Member 1: He Tong Student number: 867488 Username: the2
Member2: Wang Yao Student number: 869992 Username: yaow15

Internet Technologies – COMP90007 SM1 2018

"Resisting SYN flood DoS attacks with SYN cookies"

1. Introduction:

Suddenly your Web server becomes crippled. Then you may find that you have just become one of poor victims of a denial of service (DoS) attack, which constitutes one of the immense and pervasive threats to today's Internet. Computers that offer TCP services are easily susceptible to a variety of DoS attacks from external hosts on the network. One particular form of Dos attack is SYN flood, characterized by exploiting the vulnerabilities of TCP/IP protocol, where the intruder attempts to overwhelm the server by sending sequent TCP SYN packets (Lemon, 2002). Thus, the server has to constantly allocate memories for each new connection until exhausted. This type of DoS attack can cause the hardest Internet security problems. Owing to the seriousness of the attack many defense mechanisms have been proposed to defend against them. 'SYN cookies' is known as a major way to mitigate SYN flood attacks. This paper will provide a concise introduction to SYN flood and defense methods, analyse and evaluate 'SYN cookies', and finally indicate future works to improve the method.

2. 'SYN flood' and defense techniques:

2.1 SYN flood:

SYN flood is a type of Denial of Service (DOS) attack which exploits the vulnerability of the TCP three-way handshake to repeatedly send SYN requests to a targeted server, usually using spoofed IP addresses, in an attempt to consume memories on the server and make it unresponsive. An attacker tends to send a SYN packet to request a TCP connection. In a TCP three-way handshake process, the targeted server then allocates a table slot for the incoming connection and reply with a SYN + ACK packet. The attacker will deliberately no longer respond to the server, and hence the table slot is going to tied up for a moment until it times out. If the attacker sends countless SYN packets to request connection at the same time, all the table slots will fill up, thereby making the server processes incapable of replying to legitimate client's SYN packets for normal connections.

2.2 Defense techniques:

In essence, it is the vulnerability with implementing the three-way handshake that can be exploited by malicious senders, that is, the listening process must remember its sequence number before responding with its own SYN. For this, researchers have proposed a number of techniques to defend against SYN flood, including reducing SYN-received timer Micro blocks, RST cookies, SYN cookies, SYN cache, firewalls and proxies, stack tweaking, and recycling the oldest half-open TCP (Chang, 2002).The next part will highlight SYN cookies.

3. ‘SYN cookies’:

3.1 The concept of SYN cookies:

SYN cookies is a method that making some modifications to the TCP 3-way handshake on the server to defend against SYN flood. The principle is that, when a server is ready to return SYN+ACK packet after receiving SYN packet, it does not allocate memory, but calculate a cookie value according to the SYN packet (Peng & Wang 2007). The cookie value is regarded as the initial sequence number of the SYN ACK packet. As the client replies with an ACK packet, the receiver can calculate cookie according to the header and compare it with the confirming sequence number (initial sequence number +1). If matched, the client’s legitimacy is verified and the server will allocate memories to proceed the valid connection (Raghavan & Dawson, 2011). The core of the SYN cookies mechanism is to avoid the large amount of unnecessary connection request blocks caused by the attack, resulting in running out of memory and unable to handle normal connection requests.

3.2 SYN cookies’ calculation

The key to implementation is that cookie should include the status information of the current connection so that the attacker cannot forge.

3.2.1 Message authentication code(MAC)

The server will get a SYN packet and then compute a MAC value. MAC is a message authentication code function, namely, a cryptographic hash function that can confirm the message’s authenticity and remaining unchanged, guaranteeing the required security in calculation.

A = SOURCE_IP || SOURCE_PORT || DST_IP || DST_PORT || t || MSSIND

k is a unique server key and is actually a set of random numbers.

t is the system startup time, plus 1 every 60 seconds.

MSSIND is the index of MSS.

3.2.2 Secure Hash Algorithm 1(SHA-1)

The MAC function is SHA1 in Linux system. Secure Hash Algorithm 1(SHA-1) is a cryptographic hash function that produce a 160-bit hash value named message digest for messages less than 264 bits (Spinsante & Leggieri, 2007). As a message is captured, the message digest is used to verify the integrity of the data. Data may change during the period of transmission, and there comes different message digests. SHA-1 has two features, one is that information cannot be restored from message digests, and the other is that two different messages will not generate the same message digest.

3.2.3 SYN cookie formula and verification

SYN cookie value is calculated as:

cookie = cookie_hash(saddr, daddr, sport, dport, 0, 0) + seq + (t1 << 24) + (cookie_hash(saddr, daddr, sport, dport, t1, 1) + mssind) % 24 (Watson & Kindred, 2004)

t1 is the time for the server to send a SYN cookie

mssind is the MSS index (0 - 7).

Now we verify the cookie value by verifying time and mssind.

Verify time:

t1 = (cookie - cookie_hash(saddr, daddr, sport, dport, 0, 0) - seq) >> 24;

t2 is the time when the ACK is received. It is legal that t2 - t1 < 4 mins, that is, the ACK must arrive within 4 minutes.

Verify mssind:

mssind = (cookie - cookie_hash(saddr, daddr, sport, dport, t1, 1)) % 24;

it is legal when mssind < 8

If both t1 and mssind are valid, the ACK is considered valid and 3-way handshakes can be completed successfully.

4. Critical Analysis of the Topic:

In the so-called information era, SYN cookies is known as a simple and typical DoS and DDoS defense. It can deter spoofing of connections and prevent resource exhaustion effectively. However, SYN Cookie still has three disadvantages:

1.Reduce some TCP functions

Client puts TCP options in SYN packets instead of ACK packets. Due to the feature of SYN cookies that the server does not allocate memory to SYN, these options will be lost, and thus some functions enhancing TCP performance cannot be used.

2.A waste of CPU time

During the generation and verification of SYN cookies, the system needs extra computations to ensure security of cookies, greatly increasing the cost of connections. Hang, Hu and Shi(2011) point out that SYN cookies with high computational complexity can effectively reduce the CPU occupancy rate but demands additional storage space. Besides, if the attacker only attacks a server by sending numerous ACK packets rather than SYN packets, the server has to deal with them by running a complex algorithm, which causes a huge waste of CPU time and also makes server processes incapable of replying to legitimate senders' requests.

5. Conclusion:

Dos attacks are so simple but more dangerous than you think, which can cause significant financial losses or cause damage to online reputation for critical services such as governments, healthcare and trading platforms. SYN cookies can resist SYN flood DoS attacks effectively by modifying TCP three-way handshake connection. SYN cookies, however, has its own vulnerabilities including high time complexity and losses of several TCP functions. Thus, our aim is to optimize SYN cookies to perform better.

6. Future Works:

As mentioned above, the traditional algorithm to calculate SYN cookie value has a high computational complexity. So the following research will mainly focus on designing an enhanced SYN cookie algorithm which can utilizes a time-bound with random key to encrypt TCP packets, to improve computing efficiency and double the security of protection. Also, TCP cookie Transactions(TCPCT) as an extension of TCP protocol, does not conflict with other TCP extensions, which deserves further research.
(Word count: 1305)

7. References:

[1] Chang, R. K. (2002). Defending against flooding-based distributed denial-of-service attacks: a tutorial. IEEE communications magazine, 40(10), 42-51.

[2] Lemon, J. (2002, February). Resisting SYN Flood DoS Attacks with a SYN Cache. In BSDCon (Vol. 2002, pp. 89-97)

[3] Hang, B., Hu, R., & Shi, W. (2011). An enhanced SYN cookie defence method for tcp ddos attack. Journal of networks, 6(8), 1206-1213

[4] Peng, D., & Wang, W. (2007). Research on DDoS Defense Based on SYN Cookie [J]. China Information Security, 2.

[5] Raghavan, S. V., & Dawson, E. (Eds.). (2011). An investigation into the detection and mitigation of denial of service (dos) attacks: critical information infrastructure protection. Springer Science & Business Media.

[6] Spinsante, S., Gambi, E., & Leggieri, M. (2007). DSA with SHA-1 for space telecommands authentication. In Software, Telecommunications and Computer Networks, 2007. SoftCOM 2007. 15th International Conference on (pp. 1-5). IEEE.

[7] Watson, R. N., Gudmundsson, O., & Kindred, D. (2004). U.S. Patent No. 6,779,033. Washington, DC: U.S. Patent and Trademark Office.

Member 1: He Tong Student number: 867488 Username: the2
Member2: Wang Yao Student number: 869992 Username: yaow15

Individual reflection report of He Tong

The most tough but interesting challenge for me is that my partner and I have disagreements on the choice of the topic. At first, we both decide to choose 'DoS attack' as our group topic. However, he insists that we should study DoS attacks from the perspective of attackers like hacker, but I think it is better to study the defense methods of DoS attacks. Later, we attempt to answer the suggested questions in the template document from our own perspective, and then we find that it is difficult to answer the majority of questions from his perspective; instead, the answers to all the questions seem to be very clear from my perspective. Hence, we reach an agreement that study DoS attacks by analyzing defense methods.

The target of 'Network analysis' project is to find the relationship among different attributes of networks like jitter, hops and bandwidth. In my group, I shared many novel ideas with my partner because we both love brainstorming. We discussed whether the obtained data can be used as a basis for analysis, or whether there is better protection for cybersecurity. I am good at capturing and integrating data and he is good at analyzing data, so it is easier to work on this project based on complementary strengths.

Individual reflection report of Wang Yao

One of the most tough challenges I am confronted with is to find related documents. To write and grasp every principle involved in my topic, I read about 16 papers each of which has more than 20,000 words. At the beginning, I read very slowly due to the unfamiliarity of the field of DoS attacks. Gradually, I become to read faster after knowing many contents about a variety of DoS attacks and a great number of methods to resist these attacks. I think my reference skills have been improved and the knowledge about network information security has increased after finishing the research project.

As for the network analysis project, at the beginning, I collected analysis data on my laptop at home. Due to instability of my home's Internet, lots of hosts are not available, and thus data becomes unreliable. So, I delete all the data I captured before and begin to use servers of UNIMELB, which works better.