"By submitting this homework, I attest that the homework is my own work and I have not copied any text verbatim from any online or offline source, or from other students (past or present). I also attest that I have not used any paraphrasing tool or any homework solution websites. In addition, I attest that any information taken from course slides and handouts or any websites is properly attributed and referenced. I understand that any violation of the UAB Academic Integrity Code for any portion of the homework will result in a zero score for the entire homework and will be reported to the academic integrity coordinator per university policy."

1. When you are using a TPM or any other secure hardware based solutions for network security, any attacker already does not have authorization to the actual hardware or/and do not have the resources/capabilities to access the hardware. So the TPM focuses solely on the software and network aspect of security.
2. Pros:
    - Provide higher level of security for data center servers.
    - Strengthen image of being a difficult target to attack.

      Cons:
        - Expensive
        - Possible new vulnerabilities if configured improperly

3. A. Exploiting an opening or vulnerability in the hypervisor software.

   B. Gain access to protected memory of the host’s system with hardware device.

   C. Gain access to protected memory of the host’s system with malicious guest operating system.