### 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.

>>> One can merge message #3 with #1 in Fig. 9.17 or 9.18.

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 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?

>>>

a. Ticket Granting Ticket | it serves as a user's “credentials," that is, it enables a

user to request ordinary tickets.

b. This enables the KDC to remain stateless. In effect, the KDC distributes the

database of TGT information to the clients.

c. The KDC--and only the KDC---can decrypt a TGT, which enables the KDC to

“remember" everything it needs to know about the user.

d. Apparently, this serves no purpose, since the TGT is already encrypted and it is

freely passed about (with no additional encryption) in subsequent interactions.

1. (8pts) Describe (enumerate) the insecurity of GSM and then modify the GSM security protocol (Figure 10.25) so that it can provide mutual authentication.

>>> a. answer any four of the following insecurity are sufficient.

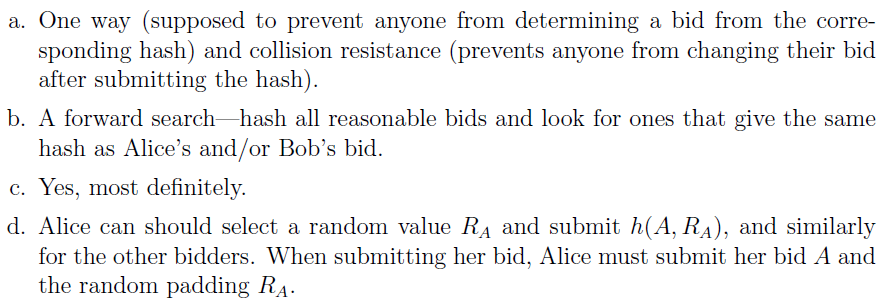
* hash functions A3/A8 and encryption function A5 are easy to break.
* **no encryption** from base station to base station controller
* Attacks on SIM card
* **Fake base station**
* Denial of service is possible
* Base station can replay

b. (4 pts) There are many other reasonable approaches as long as the BS can compute a MAC (or even digital signature if you assume public key infrastructure) or an encryption of a plaintext. Below is an examples.

The mobile could send a nonce R in message one, and the base station could return RAND and Enc(R, Kc), in message 4 .

Additional Questions:

5.17 (8pts):



5.21 (6pts):

Method (i) does not require anything to be stored. Method (ii) uses a stronger

key to encrypt the data, making an attack directly on the ciphertext more difficult.

Method (ii) could also be advantageous when Alice wants to change her password,

since it is not necessary to decrypt/re-encrypt the data.

5.33: (6 pts, part a only)

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

5.42: (10 pts, a, b 4 pts each, 2 pts for c)

(<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.

5.48: (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).