SCHOOL OF SCIENCE, ENGINEERING AND HEALTH

DEPARTMENT OF COMPUTER SCIENCE

FINAL EXAMINATION JANUARY SEMESTER-2019

ACS 332/MIS 431: COMPUTER SYSTEM SECURITY

DATE: MAY 2019 **TIME: 2.0 HOURS**

SECTION A Answer **ALL** questions.

Question 1

1. Define the following as used in computer security. **(3 Marks)**
   a. *Passphrase*
   b. *White noise*
   c. *Scrubbing*
2. Computer security is both fascinating and complex. Some of the reasons follow. State any **FOUR** challenges to computer security. **(4 Marks)**
3. Highlight any **THREE** challenges governments' likely face in implementing integrated biometric electrical process. **(3 Marks)**
4. Every computer system or application provides access criteria and tools that enhances access to resources. Access criteria can be broken up into different assign rights. Discuss any **FOUR**. **(4 Marks)**
5. Highlight **FOUR** loopholes within a computer system that compromises its security **(4 Marks)**
6. Passwords are also considered one of the weakest security mechanisms available. Justify. **(2 Mark)**
7. Any person authorized to use the computer system has the right to access the system and its resources according to the authorization criteria set up by the site security administrator.
   a. Cite **FOUR** Problems in controlling access to assets **(2 Marks)**

b. Explain **FOUR** Access criteria types **(2 Marks)**

c. There are a number of different access controls and technologies available to support the different models. State any **FOUR.** **(2 Marks)**

d. Explain the following types of access control models **(4 Marks)**

i. Discretionary Access

ii. Mandatory Access

SECTION 2: ANSWER ANY TWO QUESTIONS EACH 20 MARKS]

Question 2

The results of recent biometric voting exercises in countries such as Kenya and Ghana have taught us that governments expect fast, accurate, and reliable voter registration at the polls under any conditions that help to maintain the integrity and credibility of the electoral process and reduce mistrust and irregularities.

a) Discuss any **THREE** biometrical systems stating limitations of each type.**(9 Marks)**

b) Define *steganography*. State any **THREE** different cryptographic methods used in computer security **(5 Marks)**

c) Differentiate between **(6 Marks)**

i. Type I and Type II occurrences in biometrical systems

ii. Brute force attacks and dictionary attacks

iii. *Contact and contactless smart cards*

Question 3

a) While scanning a workstation I realized the output below on my command line interface.

```
Exception:  EXC_BAD_ACCESS (0x0001)
Codes:      KERN_INVALID_ADDRESS (0x0001) at 0x41414140

Thread 0 Crashed:

Thread 0 crashed with PPC Thread State 64:
  srr0: 0x0000000041414140  srr1: 0x000000004200f030                    vrsave: 0x0000000000000000
    cr: 0x48004242           xer: 0x0000000020000007   lr: 0x0000000041414141  ctr: 0x000000009077401c
    r0: 0x0000000041414141    r1: 0x00000000bfffe660   r2: 0x0000000000000000   r3: 0000000000000001
    r4: 0x0000000000000041    r5: 0x00000000bfffdd50   r6: 0x0000000000000052   r7: 0x00000000bfffe638
    r8: 0x0000000090774028    r9: 0x00000000bfffddd8  r10: 0x00000000bfffe380  r11: 0x0000000024004248
   r12: 0x000000009077401c   r13: 0x00000000a365c7c0  r14: 0x0000000000000100  r15: 0x0000000000000000
   r16: 0x00000000a364c75c   r17: 0x00000000a365c75c  r18: 0x00000000a365c75c  r19: 0x00000000a366c75c
   r20: 0x0000000000000000   r21: 0x0000000000000000  r22: 0x00000000a365c75c  r23: 0x000000000034f5b0
   r24: 0x00000000a3662aa4   r25: 0x000000000054c840  r26: 0x00000000a3662aa4  r27: 0x0000000000002f44
   r28: 0x000000000034c840   r29: 0x0000000041414141  r30: 0x0000000041414141  r31: 0x0000000041414141
```

a. From your experience as a security student *identify the above vulnerability* on the system. **(3 Marks)**

b. How does the *vulnerability* work? **(5 Marks)**

c. How can we *prevent* such an attack happening next time? **(3 Marks)**

b) Discuss the following terms **(9 Marks)**

i. *Authorization Creep*

ii. *Default to Zero*

iii. *Access Control Lists*

Question 4

a) Once early internet system administrators began to understand that they were frequently being attacked, the network firewall was inevitable. There was destined to be some sort of process that looked at network traffic for clear signs of attackers. Exactly how this was going to work was less clear.*AT&T's Steven M. Bellovin* is generally credited -- although not by himself -- with first using the term firewall to describe the process of filtering out unwanted network traffic, sometime around 1987.Many organizations like daystar have embraced firewalls. Briefly describe any **THREE** types of firewalls enterprises can adopt **THREE** functions of firewalls and **THREE** challenges to adopting firewalls in an organization. **(15 Marks)**

b) Intrusion Detection Systems (IDs) are different from traditional firewall products because they are designed to detect a security breach. State **THREE** components of an IDS differentiate between "*in the world*" and "*in the zoo*" viruses. **(5 Marks)**