Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Study on Ubiquitous Computing

Brijesh Kumar Singh
Computer Science & Engineering Department
JECRC UDML College of Engineering, Jaipur, India

Pradeep Sharma
Computer Science & Engineering Department
Down Town University Guwahati, India

Abstract— This is a paper that describes the Denial of service(DoS) as well as its existing challenges .It starts out by an introduction to DoS followed by the issues it face. Proactively, the ability to foresight users' intentions and self tuning , the ability to adjust the behaviour to fit the environment are described as key ideas in DoS.

Keyword: IRC, Spoofing, DOS/DDOS Attacks, scanning.

I. INTRODUCTION

Denial of service (DoS) attacks have become a major threat to current computer networks. Early DoS attacks were technical games played among underground attackers. For example, an attacker might want to get control of an IRC channel via performing DoS attacks against the channel owner. Attackers could get recognition in the underground community via taking down popular web sites. Because easy-to-use DoS tools, can be easily downloaded from the Internet, normal computer users can become DoS attackers as well. They sometime coordinately expressed their views via launching DoS attacks against organizations whose policies they disagreed with. DoS attacks also appeared in illegal actions. Companies might use DoS attacks to knock off their competitors in the market. Extortion via DoS attacks were on rise in the past.Attackers threatened online businesses with DoS attacks and requested payments for protection. Known DoS attacks in the Internet generally conquer the target by exhausting its resources, that can be anything related to network computing and service performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles, etc. Individual attackers can also exploit vulnerability, break into target servers, and then bring down services. Because it is difficult for attackers to overload the target's resource from a single computer, many recent DoS attacks were launched via a large number of distributed attacking hosts in the Internet. These attacks are called distributed denial of service (DDoS) attacks. In a DDoS attack, because the aggregation of the attacking traffic can be tremendous compared to the victim's resource, the attack can force the victim to significantly downgrade its service performance or even stop delivering any service. Compared with conventional DoS attacks that could be addressed by better securing service systems or prohibiting unauthorized remote or local access, DDoS attacks are more complex and harder to prevent. Since many unwitting hosts are involved in DdoS attacks, it is challenging to distinguish the attacking hosts and take reaction against them.

"*In recent years, DDoS attacks have increased in frequency, sophistication and severity due to the fact that computer vulnerabilities are increasing fast (CERT 2006, Houle et al. 2001), which enable attackers to break into and install various attacking tools in many computers."*

Wireless networks also suffer from DoS attacks because mobile nodes (such as laptops, cell phones, etc.) share the same physical media for transmitting and receiving signals; and mobile computing resources (such as bandwidth, CPU and power) are usually more constrained than those available to wired nodes. In a wireless network, a single attacker can easily forge, modify or inject packets to disrupt connections between legitimate mobile nodes and cause DoS effects

Texomony of DOS/DDOS attacks in the internet

DoS attacks are classified based on the material Interested readers can obtain further information on DDoS attacks from Mirkovic's book. The classification is according to the major characteristics of DdoS attacks: 1) how attackers (or zombies) scan vulnerable computers, 2) how attack packets are spoofed, 3) what attack targets are, and 4) what attack impacts are.

II. SCANNING

In the past, an attacker manually scans remote computers for vulnerability and installs attack programs. Worm scanning may cause secondary impacts on ARP (CISCO 2001) and multicast (Hamadeh *et al.* 2005) due to high router CPU utilization and memory demand.

a) Random Scanning : In a random scanning, each compromised computer probes random addresses in either global or local IP address space. Because scanning attempts are not synchronized among attacking hosts, there are often duplicate probes to the same addresses.

b) Hitlist Scanning : A compromised computer performs hitlist scanning according to an externally supplied list. When it detects a vulnerable computer, it sends a portion of the hitlist to the recipient. A complete hitlist allows an attacker to infect the entire susceptible population within 30 seconds.

c) Signpost Scanning : Signpost scanning takes advantage of habitual communication patterns of the compromised host to select new targets. E-mail worms use the information from the address books of compromised machines for their propagation. A Web-based worm could be propagated by infecting every vulnerable client that clicks on the server's Web page.

d) Permutation Scanning : This type of scanning requires all compromised computers to share a common pseudo-random permutation of the IP address space, and each IP address is mapped to an index in this permutation. Permutation scanning is preceded by a small-hitlist scanning. A computer infected in the hitlist then scans through the permutation, starting with its IP address. A compromised computer by permutation scanning starts from a random point in the permutation.

III. SPOOFING

Spoofing techniques define how the attacker chooses the spoofed source address in its attack packets.

a) Random Spoofing: Attackers can spoof random source addresses in attack packets since this can simply be achieved by generating random 32-bit numbers and stamping packets with them. Attackers may also choose more sophisticated spoofing techniques, such as subnet spoofing, to defeat some antispoofing firewalls and routers using ingress filtering and route-based filtering.

b) **Subnet Spoofing:** In subnet spoofing, the attacker spoofs a random address within the address space of the subnetwork. Subnet spoofing is useful for the attackers that compromise machines on networks running ingress filtering.

c) Fixed Spoofing: Different from the other two spoofing techniques, the spoofed address is the address of the target. For example, an attacker performing a smurf attack spoofs the victim's address so that ICMP ECHO packets will be reflected to the victim.

IV. TARGET

Although most DoS attacks work via exhausting resources, the actual target to deny services varies. The target could be the server application, the network access, or the network infrastructure.

a) Server Application : An application attack targets a given application on the victim (normally a server), thus disabling legitimate clients to use the service and possibly tying up resources of the host machine. Nevertheless, if the victim can well separate the resources for different applications, other applications and services in the victim should still be accessible to users.

b) Network Access: This type of attack disables access to the victim computer or network by crashing it or overloading its communication mechanism. An example of this attack is the UDP flooding attack. All attack packets carry the destination address of the target host without concerning the content of the target service.

c) Infrastructure: Infrastructure attacks target some critical services that are crucial for global Internet operation. Examples include the attacks on domain name servers, core routers, certificate servers, etc. The key feature of these attacks is not the attack mechanism, but the attack target and the attack impact.

V. IMPACT

Depending on the impact of a DDoS attack on the victim, the attacks are classified as disruptive and degrading attacks.

a) Disruptive: The objective of disruptive attacks is to completely stall or crash the victim's service. For instance, the victim network is completely congested under attack, or the victim server crashes or halts under attack

b) Degrading: The objective of degrading attacks is to consume some portion of a victim's resources to seriously downgrade the service performance. For example, an attack sends a high volume of authentication requests that can significantly consume computing resource in the target server.

VI. CONCLUSION

In this article, we overviewed existing DoS attacks and defense technologies in the Internet and wireless networks. DoS attackers exploit flaws in protocols and systems to deny access of target services. Attackers also control a large number of compromised hosts to launch DDoS attacks. Simply securing servers are no longer enough to make service available under attack, since DoS attack techniques are more complicated and many unwitting hosts are involved in DoS attacks. By reviewing several existing DoS attack techniques and classifying them, this chapterhighlighted challenges of DoS defense from characteristics of DoS attacks. For defenders, it is difficult to decide whether a packet is spoofed, to prevent a host from being compromised and controlled, to ask upstream routers to filter unwanted traffic, and to keep defenders themselvesfrom DoS attacks. This article reviews current DoS defense solutions in deployment and in research. They are trying to address one or several problems in DoS defense, for instance, how to distinguish legitimate traffic from flooding traffic, how to identify or trace true attacking hosts, how to filter or control flooding traffic as close as possible to attacking sources, and how to allow routers to collaborate in defense.

These solutions can handle some but not all DoS attacks due to their design principles, deployment issues, etc. New DoS attack techniques may also invalidate these solutions. This chapter acknowledged these innovative ideas and provided a fundamental understanding for developing new solutions.

Different from the Internet, wireless networks have their own unique DoS attacks due to the fact that wireless is an open communication approach and mobile devices can function as routers in wireless networks. DoS attacks in wireless networks extend to the scope not viable in the Internet.

ACKNOWLEDGEMENT

We wish to acknowledge Mr. Gajendra singh and Ms. Neelam for helping us to develop and maintain this paper .This paper won't have been completed without their guidance.

REFERENCES

[1] Aad, I., Hubaux, J.P., and Knightly, E. (2004). Denial of service resilience in ad hoc networks. Proceedings of ACM Mobicom. ACM Press, New York.

[2] Anderson, T., Roscoe, T., and Wetherall, D. (2003). Preventing Internet Denial of Service with Capabilities. Proceedings of HotNets-II. ACM Press, New York.

[3] Argyraki, K., and Cheriton, D. R. (2005). Active Internet traffic filtering: real-time response to denial-of-service attacks. Proceedings of the USENIX Annual Technical Conference. USENIX Press, Berkeley, CA.

[4] Mahajan, R., Bellovin, S. M., Floyd, S., Ioannidis, J., Paxson, V., and Shenker, S. (2002).Controlling high bandwidth aggregates in the network. ACM SIGCOMM Computer Communications Review.

