An Enhanced SYN Cookie Defence Method for TCP DDoS Attack

Bo Hang\(^1\,^2\), Ruimin Hu\(^2\), Wei Shi\(^3\)
1. School of Mathematics and Computer Science, Xiangfan University, Xiangyang, China
2. National Engineering Research Center for Multimedia Software, Wuhan University, Wuhan, China
3. Computer School, Wuhan University, Wuhan, China
bohang@163.com, hrm1964@public.wh.hb.cn, 2144568@qq.com

Abstract—With the development of network, the issues of network security are rapidly becoming a serious problem, and the Denial of Service (DoS) attack has already become the greatest threat to the network. SYN Flood attack is one of the most common distributed denial of service attack way (DDoS). This paper presents an improved SYN Cookie method, designing a novel attack detector processing and an enhanced attack responder with a new cookie verification algorithm and changing the definition of cookie field, to reduce algorithm complexity with the assurance of security. The experiment results show that the proposed method provided an average computational complexity reduction of 30% compared with the traditional method. The new method can be an effective defense against the TCP SYN Flood attack with a lower complexity.

Index Terms—DDoS; SYN Flood; SYN Cookie

I. INTRODUCTION

Network has brought great convenience to people’s lives, but the simplicity and openness of TCP / IP protocol let the traditional network vulnerable to attacks [1]. Distributed denial of service attack (DDoS) is the most common one of the network attacks ways. Denial of service attack refers to a devastating attack, which blocks or denies legitimate users’ access to a web server. It used mass packet data beyond processing capabilities of the target, consuming the available system resources, bandwidth resources, resulting in paralysis of network services. Any action, which can lead to that the legitimate users can not engage in normal behavior of network services, can be called a denial of service attack. In the current frequently used network attacks methods, it is the greatest threat to network facilities, and is very difficult to prevent.

Denial of service attacks first appeared about twenty years ago. At that time computers’ data processing capacity is low, and most networks are slow. A single attacker first use port scanner [2-4] to detect open ports of the target host, and then directly send data packets exceeding the maximum service capacity of the server to these open ports, causing the server can not provide an effective network service. At that time the main target of attack is the local host with low processing capacity. It has no apparent threat for the large-scale network and hosts with high-bandwidth; high speed data-processing capability. From 2000, with the appearance of distributed denial of service attack (DDoS, Distributed Denial of Service), the large-scale network infrastructure began to face being threatened. An attacker may exploit easily thousands of coerced puppet hosts implanted an attacking program, continuing attacking on the server. So, even large network sites can not resist.

Denial of service attacks from the continuous development occurred up to now, has become the number one security threat to computer networks, network intrusion denial of service attacks often used as a first step in damages.

It is precisely because the harm caused by denial of service attacks are large and difficult to defend. Therefore, network security industry began early in the attack and its defense in-depth study of the results of their research has been part of the business, and its mainly used for the protection of critical network equipment, such as servers, routers, firewalls and so on.

In China, it is reported by the CERT / CC [5] that initiated Distributed-Systems Intruder Tools Workshop was first published in November 1999 against DDoS issues. Denial of service attack in which the distribution of the form - DDoS attacks carried out a detailed analysis of theory, and for the system administrator, ISP, etc., from the defense, detection, response is given followed by three real-time, short-term and long-term solution. The current representative of the attacks on the United defense products are Green Union's Collpasar (black hole) products. It uses what is known as reverse detection and a new algorithm for fingerprint recognition, which can effectively withstand various types of DoS attacks.

In other countries, research related to the attack on the research work [6] is also very active. Dave Dittrich University of Washington, DDoS attacks based on its right to carry out the study, the network share a lot of DDoS attacks and defense research data. The D-WARD [7-8] attack defense system is to adopt a defensive approach based on the source for the early prevention of attacks on providing an effective way. In order to assess the effect of attacks on defense, MIT has also introduced intrusion detection evaluation data set [9] DARPA, the use of tools such as snort [10] can replay the data set [11-12], can simulate the real environment, the attack . It is divided into a representative attack defense products Catus Networks CaptIO G-2 and so on.
After a careful study of attacks on defense over the years, the whole process of attack on defense can be broadly divided into three stages: attack prevention, attack detection, attack response. Research focus of which is the real-time attack detection and attack detection algorithm used in traffic filter algorithm.

Detection algorithm which can be broadly divided into two categories: feature-based intrusion detection technology and anomaly-based intrusion detection technology. The former, as a representative of the attack detection technology, its technology is mature, widely used. While the latter is a new area of research, its theoretical study is in progress to continue to deepen them, the practical application is also be tested by practice. But it is currently a research hot spot detection technology.

Current intrusion detection and prevention technology are rapidly developing, including the representative technologies:

CUSUM-based traffic anomaly detection algorithm [13-16]. Its use to improve the CUSUM algorithm to detect data flow to send and acknowledgment of the ratio of data flow anomaly, and as the characteristics of the attack.

As the network traffic self-similarity [17-18] a result of attacks on the emergence of abnormal changes in traffic, in the analysis of network traffic self-similarity parameter Hurst of the time-varying functions based on the abnormal changes of the parameters to detect network attacks. One common method of Hurst coefficient estimates are: time analysis of variance, R / S statistical analysis, periodogram analysis, go to the top estimate, whittle analysis, wavelet analysis [19] and so on.

Wavelet [20-22] and other signal processing techniques [23-24] (Fourier changes and changes in the windowed Fourier transform) spectral analysis by flow [25-26], can be used to detect traffic anomalies.

Present a more practical DoS attack prevention technology, Lemon proposed a mechanism based on hash tables to store the SYN Cache algorithm [27], and Bernstein proposed SYN Cookie technology [28]. SYN Cookie technology is already present in the Linux operating system, such as TCP protocol stack to achieve.

Among the many defense technology, has not yet been a real full and effective DoS attack defense technologies. So for the attack on defense research, should be the main attack detection with current technology, combined with each other. And to analyze and improve its deficiencies and shortcomings on the basis put forward a more comprehensive attack on defense programs.

According to statistics, in the DDoS attacks, the TCP protocol establishes normal connections through the three-way handshake [31]: first, the client sends a SYN packet to the server; the server receives this message and will reply SYN + ACK packet to the client; at last, the client will be able to return a final ACK packet to the server, recognizing that a TCP connection is established.

If the server does not receive the third handshake packet, in order to carry out the final confirmation, the server will set the timer for the confirmation message when the timeout has not received even after, then set a larger timeout value and then wait for time, try pass the second confirmation message. After the timeout until the connection reset packet to send this link suspension.

The processing of TCP three-way handshake protocol is shown in Figure 1.

![Figure 1 TCP three-way handshake](image)

| TABLE I. THE PROPORTION OF THE VARIOUS DDoS ATTACK ON DIFFERENT PROTOCOLS |
|------------------|------------------|
| Protocols | The proportion of agreement DDoS |
| TCP | 90%-94% |
| UDP | 2.4%-5% |
| ICMP | 2.1%-2.6% |
| Others | 2.06%-2.9% |

II. SYN COOKIE PRINCIPLES

A. SYN Flood Attack

TCP protocol establishes normal connections through the three-way handshake [31]: first, the client sends a SYN packet to the server; the server receives this message and will reply SYN + ACK packet to the client; at last, the client will be able to return a final ACK packet to the server, recognizing that a TCP connection is established.

If the server does not receive the third handshake packet, in order to carry out the final confirmation, the server will set the timer for the confirmation message when the timeout has not received even after, then set a larger timeout value and then wait for time, try pass the second confirmation message. After the timeout until the connection reset packet to send this link suspension.

The processing of TCP three-way handshake protocol is shown in Figure 1.
DDoS attack aiming to the TCP layer vulnerability is called SYN Flood attack [32].

2.2 The traditional methods of SYN Cookie

The core problem of SYN Flood attack for TCP layer is that the server TCP protocol stack will allocate resources for each client request without determining the legitimacy of the client. If the server allocation of resources is only for the legitimate TCP requests, the server's resources will not be exhausted by attackers, so as to achieve the purpose of preventing SYN Flood attacks.

SYN Cookie technology used this idea [33]. Its principle is: when receiving a TCP SYN packet and returning the TCP SYN + ACK packet, the TCP server does not assign a specific data area, but calculate a cookie value according to this SYN packet. When receiving TCP ACK package, the TCP server checks the legitimacy of the TCP ACK packet, in accordance with the cookie value. If legitimate, a special data area will be redistributed for the future of the TCP connection.

SYN Cookie is an effective mean to prevent denial of service attacks against TCP [34-35], but there are also issues in SYN Cookie such as high computational complexity. Many researchers proposed some improved SYN Cookie program [36-38]. Literature [36] algorithm resolve the problem that ACK Flood attacks caused by high computational complexity of the cookie, by using temporary storage of the SYN packet basic information to identify the legality of ACK packets. This method can effectively reduce the CPU occupancy rate, but requires consumption of additional storage space. Literature [37] changed the TCP protocol response process for the SYN packet in defense system to reduce certification time and improve the defense system efficiency. But this method can only apply to scenario that the defense system is separated with the server. In [38], the method wait for the client SYN packet timeout retransmission, to reduce the computational aspects, but the method requires additional system resources to maintain a HASH table, and will increase the waiting time for a normal TCP connection.

III. ENHANCED SYN COOKIE METHODS

In order to reduce the computational complexity of traditional methods, this paper designed an improved method of SYN Cookie. The method designed a novel cookie calculation algorithm, which modify the 32 bit sequence number field definition used to store TCP cookie.

The whole system can be divided into three components: the controller, attack detector and attack responder. The system is shown in Figure 2 below.

The controller plays the main control role in the system. The other two components are single-function modules. And the system message and control communication between them are all transferred and controlled by the controller.

Attack detection device main function is real-time access to network traffic detection system, upon detection of abnormal flow in time for an exception to issue a warning, the system according to a warning message to activate the corresponding abnormal response mechanism.

Attack responder the entire system, the most important attack on defense function. Upon receipt of control information from the system when a timely response, such as closed or open the defense function, switch IP option field functions.

A. Attack Detector Process Design

Intrusion detection device is also a detection algorithm based on differences between the ideas of design. For attack detection is divided into two parts.

The first part is the primary detection of coarse-grained. That part of the way real-time online, full monitoring of network traffic. If there is no sign of an attack, you do not have to start fine-grained sub-detection. At this time the rate of the detection of functional components, only the primary detection algorithm is running. When they find out attacks in the sub-detection capabilities to start re-affirmed.

The second part is fine-grained sub-test. That part of the play the role of screening results, its main function is that when the primary detection component was found after the attack on the previous test results of a re-screening and screening results are given in the final.

The attack detection device to indicate the detection process shown in Figure 3:

The attack detector consists of two components: primary detection component and secondary detection filter components. Their main functions are nearly same, which are based on actual network traffic as the input, to get the output result whether there are the network attacks.

As shown in figure 3, the processing flow of the attack detector will be divided into two brance for different situations when the network traffic data were input into the primary detection:

When the primary detection test result shows that the traffic data is normal network traffic data, it means that the possibility of attack is low. Because the the primary detection component has a relatively low standard, the false negative rate of the primary detection component is relatively low. At this time some algorithm in the secondary detection components, which need normal traffic data for training, can use the current data sample to train the algorithm.

When the test results of the primary detection shows that the abnormal situation occurs, the algorithm should stop, using the actual network data for training at once, and awake the secondary detection filter. The secondary detection filter has a high detection standard, and can find most attack action. If the traffic data is determined as
attack data, the attack responder will be called by controller and start processing. The two stages detection algorithm can improve detection accuracy with a lower computing complexity.

![Flowchart of attack detector](image)

Figure 3 Flowchart of attack detector

Secondary detection components can be composed of at least one detection algorithm. Detection algorithm which specifies the number of the value of N is customized according to requirements of the program. Which users can set the controller number of a specific algorithm, which makes design can actually deal with efficiency and strike a balance between the specific application environment.

**B. The improved calculation method of cookie hash algorithm**

In the attack responder, the generation and validation of cookie need to calculate the cookie value. So the computational complexity of cookie directly affects the performance of the whole approach. The proposed method uses a 32-bit key Blowfish encryption algorithm, and introduced random secret value in the algorithm. The calculation of the cookie depends on not only IP packet information in the appropriate fields, but also the random secret values. If an attacker can not be a secret value within the system, he can not attack. The algorithm set the expiry time for secret values. Once the secret value is time out, the algorithm will use another new secret value. This is further increase the attacking difficulty.

However, if the direct use of original technology Hash algorithms MD5 replaced with a simpler Hash algorithm. Will exist the following two questions:

1. The security of the new algorithm may be subject to question. How to prove that the new algorithm will be better than MD5. Through the practical application test, MD5 hash algorithm is indeed very good. Such a fine algorithm, the attacker has sufficient computing resources will still be broken. How can the new algorithm to prove its safety and better. Therefore, to ensure the safety of the new algorithm, the new algorithm's security must be built on sound cryptographic basis of the theory.

2. A simple algorithm for computing the amount of reduction algorithms can not guarantee their safety. The design goal of the new algorithm is computing the amount of small, safe. How to solve the new algorithm steps to reduce the hash, while encryption algorithm with reduced intensity problems. From MD5 to SHA hash algorithms such as the development of point of view, their safety is reflected in the increasing computing step, computing the amount of the growing basis. Reduce the amount of arithmetic operations may weaken the algorithm's security; we must take other aids to further enhance the algorithm security.

In the final program design, decided to improve the hashing algorithm the same time, algorithms have been used to introduce random secret value of time. Throughout the process of arithmetic operations, Cookie the final result depends not only on IP packet in the appropriate fields of information, but also rely on a random secret value algorithm. If an attacker to implement attacks can not be only in the secret of the value of the internal algorithm, the attacker would be difficult to increase. This will increase the better protection to the system.

If only using random secret value, but also sufficient to ensure the security of the entire algorithm. As long as the attack long enough time and enough computing resources, the attacker is still possible successful attack. The new algorithm in this regard have also been improved, the use of secret values are also set an expiry date. Once the expiration of the period of its use, the original secret value is no longer used at this time algorithm to enable another new secret value. Therefore, the use of a different period, the secret values are different. So that a different period of time, even for the same packet algorithm will produce different Cookie values. If an attacker to attack the new algorithm, then he must break in a limited period of time corresponding to the secret algorithm value. This is no doubt further increase the difficulty of attacking the attacker, and thus better protection of the new system.

The implementation process steps of the new algorithm are as follows:

- If the maximum packet timeout value is L, the length of each equal portion of the packets is L / 2.
- During the n-th time piece in the algorithm, define the secret value of Kn. And each Kn in all time pieces is not same to each other. That is, K1 ≠ K2 ≠ K3 ≠ ... ≠ Kn.
Starting from the first time piece, the algorithm give all time pieces sequences number. Their numbers are repeated 0, 1, 0, 1 ...

When generating cookie value, the algorithm determines to use which secret value (Kn) at present based on the time piece sequences number (0 or 1), and use the value to calculate the cookie.

When verifying the cookie value, the algorithm determine the present secret value based on current time piece sequences number saved in the packet, and use it to calculate the corresponding cookie value in the packet, and then compare the new value with original value in the packet to get the final comparing result.

The realization of the new algorithm process is shown in Figure 4.

The value selection in the novel algorithm

First, set the connection timeout when the request length L, each value in the algorithm is a secret to survive the length of time is L / 2. Second, the figure includes the current frame in real time (K1 where the time) and the most recent period (K0 where the time), in which the time frame width of L, the current period number is 1. Every time L / 2, then the frame shift to the right one time. Dashed box location is the result of the three periods after the actual location box.

In real terms the location of wireframe cookie value, the first with the current value of K1 figure out the secret cookie, then the current period number one with the cookie value is combined, it would be as an IP packet the initial sequence number field.

The location of the dashed border to test the received ACK packet, the first message extracted from the period number (1 or 0), and determine the corresponding value of the current secret (K3 or K4). Second, the calculation of the cookie value of the corresponding packet, and then with the message in the ISN for comparison. The final results of this comparison, there are two possibilities:

If the connection is false, because the attacker can not be the current period number and its corresponding value of the relationship between the secret and thus can not generate the correct IP packet the initial sequence number field.

If the connection has timed out, according to the text in time super-Times, a secret number to be the value of the current algorithm uses a secret value is not the same, the same message would not come to the same cookie value, the comparison is not the same, the super-Times, Man abandoned.

C. The new design for cookie value field

In the traditional 32-bit cookie field, there are 8 bits used for time-out certification, which led to Hash field length is too small. So that the likelihood of cookie Hash value collision is relatively large. It is necessary to reduce the length of time-out certification field.

The proposed novel algorithm only need 1 bit for the time-out certificate. Therefore, the algorithm can use 31 bit for cookie value, as shown in Figure 5:

Figure 5 The comparision of Cookie fields between the novel algorithm and the traditional algorithm

When generating cookie, the proposed algorithm used the current secret value to calculate the 31 bit hash value of IP packet information, and then fill the current time number into the highest bit of cookie.

When validating the cookie, firstly the original cookie value is restored from the packet sequence confirmation number field. And the time number is extracted from the cookie highest bit. Then the algorithm finds the secret value based on the time number, and calculates 31 bit hash value of the packet information. Finally the original and new cookie values are compared for verification.

IV. EXPERIMENTS

A. Effectiveness

The program is implemented based on the Linux2.6 code. And Syn Killer emulates SYN Flood attack to send a large number of packets to the server port. The response of the system were tested in three cases, without SYN Cookie defence, traditional SYN Cookie and proposed SYN Cookie methods.

Figure 6 CPU occupancy rate in the attack in three cases

It can be seen from figure 6 that when there is no SYN Cookie defence, CPU occupancy rate soon reached 100%, and can not respond to requests for normal connections. Both the traditional and the proposed novel SYN Cookie methods can prevent SYN Flood attacks.

B. Performance

Since the new algorithm uses a faster encryption algorithm, so in the premise of ensuring the entire
algorithm encryption strength, the computational complexity greatly reduced. The packet processing performance of the algorithm can be verified through the performance of comparative experiments. In the two cases of the traditional algorithm and the proposed novel algorithm, packets are sent at different speeds to the server respectively. The processing time of different algorithms are calculated through the timer in program. Part of experimental data and comparison are listed in the following table.

<table>
<thead>
<tr>
<th>Packet number</th>
<th>5x10^4</th>
<th>10^5</th>
<th>5x10^5</th>
<th>10^6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed (ms)</td>
<td>36</td>
<td>76</td>
<td>379</td>
<td>743</td>
</tr>
<tr>
<td>Traditional (ms)</td>
<td>52</td>
<td>112</td>
<td>545</td>
<td>1021</td>
</tr>
<tr>
<td>Reduction (%)</td>
<td>30.8</td>
<td>32.1</td>
<td>30.5</td>
<td>27.2</td>
</tr>
<tr>
<td>Average (%)</td>
<td>30.1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

From Table 2, the average consumption of computing time of the new algorithm reduced by about 30% compared with the traditional algorithm. The total processing time of one million packets is less than 800 milliseconds. This performance is sufficient to meet the packet processing performance requirements of the large scale network nodes. So the proposed novel algorithm is superior to the traditional SYN Cookie algorithm in the packet processing performance.

C. The algorithm performance comparison with the keys of different lengths

In the previous section, reference was made through different means to effectively improve the security of the new algorithm. Among them, relying on algorithms to shorten service time random key method, and the extended algorithm key length method. They have their own advantages and disadvantages. One way to shorten the time of key services, strengthen the algorithm only as a secondary means of security is not fundamentally solve the security problems. Through the following analysis, we can see it in terms of safety enhancement algorithm there are certain limitations.

The original key-based algorithm for the efficient use of the length of time the value of (KL) for the packet when the timeout length (MEL) half. That KL = MEL/2.

If a successful attack of this algorithm to search half the key space, then the unit time required for computing the minimum amount of P_Min as follows: P_Min = 231 / KL (based algorithms used in the key length is 32-bit)

Algorithm by reducing the value of KL allows a certain enhanced security. Because the value of P_Min will follow the increase, per unit time and thus serve to increase the amount of the required operations to enhance security. The algorithm for specific security measure, by using different length of the key operations per unit time when the value (P) to quantify. P = 231 / KL (based algorithms used in the key length is 32-bit)

In fact the size of the value of KL can not be reduced without limit, and its minimum by the minimum packet length of TIMEOUT (MEL_min) constraints. In practice, the value MEL_min by the operating system, network round-trip time, network speed, and many other factors, it should be a constant value and can not be too close to 0. Therefore, there is the value of P corresponds to maximum value Pmax: Pmax = 231 / MEL_min (based algorithms used in the key length is 32-bit)

Thus, this approach in terms of safety in the algorithm is not only slow the increase in computational complexity, but the rate of increase is also subject to the minimum packet length of TIMEOUT limit. If the new algorithm is a high security requirements in situations where the use of the algorithm must be used to increase the length of the key ways to strengthen security. This method has better security features, such as the attack is successful in computational requirements grow exponentially, security based on encryption algorithms Blowfish and so on.

In addition, Blowfish encryption algorithm there is a notable feature: The increase in the length of the key ways to strengthen the algorithm for security and will not lead to arithmetic operations, a significant increase in volume. This feature of the operation with the details of the encryption algorithm. Blowfish algorithm is the source of the internal adoption of fixed-length key: sbox and pbox. The whole encryption process is divided into two parts: pre-processing and information encryption keys. Key Pre-processing variable-length keys to the sbox and pbox transformed in order to be used when encrypting the information key_pbox and key_sbox. The encryption process is used key_pbox and key_sbox for each 64-bit plaintext is encrypted.

In the performance tests, use the same hardware and software test platform, using several different lengths of random keys to test new algorithms performance. These include 32-bit key, 64-bit key and 128-bit keys, and test results using the Matlab rendering performance comparison chart, as shown in Figure 7 with the following results:

![Figure 7](image)

Figure 7, Cookie generation time comparing of the new algorithm when using different length key

As can be seen on Figure 7 through for different lengths of keys, the new algorithm is basically the same message handling efficiency. 3 Performance curves are basically at the same slope of the straight line, and the...
measurement results shown in the figure the square difference between the smaller, the deviation between the results of its average to a lesser extent. This is the Blowfish algorithm in the encryption process due to the use of fixed-length source of key results. It helped enhance the algorithm's security are large benefits can make a longer key algorithm to enhance security, the need to pay additional costs of processing performance. New algorithm for packet processing speed only with the number of messages need to be addressed, but not with Blowfish algorithm is used in the key length has nothing to do. Therefore, to enhance the security algorithm is the preferred method is used to increase the key length of the approach.

After the above performance test proved that the new algorithm's security is adjustable, and in between security and processing speed to achieve a better balance.

V. CONCLUSION

This paper introduced the principle of the distributed denial of service attacks for the TCP protocol, analyzed the shortages of the traditional SYN Cookie defense methods, and proposed an improved SYN Cookie anti-attack algorithm. Test results show that the new SYN Cookie method can effectively defend against SYN Flood attacks, and computational efficiency is higher than traditional methods with the average increase of about 30%. Meanwhile, the new algorithm uses a time-bound with the use of random key to encrypt packets of information. The randomness of the key and the effective use of time-bound algorithm can provide double the security of protection. And the algorithm in the program can be measured both the speed and safety, self-regulation in order to obtain the most suitable cost-effective. In addition, the traditional algorithm, the options field of IP packet does not carry out certification, can not be applied need to use the IP options field in the application of circumstances, the new algorithm in the design which combines the original SYN Cache technology. This new program adds the optional IP options for authentication. As SYN Cookie method are used in the TCP protocol layer, the connection time will has a corresponding increase in TCP normal connections. So the following next step research work will mainly focus on the adaptive defending method for DDoS.

ACKNOWLEDGMENT

The authors wish to thank the major national science and technology special projects (2010ZX03004 -003-03), National Nature Science Foundation of China(60832002), Nature Science Foundation of Hubei Province(2009CDB222, 2010CDB08602), Ph.D candidates self-research program of Wuhan University (2008160101000050) and Hubei Provincial Department of Education Research Project(Q20112605).

REFERENCES


[33] DJ Bernstein, SYN Cookie. Http://cy.yp.m/ syncookies.html


Bo Hang received the M.S. degree in computer science from Harbin Engineering University, Harbin, P.R.China, in 2003. He is currently a Ph.D. candidate in communication and information system at Wuhan University, Wuhan, P.R.China. He came into National Engineering Research Center for Multimedia Software, Wuhan University, in 2007, and has been a student member of IEEE since 2008. His current research interests include audio signal compression and processing for mobile communication and surveillance.