CSE 565 Fall 2018
Homework 5
Due on October 25, 2018, at 9:30am

Each question in this homework is expected to be the result of your own work (as opposed to wisdom found on the internet).

1. (20 points) Consider the following authentication protocol SKID2/SKID3 that uses symmetric cryptography. It assumes that Alice and Bob share a secret key K. SKID2 allows Bob to authenticate to Alice and proceeds as follows:

   (a) Alice chooses a random number R_A and sends it to Bob.

   (b) Bob chooses a random number R_B and sends to Alice $R_B, MAC_K(R_A, R_B, B)$.

   (c) Alice computes $MAC_K(R_A, R_B, B)$ and compares it with what the received from Bob. If the results are identical, then Alice knows that she is communicating with Bob.

   SKID3 provides mutual authentication between Alice and Bob. Steps (a)–(c) are the same as in SKID, and then the protocol proceeds with:

   (d) Alice sends Bob $MAC_K(R_B, A)$.

   (e) Bob computes $MAC_K(R_B, A)$ and compares it with what he received from Alice. If the results are identical, then Bob knows that he is communicating with Alice.

   Answer the following questions about the protocol:

   (a) If Mallory was to mount a man-in-the-middle attack, describe how she is to proceed. What would happen in the protocol as a result of her attack? Can Mallory succeed?

   (b) Repeat part (a) for a parallel session attack.

2. (10 points) What are advantages of SSL over IPsec and vice versa? Under what circumstances one is preferred over the other?

3. (30 points) Read following article: M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, "The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software," in *ACM Conference on Computer and Communications Security (CCS)*, 2012. Available from www.buffalo.edu/~mblanton/cse565/certificates-article.pdf.

   Answer the following questions (all description must be your own, not excerpts from the text):

   (a) What were the main findings and lessons of the article?

   (b) What information did you find to be most surprising? Explain why it was surprising.

   (c) Choose one example covered in the paper and explain what the weakness from the technical point of view was.