CIS 6373: Foundations of Software Security [Spring 2024]
Test III

NAME: _____

Instructions:

1) This test is 11 pages in length.

2) You have 120 minutes to complete and turn in this test.

3) Short-answer and essay questions include guidelines for how much to write. Respond in complete English sentences. Responses will be graded as described on the syllabus. Respond at the level of detail discussed in class. Avoid using bullet points and enumerated lists.

4) This test is closed everything, including books, notes, papers, computers, phones, laptops, smartwatches, smartglasses, AI, LLMs, friends, neighbors, etc.

1. [5 points] [Short essay] Compare and contrast the peer-review process in conferences and journals. Hit all the main points discussed in class.

2. [6 points] [Short essay] Briefly describe the debate about whether nonsafety properties can ever be precisely enforced.

3. [6 points] [Short essay] Describe the pros and cons of aspect-oriented programming, hitting all the main points discussed in class.

4. [3 points] [1-2 sentences]
Briefly explain the "grand unifying theory" discussed in class.

5. [6 points] [Short essay] As discussed in class, why is noninterference a nonproperty policy?

6. [3 points] [2-3 sentences]
How can temperature affect software security? Hit all the main points discussed in class.

7. [7 points] [Short essay] Explain how binary-search injection attacks proceed, as discussed in class. Ideally include a (possibly high-level) example, again as discussed in class.
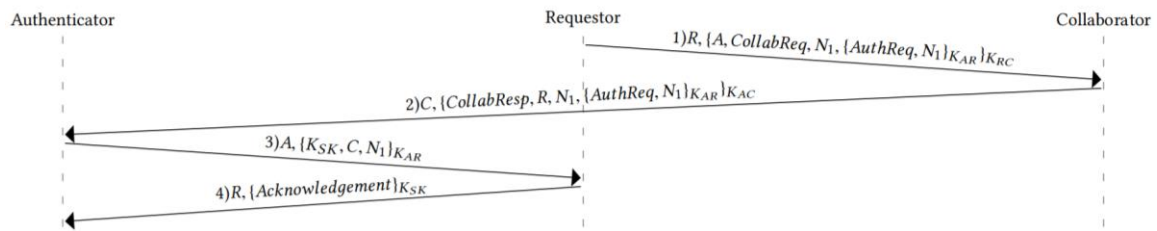
8. [3 points] [1-2 sentences] Explain SUS, as discussed in class.

9. [8 points] [Short essay] Compare and contrast BroNIE detection to using prepared statements.

10. [3 points] [1-2 sentences]   What's a current topic of debate in the field of cybersecurity insurance, as discussed in class?

11. [12 points] Formally state and prove that there exists exactly one element in the intersection of gray liveness and safety.

12. [10 points] [Essay] Hitting all the main points discussed in class, explain the protocol shown below and the guarantees it does and does not provide.

Authenticator   Requestor   Collaborator

1) $R, \{A, CollabReq, N_1, \{AuthReq, N_1\}_{K_{AR}}\}_{K_{RC}}$

2) $C, \{CollabResp, R, N_1, \{AuthReq, N_1\}_{K_{AR}}\}_{K_{AC}}$

3) $A, \{K_{SK}, C, N_1\}_{K_{AR}}$

4) $R, \{Acknowledgement\}_{K_{SK}}$

13. [5 points] [Short essay] Explain the deficit model, and a contrasting model, as discussed in class.

14. [5 points] [Short essay] How could it be argued that bitmask policies are "better" than other specifications? Hit all the main points discussed in class.

15. [6 points] [Short essay] Describe participant incentives, hitting all the main points discussed in class.

16. [5 points] [Short essay] Hitting all the main points discussed in class, compare and contrast sound, complete, and precise enforcement.

17. [7 points] [Short essay] Hitting all the main points discussed in class, what are challenges to enforcing noninterference in practice?