Denial-of-Service Reduction Research Proposal

First Lastname

New Mexico Institute of Mining and Technology
801 Leroy Pl. #2307
Socorro, NM 87801
USA

someemail@nmt.edu

Table of Contents

Project Summary 2
Tentative Outline 3
Outcome 4
Primary Research Strategies 4
Secondary Research Strategies 5
Timeline 6
Questions and Concerns 7
References 7

Project Summary

The purpose of this project will be to analyze different techniques for reducing the damage done by denial-of-service (DoS) attacks on systems connected to the open Internet. An example of a basic DoS attack is a malicious user sending so many requests to a web server that other users cannot connect. If the malicious user owns a substantial number of machines or many different attackers participate, the attack becomes a *distributed* denial-of-service attack (DDoS). Such attacks are substantially more difficult to defend against because they come from many locations simultaneously. While there are several different strategies designed to reduce the effect of these attacks, a distinct solution has yet to be discovered. This project will show a clear need for a solution, compare and contrast the strengths and weaknesses of available alternatives, and suggest what can be done to mitigate the damaging effects of DoS on equipment connected to the Internet.

From a computer science perspective, DoS problems are significant – they impact the workings of everything that relies on communication between computers. From an electrical engineering perspective, any solution that could be constructed into a piece of hardware has an enormous potential customer base.

This topic is very important in today’s cybernetic world, and impacts everyone at some level. Much of the nation’s critical infrastructure, including banks and power companies, is hooked into the Internet. These important systems depend on the Internet to reliably transport important information, such as transfers of money or power control commands. While the Internet normally performs this task remarkably well, malicious Internet users spend a lot of time trying to bring down such systems using DDoS style attacks. There has also been a significant amount of speculation as to the role of such attacks in the warfare of the future.

While the Internet and its workings are programmatically complex, it can be broken down and explained in fairly simple terms. The possible solutions to DoS based attacks are similarly easy to explain. The potential benefits and drawbacks of implementing each various alternative should be straightforward enough to convey to an audience that does not have a background in this field.

Tentative Outline

- How the current Internet system works
    - Basic communication protocols
        - Internet Protocol (IP)
        - Transmission Control Protocol (TCP)
    - Physical architecture
        - Infrastructure (Servers)
            - Network Address Translation (NAT)
            - Gateways
            - Firewalls
        - Users
            - Average users
            - Enterprise users
            - Malicious users
                - Botnets
- Problems with the system
    - Congestion
        - No down-stream congestion information
    - Attacks
        - Distributed denial-of-service attacks
- Potential impacts of these problems
    - Day-to-day disruption
    - Critical infrastructure
        - Power distribution
        - Water & wastewater systems
        - Financial system
    - Wartime implications
- Available alternatives
    - Traffic filtering
    - Bandwidth limiting
    - Explicit Congestion Notification (ECN)
        - Re-feedback of Explicit Congestion Notification (re-ECN)
    - Vouch by reference
    - Private networks
- Recommendation

Outcome

This project will suggest how the negative impact of distributed denial-of-service attacks can be mitigated on the open Internet. This report will be written in IEEE format and will be made available both as a hard copy and a digital PDF.

Primary Research Strategies

Primary research for this project will be collected by conducting interviews with experts in the field. Pete McCann of Motorola Research will be a particularly valuable source of information; Pete has done a substantial amount of research and work on robust Internet systems and is very knowledgeable about this topic. Interviews with Pete will involve asking for his opinion on several different key alternatives, and he will undoubtedly be consulted several times throughout this project.

Another invaluable source of information will be John Grosspietsch, an electrical engineering PhD. also working for Motorola Research. John has done a substantial amount of work on upcoming Smart Grid power technology, and will be a good source of information regarding the current state of the system.

Secondary Research Strategies

Secondary information for this project will be obtained primarily through Internet research. The majority of the reference materials for this project will be formal publications and journal articles, with the remaining minority being informal web articles. It is unlikely that any books will be cited in this project.

One particularly useful source will be the Internet Engineering Task Force (IETF) Request for Comments (RFC) number 3168, as referenced in [1]. This document details the operation of the Explicit Congestion Notification (ECN) system, which is designed to notify down-stream systems that there is potential congestion along the path traveled by a piece of information. Such a system is built directly into the Internet Protocol (IP), and helps to reduce congestion before packets start being dropped. Despite being built directly into the protocol, ECN is not always used. For this system to work properly, it must be supported by all computer systems between the source and the destination. The information in this source will be examined further during the research project.

Another useful source of information is the IETF RFC number 5681, referenced in [2]. This document describes the newer TCP congestion control mechanisms designed to improve the performance of reliable communication on the Internet. In contrast to the ECN system detailed in [1], this system measures congestion by dropping packets instead of marking them. In this way, the up-stream system, the one that is sending the information, is notified of congestion. This mechanism will be further investigated in the research project.

A third source of useful information is shown in [3]. This source describes congestion problems on the Internet in a simple and easy to understand way, and suggests how the TCP transmission protocol might be modified to more easily detect congestion. This model, known as re-feedback explicit congestion notification (re-ECN) is an important alternative to research throughout the project.

This entire project will be formatted to IEEE style, including citations.

Timeline

November 3 – November 10

- Secondary research into how the system works currently
- Text describing these workings
- Associated graphics
- Conference with instructor

November 11 – November 12

- Progress report

November 13 – November 17

- Secondary research into problems with the system
- Text describing these problems
- Associated graphics
- Interview with John Grosspietsch

November 18 – November 19

- Progress report

November 20 – November 24

- Secondary research into solutions
- Text describing these solutions
- Associated graphics
- Interview with Pete McCann

November 26 – November 29

- Combine text pieces into a seamless IEEE paper
- Abstract, introduction, conclusion, proofreading

November 30 – December 3

- Assemble PowerPoint presentation
- Peer review

December 4 – December 5

- Rehearse for presentation

December 6 – December 10

- Finalize project
- Presentation
- Submit project

Questions and Concerns

The goal of this project will likely be to persuade the reader that there is indeed a problem with the current system, rather than to persuade the reader to adopt a particular solution. Because of this, a substantial portion of this project will be to describe how the system currently works. The concern here is that this project may end up being too informative and not persuasive enough.

References

[1] K. Ramakrishnan, S. Floyd, and D. Black. (2010, October 29) The Addition of Explicit Congestion Notification (ECN) to IP - RFC 3168. [Online]. Available: http://tools.ietf.org/html/rfc3168

[2] M. Allman, V. Paxson, and E. Blanton. (2010, October 30) TCP Congestion Control - RFC 5681. [Online]. Available: http://tools.ietf.org/html/rfc5681

[3] B. Briscoe. (2010, November 1) A Fairer, Faster Internet Protocol. [Online]. Available: http://spectrum.ieee.org/telecom/standards/a-fairer-faster-Internet-protocol/0