IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. VI (Nov.-Dec. 2016), PP 42-45
www.iosrjournals.org

Detection And Handling of Denial – of – Service, That Uses Encrypted Protocol Headers.

B.Mallikeswari., M.TECH.
Assistant Professor, Department of Computer Science, Justice Basheer Ahmed Sayeed College For Women, Chennai

Abstract: *One type of attack of Denial of service is Reflector attack, which is very difficult to be traced by traditional IP trace back techniques. There are many solutions to these problems, which resolves any one of factors causing the problems. This is because solution is not designed to analyze all the factors. In this context the purpose of this research paper is to detect the attacks and handle the encrypted protocol header of packets by traditional decryption algorithm from reflector. This research work identifies attackers data and send that to detection filter which in turn identifies types of encryption applied in protocol header . The output this process is taken to encryption classifier to decrypt data to find the attacker encrypted address. Encrypted Denial of service attack is uncommon approach because it attacks very slowly and high latency is introduced.*

Keywords: *DoS, Encrypted Header, Reflector attack, Detection filter, Encryption classifier, SSL/TL and Decryption.*

I. Introduction

Cyber attacks have become a fact of with data breaches of high profile businesses and organizations making headline news practically on a daily basis. One common cyber threat is a denial of service (Dos) that as its name implies renders websites and other online resources unavailable to the users[1]. The attacked system are controlled remotely either by Trojans(self-installed) which are programmed for packet floods to be launched. DDos structural design used by DDos engineers to launch fruitful attacks are given in[2]. DDos attack the causes serious issues that affects organizations cost and also individual time, money and reputation.

II. Related Work

In 2015, G.Florance [3] briefs various Internet Protocol Trace back techniques of DDoS survey to give the better solution of the attacks. The author discusses attacks in a collaborative environment and identifies their impacts of serious threat of which denial of service. There are many Trace back methods are available to identify the attacks. The real challenge in security provisioning is to identify the source of unknown attack at the earliest possible which motivated us to work on novel fast Trace back mechanism with less computation and storage costs, scalability to high attacker population, and providing best network performance. Hash-based traceback [4], based on the former technique, digests and logs some particular information of each packet on the routers. The victim can query its upstream routers whether a certain packet has passed through them[5]. This method has two drawbacks: it requires a large-scale database on each router to store and manage the packets information; the queries must be done before the relevant records in the database have been updated.

Reflectors

Reflector attacks belongs to the category of the serious DoS attacks. The victim's network is flooded by number of attack packet delivered by the reflector attackers might be amplified many times. Here two process takes place 1) Reflection DDoS Attacks 2) DdoS Amplification.

Reflection DdoS Attacks

In a reflection DdoS attack, the attacker imitates ("spoofs") [6] the victim's IP address and sends a request for information via UDP to servers ("reflectors") known to respond to that type of request. The servers answer the request and send ("reflect") the response to the victim's IP address. Thus, from the servers' perspective, the victim sent the original request. All the data from those servers adds up to significant bandwidth, enough to congest the target's Internet connectivity. With bandwidth maxed out, "normal" traffic cannot be serviced and legitimate clients can't connect. Any server open to the Internet and running UDP-based services can potentially be used as a reflector. Spoofing is the basis of a reflection DdoS attack; it is what tricks the reflectors into flooding the target. Spoofing is possible because the attack uses UDP – a unidirectional, stateless protocol – as the transport protocol for the requests[7].

DdoS Amplification

The byte count of the reflector's response is much larger than in the original request. So, a very small DNS request can result in a very large DNS response . In other words, the attack is amplified. Amplification (size of response compared to size of request) is what makes the attack so dangerously effective. In the example above, the attacker is sending 50 bytes to the target for every byte sent to reflectors[8].

With enough reflectors, an attacker with only 10 Mbps of network capacity can easily send over half a gigabit of traffic toward the victim. Expand the attacker's network capacity to 100Mbps and the number of reflectors to a couple hundred – both are easy to obtain – and the amount of malicious traffic exceeds several gigabits, enough to take down most business websites and servers. When the attacker continues to add network capacity and reflectors, the attack can reach hundreds of gigabits[9].

Proposed Method

The world´s largest DdoS mitigation service Prolexic, stated that ICMP , UDP and TCP, are used protocols to launch DdoS attacks [10]. My primary aim to detect the encrypted packets by sending the packets to detection filter.The job of this filter to classify the type encryption algorithm is used and uses the corresponding decryption algorithm to find the attackers packet source address. The aims, architectural structure and implementation processes of my work is summarised as follows:

1. Detection of known and unknown attackers packets.
2. My detection filter will detect the encrypted protocol header by routing table.
3. Encrypted packets will be sent to my Encryption classifier, which indentifies encryption algorithm applied for encryption process. And uses appropriate decryption algorithm to get decrypted data.
4. Decrypted packets will be sent to Ddos Detector Instance.

The pictorical representation of process is depicted as follows:

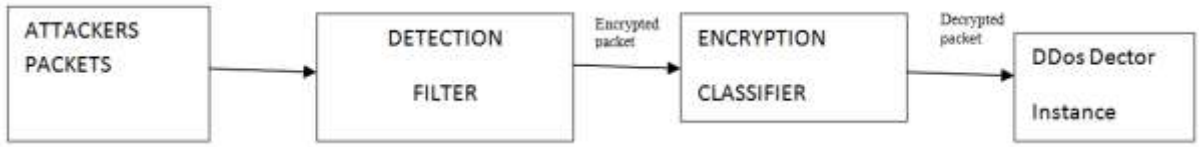

Fig.1 Representation of Detection filter Encryption Classifier

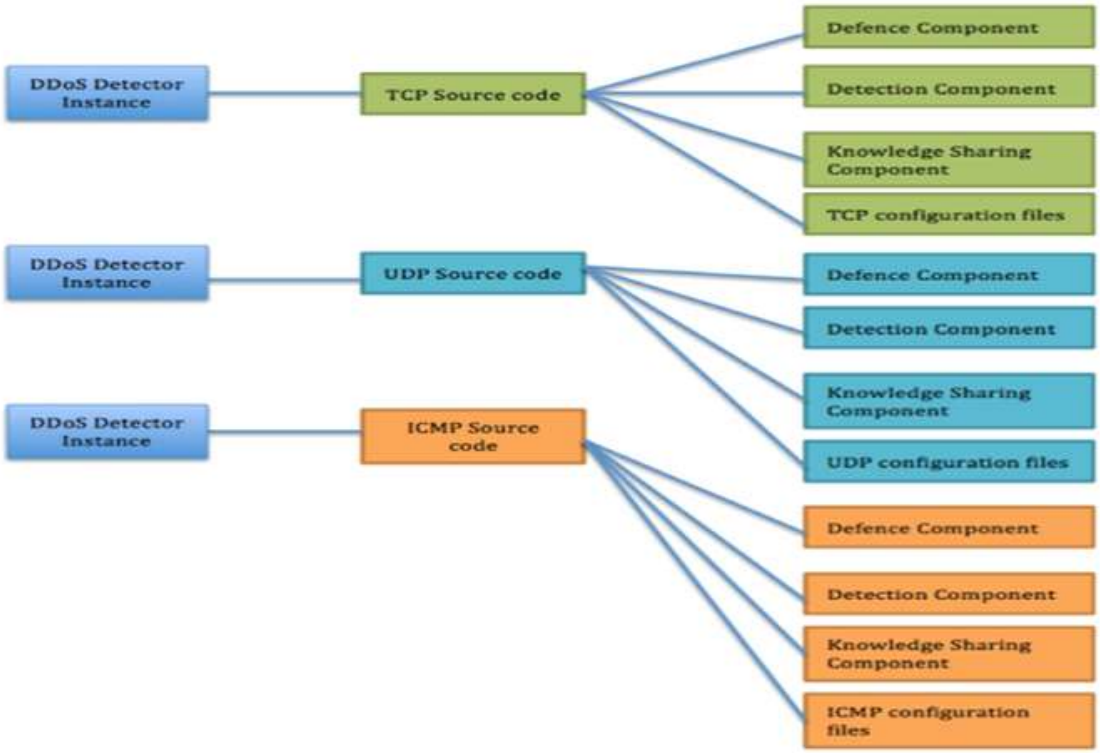

Fig. 2. Representations of three DDoS detector instances

5. DDos Detector Instance is an algorithm detects whether code is UDP or ICMP or TCP .
6. For example, As sample physical environmental research I started with TLS 1.1, if a block cipher in CBC mode has been negotiated, an explicit IV will be inserted at the start of the encrypted data:

01 (plain) | ContentType | ProtocolVersion | RecordLength |
02 IV
03 (encrypted) GET /index.html HTTP/1.1
04 (encrypted) Host: helpme.com
05 (encrypted) | HMAC | Padding |

The IV is there to make the cipher text unpredictable and less susceptible to certain cryptographic attacks. Implementations might treat it differently both at encryption and at decryption. Some implementations might generate it from random, while others might generate it as the cipher text of the last block of the previous fragment XORed with a constant value. Conversely, at decryption, implementations might treat it as either an independent field or as the first block of cipher text (and discard the corresponding decrypted block before outputting the decrypted plain text fragment, just as the HMAC and Padding is discarded).
Starting with TLS 1.2, an AEAD cipher might be negotiated, which means that the MAC mechanism is integrated into the cipher mode and no HMAC will be required. In this case the layout will be as follows:

01 (plain) | ContentType | ProtocolVersion | RecordLength |
02 (plain) Nonce
03 (encrypted) GET /index.html HTTP/1.1
04 (encrypted) Host: helpme.com

Note that the length of the cipher text corresponding to field 03 and 04 will be longer than the length of the corresponding plain text. The exact layout will depend on the details of the AEAD cipher mode. Normally, it will just end with a MAC. Now, to complicate things further, in all protocol versions and cipher modes the MAC will be calculated over data that differs from both the plain text (optionally compressed) fragment and from the encrypted fragment. In particular, the Record Length field will have the plain text / compressed value (not the encrypted value) and a Sequence Number will be inserted to prevent replay attacks. The MAC itself is obviously not included in the data the MAC is calculated over, and neither is the padding. The last part, the MAC not being calculated over the padding, is the reason some of the attacks against SSL/TLS are possible.

7. If the TCP Detection code requires an update, ICMP and UDP detection codes should be able to function without any downtime.

III. Limitations and Suggestions

In this research paper , the MAC cannot be calculated over the padding, causes the possibility of the attacks against SSL/TLS. Further research work are to be continued in physical Environment and algorithms dealing with this. In future, the implementation of the entire processing is provided on further works and gives a better solution in later.

IV. Summary and conclusions

An attempt is made in this paper to introduce about the Detection filter to detect the genuine data from trusted source by pass and detect the encrypted data from untrusted source .Detected data packet sent to Encryption classifier to find the implemented encryption algorithm. Using the same the packets are decrypted and attacker address is found .Unfortunately it is difficult to calculate the MAC if the attacks against SSL/TLS.

References

[1]. E. Alomari, B.B.Gupta, S.Karuppayah, Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art, Int. J.Comput. Appl. 49(7)(2012)24–32.
[2]. Lau, F., Rubin, S.H., Smith, M.H., and Trajkovic, L,"Distributed denial of service attacks"
[3]. Systems, Man, and Cybernetics, 2000 IEEE International Conference on, Volume:3 , 2000, pp. 2275 -2280 vol.3.
[4]. K. Park and H. Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," Proc. ACM SIGCOMM '01, pp. 15-26, 2001.
[5]. W. H. Press, B. P. Flannery, S. A. Teukolsky, and W. T. Vetterling, "Numerical Recipes in FORTRAN: The Art of Scientific Computing", Cambridge University Press, 1992, pp.83-84.
[6]. D.K.Y. Yau, J.C.S. Lui, F. Liang, and Y. Yam, "Defending against Distributed Denial-of- Service Attacks with Max-Min Fair Server-Centric Router Throttles," IEEE/ACM Trans. Networking, no. 1,
[7]. P. Ferguson and D. Senie, "RFC 2267: Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," The Internet Soc., Jan. 1998.

[8]. Vern Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", ACM Comp. Commun. Rev., vol.31, no.3, July 2001, pp. 3-14.
[9]. A.John and T Sivakumar, "DDoS: Survey of Traceback Methods", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009, pp. 241-245.
[10]. H. I. Liu, and K. C. Chang, Defending systems Against Tilt DDoS attacks, Telecommunication Systems, Services, and Applications (TSSA), October 20-21, 2011, pp. 22-27.
[11]. Prolexic.Global Leader in DDoS Protection and Mitigation 2003–2014.[Online] Available from http://www.prolexic.com