CS 591: Introduction to Computer Security

Midterm Grading Comments

James Hook

Grading Guide:

• Q1: Availability, Integrity, Confidentiality
  – 2 points each definition
  – 1 point each illustration of violation
  – 1 point for attempting problem
• Q2: Policy and Mechanism
  – 3 points each definition
  – 2 points each example
Grading Guide:

• Q3: Chinese Wall
  – 3 points for motivating scenario
  – 3 points for mechanisms (COI, simple security rule, *-rule)
  – 2 points how to model with Bell LaPadula
  – 2 points shortcomings of using Bell LaPadula

• Q4: Digital signature
  – 3 points: agreement adjudicated by trusted third party
  – 2 points: property: non-repudiation
  – 2 points: property compromised by bogus (non-repudiation)
  – 3 points: justification of forgery attack

Grading Guide:

• Q5: Access controls
  – 2 points each AC control mode
  – 3 points which plays with which (1 per pair)
  – 1 point for attempting problem

• Q6: DG/UX confidentiality & integrity
  – 4 points: range of levels (MAC tuples)
  – 3 points: why confidentiality; what protected
  – 3 points: why integrity; what protected
Grading Guide:

• Q7: Denning Information Flow
  – 5 points: a flow exploiting exceptions
  – 5 points: discussion of how to control
    • Looked for evidence of how to control within the model of Denning and Denning, e.g. assigning labels and constraints to exception handlers

• Q8: Nonces
  – 5 points: Nonces prevent replay
  – 5 points: Give a replay attack of simplified protocol

Grading Guide:

• Q9: Block/Stream
  – 2 points each definition (block/stream)
  – 2 points each classification

• Q10: Crypto facts
  – 2 points each
    • Diffie-Hellman allowed either DH algorithm for key negotiation (intended answer) or general contribution of public key encryption framework [consulted text; this was stressed DH contribution]
<table>
<thead>
<tr>
<th>Distribution:</th>
<th>Average = 70.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td></td>
</tr>
<tr>
<td>94 92 92</td>
<td></td>
</tr>
<tr>
<td>87 87 85 84 84 83 83 83 81 81 80</td>
<td></td>
</tr>
<tr>
<td>78 75 74 71</td>
<td></td>
</tr>
<tr>
<td>65 64 64 64 63 60 60</td>
<td></td>
</tr>
<tr>
<td>59 59 57 56 54 50</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td></td>
</tr>
<tr>
<td>28 28</td>
<td>Exam will be graded on a curve.</td>
</tr>
</tbody>
</table>