An Anomaly Traffic Detection Method for VoIP Applications using Flow Data

Hyeongu Son
Chungnam National University
Daejeon, Republic of Korea
hgson@cnu.ac.kr

Youngseok Lee
Chungnam National University
Daejeon, Republic of Korea
lee@cnu.ac.kr

ABSTRACT

Recently VoIP applications have been popular due to the wide deployment of the wired/wireless Internet. Commercial VoIP services typically employ SIP and RTP for signaling and media transport protocols. Therefore, the VoIP service is vulnerable to a lot of threats because it uses the Internet where security is not guaranteed. For example, anomaly traffic cases such as hindering call connections, maliciously canceling calls, and deteriorating quality of voices have already been known. In this paper, we propose an anomaly traffic detection method for VoIP applications based on the flow-monitoring traffic measurement architecture, called IETF IPFIX. Under IPFIX, we present algorithms to detect BYE DDoS and RTP flooding anomaly traffic by defining new IPFIX templates for monitoring SIP and RTP flows.

Keywords

IPFIX, VoIP, anomaly, detection, algorithm

1. INTRODUCTION

Voice over IP (VoIP) delivers voice communication between users through IP networks. Except Skype which uses a proprietary protocol, most of VoIP services employ Session Initation Protocol (SIP) [1] and Real-time Transport Protocol (RTP) [2] for connecting call and communicating voice between users. Thereby VoIP are exposed to several security threats. For example, anomaly traffic such as interfering calls or degrading voice quality have been already known. Although secure protocols for SIP and RTP exist, they have not been fully implemented and deployed. Therefore, we have to devise an anomaly traffic method for the current VoIP services.

In this work, we aim at proposing a flow-based VoIP anomaly traffic detection method which uses the IETF IP Flow Information eXport (IPFIX) [3] standard. We use the flow-based traffic monitoring standard called IPFIX because it could provide flexible templates useful for monitoring various protocols. In addition, flow-based traffic monitoring architecture could be easily utilized since routers are typically eqiupped with flow monitoring functions such as Cisco NetFlow.

Among several VoIP anomaly traffic, we consider only two representative anomalies called BYE Denial of Service (DoS) and RTP flooding. Malicious attacker can generate these anomalies through sniffing normal VoIP traffic in wireless network. When these anomalies are sent to proxy server or users, they cause fatal problems such as force call termination and voice quality degradation. In this paper, we propose two VoIP-related anomaly traffic detection methods against BYE DoS and RTP flooding. We use SIP header information such as Call-ID and message type, and RTP traffic statistics such as timestamp for detecting BYE DoS anomaly traffic. For RTP flooding detection, we utilize SSRC and sequence number values of the RTP header.

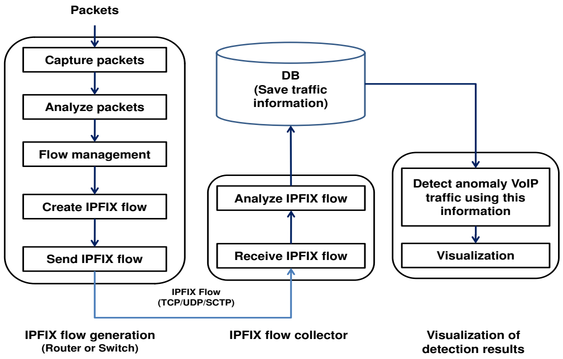

Figure 1: A flow-based anomaly traffic detection architecture

There are several similar studies to detect anomaly traffic using NetFlow [4]. Aurora [5], flowscan [6] and nfsen [7] focus on monitoring traffic based on NetFlow, which provide traffic trend information or statistics. Peakflow[8] and NetQoS [9] could detect anomaly traffic based on NetFlow data. However, these are not suitable for finding VoIP-related attacks. Especially, in [10], it is shown that INVITE and RTP flooding attacks could be detected using Hellinger Distance. However, this may not extended to support finding various VoIP attack traffic, because it uses the packet count information.

2. AN ANOMALY VOIP TRAFFIC DETECTION METHOD

2.1 Traffic monitoring architecture

Figure 1 describes an architecture for detecting anomaly VoIP traffic using the IPFIX protocol. This architecture

PAM2009, April 1-3, 2009, Seoul, Korea.
.

consists of IPFIX flow generator, IPFIX flow collector and flow visualizer.

The IPFIX flow generator at the flow monitoring servers or within routers/switches creates and exports IPFIX flows periodically while monitoring IP packets. The routers or switches in wired networks can be performed IPFIX flows generation. In addition, we can generate IPFIX flows through monitoring IP packets at wireless access routers or access points (AP). In the generator, the IP packets are captured, then analyzed in detail. Analyzed information of the packet is maintained by flow entries. Periodically, the generator makes the IPFIX flows from the flow entries, then send them to the IPFIX flow collector using TCP, UDP or SCTP. We define two IPFIX templates for monitoring SIP and RTP traffic, because the default IPFIX template is not useful for delivering VoIP-related information. The defined templates carry the interesting fields of SIP and RTP headers. For instance, we catch Call-ID and voice transmission information from SIP headers. From RTP header, we capture sequence number and SSRC (Synchronization SouRCe). The IPFIX flow collector receives IPFIX flows from the IPFIX generator. The collector analyzes IPFIX flows and saves the results to database. Our anomaly VoIP traffic detection algorithm periodically runs whether anomaly VoIP traffic exist at the saved traffic measurement information in database or not. Then, at the visualizer, we present results of detecting anomaly VoIP traffic.

2.2 Anomaly VoIP traffic detection algorithms

For detecting anomaly VoIP traffic using the IPFIX framework, we propose two algorithms that could detect BYE DoS and RTP flooding anomaly traffic.

2.2.1 BYE DoS anomaly traffic detection

Figure 2 shows the method for detecting BYE DoS anomaly traffic. When we observe SIP and RTP packets, we extracts session information of IP address and port number from SIP INVITE and OK messeges. Then, we investigate media traffic information after observing the BYE message. If RTP traffic is observed after BYE message, it could be highly considered that this RTP traffic is a flooding anomaly.

2.2.2 RTP flooding anomaly traffic detection

Figure 3 depicts a RTP flooding anomaly traffic detecting method that utilizes SSRC and sequence number of RTP header. First, we check SSRC in a flow because it should be the same with the SSRC value within the same RTP session. If SSRC has been changed at the RTP flow, it should be anomaly traffic. Second, we use sequence number information because it is possible to inject irrelevant RTP packets through sniffing RTP sessions. In our method, we compare the first and last sequence numbers with the maximum and minimum sequence numbers in a RTP flow.

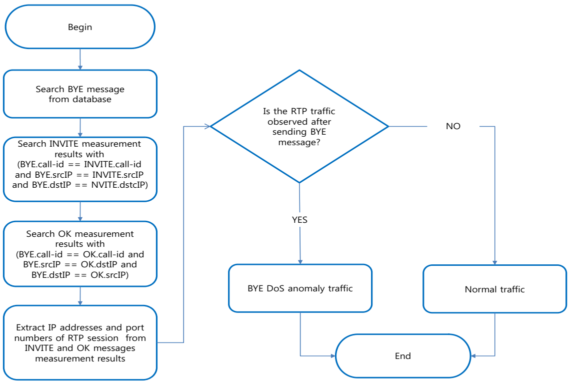
Begin
Search BYE message from database
Search INVITE measurement results with (BYE.call-id == INVITE.call-id and BYE.srcIP == INVITE.srcIP and BYE.dstIP == NVITE.dstcIP)
Search OK measurement results with (BYE.call-id == OK.call-id and BYE.srcIP == OK.dstIP and BYE.dstIP == OK.srcIP)
Extract IP addresses and port numbers of RTP session from INVITE and OK messages measurement results
Is the RTP traffic observed after sending BYE message?
NO
YES
BYE DoS anomaly traffic
Normal traffic
End

Figure 2: An algorithm to detect BYE DoS anomaly traffic

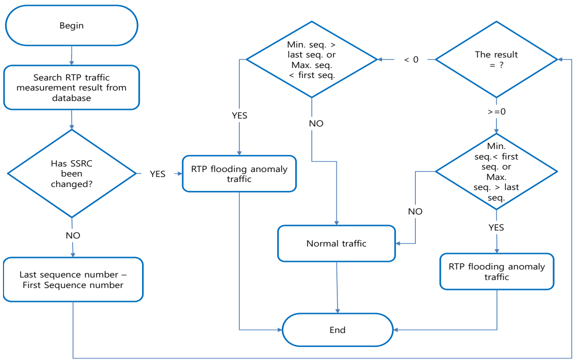
Begin
Search RTP traffic measurement result from database
Has SSRC been changed?
YES
NO
RTP flooding anomaly traffic
Last sequence number – First Sequence number
Min. seq. > last seq. or Max. seq. < first seq.
< 0
The result = ?
>=0
YES
NO
Min. seq.< first seq. or Max. seq. > last seq.
NO
YES
Normal traffic
RTP flooding anomaly traffic
End

Figure 3: An algorithm to detect RTP flooding anomaly traffic

3. CONCLUSION

In this paper, we propose an anomaly VoIP traffic detection method using the IPFIX protocol. For monitoring VoIP flows, we defined two IPFIX templates which provide information of SIP and RTP header. Based on the flow-monitoring traffic measurement architecture, we present two VoIP anomaly traffic detection algorithms against SIP BYE DoS attack and RTP flooding. For the future work, we will look for VoIP anomalies influenced commercial VoIP services, then proposed these anomalies detection algorithms. Using IPFIX, [11] has already tried monitoring traffic at 1/10Gbps links with low packet loss rate. Therefore, our proposed system will be useful for monitoring VoIP traffic at these links.

4. REFERENCES

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, *SIP: Session Initiation Protocol*, IETF RFC3261, June 2002.

[2] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson, *RTP: A Transport Protocol for Real-time Applications*, IETF RFC3550, July 2003.

[3] J. Quittek, T. Zseby, B. Claise and S. Zander, *Requreiements for IP Flow Information Export(IPFIX)*, IETF RFC3917, October 2004.

[4] Cisco NetFlow, http://www.cisco.com/warp/public/732/netflow/.

[5] IBM Research, "Aurora - A Flow-based Network Profiling System", http://www.zurich.ibm.com/aurora, 2005

[6] D. Plonka, *FlowScan: A Network Traffic Flow Reporting and Visualization Tool*, ACM the 14th USENIX conference on System administration, pp. 305-318, December 2000

[7] nfSen, http://nfsen.sourceforge.net/.

[8] Arbor networks Peakflow, http://www.arbornetworks.com/.

[9] NetQoS, http://www.netqos.com/index.html.

[10] H. Sengar, H. Wang, D. Wijesekera, S. Jajodia, *Detecting VoIP Floods Using the Hellinger Distance* IEEE Transactions on Parallel and Distributed systems, Vol. 19, No. 6, pp. 794-805, June 2008.

[11] nProbe, http://www.ntop.org/nProbe.html