CSEC640 - Weeks 4 and 5 Individual Assignment #1

DUE DATE: End of Week 5 (Two Weeks Assignment)

Description

The course module #4 covers very important concepts of how Denial of Service (DoS) attacks work. However, the module does not discuss detection, prevention, or mitigation of DoS attacks (or Distributed DoS). The task of this individual assignment is to ***write a research paper/report*** in these topics.

Topic of the Paper:

Technique(s) or scheme(s) or method(s) for detecting, preventing or mitigating DoS or Distributed DoS (DDoS) attacks.

Assignment Guidelines

The following must be considered when you write the paper:

1. Select 3-4 research papers **(in addition to those provided/suggested for the class)** which discuss detection, prevention, or mitigation techniques for DoS or DDoS attacks:
    a. The research papers **must** be published by a peer reviewed journal or be published in conference proceedings (e.g., IEEE, ACM, IBM Systems Journal, Lecture Notes in Computer Science (LNCS), etc.). Use the UMUC online library resource if necessary.
    b. You **must not** choose papers or research works from magazines or periodicals that are not research-oriented (e.g., Wikipedia, SANS, etc.).
    c. Briefly **explain your rationale for selecting** a specific research paper.
    d. **Allocate sufficient time** to read the research papers. Reading a research paper requires more time than most people realize.

2. Summarize each research paper and identify the detection, mitigation, or prevention techniques described in **the papers you selected.** The first paper is selected because of its extensive presentation of a detection technique; the second paper is selected because of a presentation of a prevention technique, and the third paper because of the presentation of a mitigation technique. Finally, a fourth research paper from which you select to analyze any of the three techniques. You can select 3 papers if you can justify that the depth and completeness of the selected papers cover the topics of your research paper. Otherwise, a selection of at least 4 papers is advisable.

NOTE: Please see the Appendix at the end of this document for further clarification on the Assignment Guidelines.

Further Instructions:

1. Describe how each technique works. Clearly describe (in detail using your own words), how each technique works. **Assume that you are explaining the author's technique to**

someone with a fairly strong fundamental knowledge in network and security (e.g., a first year computer science graduate student) **and assume the student has no knowledge of the author's research (never read the article before).** Discuss each technique or method using the following questions:

a. Is the proposed technique a promising, practical approach which can be effectively implemented into an existing platform? Clearly explain your answer.
b. What are the strengths and weaknesses (limitations) of this technique?

2. Make sure there are No IPR (Intellectual Property Right) issues. This requires the following:
   a. Re-draw all figures and tables.
   b. Summarize all concepts using your own words.
   c. Do not copy any part of text or unmodified figures (short quotes are acceptable.)
   d. Cite references as needed using APA format.

3. It is important that you start Week 4 reading the "**Week 4 Overview**", the Week 4 Module, and the book chapters and articles listed in the reading assignment for Week 4. Doing this will allow you to make a better selection of the research papers to be used for your research/critique. You are required to support the presentation of your analysis with in-text citations of reference sources from the Week 4 module and the book chapters and articles listed in the Week 4 reading list. To support your claims or statements from peer-reviewed sources, you may also cite/reference non-peer reviewed papers and journals (including white papers, SANs documents, etc. from non-academic sources, however, **no Wikipedia or blogs**).

Submission Guidelines

- Print format: MS Word.
- The paper length: A minimum of 10 double space pages, font size 12, not including the cover page and reference page(s).
- Follow the APA 6th edition format for in-text citations and references.
- **Upload your report to your Assignment Folder**.
- **DUE DATE**: End of Week 5 (Two Week assignment – Week 4 and Week 5).

Naming of the documents to be delivered:

LastName_FirstName_IndAssig1.docx

Example: Fernandez_Rolando_IndAssig1.docx

APPENDIX

Clarification about "Assignment Guidelines"

These directions given in the Assignment Guidelines, bullet 2, need further explanation:

My recommendation is:

You are expected to base your paper on research that you have found through the library sources along with the papers provided/suggested for the class.

Summarize each research paper and identify the detection, mitigation, or prevention techniques described in **the papers you selected.** The first paper is selected because of its extensive presentation of a detection technique; the second paper is selected because of a presentation of a prevention technique, and the third paper because of the presentation of a mitigation technique. Finally, a fourth research paper from which you select to analyze any of the three techniques or a combination of them. You can select 3 papers if you can justify that the depth and completeness of the selected papers cover the topics of your research paper. A selection of at least 4 papers is strongly advisable.

Total number of papers you summarize = 3 - 4

Total number of techniques you cover = 3 (detection, mitigation, and prevention of DoS and DDoS attacks)

Total number of techniques analyzed per paper = 1

Use other additional sources to back up your review.

NOTE: When you select a research paper, please avoid survey papers. Survey papers are not a good selection for your research paper because they usually do not analyze a technique with the required depth.

You need to select papers that are current and address one technique in depth.

There will be cases where the selected paper may cover more than one technique; however, you need to make sure that the paper does extensive and detailed work in the one technique for which it has been selected.

Suggested Research Paper Structure

The following is a suggested general structure of your research paper:

<Title page>

Abstract

Table of Contents (Recommended in most technical papers)

Introduction

Background (Optional)

Denial of Service Attacks explained

- **Symptoms of Denial of Service (DoS) Attacks**
- **Common Types of Denial of Service (DoS) Attacks**

Paper 1 – Detection

Reviewed Research Paper One – <paper title> by <author(s)>

- **Paper's Entry in APA Notation Format**
- **Rationale for the Selection of the Paper with Supporting Documentation**
- **(Above subsection to include the paper's peer reviewers)**
- **Relevance of this Paper**
- **Summary of Research**
- ***Techniques Examined*** **---- Or Techniques Description**
  - **(" . . Clearly describe how each technique works . . .")**
- **Strengths and Weaknesses of Each Technique**
- **Ease of Implementation**

Topic 2 – Prevention

Reviewed Research Paper Two – <paper title> by <author(s)>

- **Paper's Entry in APA Notation Format**
- **Rationale for the Selection of the Paper with Supporting Documentation**
- **(Above subsection to include the paper's peer reviewers)**
- **Relevance of this Paper**
- **Summary of Research**
- ***Techniques Examined*** **---- Or Techniques Description**
  - **(" . . Clearly describe how each technique works . . .")**
- **Strengths and Weaknesses of Each Technique**
- **Ease of Implementation**

Topic 3 – Mitigation

Reviewed Research Paper Three – <paper title> by <author(s)>

- **Paper's Entry in APA Notation format**
- **Rationale for the Selection of the Paper with Supporting Documentation**
- **(Above subsection to include the paper's peer reviewers)**
- **Relevance of this Paper**
- **Summary of Research**
- ***Techniques Examined* ---- Or Techniques Description**
  - **(" . . Clearly describe how each technique works . . .")**
- **Strengths and Weaknesses of Each Technique**
- **Ease of Implementation**

Topic 4 – (Optional) <Detection, Prevention, Mitigation or a combination>

Reviewed Research Paper Four – <paper title> by <author(s)>

- **Paper's Entry in APA Notation format**
- **Rationale for the Selection of the Paper with Supporting Documentation**
- **(Above subsection to include the paper's peer reviewers)**
- **Relevance of this Paper**
- **Summary of Research**
- ***Techniques Examined* ---- Or Techniques Description**
  - **(" . . Clearly describe how each technique works . . .")**
- **Strengths and Weaknesses of Each Technique**
- **Ease of Implementation**

Further Discussion on DoS and DDoS Attacks

Conclusions and Synopsis

References