### Homework 3

1. (10 pts) Consider the following mutual authentication protocol. Give two different attacks Trudy can convince Bob she is Alice.



>>>The following attacks will work: 1) Trudy opens one connection to Bob and sends the first message, obtaining Bob's reply. Then she opens a second connection and sends

R+1 to Bob. She uses Bob's response to complete the first connection, letting second

one time out. 2) Trudy can record messages 1 and 3 in a legitimate connection between

Alice and Bob, then replay them later. 3) Trudy record messages 1 and 2, and then later challenge Bob with R-1 and finally responds with message 2 she recorded previously.

Any 2 out of 3 attacks are accepted here.

1. (10 pts) Design a secure two-message authentication protocol that provides mutual-authentication and establishes a session key K. Assume that Alice and Bob know each other’s public keys beforehand.

>>>The protocol in Figure 9.23 is an example (in any case, you'll need to use timestamps to use only two messages instead of three messages).

>>> This timestamp-based authentication is not covered in details, so you will not lose any point if you answered wrong here.

1. (10 pts) SSL and IPSec are both designed to provide security over the network.
2. What are the significant similarities between the two protocols?
3. What are the significant differences between the two protocols?
4. For SSL, what protocol does it use to establish security contexts (e.g., keys and algorithms) between two parties? How about IPSec?
5. What will a packet look like if you (IP address A) send a packet to another machine (IP address B) with AH at tunnel mode?

a. They both accomplish essentially the same thing ---authentication, session key,

etc.

b. Complexity, layer at which they operate, etc.

c. SSL Handshake protocol vs. IKE protocol

d. New IP Header| AH Header | Original packet (including old IP header, TCP , and Data)

1. (10 pts) Consider the Kerberos interaction discussed in this chapter.
   1. Why is the ticket to Bob encrypted with KB?
   2. Why is “Alice” included in the (encrypted) ticket to Bob?
   3. In the REPLY message, why is the ticket to Bob encrypted with the key SA?
   4. Why is the ticket to Bob sent to Alice (who must then forward it to Bob) instead of being sent directly to Bob?

This question will be assigned in homework 4.

1. (10 pts) Consider the Kerberized login discussed in this chapter.
2. What is a TGT and what is its purpose?
3. Why is the TGT sent to Alice instead of being stored on the KDC?
4. Why is the TGT encrypted with KKDC?
5. Why is the TGT encrypted with KA when it is sent from the KDC to Alice’s computer?

This question will be assigned in homework 4.

Additional Questions:

5.33: (6 pts for part a) (2 bonus points for part b)

a. The secret is S = 6 and the line is 2x + 3y = 18.

b. The secret is S = 8 and the line is 5x + 6y = 9 mod 13.

Note that in b, you may get different lines. E.g., 3x +y = 8 mod 13, or 7x - 2y = 10 mod 13

but the secret S should be S = 8 mod 13. That is, you may get -5, or 21 or other values.

5.42: (10 pts)

(<http://www.cs.sjsu.edu/~stamp/infosec/files/>)

a. The Alice books, in pdf.

b. it should be easy to do.

c. note: They should be indistinguishable.

5.43: (12 pts)

a. You could randomize (or zero out) the low order RGB bits. Alternatively, you

could replace the bits with some other information of your choosing.

b. If you randomized the bits, you will get nothing useful.

5.48: (6 pts)

a. Symmetric keys and IVs.

b. Randomly selecting primes (RSA) and generating random exponents (DH).

5.49: (8 pts)

a. Given a sequence of such numbers, the remaining number in the sequence can be

determined. If such a sequence was used as a keystream, then a known plaintext

attack might be devastating.

b. Yes, since an attacker might know some plaintext, in which case they would know

the keystream bits.

10.1. (8 pts)

a. The signature SA, since only Alice could have signed it, and Bob can verify the

signature. Note that H is included in SA, and H contains Bob's challenge, RB,

so this provides the replay protection.

b. Trudy would have to break the Diffie-Hellman key exchange by, presumably, solving

an intractable discrete log problem.

c. Put Trudy in the role of Bob. Then after the 4th message, she and Alice will have

agreed on a key K = gat mod p. This does not break the protocol--the authentication

will fail, since Trudy cannot forge the required signature in message 4. So

Alice will terminate the protocol, and she'll never use K.

d. In this version of the protocol, the encryption serves no purpose. However, in the

password version, the encryption does have a purpose (see the next problem).