ITIS 6200/8200 Principles of Information Security and Privacy

Weichao Wang

Fall Semester of 2018

Homework 4

Hand out: Nov 9th, 2018

Due time: Nov 19th, 2018 before 11:59 pm

Question 1. In a mobile shopping App Bmazon of cell phones, the company uses a third party payment company PayTal. When a user *X* needs to pay for the transaction *T* with the price *P*, her/his cell phone will do the following operations. Here we assume that the user, Bmazon, and PayTal each has a public/private key pair. The public keys are secured by certificates, which means an attacker cannot impersonate PayTal or Bmazon.

1. Bmazon 🡪 User X: [Bmazon, X, E\_pub\_PayTal (Sign\_pri\_Bmazon (X, PayTal, Bmazon, T))],

[Bmazon, X, E\_pub\_PayTal (Sign\_pri\_Bmazon (X, PayTal, Bmazon, P))];

1. User X 🡪 PayTal: [X, PayTal, E\_pub\_PayTal (Sign\_pri\_Bmazon (X, PayTal, Bmazon, T))],

[X, PayTal, E\_pub\_PayTal (Sign\_pri\_Bmazon (X, PayTal, Bmazon, P))];

1. Then the user *X* pays the price *P* for *T*;
2. PayTal 🡪 Bmazon: [PayTal, Bmazon, E\_pub\_Bmazon (Sign\_pri\_PayTal (X, PayTal, Bmazon, T, state = paid))];

In (1), Bmazon sends two messages to user *X* based on his order *T*. The first message contains the order number *T*, and the second message contains the price *P*. Each message is protected by both the private key of Bmazon and public key of PayTal.

In (2) and (3), user *X* cannot open the messages but just forward the messages to PayTal. And he will pay the price *P*.

In (4), PayTal sends a message to Bmazon and tell it that the transaction *T* has been paid. It can ship the goods to user *X*. The message is protected by the private key of PayTal and the Public key of Bmazon.

Now please illustrate, how can a malicious user M pays a very low price and gets a very expensive good. Here we assume that each user can initiate multiple transactions with Bmazon simultaneously [10pt].

Question 2. Mr. Edison decides to run an online version of Zero-Knowledge Proof for a very difficult problem that he claims that he solves (although he does not really solve it). He decides to run 20 rounds of challenge-response for the proof. To do that, he needs to generate 20 pairs of the questions that are isomorphic to the original problem, hashes the concatenation of the 20 pairs of questions, and chooses the first 20 bits of the hash value as the challenges: if the bit is “0”, he will answer the left question in the pair. On the contrary, if the bit is “1”, he will answer the right question in the pair. Now assume that Mr. Edison has an old computer that can generate 20 pairs of such questions and hash the results in 0.01 second. (In other words, he can try 100 times of the generation each second.). How much time (in seconds) does Mr. Edison need so that he has 50% chance to locate 20 pairs of the questions to fool the world? [10 pt]