A Senior Design Project on Network Security

by

Yu Cai and Howard Qi

Michigan Technological University

1400 Townsend Dr.

Houghton, Michigan 49931

cai@mtu.edu

Abstract

Distributed denial-of-service (DDoS) attack is a rapidly growing threat to today's Internet. Significant works have been done in this field. It is vital to incorporate the latest development of technology into academic programs to provide training and education to students and professionals.

In this paper, we present the design and implementation of a senior design project named DDoS Attack, Detection and Defense Simulation. We aim to build a test bed and configure the network environment to simulate "real-world" DDoS attack, detection and defense. We study several DDoS attack tools, as well as some commonly-used DDoS detection and defense software. We perform extensive tests, collect and analyze the experimental data, and draw our conclusions. This is an on-going project. Some preliminary results have been reported here.

The purpose of this project is to help students to apply their technical skills and knowledge on a simulated "real world" project, and gain better understanding and more hands-on experience on Internet security, especially DDoS attack, detection and defense mechanisms.

1. Introduction

Network security is a topic gaining tremendous interests in today's Information Technology world. The increasing frequency and severity of network attacks in recent years reveal some fundamental security issues of Internet environment. Significant efforts from university and industry have been made to improve computer and network security. It is vital to incorporate the latest research results in higher education and academic programs to provide training and education to college students and cyber security professionals.

College seniors in Computer Network & System Administration (CNSA) program [1] at Michigan Technological University are required to complete a capstone senior design project during their final year. The senior design project affords students the opportunity to apply

their individual technical skills and knowledge on a real world project, as well as develop their problem solving skills, communication skills, and teamwork skills.

In this paper, we present the design and implementation of an Information Technology senior design project named DDoS (Distributed denial-of-service) Attack, Detection and Defense Simulation. In this project, we aim to set up test bed and configure the network environment to simulate the "real-world" DDoS attack, detection and defense mechanism. We test several DDoS attack software, as well as some leading DDoS detection and defense products and tools.

The purpose of this project is to help student gain better understanding and more hands-on experience on Internet security, especially DDoS attack, detection and defense mechanisms.

2. Background

DDoS attack has become a rapidly growing threat to today's Internet. A large number of DDoS detection and defense mechanisms have been proposed to combat the problem.

A DDoS attack is one in which a multitude of compromised computer systems attack a selected target, thereby causing denial of service for legitimate users of the targeted system. The flood of incoming traffic to the target system essentially forces it to shut down, thereby denying service to users.

Figure 1 shows a typical DDoS attack [2]. A hacker begins a DDoS attack by exploiting vulnerability in a computer system and making it the DDoS "master". From the master system, the intruder identifies and communicates with other systems that can be compromised also. The intruder loads DDoS attack tools on those compromised systems. The intruder can instruct the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service. Some DDoS attacks utilize Internet worms to automate the process of exploiting and compromising computer systems, as well as launching DDoS attacks.

In general, DDoS defense research can be roughly categorized into four areas: intrusion prevention, intrusion detection, intrusion response, and intrusion tolerance. Intrusion prevention focuses on stopping attacks before attack packets reach the target victim. Intrusion detection explores the various techniques used to detect attack incidents as they occur. Intrusion response investigates various techniques to handle an attack once the attack is discovered. Intrusion tolerance responds to attacks by minimizing the attack impact.

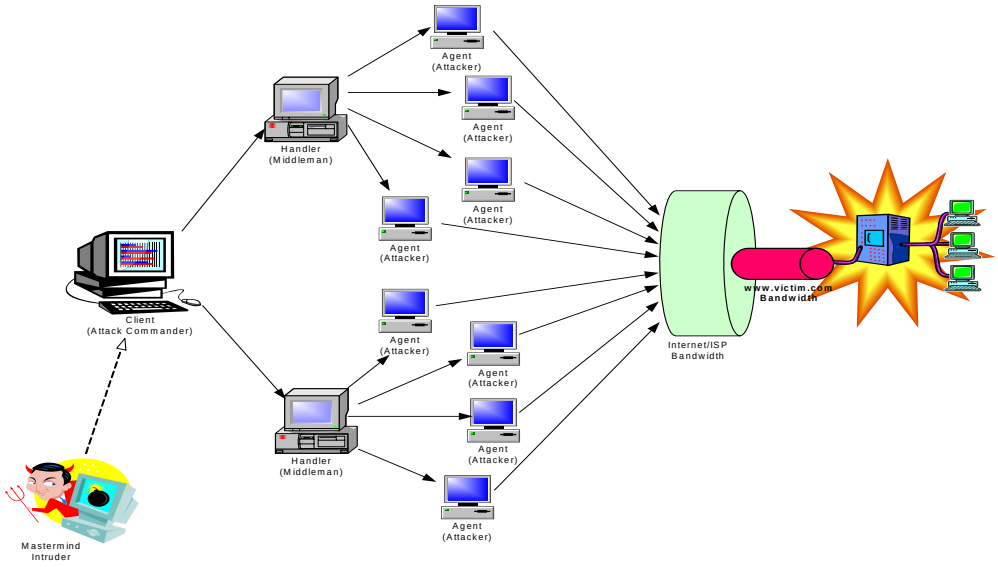

Figure1 – A typical DDoS attack

Extensive research works have been done on the topic of DDoS attacks. J. Mirkovic, et al. from UCLA presented a review paper on DDoS attacks and DDoS Defense Mechanisms [15]. The paper presented two taxonomies for classifying attacks and defenses, and thus provided researchers with a better understanding of the problem and the current solution space. The attack classification criteria were selected to highlight commonalities and important features of attack strategies. The defense taxonomy classifies the body of existing DDoS defenses based on their design decisions; it then shows how these decisions dictate the advantages and deficiencies of proposed solutions.

3. Project Design and Implementation

This project is divided into three phases.

The first phase of this project is to build a DDoS attack network and simulate the DDoS attacks. We test some existing DDoS attack tools, like StacheldrahtV4 [3]. We also develop several simple DDoS attack programs by ourselves. For example, programs that can launch ping flood attack or UDP attack. On the victim network, we use Apache web server [6] and RealPlayer Multimedia Server [7]. The students can observe how DDoS attacks affect the normal users and normal traffic.

The second phase of this project is to set up DDoS Intrusion Detection and Defense systems. We use Snort [8], as well as several other products in market, i.e. OSSEC [14]. We perform extensive tests and compare these DDoS defense products. We design our own defense mechanism by integrating Snort with firewall and router to enable effective rate-limiting and QoS provisioning. This requires students to have good understanding on TCP/IP, iptable [9], firewall and router technologies.

The last part of this project is to further the studies on DDoS attacks. For example, there is a new type of DDoS attack called degrading DDoS attacks, or non-disruptive DDoS attacks. This type of DDoS attack consumes a large portion of victim network resources but does not stop the network services completely. The traditional DDoS defense mechanisms react poorly

to degrading DDoS attacks. We also try to combine Internet worms with DDoS attacks such as Code Red worm [4] and SQL Slammer worm [5].

Phase III is probably too challenging and may go beyond the capability of college seniors from a technological university. We decide to make phase III optional, but strongly encourage students to further their studies. Student will get extra credit if they can make progress in this research area.

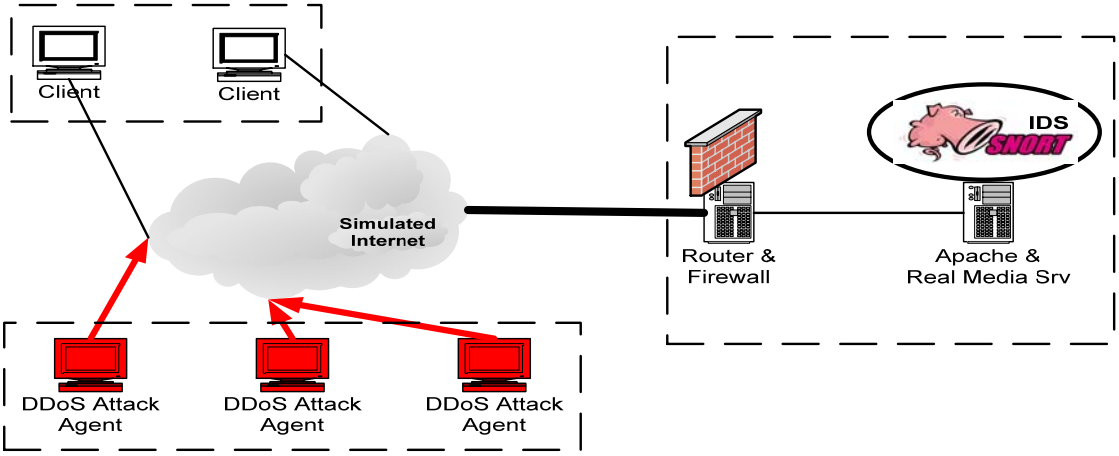

Figure 2 – DDoS Attack, Detection and Defense Test-bed

Figure 2 shows the test bed built for the DDoS attack, detection and defense simulation. The machine configuration is as follows: PIII 667MHz, 256MB RAM, and100Mb Ethernet connection. We build several virtual machines to expand the test bed. The operating systems are Linux Fedora Core 4 [11] and Windows server 2003. StacheldrahtV4 is used as the DDoS attack tool.

4. Experimental Result

This is an on-going project. We report some experimental results as follows. The data is collected by using TCPdump [12]. The figures are drawn using GNUplot [13].

Figure 3 shows the normal traffic condition without DDoS attacks. X axis is the time in second; Y axis is the amount of traffic in packet/second. It is observed that the amount of traffic is around 40 packets per second, except for the initialization stage. It is normal to have larger data transmission rate at the initialization stage.

Figure 4 shows the traffic condition after DDoS attacks. The attacks are launched at 150 second. It is observed that the normal traffic is interrupted. The traffic is either being almost stopped, or becoming bursty and unpredictable.

Figure 5 shows the traffic condition after DDoS detection and defense. The Intrusion Detection System (IDS) on end server raises intrusion alert and notify the firewall system. The firewall takes appropriate actions based on the intrusion alert and traffic condition. For example, firewall can drop packets from certain IP addresses, or rate-limit traffic from certain sources. It is observed that the traffic is brought back to normal after the intrusion detection and defense.

Figure 6 is the screenshot of the SNORT BASE system receiving DDoS alerts. Different detection rules have been configured in SNORT, and alerts are raised based on the traffic condition. Figure 7 is the detailed look of individual BASE alerts, which are mostly Stacheldraht spoofed IP address DDoS attacks.

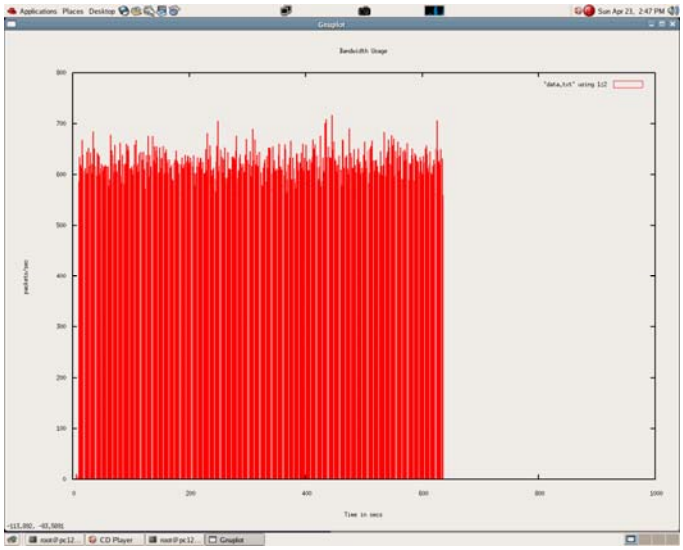

Figure 3: Traffic condition before DDoS attack

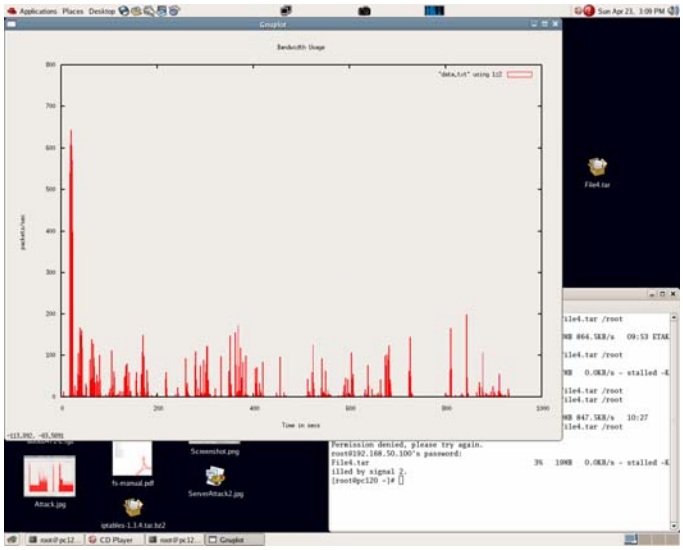

Figure 4: Traffic condition after DDoS attack

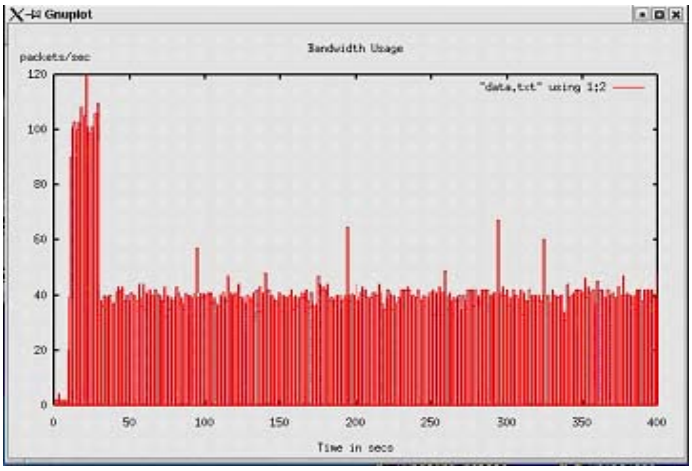

Figure 5: Traffic condition after DDoS defense

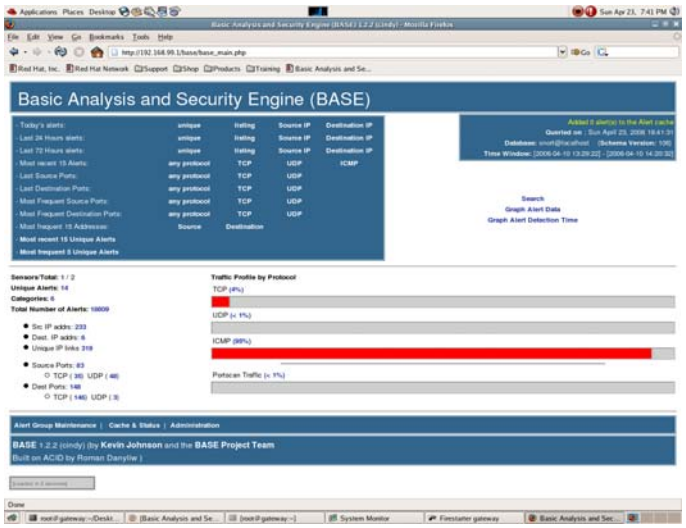

Figure 6: SNORT BASE receiving DDoS alerts

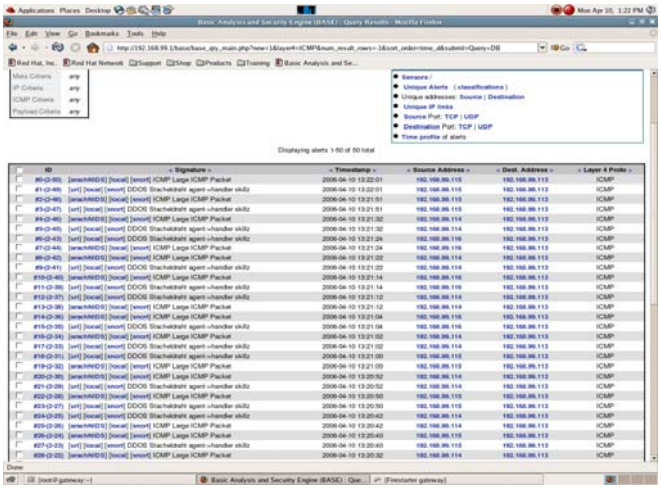

Figure 7 – Individual BASE Alerts: Stacheldraht spoofed IP address

5. Project Management and Assessment

This is a project for two senior students. They work as a team. Each team member must play an active role in designing, building, testing and troubleshooting the project. Every week students are required to submit a progress report and meet with the project advisor (faculty) for one hour. There is a monthly presentation meeting where different senior project teams will meet together and give a 15 minutes presentation to the advisor and their peers. Students are required to use Microsoft Project [10] to manage the progress of the project. At the end of the spring semester, students need to submit their final project report and take the oral project defense.

The department uses the senior project as an assessment tool to evaluate students' academic achievements. Students' final grades are based upon the following factors.

- Quality of the project
- Quality of the report
- Project defense
- Documentation
- Monthly presentation and weekly report
- Peer evaluation

6. Conclusion

In today's computer-dominated society, the practice of securing and administrating computer systems & enterprise network become critical and challenging. The importance of systems administration and security management has grown with the ever-increasing number of devices, software, users and new technologies. In this paper, we present the design and implementation of a senior design project named DDoS Attack, Detection and Defense Simulation. This project helps student apply knowledge learned in classroom, gain better understanding and more hands-on experience on Internet security. Future jobs include implementing an Internet Worm Farm, configuring a HoneyPot system, and setting up a QoS based intrusion defense system.

Bibliography

1. CNSA at MTU, http://www.tech.mtu.edu/cnsa/
2. Angela Cearns, Design of an Autonomous anti-DDoS Network. Master thesis, University of Colorado at Colorado Springs, 2002.
3. StacheldrahtV4, http://cs.uccs.edu/~scold/ddos
4. Code Red Worm, http://www.symantec.com/avcenter/venc/data/codered.worm.html
5. SQL Slammer Worm, http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html
6. Apache, http://www.apache.org
7. Realplayer, http://www.realplayer.com
8. Snort, http://www.snort.org
9. Iptable, http://iptables-tutorial.frozentux.net/iptables-tutorial.html
10. Microsoft Project, http://www.microsoft.com/office/project/prodinfo/default.mspx
11. Fedora Core 4, http://fedora.redhat.com/
12. TCPdump, http://www.ethereal.com/docs/man-pages/tcpdump.8.html
13. GNUplot, http://www.gnuplot.info/
14. OSSEC, http://www.ossec.net/
15. Jelena Mirkovic, et al. “A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms”, UCLA Technical Report