Submitted By: Ruchira Pokhriyal
Student ID:801085619

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))];

(2) 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))];

(3) Then the user *X* pays the price *P* for *T*;

(4) 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].

Submitted By: Ruchira Pokhriyal
Student ID:801085619

Answer 1:

It is given in the scenario mentioned above that the user, Bmazon and PayTal have public/private key pairs. Since the public keys are secured by the certificates, the attacker cannot impersonate PayTal or Bmazon. Furthermore, The Bmazon is not making use of any session keys valid for that particular transaction.

So first let's assume that the malicious user 'M' wants to buy an expensive product, let's say **A Dell XPS 13 Laptop worth $600.** He would even add a good/gadget which is comparatively cheaper, let's say **a wired mouse worth $14**. Here we assume that the user, Bmazon, and PayTal each has a public/private key pair. Therefore, Bmazon would send the following two messages to malicious user 'M' based on his order number T and price P:

Here,

- $\mathbf{T_{laptop}}\rightarrow$ Order number for Dell XPS 13 Laptop
- $\mathbf{P_{laptop}}\rightarrow$ Price of the Dell XPS 13 Laptop
- Also, $\mathbf{T_{WM}}\rightarrow$ Order number for the wired mouse.
- $\mathbf{P_{WM}}\rightarrow$ Price of the wired mouse.

Therefore:

- Bmazon → User M: [Bmazon, M, E_pub_PayTal (Sign_pri_Bmazon (M, PayTal, Bmazon, T_{laptop}))], [Bmazon, M, E_pub_PayTal (Sign_pri_Bmazon (M, PayTal, Bmazon, P_{laptop}))];

- Bmazon → User M: [Bmazon, M, E_pub_PayTal (Sign_pri_Bmazon (M, PayTal, Bmazon, T_{WM}))], [Bmazon, M, E_pub_PayTal (Sign_pri_Bmazon (M, PayTal, Bmazon, P_{WM}))];

As shown below, the malicious attacker 'M' will then forward two packets to PayTal, for order number of the Dell XPS 13 Laptop and the price of the wired mouse i.e. price of the cheaper good in place of the actual price of the expensive good.

- User M → PayTal: [M, PayTal, E_pub_PayTal (Sign_pri_Bmazon (M, PayTal, Bmazon, T_{laptop}))], [M, PayTal, E_pub_PayTal (Sign_pri_Bmazon (M, PayTal, Bmazon, P_{WM}))];

So, as described above, while sending the transactions to PayTal, the malicious user 'M' will simply replace **[Bmazon, M, E_pub_PayTal (Sign_pri_Bmazon (M, PayTal, Bmazon, $\mathbf{P_{laptop}}$))];** with **[Bmazon, M, E_pub_PayTal (Sign_pri_Bmazon (M, PayTal, Bmazon, $\mathbf{P_{WM}}$))];**

By doing this, the malicious user 'M' will be able to pay a much lower price of P_{WM} for a very expensive good T_{laptop}.

Now, Paytal will send payment confirmation of T_{laptop} to **Bmazon** as follows (Here we assume that each user can initiate multiple transactions with Bmazon simultaneously.):

- PayTal → Bmazon: [PayTal, Bmazon, $E_{\_pub\_Bmazon}$ ($Sign_{\_pri\_PayTal}$ (M, PayTal, Bmazon, T_{laptop}, state = paid))];

Thus, in this way, the malicious user 'M' will get the expensive good T_{laptop} for a much lower price of P_{WM} i.e., user 'M' will pay a very low price and gets a very expensive good.

Submitted By: Ruchira Pokhriyal
Student ID:801085619

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]

Answer 2:

The scenario mentioned above is a non-interactive zero knowledge proof, since the challenger isn't involved.

Now, Mr. Edison decides to run 20 rounds of challenge-response for that proof. So, let's assume that to get the first 20 bits to be either 0 or 1, Mr. Edison needs to run 'X' rounds.

Therefore, the chance that in 'X' rounds, the first 20 bits are all '0' at least one time, would be given as follows:

$$\rightarrow 1 - \left[1 - \frac{1}{2^{20}}\right]^{x}$$

Hence, for Mr. Edison to have 50% chance to locate 20 pairs of the questions (where the first 20 bits of the hash be all 0s in 'X' rounds)

$$\rightarrow 1 - \left[1 - \frac{1}{2^{20}}\right]^{x} = 0.5$$

$$\rightarrow \left[1 - \frac{1}{2^{20}}\right]^{x} = 0.5$$

By applying logarithm on both sides, we get:

$$\rightarrow x\ log\left[1 - \frac{1}{2^{20}}\right] = \log(0.5)$$

$$\rightarrow x \log\left[1 - \frac{1}{1048576}\right] = \log(0.5)$$

$$\rightarrow x \log\left[\frac{1048575}{1048576}\right] = \log\ (0.5)$$

$$\rightarrow x = log_{\frac{1048575}{1048576}}[0.5] \qquad [Since\ \log m/\log n = log_n m]$$

$\rightarrow x = 726817\ Times,$ which means that Mr. Edison must generate 20 such pairs of questions 726817 times.

Now, since Mr. Edison's computer generates 100 times per second, the amount of time 'T' required for 726817 times generation would be given by:

$$\frac{726817}{100} = 7268.17\ Seconds$$

Therefore, $\mathbf{T = 7268.17\ Seconds}$

Submitted By: Ruchira Pokhriyal
Student ID:801085619