DDoS Final

Feng Wei

April 26, 2020

Chapter 8: Attack Detection

- **Compare the signature and anomaly based detection approaches. Discuss their pros and cons.**
  Answer: Traditional signature based detection systems work well for those well-defined DDoS attacks which means low false positive rate and high accuracy. But at the same time those signature based detection systems lack the abilities to detect unseen or unknown attack, meanwhile those anomaly based detection systems have the capabilities to detect unseen attacks, however with a relatively high false positive rate.
- **If you need to choose an anomaly based detection approach for real time DDoS detection, what approach would you choose? Why? In your reasoning consider detection rate, false positive rate and detection delay.**
  Answer: I will choose the *statistical anomaly detection* method considering the real-time requirements. The machine learning based methods are time consuming and have a high false positive rate as well as a lager time delay.
- **What new DDoS detection approaches exist in the current literature that does not fit in the classification given in this chapter? Discuss the differences.**
  Answer: The wavelet and entropy based detection methods don't fit the classification in this chapter. Those methods are not statistical or machine learning based ones, they use information theories to detect the DDoS attacks.

Chapter 9: Deceiving DDoS Detection

- **List possible dependencies / vulnerabilities of DDoS detection systems in a decreasing order based on number of systems they can effect. Briefly explain how these dependencies / vulnerabilities can be exploited.**
  Answer: False perception, Tampering statistical deviation, Exploratory, Evasion and Poisoning

  Using polymorphic code in virus and worms is a known approach used by attackers to evade signature based detection systems. Just like exploiting the dependence of finding a distinct pattern in signature based detection, deception techniques can be generalized to anomaly based approaches considering their dependencies.

  Tampering these statistics would cause detection performance degradation and eventually lead to mitigation performance problems.

  Exploratory attacks target discovering ML technique used by the system. This kind of prior knowledge would give attackers leverage to generate attack patterns invisible to detection system

that is also classified as the Evasion attacks. Poisoning attacks affects the learning stage of the ML approach and require manipulating training data.

- **Propose a solution to prevent a common detection system vulnerability.**
  Answer: It's hard to design a new signature based or statistical based detection system which can prevent the common vulnerabilities. I am think about build a machine learning based detection system which may have the capabilities to prevent those common vulnerabilities such as find a simple pattern or tampering the statistical. But at the same time there will be new vulnerabilities within the machine learning models.
- **Propose a detection system that has minimum (none if possible) number of vulnerability and/or minimize the risk of exploitation by using additional mechanisms.**
  Answer: Considering build a Deep learning based detection system which can prevent those traditional vulnerabilities such as find a simple pattern or tampering the statistical. The problem is how to get enough labeled train data. I know this is really time and resource consuming, but it is really promising.

Chapter 10: Attack Mitigation

- **If you need to design a DDoS mitigation system, what reaction type would you prefer? Why?**
  Answer: I prefer Moving target method. Because we can try some new technologies to prevent DDoS attacks. I want to try SDN as well as Cloud computing to see how far we can get.
- **Design a mitigation system and describe your system based on the aspects presented in the mitigation system classification section. Explain your key decision choices.**
  Answer: I prefer a DDos mitgation system which has the abilties list below:
  Before an attack, I prefer prevention before those attacks cause potential damage.
  Distributed, A distributed system is more robust.
  Network based, This method can both take the source and destination information into consideration.
  In the cloud, Cloud is more powerful than the premises.
  Moving target, This method can make the system more robust.
- **What new DDoS mitigation approaches exist in the current literature that does not fit in the classification given in this chapter? Discuss the differences.**
  Answer: The Dynamic DDoS Mitigation system does not fit the classification given in this chapter. DDoS Mitigation system (DDM) increases service availability by scaling up the system resources using multiple cloud service providers when it is necessary. If users want to have their own infrastructure instead of using Deflect, they do not need to get dedicated servers from cloud service providers when they use DDM system.
- **List and briefly explain attacks targeting sustainability of the cloud based systems.**
  Answer: An Economic Denial of Sustainability (EDoS) attack is an attack targeting the automatic provisioning system of the cloud service provider. The goal of this attack is not to disable the network or the client's server, but to cause high resource usage and generate large service fees for the client. By targeting the client's economic resources, these attacks seek to make cloud computing unsustainable because it becomes a nonviable service for the client. Sometimes it is refered as Energy Oriented Denial of Service or Economic Denial of Service.
- **EDoS is a big challenge for cloud based (mitigation) systems. Propose ideas to mitigate these attacks.**
  Answer: I am thinking about strike back when attacked by DDoS attackers. Since those cloud

provider usually are big companies, they have the abilities and resources to take down the botnet controlled by the attackers.

Discussion

After taking this class and reading the book[1], I learned a lot about what is DDoS attack and how to detect and mitigate those attacks. I am thinking about using state-of-the-art hard-wares and SDN, cloud system as well as deep learning method to design a new system to defend DDoS attacks. Using new hard-wares to accelerate the prepossessing of the raw network packets. We can even get some statistical at real time. Then implement deep-learning method to detect the anomaly. At the same time we may use SDN and other techniques to do a real-time mitigation or defense.

References

[1] Liker Ozcelik and Richard Brooks. "Distributed Denial of Service Attacks: Real-world Detection and Mitigation". In: (2020).