Name:

Computer Security: Homework 4

Due September 28, 2009 on compass. Shortened late hand in period to October 2, 2009 to ensure adequate time to post answers before exam.

1. Alice and Bob use Diffie-Hellman to compute a shared secret. They select p=67 and g=13. Alice picks a k_{Alice} of 11 and Bob picks a k_{Bob} of 7.
   a. Show the computations for K_{Alice} and K_{bob}.

   b. Show how Alice and Bob use K_{Alice} and K_{Bob} to compute the shared secret

   c. Which values of p, g, k_{Alice}, k_{Bob}, K_{Alice}, and K_{Bob} can be made public without affecting the security of the key exchange?

   d. Explain how Eve could launch a replay attack against Alice and Bob.

   e. How could the the basic Diffie-Hellman exchange be augmented to protect against your replay attack?

2. Work with Gnu Privacy Guard (GPG). You can access GPG from http://gnupg.org. I have used this on Linux and installed it via yum on my personal system. I am running it on my Windows system via cygwin. It is already be installed on the University Linux systems. Type “man gpg” to check if it is installed. Once you get your GPG system operational perform the following tasks:
   a. Create a key pair and submit your exported public key.

   b. Sign the class public key posted at http://www.cs.illinois.edu/class/fa09/cs461/assignments/cs461-pub.asc with your key. Submit the exported signed key.

   c. Select an ascii file. Encrypt it with the class key and sign it with your key. Submit the signed and encrypted file.

Name:

3. Alice is posting her open source program. It is potentially going to be mirrored at other sites.

   a. She uses DES-CBC to create a hash of her open source program files. What information would she need to make available for any person downloading the program to verify its integrity.

   b. If Alice is worried about Eve launching a birthday attack, what order of number of hash tests would Eve have to perform to find a pair of messages that breaks the hash?

   c. If Eve has access to a machine that can compute 10 million hashes per second, roughly how long would it take her to find a hash collision with better than 50% probability.

   d. Alice changes to use MD5. How many operations would a birthday attack take?

   e. Assuming Eve can still compute 10 million hashes per second, how long would it take for her to find a collision with 50% probability?