LAST_SSRC
SIP_RTP_CODECS	RTP_LAST_TS
SIP_INVITE_TIME	RTP_IN_JITTER
SIP_TRYING_TIME	RTP_OUT_JITTER
SIP_RINGING_TIME	RTP_IN_PKT_LOST
SIP_OK_TIME	RTP_OUT_PKT_LOST
SIP_ACK_TIME	RTP_OUT_PAYLOAD_TYPE
SIP_RTP_SRC_PORT	RTP_IN_MAX_DELTA
SIP_RTP_DST_PORT	RTP_OUT_MAX_DELTA

2.2. Previous Proposals

Currently, research about VoIP security is underway, and some proposals have been released. Geneiatakis proposed a framework for detecting malformed SIP messages[6]. And Wu proposed an abstract intrusion detection framework called SCIDIVE for VoIP system[7]. In 2007, Kang et' al. proposed a methodology to profile the behavior of SIP-based VoIP traffic. He profiled the service behavior at multiple levels, server host, server entity, individual user levels[8].

Besides these, some other ideas were proposed for VoIP security. However, most of them are about signature-based detection. And a practical system for monitoring and detecting VoIP traffic is not proposed yet.

3. Threat Model

In this paper, we define VoIP network threats as a network attack that uses characteristics of VoIP service and is able to be detected by analyzing traffic. VoIP network threats are categorized into 3 groups, SIP flooding attack, RTP flooding attack, SIP scan.

In SIP flooding attack, an attacker sends a specified SIP proxy server or UA (User Agent) numerous SIP request messages (e.g. INVITE, REGISTER etc.) in a short time. It causes system resource starvation at victim device and makes it impossible to provide normal VoIP

service. Especially, in INVITE flooding's case, it does not cause only service destruction but second damage that ring phones continuously.

RTP Flooding sends numerous RTP packets to the victim in a short time without following any media encoding scheme. It can cause decline of voice QoS , and service destruction. VoIP is a real-time service and is very sensitive at voice QoS. Even if QoS decline is very small, it can give very critical damage to the service.

In order to perform more complicated VoIP attacks, it is necessary to know some information (e.g. valid URI etc.). SIP Scan attack is performed to get some information to execute second attacks (e.g. eavesdropping, SIP/RTP flooding etc.). In SIP scan attack, attacker tries to register a random URI to registrar server. When the server responses to the REGISTER request, the attacker can check a validation of the URI. And the attacker can check users whose status is on-line, by sending INVITE messages to various users in the network. SIP scan attack does not cause a critical damage by itself, but it has a potential risk for the second attacks.

4. Proposed System

In this chapter, we propose a system that monitors VoIP service and detects VoIP network threats described above.

4.1. Overall System Components

Figure 2 depicts overall system components of the proposed system. The proposed system consists of VoIP Traffic Observation Point, VoIP Traffic Monitoring and Detecting System, and GUI (Graphic User Interface). VoIP Traffic Observation Point generates NetFlow that includes VoIP Traffic aware information. It is developed as a software type, and can be installed in a third-party server device or network devices (e.g. router), security devices (e.g. IPS). VoIP Traffic Monitoring and Detecting System executes monitoring, analyzing VoIP traffic and detecting VoIP network threats. Monitoring statistic and results of detections are sent to GUI to be reported to a system administrator. The administrator can configure the rules for analyzing and detecting through GUI.

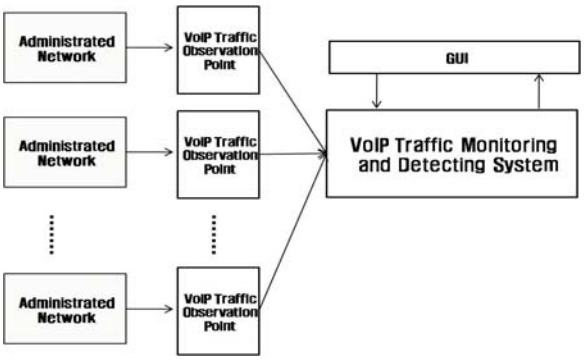

Figure 2. Overall System Components

4.2. VoIP Traffic Observation Point

VoIP Traffic Observation Points are located at a number of administrated networks, and collects VoIP traffic information of corresponding network. At first, it collects every raw IP packets from the network, and inspects application headers of them. Now it can distinguish SIP/RTP packets from the other types of IP packets and gathers SIP/RTP attributes (e.g. call-ID, caller/callee URI, SIP method type etc.). Using this information, it generates NetFlow that includes SIP/RTP information. We have chosen NetFlow version 9 as the flow format. NetFlow version 9 supports extended header and appropriate to measure VoIP traffic. The generated NetFlow is sent to VoIP Traffic Monitoring and Detecting System.

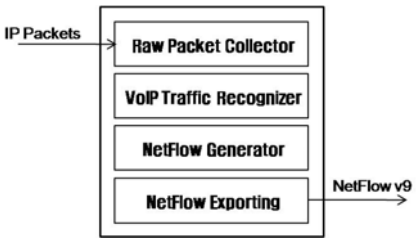

Figure 3. VoIP Traffic Observation Point

4.3. VoIP Traffic Monitoring and Detecting System

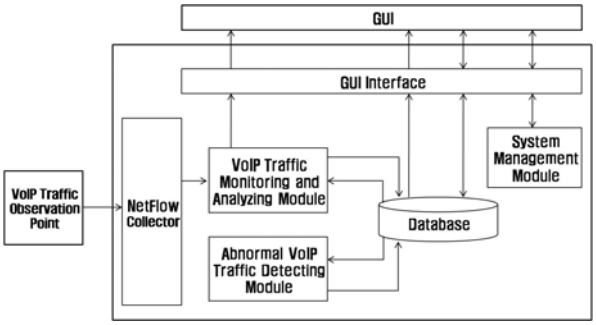

Figure 4. VoIP Traffic Monitoring and Detecting System

VoIP Traffic Monitoring and Detecting System consists of NetFlow Collector, VoIP Traffic Monitoring and Analyzing Module, Abnormal VoIP Traffic Detecting Module, System Management Module, and GUI Interface. The roles of each module are as follow.

- NetFlow Collector controls connections between a number of VoIP Observation Points and SIP Traffic Monitoring and Detecting System. And it collects NetFlow version 9 data. It decodes the NetFlow and itemizes SIP/RTP information to measure VoIP traffic for each item. The itemized information is sent to VoIP Traffic Mornitoring and Analyzing Module.

- VoIP Traffic Monitoring and Analyzing Module calculates the value of statistics for VoIP traffic monitoring(e.g. SIP/RTP traffic volume, session count etc.) and the value of statistics for VoIP traffic analyzing (e.g. ratio of caller/callee IP, the number of each SIP method etc.). The statistics

are stored in DB, and are used to report traffic information or to detect abnormal VoIP traffic. Out of the statistics some items are sent to GUI, through GUI interface, in real-time, to report service status.

Table 2. Metrics to analyze

Object	Metrics
Network monitoring	• SIP/RTP traffic volume • the number call sessions • duration of calls
Detecting abnormal VoIP Traffic	• the number of messages for each method • the number of source/destination IPs • the number of caller/callee URIs
QoS measuring	• jitter of RTP traffic • delay of RTP traffic • packet loss of RTP traffic

- Abnormal SIP Traffic Detecting Module executes to detect VoIP network execute to detect VoIP network threats in accordance with detecting rules. It calculates threshold value for each metrics continuously, and store the threshold in a hash table. And every unit time, it executes detecting VoIP network threats by comparing statistics of each metric with correspondent threshold value. The rules for detecting are described in chapter 5.

- GUI Interface sends VoIP traffic statistics, alert/log of VoIP network threats detection to GUI, to report the status of the service to the administrator, and receives some configuration request from GUI.

- System Management Module sends system status information (e.g. CPU/Memory usage, network status etc.) to GUI, through GUI Interface. And if it receives system configuration request from GUI Interface, it applies the request to the system.

5. Detecting VoIP Network Attacks

Symptoms of INVITE flooding attacks are appeared differently at SIP proxy server and UA. When numerous INVITE messages are centralized on specified device, whole traffic volume of SIP increases abnormally. And SIP proxy server can not process every INVITE request, and can not send RINGING messages for every INVITE requests. If INVITE Flooding targets on UA, you can see the symptom at a number of INVITE requests and 200OK responses. With the same way, you can detect REGISTER flooding using ratio of REGISTER and 200OK messages count.

RTP is a UDP based bidirectional protocol, and there is no specified response process after media receiving. Therefore, it is very difficult to detect RTP Flooding based on behavior. But, RTP packets that have same SSRC (Synchronizing Source Collision Resolution), should be sent from a same host. Therefore, By measuring the number of source IPs of RTP packets that has same SSRC, you can suspect of distributed RTP Flooding attack.

SIP Scan Attacks are divided into REGISTER Scan, that targets registrar, and INVITE Scan, that targets UA. In REGISTER Scan, a specified user tries to register various URIs in a short time. Therefore, to detect REGISTER scan, you should check the number of REGISTER messages heading to the registrar server and find out if there is an IP address that tries to send REGISTER messages that include various URI each, out of REGISTER messages heading to the registrar server. In INVITE Scan's case, there should be an unique IP address that tries to send INVITE messages to various URI in

a short time. Therefore, you can check unique number of URI at the To filed of INVITE messages that is originated from specific IP address.

Table 3. Metrics to check for detection

Attack	An object of analyze	Metrics to check
INVITE flooding	SIP traffic heading to SIP proxy server	• SIP traffic volume • ratio of INVITE and RINGING
	SIP traffic at each user's level	• SIP traffic volume • ratio of INVITE and 200OK
REGISTER flooding	SIP traffic heading to registrar	• SIP traffic volume • ratio of REGISTER and 200OK
RTP flooding	RTP traffic in each call session	• RTP traffic volume • the number of src IPs in RTP packets that has same SSRC
REGISTER scan	SIP traffic heading to registrar	• SIP traffic volume • ratio of src IP and URI in REGISTER messages
INVITE scan	Whole SIP traffic	• ratio of src IP and callee URI in INVITE messages

6. Conclusion

VoIP service is still on developing, and accordingly security threats are becoming more risky. However, there is no practical solution for monitoring VoIP service and detecting abnormal VoIP traffic. In this paper, we described some VoIP network threats and proposed a system to detect them. The proposed system can collect VoIP information and executes VoIP-aware network monitoring and VoIP traffic anomaly detecting.

However, there are still more potential VoIP network threats, and in accordance with it, the system should be more detailed and the rules for detection should be extended. It will be the future work of our research.

References

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[2] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobsonm, "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, January, 1996.

[3] Cisco Systems "NetFlow Services and Applications", White Paper, July 2002.

[4] Cisco Systems "Cisco IOS NetFlow version 9 Flow-Record Format", White Paper, 2004.

[5] L. Deri, "nProbe: an Open Source NetFlow Probe for Gigabit Networks", TERENA Networking Conference, 2003.

[6] D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis and S. Gritzalis, "A Framework for Detecting Malformed Messages in SIP Networks", the 14th IEEE Workshop on Local and Metropolitan Area Networks LANMAN), Greece, September 2005

[7] Y. Wu, S. Bagchi, S. Garg, N. Singh and T. Tsai, SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments", 2004 International Conference on Dependable Systems and Networks (DSN'04), Florence, Italy, 2004

[8] H. Kang, Z. Zhang, S. Ranjan and A. Nucci, "SIP-based VoIP Traffic Behavior Profiling and its Application", MineNet'07, San Diego, USA, June 2007.