**INFA 670, Spring 2013**

**Final**

**Prof. J. Bonner**

Student Name:

Note: Answer questions succinctly and clearly, explain your answer, and show your work. Answers, even if right but without an explanation, will get no credit. Test is open book/notes, but individual, NOT TO BE SHARED. Do keep the questions/instructions in this word file with your answers. **(DUE TO THE ASSIGNMENT FOLDER BY 2359(EST) –Sunday, 28 APR 2013 –EASTERN STANDARD TIME).**

**GRADING COMMENTS: NOTE: Your word document shall be prepared in the APA format (just like your HW assignment) and make sure you include your references to each question. Please!!!! Save the word document as (YOUR NAME\_\_\_\_\_\_\_INFA670FINAL). The point distribution is listed at the end of the exam and any questions on the exam must be e-mailed to me direct (jeffrey.bonner@faculty.umuc.edu)/private messaging on Web Tycho.**

**You will not have to submit your test through Turnitin. However, each problem must have reference(s) and if you decide to use the Bishop textbook as one (1) of your reference: you must identify the Chapter and page # of your reference. You will not be allowed to reference Chapter 24 for example without a page # associated with it. When I am grading your final, I plan on checking out all your references since we will not be using Turnitin for this specific case. Lack of references or incorrect references/problem will result in a failure in your final.**

**LATE-PENALTY – FROM THE SYLLABUS (**Late Policy**:** Assignments are due as outlined in the Web Tycho Site. Late assignments will not be accepted due to the end of class on 29

APR 2013.)

Answer the following questions.

**1) (12 pts.) Chapter 18 (pgs. 494-495) –Problem#7**

**A company develops a new security product using the extreme programming software development methodology. Programmers code, then test, the en add more code, then test, and continue this iteration. Every day they test the code base as a whole. The programmers work in pairs when writing code to ensure that at least two people review the code. How would you explain to this company how their software is in fact not high assurance” software?**

**2) (15 pts.) Chapter 22 (pgs. 642-643) –Problem#2**

**Consider how a system with capabilities as its access control mechanism could deal with Trojan Horses.**

**A) In general, do capabilities offer more or less protection against Trojan horses than do access control lists? Justify your answer in light of the theoretical equivalence of ACLs and C-Lists**

**B) Consider now the inheritance of properties of new processes. If the creator controls which capabilities the created process is given initially, how could the creator limit a damage that a Trojan Horse will do?**

**C) Can capabilities protect against all Trojan Horses? Either show that they can or describe a Trojan horse process that can C-Lists cannot protect against**

**3) (18 pts.) Chapter 22 (pgs. 642-643) –Problem#12**

**Assume that the Clark –Wilson model is implemented on a computer system. Could a computer virus that scrambled constrained data items be introduced into the system? Why or why not? Specifically, if not identify the precise control that would prevent the virus from being introduced, and explain why it would prevent the virus from being introduced; if yes identify the specific control or controls that would allow the virus to be introduced and explain why they fail to keep it out.**

**4) (20 pts.) Chapter 23 (pgs. 685-687) –Problem#1**

**Classify the following vulnerabilities using the RISOS model. Assume that the classification is for the implementation level. Justify your answer:**

**a)The presence of the wiz command in the sendmail program(see Sect. 23.2.8)**

**b) The failure to handle the IFS shell variable by loadmodule(see section 23.2.8)**

**c) The failure to select an Administrator password that was difficult to guess(see sect. 23.2.9)**

**d)The failure of the Burroughs system to detect offline changes to files(see section 23.2.3.6)**

5) (**15 pts.) Chapter 23 (pgs. 685-687) –Problem#4**

**A common error in the UNIX system occurs during configuration of bind, a directory name server. The time-to-expire field is set at 0.5 because the administrator believes that this field unit is minutes (and wishes to set the time to 30 seconds) However, bind expects the field to be in seconds and reads the value as 0 – meaning that no data is ever expired.**

1. **Classify this vulnerability using the RISOS model, and justify your answer**
2. **Classify this vulnerability using the PA model and justify your answer**
3. **Classify this vulnerability using the Aslam’s model and justify your answer**

6) (**20 pts.**) Essay Question: Secure software certification. Your present company (assignment#2) is at EAL4. You are the new program manager on this effort and your job is to bring your present software secure package to EAL7. Explain to me your management plan on upgrading your present software package from EAL4 to EAL7. Your management plan should include discussing your past documentation (assignment#2), the difference between EAL4 and EAL7, what additional paperwork will be needed to reach EAL7 certification, and finally, define your risk based on reusing software code for this migration from EAL4 to EAL7 certification.

Link to the book.

<http://books.google.com/books?id=pfdBiJNfWdMC&pg=PA495&lpg=PA495&dq=A+company+develops+a+new++security+product+using+the+extreme+programming+software+development&source=bl&ots=zZfry6w-sD&sig=J_8pCa1jPMjP8bLpExPx3WnNLhk&hl=en&sa=X&ei=FsF2UdzcA8m50AGa6oHICA&sqi=2&ved=0CDwQ6AEwAA>

**GRADING:**

1.\_\_\_\_\_\_\_\_\_ (12 pts.)

2.\_\_\_\_\_\_\_\_\_ (15 pts.)

3.\_\_\_\_\_\_\_\_\_ (18 pts.)

4.\_\_\_\_\_\_\_\_\_ (20 pts.)

5.\_\_\_\_\_\_\_\_\_ (15 pts.)

6.\_\_\_\_\_\_\_\_\_(20 pts.)

**FINAL EXAM GRADE = “ “**