CSci 4554 Assignment 7

Due Wednesday, April 21st in class

Problem 1 (8 points). Consider a block cipher operating in CBC mode. Mallory (an active attacker) happens to know the plaintext of the first block. Describe how Mallory can modify the transmitted encryption so that she can substitute the plaintext of the first block by anything she wants and remain undetected. Give a short example. Hint: think of the role of IV in the CBC mode. Suggest a way to fix the problem (don't go into details).
Explain why this attack doesn't work in CFB and OFB modes.

Problem 2 (8 points). A (deprecated) Wired Equivalent Privacy (WEP) protocol uses a 24-bit initialization vector to create a stream cipher, in addition to a key shared by all machines in the network. Each packet in the network uses its own IV. A repeated IV means a repeated stream. WEP uses a message authentication code so modifying a ciphertext is not an option. It also uses authentication so impersonating another user is not an option.

- Explain vulnerabilities created by reusing an encryption because of a reused IV. Clearly explain what an attacker needs to do and what they gain.
- Estimate the number of packages that need to be sent within the network for an IV to repeat with at least 50% probability.