

Name:

## Information Assurance: Homework 9

No due date. Answer key will be posted December 7..

1. One problem with WEP is that a linear CRC is used to detect changes to the packet. The CRC is encrypted with RC4.
  - a. Assume an attacker has changed the first byte of the packet. He does not know the key sequence. Show how the attacker can compute the new CRC without having knowledge of the key or the plaintext.
  - b. If the packet and CRC had been encrypted using AES in electronic code book or cipher block chaining mode, could the attacker fix up the CRC to hide changes without knowledge of the key? Why or why not?
2. Suppose you are performing an investigation on a computer of someone who has recently left the company. Your boss suspects he had been selling information to your company's competitors, and he would like you to look for evidence.
  - a. What two things should you do to preserve the chain of custody, and make it more likely that the evidence you find would be admissible in court?
  - b. Identify three places you would look for information on the computer.
3. Your boss is concerned about having information leak through emanations scanning. He wants you to analyze option of buying shielded computer monitors and cables for the security sensitive systems vs building a shielded room for all of your organization's computers. Which option would you recommend and why?
4. Explain one problem with the standard SQL view-based security model that Oracle's Virtual Private Database (VPD) attempts to solve.