Effect of Distributed Denial of Service (Ddos) Attacks under Different Number of Attackers and Different Node Mobility

Kamlesh[1]* Anju Dhull[2]

[1]Research Scholar, CMJ University Shillong

[2]Research Scholar, CMJ University Shillong

Abstract – In risk management one must understand the most important risks and decide how to mitigate them. Risks can be either accepted as such, mitigated by using one or more defense mechanisms, or transferred to third parties (such as with insurances). The primary goal is to ensure business continuity and, at the same time, keep the associated costs at a reasonable level. Effective risk management, however, is not possible without a good knowledge in existing attack mechanisms and available defense mechanisms. A widely exploited attack mechanism can be associated a high risk requiring effective mitigation. Completely different actions should be taken in a risk management process when no defense mechanisms exist against a specific attack, and when effective defense mechanisms can be easily deployed.

----------♦----------

1. INTRODUCTION

Current network protocols do not have the capability to detect the malicious packet dropping attack. Network congestion control mechanisms do not apply here since packets are not dropped due to congestion. Link layer acknowledgment, such as IEEE 802.11 MAC protocol, can detect link layer break, but cannot detect forwarding level break. Although upper layer acknowledgment, such as TCP ACK, allows for detecting end-to end communication break, it can be inefficient and it does not indicate the node at which the communication breaks. Moreover such mechanism is not available in connectionless transport layer protocols, such as UDP. For attacks which target the bandwidth of the victim, the architecture of the victim network decides how large a volume of attack traffic is needed. Increasing the bandwidth of links and erasing bottleneck links in its own network can increase the ability of a victim to tolerate flooding-based attacks. An attack which target connection control resources usually relies on flaws of the control mechanism of the operating system of the victim. Regularly updating software patches for the perating system can fix these problems and avoid being effectively attacked in future.

DETECTION OF DDOS ATTACKS

It is essential that a detection system not only detects malicious node but also identifies the attack type and the attacker whenever possible. Without them, it is hard to determine how to respond meaningfully without interrupting normal communication. Here we study an approach to obtain this information after malicious nodes have been discovered through detection system [11]. The basic idea is to determine the detailed attack information from a set of identification rules, which are pre-computed for known attacks. Rules are available for a lot of well-known attacks.

First of all, these rules may involve more features other than those have already been computed and used in detection system. One may point out these rules can be applied in parallel with malicious node detection to save computation time, the extra cost to compute these features may defeat this “optimization" as they are fairly expensive. As a result, they should only be computed after an attack is reported, which should be rare.

For each attack, the node that runs the corresponding detection rule the is “monitoring" node, and the node whose behavior is being analyzed (i.e., the possible attacking or misbehaving node) the “monitored" node. For attacks related to Packet Dropping, the monitoring node is

a 1-hop neighborhood of the “monitored" node. Both the attack type and the attacker can be identified because the monitoring node can overhear traffic within its 1-hop neighborhood. For Flooding, only the attack type, but not the attacker, can be identified by a monitoring node.

Now, some notations of statistics (features) used in these rules are described. Here, M is used to represent the monitoring node and m the monitored node.

- # (*,m): the number of incoming packets on the monitored node m.
- # (m,*): the number of outgoing packets from the monitored node m.
- # ([m],*): the number of outgoing packets of which the monitored node m is the source.
- # (*,[m]): the number of incoming packets of which the monitored node m is the destination.
- # ([s],m): the number of incoming packets on m of which node s is the source.
- # (m,[d]): the number of outgoing packets from m of which node d is the destination.
- # (m,n): the number of outgoing packets from m of which n is the next hop.
- # ([s],M, m): the number of packets that are originated from s and transmitted from M to m.
- # ([s],M,[m]): the number of packets that are originated from s and transmitted from M to m, of which m is the final destination.
- # ([s],[d]): the number of packets received on the monitored node (m) which is originated from s and destined to d.

These statistics are computed over a feature sampling interval, denoted as Ts. In addition, we often need the same set of statistics that are computed over a longer period. These longer-term statistics can be computed directly from basic features by aggregating them in multiple feature sampling intervals. We use FEATURET to denote the aggregated FEATURE over long period T. We always assume that time interval T is multiples of Ts, for simplicity. For example, the notion #T (*, m) are computed by summing up all # (*, m) in T/ Ts rounds of feature sampling intervals.

RESULTS AND ANALYSIS

A multicast member node joins the multicast group at the beginning of the simulation and remains as a member throughout the whole simulation. Hence, the simulation experiments do not account for the overhead reduced when a multicast member leaves a group. Multicast sources start and stop sending packets in the same fashion (four packets per second, each packet has a constant size of 512 bytes). Nodes in the network are placed uniformly. For fairness, identical mobility and traffic scenarios are used for different attack mechanisms. Only one multicast group was used for all the experiments.

Each mobile node moves randomly at a preset average speed according to a “random waypoint model”. Here, each node starts its journey from a random location to a random destination with a randomly chosen speed (uniformly distributed between 0 – some maximum speed). Once the destination is reached, another random destination is targeted after a pause. By varying the pause time, the relative speeds of the mobiles are affected. In our experiments the pause time was always set to zero to create a harsher mobility environment. The maximum speeds used were chosen from between 0 m/s to 20 m/s.

Two types of DDoS attacks mechanisms are implemented; first we measure the effect of Packet Dropping and Flooding attack on network performance. Then, we prevention techniques and shows that our proposed technique is better than existing prevention technique.

CONCLUSION

Detection & Prevention of DDoS attacks is a part of an overall risk management strategy for an organization. Each organization must identify the most important DDoS risks, and implement a cost-effective set of defense mechanisms against those attack types causing the highest risk for business continuity. Studies and news about real-life DdoS attacks indicate that these attacks are not only among the most prevalent network security risks, but that these attacks can also block whole organizations out of the Internet for the duration of an attack. The risk from DDoS attacks should not thus be underestimated, but not overestimated, either.

In the future the problem from DDoS attacks will most probably increase because the number of hosts connected in the Internet increases, access lines get faster, software products get more complex, and security continues to be difficult for an ordinary home user and even many organizations. The more there are hosts in the Internet, the more of them can potentially be used for DDoS purposes.

The intensity of DDoS attacks can also increase, as a higher number of hosts can produce more traffic over

faster Internet access lines. As software gets more complex, more vulnerability will reside in them to be used for compromising hosts. The fast pace of new revisions does not make the situation easier. Finally, it will continue to be difficult to evaluate security risks in existing computer systems, especially by ordinary people.

REFERENCES

F.A. El-Moussa, N. Linge and M. Hope; Active router approach to defeating denial-of-service attacks in networks; © The Institution of Engineering and Technology 2007; doi:10.1049/iet-com:20050441.

Gregory Safko; Defending against Denial of Service Attacks Using a Modified Priority Queue: Bouncer; 0-4244-0169-0/06/$20.00 © 2006 IEEE.

Vicky Laurens and Abdulmotaleb El Saddik, Pulak Dhar compare these two attack mechanisms and analyze their and Vineet Srivastava; Detecting Distributed Denial of effects. In next section, we analyze the effect of different Service Attack Traffic at the Agent Machines; IEEE CCECE/CCGEI, Ottawa, May 2006.

Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia and Nirali Mody, Sugata Sanyal and Ajith Abraham; A Distributed Security Scheme for Ad Hoc Networks; www.softcomputing.net/iwdc-manet.pdf.

A. Sun; The design and implementation of fisheye routing protocol for mobile ad hoc networks; M.S. Thesis, Department of Electrical and Computer Science, MIT; May 2002.

Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

"Honeypots, Honeynets"". Honeypots.net. 2007-05-26. Retrieved 2011-12-09.

"The six dumbest ways to secure a wireless LAN | ZDNet". Blogs.zdnet.com. Retrieved 2011-12-09.

Julian Fredin, Social software development program Wi-Tech

"Introduction to Network Security". Interhack.net. Retrieved 2011-12-09.

"Welcome to CERT". Cert.org. 2011-10-17. Retrieved 2011-12-09.

Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Pubblications Elsevier Inc p. 257

Corresponding Author

Kamlesh*

Research Scholar, CMJ University Shillong

E-Mail – anju_jind@rediffmail.com