“Authorization functions” is a process by which access to a particular IT asset can be granted or denied, while access control is used to enforce the rules for authorization. There are several access control models, including "role-based" AC, "discretionary" AC, "mandatory" AC, and "attribute-based" AC. Imagine that, as the security administrator for a medium-sized retail-based organization with around 2000 users, you are tasked with determining the appropriate level of access for a new user in the Human Resources department. What approach would you take to determine access for this person? What methods would you use to verify that the choice of access controls is appropriate for this user?

To be added…

Imagine that, as the security manager at XYZ Corporation, you are responsible for managing the intrusion detection environment. If you were given the ability to build the environment from scratch, would you use network-based IDS, host-based IDS, or a combination? Why? How would you structure your staff and organization to get the most out of your investment? Are there any strengths of one over the other that you may take into consideration? Which one is more expensive?

To be added…

Authentication, Access Control, and Network Security

Unit 2 discusses three very important areas of computer security: authentication, access control, and network security.

Please click the Overview button below for a brief summary of the concepts that are being covered in this unit.

Outcomes

After completing this unit, you should be able to:

- Assess access control models
- Analyze denial of service response.

- Prepare worm countermeasures
- Assess denial of service attacks

Course outcome(s) practiced in this unit:

IT541-2: Compare authentication and encryption methods.

IT541-4: Apply basic information security Best Practices to business scenarios.

What do you have to do in this unit?

- Complete assigned Reading.
- Participate in the Discussion.
- Complete unit Assignment.
- Participate in Seminar or complete Alternative Assignment.
- Read Overview.
- Complete Learning Activities.

Readings for Unit 2

Read the following chapters in *Computer Security: Principles and Practice:*

- Chapter 3: “User Authentication”
- Chapter 4: “Access Control”
- Chapter 5: “Denial of Service Attacks”
- Chapter 6: “Intrusion Detection”
- Chapter 7: “Malicious Software”
- Chapter 8: “Database Security”

Chapter 3 discusses the various forms of user authentication that facilitate secure use of computing resources. In Chapter 4, you will learn about current models for controlling user access to computing resources, allowing access to the users who need it while preventing unwanted users from accessing systems. Chapter 5 presents methods for securing data in databases, while Chapter 6 explores network-based and host-based intrusion detection systems. In Chapter 7, you will read about the most prevalent types of malicious software and about development methods. Finally, Chapter 8 discusses some famous DoS attacks and explains how DoS attacks take place.

Also, read “Reading 9: The Provision of Defenses Against Internet-Based Attacks” in *Readings and Cases in the Management of Information Security*.

Attending live Seminars is important to your academic success, and attendance is highly recommended. The Seminar allows you to review the important concepts presented in each unit, discuss work issues in your lives that pertain to these concepts, ask your instructor questions, and come together in real time with your fellow classmates. There will be a graded Seminar in Units 1 through 5 in this course. You must either attend the live Seminar or complete the Seminar alternative assignment in order to earn points for this part of the class.

Option 1: Attend Seminar

You are encouraged to attend the graded Seminar as an active participant. If you cannot attend, you may submit the alternative assignment to the unit Seminar Dropbox.

This week’s Seminar will focus on a discussion of authentication, access control, and network security.

Remember, if you do not participate in the weekly Seminar, you need to complete the alternative assignment.

Option 2: Alternative Assignment

You will benefit most from attending the graded Seminar as an active participant. However, if you are unable to attend, you have the opportunity to make up the points by completing the alternative assignment.

The alternative assignment consists of reviewing the recording from the live Seminar and then submitting a paper of at least 3 pages in length that presents an overview of the topics covered during the Seminar. The paper must include at least one citation to a research paper relating to one of the topics from the Seminar. Your paper should be in APA format and cite all references used. Submit to the Seminar Dropbox.

Brief Overview of Unit 2

Unit 2 discusses three very important areas of computer security: authentication, access control, and network security. Why is authentication important? What types of

authentication are the most secure? What exactly does access control encompass? What techniques can you use to secure databases? In this unit, you will learn answers to all of these questions and understand the key strategies used in each of these areas.

This unit also discusses the detection and mitigation of malicious activities in the computing environment. Tools such as intrusion detection systems can report the existence of malicious software or the presence of a denial of service attack to administrators. In order to accurately interpret intrusion detection tools, a solid understanding of the types of malicious software and denial of service techniques is required.

Assignment 2

Outcomes addressed in this activity:

- Assess access control models.
- Analyze denial of service response.
- Prepare worm countermeasures.
- Assess denial of service attacks.

Course Outcomes:

IT541-2: Compare authentication and encryption methods.

IT541-4: Apply basic information security Best Practices to business scenarios.

Assignment Instructions

This Assignment provides a "hands on" element to your studies. It gives you the opportunity to work with the protocols and see how they operate in real-world environments. Read and perform the lab entitled **"IT541 Assignment 2 Lab"** found in Doc Sharing; use the lab sheet included at the end of the lab file to submit your results.

Directions for Submitting Your Assignment:

Use the Lab #2 Worksheet document found at the back of the lab instructions as a guide for what to submit, and save it as a Word document entitled Username-IT541 Assignment-Unit#.doc (Example: **TAllen- IT541 Assignment-Unit2.doc**). Submit your file by selecting the Unit 2: Assignment Dropbox by the end of Unit 2.

Assignment Requirements:

- Answers contain sufficient information to adequately answer the questions
- No spelling errors
- No grammar errors

*Two points will be deducted from your grade for each occurrence of not meeting these requirements.

For more information and examples of APA formatting, see the resources in Doc Sharing or visit the KU Writing Center from the KU Homepage.

Also review the KU Policy on Plagiarism. This policy will be strictly enforced on all applicable assignments and discussion posts. If you have any questions, please contact your professor.

Review the grading rubric below before beginning this activity.