CS 531 – Fall 2020

SECURITY IN CYBER-PHYSICAL SYSTEMS

QUIZ #4

9/17/2020

If there are more than one answer, please select both. Hint: Some questions may have multiple answers.

Please write justification for each answer for partial credits.

1) Which of the following features Modbus provides? (10p)
    a. Integrity
    b. Non-repudiation
    c. Authentication
    d. Confidentiality

2) Which of the following features DNP3 provides? (10p)
    a. Integrity
    b. Non-repudiation
    c. Authentication
    d. Confidentiality

3) Which of the following is an example of real time communication? (10p)
    a. Sending email through Outlook
    b. Attending class through Zoom
    c. File sharing through Dropbox
    d. Scrolling through Facebook app

4) Which of the following can be considered as Modbus attack? (can exploit Modbus) (10p)
    a. Buffer overflow
    b. MAC poisoning
    c. TCP Session Hijacking
    d. MiTM
    e. DoS

5) Which of the following is vulnerable to rogue server deployment? (10p)
    a. ICCP
    b. DNP3
    c. OPC
    d. Modbus

6) Which of the following is true about <u>secure</u> DNP3? (10p)
    a. Uses MAC
    b. Challenge-response is used for authentication
    c. Enables authentication at the application layer
    d. Provides reliability CRC
    e. Uses public-private keys

7) What is the mechanism that DNP3 uses for prioritization of messages? (10p)

8) What is the ICCP feature that provides access control? (10p)

9) What is the scalability difference between Modbus and DNP3? What is the reason behind this difference? (20p)
   Hint: Consider how many devices can be connected through Modbus vs. DNP3.