J. Software Engineering & Applications, **2008, 1: 60-67**
Published Online December 2008 in SciRes (www.SciRP.org/journal/jsea)

Two-Tier GCT Based Approach for Attack Detection

Zhiwen Wang, Qin Xia, Ke Lu

MOE KLINNS Lab and SKLMS Lab, Department of Computer Science & Technology, Xi'an Jiaotong University, Xi'an, 710049, P.R.China
Email: wzw@mail.xjtu.edu.cn, qxia@ctec.xjtu.edu.cn, luke@stu.xjtu.edu.cn

Received November 23rd, 2008; revised November 27th, 2008; accepted December 2nd, 2008.

ABSTRACT

The frequent attacks on network infrastructure, using various forms of denial of service attacks, have led to an increased need for developing new techniques for analyzing network traffic. If efficient analysis tools were available, it could become possible to detect the attacks and to take action to weaken those attacks appropriately before they have had time to propagate across the network. In this paper, we propose an SNMP MIB oriented approach for detecting attacks, which is based on two-tier GCT by analyzing causal relationship between attacking variable at the attacker and abnormal variable at the target. According to the abnormal behavior at the target, GCT is executed initially to determine preliminary attacking variable, which has whole causality with abnormal variable in network behavior. Depending on behavior feature extracted from abnormal behavior, we can recognize attacking variable by using GCT again, which has local causality with abnormal variable in local behavior. Proactive detecting rules can be constructed with the causality between attacking variable and abnormal variable, which can be used to give alarms in network management system. The results of experiment showed that the approach with two-tier GCT was proved to detect attacks early, with which attack propagation could be slowed through early detection.

***Keywords*:** *Network Behavior, Attack Detection, Granger Causality Test, Management Information Base*

1. Introduction

The frequent attacks on network infrastructure, using various forms of denial of service (DoS) attacks and worms, have led to an increased need for developing techniques for analyzing and monitoring network traffic. If efficient analysis tools were available, it could become possible to detect the attacks and take action to suppress them before they have had much time to propagate across the network. In this paper, we study the possibilities of SNMP MIB based mechanisms for attack detection.

Detecting attacks close to the attacker allows us to limit the potential damage close to the target. Traffic monitoring close to the source may enable the network operator quicker identification of potential attack and allow better control of administrative domain's resources. Attack propagation could be slowed through early detection.

The current approach passively monitors network traffic at regular intervals and analyzes it to find any abnormalities. By observing the traffic and correlating it to previous states of traffic, it may be possible to see whether the current traffic is behaving in a correct manner. The network traffic could be different because of flash crowds, changing access patterns, infrastructure problems such as router failures, and DoS attacks. In the case of bandwidth attacks, the usage of network may be increased and abnormalities may show up in traffic volume. These approaches rely on analyzing regularity of network traffic in order to provide indications of possible attacks in the traffic.

However, all the approaches on detecting attack mentioned above absolutely depend on individual network behavior at the target, which usually ignore the causality among different network behaviors and the impact of time series. Those impacts may be caused by attacking behaviors at the attacker in most cases, so it is prone to produce a high rate of failed and false alarm [1]. It's important to study how to construct network behaviors influenced by attacks in a complex environment. The causal relationship of network behavior between the attacker and the target make it become possible to detect the attacks early at the attacker and to take appropriate action to weaken those attacks before they have had time to propagate across the network.

In this paper an SNMP MIB oriented approach based on two-tier GCT (Granger Causality Test) is presented, which can detect attack before the security was damaged at the target. According to the abnormal behavior constructed at the target, GCT is executed initially to find preliminary attacking variable, which has whole causality with abnormal variable in network behavior. Relying on the behavior features extracted from abnormal behavior, GCT is executed again to recognize attacking variable,

Funding for this work was provided by China NSF Grant (60633020, 60473136, 60373105), and National High Tech. Development Plan (2006BAH02A24-2, 2006BAK11B02, 2007AA01Z475).

Copyright © 2008 SciRes

which has local causality with abnormal variable in local behavior. The causality between attacking and abnormal variable is used to build detecting rules. These detecting rules make it possible to detect attacks at the attacker early. SNMP MIB traffic variable of *udpOutDatagrams* is successfully recognized as attacking variable and detecting rules was built well under the experiment of Trin00 UDP Flood. The final results showed that the approach with two-tier GCT is proved to detect attacks at the attacker early, which has great effect on slowing the attack propagation to the target.

This paper makes the following contributions: 1) considers the time series analysis of network behaviors; 2) presents a novel approach based on two-tier GCT for detecting attack; 3) uses prevalent SNMP MIB traffic variable as input of detecting model; and 4) shows the approach with two-tier GCT is more accurate than that with single GCT under the experiment of Trin00 UDP Flood.

The rest of the paper is organized as following. Section 2 gives an overview of related work. Section 3 analyses the time sequence of network attack. Section 4 gives some basic definitions and presents the correlation method and correlating procedure of network behavior. Section 5 describes a novel approach on detecting attack based on two-tier GCT, which is SNMP MIB traffic variable oriented. Trin00 UDP Flood experiment is carried out in Section 6, which shows the effect that attack propagation could be slowed through early detection. Section 7 draws conclusions of the paper.

2. Related Work

Many approaches have been studied to detect, prevent and mitigate malicious network traffic. For example, rule-based approaches, such as IDS, try to apply previously established rules against incoming traffic to detect and identify potential DoS attacks close to the victim's network. To cope with novel attacks, however, IDS tools such as Snort [2] require to be updated with the latest rules. This paper pays attention to the problem of designing generalized measurement based real-time detection mechanisms. Measurement-based studies have considered traffic volume [3,4,5], number of flows [6] as potential signals that can be analyzed in order to detect anomalies in network traffic, while we further utilize the SNMP MIB traffic variables such as *ipOutRequests, udpInDatagrams, tcpInErrs*, etc. Work in [5] relies on input data from multiple sources, while our work focuses on the traffic variables located in each machines.

Some approaches proactively seek methods to suppress the overflow of traffic at the source [7]. Controls based on rate limits have been adopted for reducing the monopolistic consumption of available bandwidth, to diminish the effects of attacks, either at the source or at the destination [7,8,9]. The apparent symptoms of bandwidth attack may be sensed through monitoring bit rates [10] and/or packet counts of the traffic flow. Bandwidth accounting mechanisms have been suggested to identify and restrain attacks [11,12,13,14,15,16]. Packeteer [17] and others offer commercial products that can account traffic volume along multiple dimensions and allow policy-based rate control of bandwidth. Pushback mechanisms have been proposed to contain the detected attacks closer to the source [9,13,18]. Traceback has been proposed to trace the source of DDoS attacks even when the source addresses may be spoofed by the attacker [19]. Seong [20] proposes a traffic anomaly detector, operated in postmortem and in real-time, by passively monitoring packet headers of traffic.

However, sophisticated low-rate attacks [21], which do not give rise to noticeable variance in traffic volume, could go undetected when only traffic volume is considered. Recently statistical analysis of aggregate traffic data has been studied. In general, the generated signal can be analyzed by employing techniques such as FFT (Fast Fourier Transform) and wavelet transforms. FFT of traffic arrivals may reveal inherent flow level information through frequency analysis. Fourier transforms and wavelets have been applied to network traffic to study its periodicity [22,23].

Among the detecting methods, Cabrera first attempted to detect network attack by using GCT whose core is to check whether the lag information of a random variable will make an statistically effective forecasting to another random variable with statistical tools [24]. GCT has been applied to many fields successfully, such as earthquake warning, stock-market analyzing, network security etc. Cabrera carried out an experiment on detecting attack in which SNMP MIB was chosen to act as detecting variables in order to recognize some attacking variables reflecting the attacking procedure, but the time interval between units in the same data series is too long to reflect the causality between data series exactly. WANG Sheng [25] considered that attacking procedure may have various causality in whole and local network behavior, and he put forward the idea of GCT based on local data series. There is no experiment done by WANG to support his idea.

Based on the foundation mentioned above, the detecting method of Causality in network behavior was studied in-depth by making full use of existing SNMP MIB traffic variables. A novel approach with two-tier GCT characterized by *whole causality first, local causality second* is presented in this paper and will be described detailed in below sections.

3. Time Sequence of Attack

Typical network attack includes spatial and temporal dimensions. Spatial dimension means the physical location of network entities involved in attacking procedure is arbitrary, and temporal dimension means there is time sequence between mutual interactions produced by network entities involved in an attacking procedure. The time sequence of network attack is

Copyright © 2008 SciRes

depicted in Figure 1, where a complete attacking procedure consists of the following four stages.

1) Prepare to attack (T_0). Attacker scans vulnerabilities and identifies system to choose target.

2) Attacking (T_1). Attacker initiates attacking command, such as TCP semi-connection, ICMP Flood etc.

3) Attack takes effect (T_2). Attacking command arrives at target and leads to abnormal behavior on target.

4)Target damaged (T_3). Sustained attacks make the security of target damaged.

The arbitrary of spatial distribution and uncertain of time lag exacerbate the complexity of detecting attack. The common principle of detecting approaches is that relevant data originating from temporal dimension or spatial dimension is collected first, and then some methods, such as rules reasoning, FSM, pattern matching and statistical analysis are applied to extract the feather of network attack so as to avoid the attacking procedure to enter in T_3 or T_2 stage.

4. Behavior Correlation Method

4.1 Definition

In order to describe the approach with two-tier GCT used for detecting network attack exactly, some necessary items are defined as follows.

1) Network behavior. The numerical value sequence of detecting variables which represents the running state of network, such as CPU utilization, available network bandwidth and memory consumption, is observed over a continuous period and which is denoted by $B=\{v_k\}$ (k=1,2,3,…,N), where v_1 and v_N stand for the value of detecting variable V at the starting time t_{init} and end time t_{end} respectively. The variable $t_{\text{intervat}}=(t_{\text{init}} - t_{\text{end}})/N$ is defined as observation interval, which will directly affect the accuracy of network behavior description.

2) Time window. The part of detecting time corresponding to constructing the network behavior, denoted by W (t_{low}, t_{upper}), where t_{low} and t_{upper} stand for the bottom and top of a time window respectively. The difference of top and bottom is defined as time window size t_{win}.

3) Behavior feature. Some certain regularity in a time window or among time windows is showed by the observational numerical value in network behavior. The behavior feature is denoted as $F=\{v_\lambda\} \subseteq B$ (λ=1,2,3,…,n), where v_1 and v_n stand for the observational numerical values corresponding the time of t_{low} and t_{upper}. There are five types of regularity for behavior feather, ie. ① The observational numerical value is increased monotonously during a time window. ② The observational numerical value is diminished monotonously during a time window. ③ The observational numerical value is above the special threshold in a time window. ④ The observational numerical value is below the special threshold in a time window. ⑤ The observational numerical value is changed in periodicity among time windows.

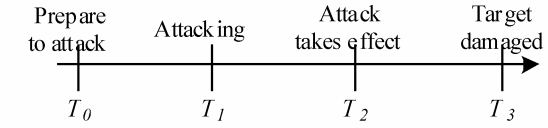

Figure 1. Time sequence of network attack

4) Local behavior. Defined as the observation numerical sequence which is acquired when t_{low} of a time window corresponding to behavior feature is moved backward a time window size, and whose length is double of the length of behavior feature on the time sequence.

5) Abnormal behavior. The network behavior represented by network entities on targets whose security will be damaged at stage of T_3 or T_2. The detecting variables used in constructing abnormal behaviors are called abnormal variables.

6) Attacking behavior. The network behavior represented by attacker at stage of T_0 or T_1, which will damage the security of one or more network entities with some possibility.

7) Preliminary attacking variables. The detecting variables which has whole causality with abnormal variables in network behavior.

8) Attacking variables. The detecting variables which has local causality with abnormal variables in local behavior. Attacking variables are always used in constructing attacking behaviors.

9) Behaviors correlating. The procedure which is to mine the causality between abnormal variables and detecting variables with GCT. There are two types of behaviors correlation named whole correlation and local correlation respectively. The former is used to find preliminary attacking variables and the later is used to recognize attacking variables.

10) Detecting Rule. The reflection of causality between attacking variable and abnormal variable, denoted as ({Vattack}, Vabnorm), which make attacker oriented detection possible.

4.2 Correlation Method

Given a large database describing the operation of an Information System, we view the problem of extracting proactive Detecting Rules for security as consisting of the three steps delineated below. These steps are performed off-line, and produce a set of rules to be used for detecting security violations on-line. The correlation of causal relationship can be inferred from measured variables in this paper.

1) Detecting Anomaly. The objective here is to determine the variable in the target machine, which is better characterizing the occurrence of an attack. The final product of this step is the list of abnormal variables at the target. There are two procedures for determining the abnormal variable at the target. One way is to use domain knowledge about the special attack. For example, for Ping Flood, it is known that *icmpInEchos* is the right

Copyright © 2008 SciRes

variable to look for, sine Ping Floods are affected by sending much *icmpInEchos* packets to a target. A second way is to compare the evolution of each variable during an attack with the evolution of the variable during normal operation. Variables that display a large variation between normal operation and attack should be declared abnormal variables at the target. Since we are looking for localized variation in the variable, the time series should be segmented on small sub-time series, which are then compared with normal profiles. This procedure was used in [26] for detecting anomalies in network operation due to component faults. Anomalies were detected as variation on the parameter of AutoRegressive models. In this paper, we will utilize domain knowledge about the attacks for extracting the abnormal variable at the target.

2) Computing Correlation. Once the abnormal variable at the target are determined, we need to determine variables in the prospective attacker that are causally related with them. These variables at the attacker are related to T_2 and T_3 events. Recall that we do not know which ones are the attacker. We only know a list of candidates and their corresponding variables. We make the assumption that any causal relationship between variables at prospective attackers and the abnormal variables at the target is to be inferred as a link between that attacker and the target. The final product of this step is the list of attacking variables.

3)Constructing Detecting Rules. Following the computing correlation, the objective here is to extract particular features of the attacking variables at the attacker that precede the attack at the target. Recall that these variables were found to be causally related with the attack; hence we may expect that certain anomalies in these variables can be indicative of an incoming attack. Once these features are determined and are shown to precede the attack, we can construct proactive detecting rules that constitute the end product of this step. These rules can be used to implement alarms on a network management system.

4.3 Network Behavior Correlation

According to above definition we attempt to recognize the variables at the attacker that are causally related to the abnormal variables at the target. Since we are looking for proactive detecting rules, we should recognize variables at attacker which contains events that precede the damage at the target. These events can be T_2 events, or T_3 events, as described in Section 3. In this section, the use of Causality Tests is to be investigated for correlating the network behaviors at the attacker with the network behavior at the target [27]. Testing for causality in the sense of Granger, involves using statistical tools for testing whether lagged information on a variable *u* provides any statistically significant information about another variable *y*. if not, then *u* does not Granger-cause *y*. GCT compares the residuals of an AutoRegressive Model with the residuals of an AutoRegressive Moving Average Model. Assuming a particular lag length *P*, and estimate the following unrestricted equation.

$$y(k)=\sum_{i=1}^{P}\alpha_i y(k-i)+\sum_{i=1}^{P}\beta_i u(k-i)+e_1(k);\quad k=0,1,2,\cdots,N-1$$

The null hypothesis of the H_0 GCT is given by:

$$H_0:\qquad \beta_i=0,\ \ i=1,2,\cdots,p$$

i. e. *u* does not affect *y* up to a delay of *p* units. The null hypothesis is tested by estimating the parameters of the following restricted equations.

$$y(k)=\sum_{i=1}^{P}\gamma_i y(k-i)+e_0(k)$$

Let R_1 and R_0 denote the sum of the squared residuals under the two cases.

$$R_1=\sum_{t=1}^{T}e_1^2(t),\quad R_0=\sum_{t=1}^{T}e_0^2(t);\ \ T=N-P$$

If the test statistic *g* given by

$$g=\frac{(R_0-R_1)/P}{R_1/(T-2P-1)}\sim F(P,T-2P-1)$$

is greater than the specified critical value, then reject the null hypothesis that *u* does not Granger-cause *y*. Here, $F(a, b)$ is Fisher's *F* distribution with parameter *a* and *b*. In other words, high values of *g* are to be understood as representing strong evidence that *u* is causally related to *y*. In the traditional sense, we say that u_1 is more likely to u_2 to be causally related with *y* if $g_1>g_2$, where g_i, i=1,2 denote the GCT statistic for the input-output pair (u_i, *y*).

5. Our Approach

Our approach, which is based on two-tier GCT, is modeled in Figure 2. The model consists of four main components, ie constructing network behavior, detecting anomaly, recognizing attacking variable and preventing attack.

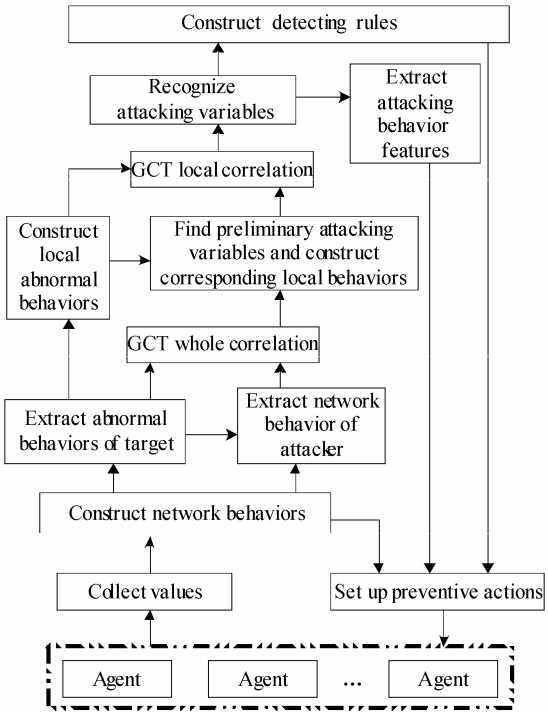

Figure 2. Two-tier GCT based approach

Copyright © 2008 SciRes

5.1 Constructing Network Behavior

According to the definition of network behavior, we find that SNMP/MIB is able to meet the requirements of detecting variables completely. There are still three technical problems needed to be solved before the appropriate network behavior is constructed for detecting attack.

1) Choose detecting variables. In order to reduce the number of network behavior and improve the accuracy of recognizing detecting variables, it is necessary to choose detecting variables from SNMP/MIB exactly. As we know, both attacker and target act as network termination entities in most cases, and the data transmission between them is executed on network layer or higher layer, so we are like to choose 32 variables from IP, ICMP, TCP and UDP variable group as detecting variables, which represent the dynamic performance of network.

2) Decide the way of collecting value. Collecting values of detecting variables period is a necessary step for constructing network behaviors correctly. Various ways will bring different effect in collecting values and polling is rather appropriate because of its simplicity and robust.

3) Determine the period of network behavior. According to working situation network behaviors can be measured by hour, day, week or month. The fact that normal network traffic is varying in a one-day circle is found in reference [28], which is accomplished through many times of observation and experiment. The period of network behavior is measured by day in this paper.

5.2 Detecting Anomaly

The key of detecting anomaly is to recognize abnormal variable from detecting variables. There are two methods used commonly, which include special analysis based on domain knowledge and statistical analysis. The former is suitable to attacks with manifest procedure, by which abnormal variable can be recognized directly from SNMP MIB by making use of domain knowledge. The latter is more suitable to attacks where abnormal variables can't be recognized directly through the attack procedure. Statistical deviation of network behavior must be calculated for every detecting variable in attacking and normal environments independently, and detecting variables with the largest deviation are confirmed to be abnormal variables.

After abnormal variables were recognized, attack test can be carried out repeatedly and abnormal behavior will be monitored successively. As a result, the abnormal behavior feature can be extracted by checking whether it is consistent with the behavior feature defined in Section 4.

5.3 Recognizing Attacking Variables

Causality in network behavior between attacker and target can be correlated based on the features of attack procedure with time backward tracking. According to the abnormal behavior on target, preliminary attacking variables which have whole causality with abnormal variables in network behavior can be found first from detecting variables by using GCT. Then according to the behavior features of abnormal behaviors, attacking variables which has local causality with abnormal variables in local behaviors can be recognized from preliminary attacking variables by using GCT again. The detecting variables whose value exceeds the threshold set in the two GCT will be recognized as attacking variables.

The whole correlation in network behavior is processed as following.

1) Obtain abnormal behavior b_{abnorm} from network behavior base on target,

2) Obtain all the network behaviors $h_{\text{attack}}(j)$ from network behavior base on attacker, which are coincided with b_{abnorm} in detecting period;

3) Calculate the GCT detection statistics g_{whole} of all input/output pair $h_{\text{attack}}(j)$, b_{abnorm});

4) If g_{whole} corresponding to any $h_{\text{attack}}(j)$ is beyond the critical value F_α of F distribution under significance level α, it is showed that $h_{\text{attack}}(j)$ has whole causality with b_{abnorm} and the detecting variables used to construct $h_{\text{attack}}(j)$ will be recognized as preliminary attacking variables [27].

Because GCT is a statistical method, the preliminary attacking variables recognized by executing whole correlation only once is some fortuitousness. As a result, it is necessary to execute whole correlation many times so as to recognize preliminary attacking variables with more accuracy.

The process of local correlation between local behaviors is described as follows.

1) Extract all behavior features of abnormal behavior b_{abnorm}, denoted as $f(i)$, i=1,2,3,…,M;

2) Construct local abnormal behavior corresponding to the abnormal behavior feature, denoted as $local\_b_{\text{abnorm}}(i)$, i=1,2,3,…,M.

3) If $h_{\text{attack}}(j)$ has whole causality with b_{abnorm}, local behavior $local\_h_{\text{attack}}(i, j)$ which is in the same detecting period with $local\_\ b_{\text{abnorm}}(i)$ will be constructed.

4) Calculte GCT statistics $g_{\text{local}}(i, j)$ of all input/output data pairs ($local\_h_{\text{attack}}(i, j)$, $local\_\ b_{\text{abnorm}}(i)$).

5) If $g_{\text{local}}(i, j)$ is below the critical value F_α of F distribution under significance level α, it's showed that $h_{\text{attack}}(j)$ doesn't have local causality with b_{abnorm}.

6) Define $g_{\text{local}}(j)$ of $h_{attack}(j)$ as the sum of $g_{\text{local}}(i, j)$ belong to the same $h_{attack}(j)$. The higher $g_{\text{local}}(j)$ is, the more possibility $h_{\text{attack}}(j)$ is recognized as attacking behavior.

$$g_{\text{local}}(j) = \sum_{i=1}^{M} (g_{\text{local}}(i, j) t_{\text{win}}(i)) \Big/ (\sum_{i=1}^{M} t_{\text{win}}(i))$$

In the expression depicted above, $t_{win}(i)$ represents the size of time window corresponding to the ith behavior feature of abnormal behavior.

1) Construct the attack detecting rules according to the recognized attacking variables.

Copyright © 2008 SciRes

5.4 Preventing Attack

The attacking variables recognized at the attacker are labeled as causally related with the abnormal variables at the target, but we still need to find trigger, or a key event at the attacker. This is an anomaly detection problem. We postulate that any anomalous behaviors in attacking variables at the attacker are to be considered key events at the attacker. One possible approach is to look for jumps in the attacking variables, by monitoring the absolute values of the differentiated time series. Using many normal runs, we constructed a normal profile of jumps for each of the 32 MIB traffic variables. Given a attacking variable, key events at the attacker are defined as jumps larger than the largest jump encountered the normal profile of jumps. Those key events are used to set the alarms.

6. Experiment Simulation

The certainty of attacking variable and effect of attack detection will be verified in the following experiments in order to validate the approach with two-tier GCT.

Experimental environment consists of an attacker host, a target host and a security management host, which are connected through Ethernet. SNMP Agent is deployed on the attacker host and target host and the security management host is responsible for detecting attack. Trin00 UDP Flood [29] is selected on attacker in experiments. According to its principle, SNMP MIB traffic variable of *udpInDatagrams* is selected as abnormal variable in Trin00 UDP Flood. The unit of time for experiment is measured by days and the duration of each attack procedure persists for 1 hour. The value of 32 traffic variables acted as detecting variables at the attacker and *udpInDatagrams* at the target are collected every 10 seconds and 1 minute respectively. All tests are carried out against attacker under three types of running configuration, which is depicted as following.

① execute attack only
② execute attack and FTP
③ execute both attack and Netflow

6.1 Certainty of Attacking Variable

Based on detecting variable and abnormal variable, certainty of attacking variables is validated by checking whether the attacking variables recognized in different environments are identical. The results acquired by using single GCT (proposed by CABRERA in [24]) and two-tier GCT respectively are compared to validate the advantage of the approach presented in this paper.

Table 1 shows the critical value F_α（p, T-2p-1）of F distribution for GCT causality statistics g_{whole} and g_{local} under significance level α of 0.05. The approach with single GCT needs only whole correlation which computes the whole causality statistics g_{whole} in network behavior between each of 32 detecting variables and *udpInDatagrams* at the target. Among the detecting variables exceeding critical value F_α, one with the largest g_{whole} is recognized as attacking variable. Table 2 shows the results of test with sampling interval of 1 minute.

It's different from the approach with single GCT, detecting variables with g_{whole} over critical value F_α are just treated as preliminary attacking variables in the approach with two-tier GCT. Comparing to the original 32 detecting variables, the number of preliminary attacking variables is reduced greatly, which is good to perform local correlation in local behavior and to reduce the cost of implementing GCT. Three monotonous increasing behavior features corresponding to the three attacking actions taken by attacker host are observed by analyzing the abnormal behaviors, and the duration of each is not the same as the duration of attacking action. In order to keep the consistency of detecting in time dimension, only the first 60 minutes of monotonous increase duration is considered as time window of behavior feature. Accordingly, the period of local behavior should be set by120 minutes. In order to recognize attacking variable, each of the local causality statistics g_{local} between preliminary attacking variable and abnormal variable should be computed. The variable exceeding the critical value F_α with the largest g_{local} is recognized as attacking variable. Table 3 shows the attacking variable recognized by using two-tier GCT with sampling interval of 10 minutes.

By comparing the results in Table 2 and Table 3 we found that the attacking variable recognized with single GCT is uncertain in different environments, where *ipOutRequests* was recognized as attacking variable in the first 2 running configurations and *udpOutDatagrams* was recognized in the third running configuration. On the contrary, the attacking variable recognized with two-tier GCT is certain well, where *udpOutDatagrams* was recognized as attacking variable in three different running configurations.

6.2 Effect on Attack Detection

To demonstrate the effect of attack detection with attacking variables *ipOutRequests* and *udpOutDatagrams* independently in preventing attack, an experiment lasted 5 days was carried out incessantly. Trin00 UDP Flood was initiated random by 10 times for each day in the identical running environments configured as before. The detecting results acquired with *udpOutDatagrams* and *ipOutRequests* respectively were listed in Table 4. According to the results, we found that the success rate of detection with *udpOutDatagrams* is significantly higher than detection with *ipOutRequests*. It's obvious that the performance of approach with two-tier GCT is better than the approach with single GCT.

Table 1. Critical value of F distribution

statistics	interval	times	P	T	95%
g_{whole}	1 min	1440	200	1240	1.19
g_{local}	10 s	720	100	620	1.28

Copyright © 2008 SciRes

Table 2. Results acquired with single GCT

running configuration	number of detecting variable	maximum of g_{whole}	minimum of g_{whole}	number of detecting variable satisfying $g_{whole} \geq F_\alpha$	attacking variable
①	32	4.11	1.04	8	ipOutRequests
②	32	3.67	0.91	7	ipOutRequests
③	32	3.50	0.79	11	udpOutDatagrams

Table 3. Results acquired with two-tier GCT

running configuration	number of preliminary attacking variable	duration of abnormal features	maximum of g_{local}	minimum of g_{local}	number of detecting variable satisfying $g_{local} \geq F_\alpha$	attacking variable
①	8	61.2	3.65	1.22	5	udpOutDatagrams
②	7	59.4	3.41	1.02	6	udpOutDatagrams
③	11	64.4	2.87	0.98	5	udpOutDatagrams

Table 4. Detecting effect with different attacking variables

running configuration	number of attacking	detecting with udpOutDatagram			detecting with ipOutRequestss		
		actual	false	failed	actual	false	failed
①	50	51	1	0	58	8	0
②	50	52	2	0	62	14	2
③	50	55	7	2	65	21	6

7. Conclusions

Since the conventional method of network attack detection is focused on stage T_3 of attacking procedure, it is difficult to detect the attack before security of target is damaged. An SNMP MIB oriented approach based on causality of network behavior is presented in this paper. According to the abnormal behavior features hidden in detecting variables on target in attacking procedure, backward retrospection is executed twice with two-tier GCT. Depending on whole causality between detecting variables and abnormal variables the preliminary attacking variables is found first. Then according to behavior features extracted from abnormal behaviors, attacking variables which has local causality with abnormal variables can be recognized by using GCT again and the corresponding rules for attack detecting can be constructed subsequently. The results of experiment showed that the approach was proved to detect attack on attacker, which has effect on blocking the pervasion of attacking procedure to target.

As an on-line detecting method, the approach with two-tier GCT employs small amounts of SNMP MIB traffic data in order to keep such analysis simple and efficient. At the same time, the data cannot be so small that meaningful statistical conclusions cannot be drawn. However, on-line detection may also require that any indications of attacks be provided with short latencies. The tension between robustness and latency makes on-line detection more challenging.

REFERENCES

[1] M. Thottan and C. Y. Ji, "Anomaly detection in IP networks," IEEE Transactions on Signal Processing, 51(8): pp. 2191–2204, 2003.

[2] M. Roesch, "Snort-lightweight intusion detection for networks," in USENIX LISA 1999, Seattle, WA, November 1999.

[3] P. Barford et al., "A signal analysis of network traffic anomalies," in ACM SIGCOMM Internet Measurement Workshop, November 2002.

[4] A. Hussein, J. Heidemann, and C. Papadopoulus, "A framework for classifying denial of service attacks," in ACM SIGCOMM, August 2003.

[5] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing network-wide traffic anomalies," in ACM SIGCOMM, September 2004.

[6] D. Plonka, "FlowScan: A network traffic flow reporting and visualization tool," in USENIX LISA 2000, New Orleans, LA, December 2000.

[7] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source," in IEEE International Conference on Network Protocols, November 2002.

[8] A. Garg and A. L. N. Reddy, "Mitigation of DoS attacks through QoS regulation," in Proceedings of IWQOS, May 2002.

[9] J. Ioannidis and S. M. Bellovin, "Implementing pushback: Router-based defense against DDoS attacks," in Proceedings of Network and Distributed System Security Symposium, February 2002.

[10] Y. Zhang, L. Breslau, V. Paxson, and S. Shenker, "On the characteristics and origins of internet flow rates," in ACMSIGCOMM, August 2002.

[11] Smitha, I. Kim, and A. L. N. Reddy, "Identifying long term high rate flows at a router," in Proceedings of High Performance Computing, December 2001.

[12] I. Kim, "Analyzing network traces to identify long-term high rate flows," M. S. thesis, TAMU-ECE-2001-02, May

Copyright © 2008 SciRes

2001.

[13] R. Mahajan, et al., “Controlling high bandwidth aggregates in the network,” ACM Computer Communication Review, Vol. 32, No. 3, July 2002.

[14] C. Estan and G. Varghese, “New directions in traffic measurement and accounting,” in ACM SIGCOMM, August 2002.

[15] A. Medina et al., “Traffic matrix estimation: Existing techniques and new directions,” in ACM SIGCOMM, August 2002.

[16] D. Tong and A. L. N. Reddy, “QOS enhancement with partial state,” in Proceedings of IWQOS, June 1999.

[17] Packeteer, “PacketShaper Express,” white paper, 2003, http://www. packeteer. Com / resources / prod-sol/Xpress_ Whitepaper.pdf.

[18] S. Floyd, S. Bellovin, J. Ioannidis, K. Kompella, R. Mahajan, and V. Paxson, “Pushback messages for controlling aggregates in the network,” IETF Internet draft, work in progress, July 2001.

[19] S. Savage, D. Whetherall, A. Karlin, and T. Anderson, “Practical network support for IP traceback,” in ACM SIGCOMM, 2000.

[20] S. S. Kim and A. L. N. Reddy, “Statistical techniques for detecting traffic anomalies through packet header data,” IEEE/ACM Transaction on Networking, Vol. 16, No. 3, pp. 562–575, June 2008.

[21] A. Kuzmanovic and E. Knightly, “Low-rate TCP-targeted denial of service attacks,” in ACM SIGCOMM, Karlsruhe, Germany, August 2003.

[22] A. Feldmann, A. Gilbert, P. Huang, and W. Willinger, “Dynamics of IP traffic: A study of the role of variability and the impact of control,” ACM Computer Communication Review, Vol. 29, No. 4, pp. 301–313, 1999.

[23] C. M. Cheng, H. T. Kung, and K. S. Tan, “Use of spectral analysis in defense against DoS attacks,” in IEEE Globecom, 2002.

[24] J. B. D. Cabrera, L. Lewis, and X. Z. Qin, “Proactive detection of distributed denial of service attacks using MIB traffic variables–a feasibility study,” IEEE Transactions on Signal Processing, 49(6): pp. 609–622, 2001.

[25] S. Wang, L. C. Sun, and G. Z. Gan, “Application research based on Granger causality test for attack detection,” Computer Applications, 25 (6): pp. 1282–1285, 2005.

[26] F. Zhang and J. Hellerstein, “An approach to on-line predictive detection,” in proceedings of the Eighth International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems, San Francisco, CA, IEEE Computer Society, pp. 549–556 August 2000.

[27] J. Hamilton, “Time series analysis,” Princeton University Press, 1994.

[28] B. X. Zou and Z. Q. Yao, “A method to stabilize network traffic,” Journal of China Institute of Communications, 25(8): pp. 14–23, 2004.

[29] P. J. Criscuolo, “Distribution denial of service — trin00, tribe flood network, tribe flood network 2000, and stacheldraht,” CIAC–2319, Department of Energy — CIAC (Computer Incident Advisory Capacity), 2000.

Copyright © 2008 SciRes