Global Scientific JOURNALS

GSJ: Volume 8, Issue 6, June 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

Research Project on DDoS Attack

Sarah Alowais

INFS6490-A

Computer Network Security

Dr. Ping Wang

Abstract

Summary

The chosen topic is a new kind of DDoS attack called the temporal lensing DDoS attack. This is a kind of DDoS attack that applies the principle of creating pulsing DDoS but it is conducted in a way that it only uses a very low bandwidth of the attacker's system to create a very high bandwidth of requests to the victim's servers thus creating DDoS when the requests overwhelm the servers. The purpose of this study is to explore how this kind of attack is used by attackers and also identify ways in which the threat of this kind of attack can be mitigated.

Keywords: DDoS, pulsing, temporal lensing, UDP, TCP, load balancing

Description

Through the temporal lensing DDoS attack, it is possible for requests to be sent by the attacker at different latency times but they reach the victim servers at the same time even if they were sent at different times. When this is coupled with amplification of the requests, it can easily cause a successful DDoS attack with very little resources needed on the attacker's side. Since this is one of the new concerns of variabilities in DDoS attacks, it is a kind of attack that needs more research on how it is effectively created and how systems can be protected from this kind of attack. From research, one of mitigation methods indicated is by global load balancing. Other methods will be explored and their potency compared.

Plan

The plan for this research is to gather information from secondary sources through library resources. The focus suing peer reviewed journals and books that discuss this kind of attack. There will be a greater attempt to learn and explore what kind of resources an attacker will need in order to create a successful attack. The idea is that if the kind of resources needed by the attacker are very low and if the attacker can easily amplify the pulses of requests, this can be a very significant threat. Solutions and methods of protecting a system from this kind of attack will be explored and note the most potent of the solutions and recommendations gathered.

Conclusion

The possibility of an attacker being able to create traffic to a client that is high enough to cause DDoS using very meager resources is a serious issue of concern. This is due to the sheer number of potential attackers with that capability and thus the likelihood of an attack will be very high. The Temporal Leasing DDoS attack is one of this kind of attacks and thus network systems need to be adequately equipped with this kind of attack.

References

Luo, X., Chan, E., & Chang, R. (2009). Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals. *EURASIP Journal on Advances in Signal Processing*, *2009*(1). doi: 10.1155/2009/256821

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, *13*(12). doi: 10.1177/1550147717741463

Rasti, R., Murthy, M., Weaver, N., & Paxson, V. (2015). Temporal Lensing and Its Application in Pulsing Denial-of-Service Attacks. *2015 IEEE Symposium on Security and Privacy*. doi: 10.1109/sp.2015.19

Zhou, L., Liao, M., Yuan, C., & Zhang, H. (2017). Low-Rate DDoS Attack Detection Using Expectation of Packet Size. *Security and Communication Networks*, *2017*. doi: 10.1155/2017/3691629