ITBU 313: Introduction to Cyber Security, Homework 09

Chapter 03, *Computer Security, Principles and Practices*

Readings

Read chapter 03 in the *Computer Security, Principles and Practices* book.

Discussion Questions

Answer the discussion questions in writing.

1. Explain the difference between user identification, user authentication, and message authentication.
2. What are the four general means of establishing a user's identity? Give one example of each.
3. How does *multifactor authentication* work?
4. Describe five methods of attacking passwords.
5. In the last chapter, you had a question on the use of hashed passwords. Now, explain in detail how you would design a system to use hashed passwords. This is a common coding exercise for beginning programming students.
6. What is a *rainbow table*? How is it used?
7. Describe the three protocols used in a system implementing smart tokens.
8. What is the most secure means of biometric user identification? What is the worst? Explain your answer. Note that opinions may differ.
9. What is a *nonce*? How is it used?
10. What is a *replay attack*? Explain how an attacker would initiate such an attack. Explain how a defender would prevent it.
11. Describe the general concept of a *challenge-response* means of user authentication.