Monitoring SIP Traffic Using Statistical Approaches

Cao Hui[1, a], Hou Hui Chao[2,b]

[1]College of Information Science and Engineering, Shenyang University, Shenyang,110044, China.

[2]Shenyang Institute of Computing Technology Chinese Academy of Science, Shenyang, 110171, China.

[a]china_hui2003@yahoo.com.cn , [b]houhuichao@sict.ac.cn

Keywords: Session Initiation Protocol, Chi-square statistic, Entropy, Traffic monitoring.

Abstract. To monitor Session Initiation protocol (SIP) traffic effectively, a statistical approaches-based traffic monitoring solution is proposed in this paper. According to the process of SIP session, Chi-square statistic is used for monitoring the anomaly of SIP traffic. It classifies the anomaly reason using entropy theory. SIP packets are captured utilizing the kernel SIP packet filtering technology. Experimental result shows that this solution of SIP traffic monitoring is feasible and effective.

Introduction

Because of it's easiness for using, Session Initiation Protocol (SIP)[1] has been a focus that people concerned. But at the same time, the safety of SIP has not been paid much attention to, so when using SIP, we have to deal with so many security threats. Discovering anomaly traffic and then alarming through the monitoring of the SIP traffic, has an important effect to design security solution. In this paper, a kind of statistical-based traffic monitoring solution is proposed.

Related Knowledge

Chi-square statistic. Pearson's chi-square test is used to measure the correlation of discrete distribution and Chi-square statistic (χ^2) as the quantization value of the correlation. Its calculating method is given in formula 1, where k is the dimensions, P_i is the expectation, P_i is the observed value.

$$\chi^2 = \sum_{i=1}^{k} (P_i - p_i)^2 / P_i \tag{1}$$

Entropy theory. Entropy can be used as the measurement of chaos level. Suppose that an information source can create n kinds of independent signals, and each kind has a probability of Pi, then the entropy of this information source is H, which is calculated in formula 2. The bigger is the entropy, the higher is the chaos level. Conversely, the lower will it be.

$$H = -\sum_{i=1}^{n} P_i \log_2 P_i \tag{2}$$

SIP Traffic Monitoring System Based on Statistical Approaches

SIP traffic monitoring system is described in detail, which includes system architecture every module descriptions. It uses bypass package-obtained technology to monitor the SIP data traffic, and decide if anomaly one happens by analyzing the SIP traffic. What's more, it can also explain the cause of the anomaly according to the traffic data and then alarm it. The system can be divided into four parts, packets filtering module, packets analyzing module, data analyzing module and alarming module.

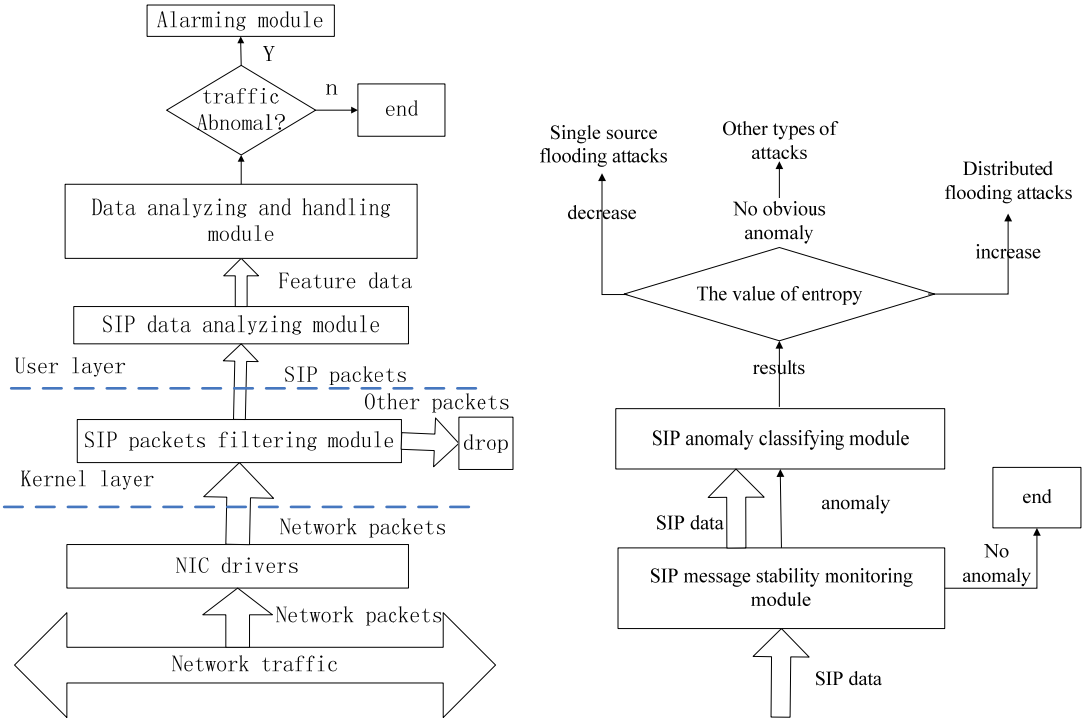

Figure 1. Architecture of SIP traffic monitoring and system SIP data analyzing

Packets filtering module. This module is mainly responsible for capturing SIP data form the network interface card (NIC) and giving them to the data analyzing module. It uses PF_RING technology [2] to realize bypass data capturing, and abandons non-SIP data directly in the kernel space by fixing SIP packets filtering plug-in in the kernel.

Packets analyzing module. This module is mainly responsible for handling the SIP packets captured by the packets filtering module, analyzing SIP packets analyzing, extracting the features of the SIP message, such as timestamp, source IP,destination IP, SIP message type, RPOM head filed, TO filed, CALL-ID, etc. This module uses oSIP protocol stack [3], optimized the traffic monitoring, and removed unnecessary head filed and analysis of SIP message.

Data analyzing module. This module is responsible for handling SIP feature data analyzed by the SIP packets analyzing module, the process of the monitoring of the SIP traffic is as in figure 1.

Stability monitoring module is responsible for monitoring if the SIP traffic is abnormal. Though the analyzing of the SIP session process, we can know that SIP me-

ssages (INVITE, ACK, 200 OK) show very strong stability when it is normal.

SIP anomaly classifying module mainly analyzes SIP anomaly traffic, determine the reasons causing the anomaly, and is helpful for defense. Entropy theory can be used to classify the reasons causing anomaly. We use the distribution of the source IP in the SIP require message to calculate the entropy. As for the flooding attacks, they need lots of SIP request messages to achieve their goals and as for single source flooding attacks, it will cause the obviously increment of the request messages form an IP address making the entropy decrease. As for distributed flooding attacks, there will be lots of request messages form different source IP addresses making the entropy increase obviously. As for other types of attacks, such as attacks using the system vulnerabilities, they will not cause obvious change of the entropy.

Experiment Results and Analysis

This section tested the SIP traffic monitoring system provided in the paper through experiment. In the experiment, KUTE [4] is used to simulate other traffic (UDP), SIPp tools [5] are used to create the SIP data traffic, attacks include single source, distributed flooding attacks and attacks based on SIP abnormal messages. SIP server uses OpenSIPS, and we use bypass technology[6] to monitor the SIP traffic.

We made abnormal attacks, single and distributed flooding attacks separately at 45, 120, 180 seconds, figure 2 shows the χ^2 of the SIP traffic under attacks. It can been seen that χ^2 is in a very

narrow area (0~0.003) in most cases, and in the attacking period, χ^2 changed obviously. Figure 3 shows the entropy of the SIP traffics, It can been seen that the attacks exactly using the change of the entropy are classified.

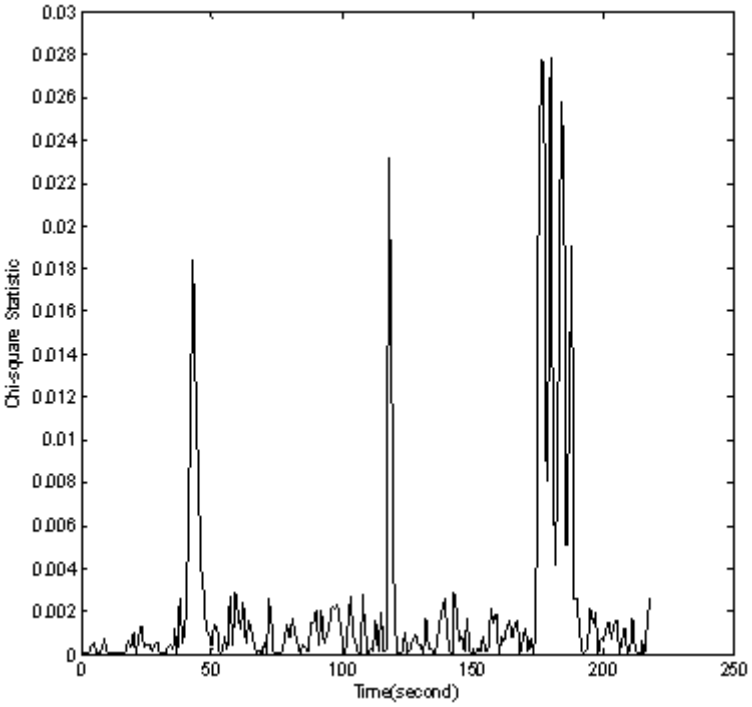

Figure 2. χ^2 of the traffics

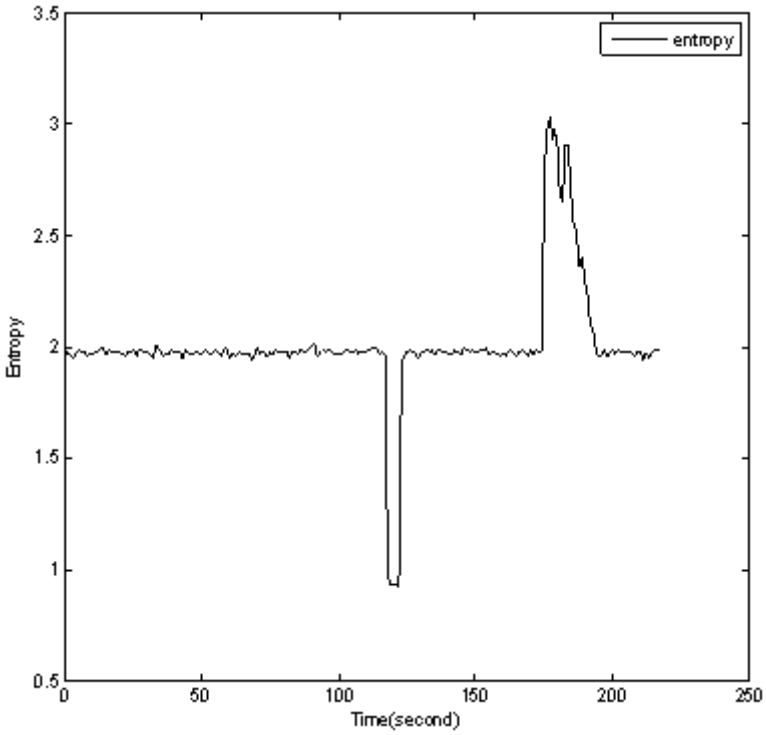

Figure 3. entropy of the traffics

Conclusion

An SIP traffic monitoring solution is proposed in the paper. It analyzes the features of SIP session process, captures SIP messages utilizing kernel layer filtering technology, and monitors the traffic

with the help of χ^2 test and entropy theory. The experimental result shows that this solution of SIP traffic monitoring in different network traffics is feasible and effective.

References

[1] J Rosenberg, H. Schulzrinne, G. Camarillo, A.R.Johnston, J. Peterson, R. Sparks, M. Handley, E.Schooler, "SIP: Session Initiation Protocol," RFC3261, IETF, June 2002.
[2] Deri L. Improving passive packet capture: Beyond device polling. http://luca.ntop.org/Ring.pdf. Nov. 2003.
[3] Aymeric M. The GNU oSIP Library.
[4] ZANDER S, Kennedy D, ARMITAGE G. KUTE. "A high performance kernel-based UDP traffic engine." Melbourne: Centre for Advanced Internet Architectures (CAIA), 2005.
[5] Richard G, Olivier J. SIPp. http://sipp. sourceforge.net. Oct 2010.
[6] V.Jacobsen and C. Leres. Tcpdump/libpcap, http://www.tcpdump.org, 2005.