CS 161 – Computer Security
Instructor: Tygar
13 October 2015

Homework 5 Answer Set

Notes

- Homework 5 is due on 13 October 2015 at 3PM.
- Please work on this homework individually – no collaboration allowed.
- Please keep your answers brief
- Submit this homework using Gradescope.

Please start the answer to each question (including subquestions) on a new page

1. Show a man in the middle attack on the following authentication protocol:

$A \rightarrow S$: A, B, Na
$S \rightarrow A$: $A, B, \{A, Na, Kab\}_{Ka}, \{B, Na, Kab\}_{Kb}$
$A \rightarrow B$: $A, B, \{B, Na, Kab\}_{Kb}$

$A \rightarrow M$: A, B, Na
$M \rightarrow S$: M, B, Na
$S \rightarrow M$: $M, B, \{M, Na, Kmb\}_{Km}, \{B, Na, Kmb\}_{Kb}$
$M \rightarrow S$: M, A, Na
$S \rightarrow M$: $M, A, \{M, Na, Kma\}_{Km}, \{A, Na, Kma\}_{Ka}$
$M \rightarrow A$: $A, B, \{A, Na, Kma\}_{Ka}, \{B, Na, Kmb\}_{Kb}$
$A \rightarrow B$: $A, B, \{B, Na, Kmb\}_{Kb}$

Now A and B think they are talking to each other, but A is using Kma (also known to M) and B is using Kmb (also known to M) allowing him to perform the MITM attack.

2. For questions 2 and 3, use the web site https://blockexplorer.com. For question 2, examine block 378741.
    a. How many transactions are there in this block?

444 transactions

    b. The block reward is 25 BTC, but how much in total did the miner who found this block receive for doing so? What accounts for the discrepancy?

25.07264926 BTC. The extra amount is transaction fees.

    c. Look at the fourth transaction (the third after the coinbase transaction). How many inputs and outputs are there? What is the most likely explanation of why the recipients did not receive the same amount?

One input, two outputs. One of the outputs was "change" from the transaction.

d. What is the sum of the inputs? What is the sum of the outputs? What are the first six characters of the address of the recipient of the difference between (inputs – outputs)?

Input: 8.81701738 BTC. Outputs: 8.81612307. Recipient address: 1M5hoG…

3. Examine block 378732.
    a. What is unusual about this block? What is the most likely reason that this unusual occurrence happened?

It only has one transaction – the coinbase transaction. This happened because this block was mined only three seconds after the previous block was mined and there were no transactions to include.

b. What nonce did this miner find?

2933092036

c. On average, how many hashes would you expect a miner to need to try to find this particular nonce?

$60813224039.440346 \times 2^{32} \approx 2.6 \times 10^{20}$

d. Look at all the transactions that the miner who mined this block has received (state the precise time (in PDT) that your figure is accurate as of – which should be a time between 10/13/15 and 10/20/15). Roughly how much is this in US dollars? How has this miner managed to receive so many bitcoins in transactions?

As of 1:56PM on 10/13/15, 11789.04104597 BTC, or approximately 2.9 million US dollars. AntMiner is a mining pool which uses specialized equipment (advertised on https://bitmaintech.com/product.htm)