CS 591: Introduction to Computer Security

Midterm Grading Notes

James Hook
Notes

• Q1: Availability, integrity, confidentiality
  – Definition: 2 correct, 1 relevant, 0 irrelevant
  – Example: 1 right, 0 otherwise
  – Attempt: 1

• Note:
  – Several proposed a user sharing a password as a violation of confidentiality. This may enable a breach of confidentiality, but it is the disclosure of information outside of the set of authorized individuals that constitutes a breach of confidentiality
Notes

• Q2: Policy/Mechanism
• Q3: Ciphers
  – Describe algorithms: 2 points each algorithm
  – Example: 1 point each algorithm
  – Attempt: 1 point (should have had a one point question about why “bad” is a bad key ;-) )
  – Notes: I tried to be very forgiving with calculation errors, but not with conceptual errors.
Notes:

• Q4: Crypto short answer
  – 2 points each part
• Q5: Confinement
  – Expected: confinement definition, virtual machine discussion, sandboxing discussion, contrasting discussion
  – Answers varied.
    • Confinement w/o describing mechanisms (5 points)
    • Both mechanisms w/o confinement (5 points)
    • One mechanism w/o confinement (2 points)
Notes

• Q6: Separation of Duty
  – Separation of Duty: 5 points
  – RBAC with mutually exclusive role relationship: 5 points
  – RBAC w/o mutual exclusion: 3 points
  – Relevant discussion: 2 points

• Q7: Clark-Wilson
  – Most got this question
  – 2 points each plus 2
Notes

• Q8: DG/UX Confidentiality, Integrity
  – A:
    • range = 2 points
    • modified *-property = 2 points
  – B, C: 3 points each

• Q9: Information Flow
  – Why high: 4
  – Why not useful: 3
  – Why ok if policy explicitly allows it (including bandwidth control): 3
Notes

• Q10: Access Control
  – A) 3 points, 1 each definition
  – B) 2 points
  – C) 3 points (looking for “abbreviated ACL” concept)
  – D) 2 points
Distribution

- 90 91 93 95
- 70 75 79
- 62 62 63
- 53
- 46

Curve by $f(x) = x/2 + 50$