CSC318/M18 – Cryptography and IT-Securityy

Phillip James

Lab Class 7 – Tuesday 04/04/2017

This week's lab will consider possible attacks on Bitcoin in terms of attacking the underlying Blockchain technology.

As we have seen in Lectures, Bitcoin relies upon the concept of "proof-of-work". That is, Bitcoin operates via a distributed consensus, in which every participant agrees on the true state of the network, including the full transaction history and how many coins each address controls (i.e, the blockchain). Here, participants trust the state of the blockchain due to the amount of work that has been required to compute the chain, and the fact that there is an easily verifiable link between a block and it's predecessor. The bitcoin network will always accept, i.e. confirm, the longest proof-of-work chain.

□ Task 1

Consider a Bitcoin network with only two participants with equal computation power. Does the Bitcoin "proof-of-work" concept provide a trusted block chain?

□ Task 2

Consider a Bitcoin network with only 3 participants with equal computation power. Can you think of a possible attack on such a network? Explain how such an attack would work.

□ Task 3

Based on your answer to Task 2. Can you think of a general attack on the current Bitcoin network? Explain how such an attack would work.

□ Task 4

Consider the following scenario:

A group of generals, each commanding a portion of an army, encircle a city. These generals wish to formulate a plan for attacking the city. The generals must decide and agree on a time to attack the city, if the attack is to be succesful. It has been decided that any general who feels like it will announce a time, and whatever time is heard first will be the official attack time. The problem is that announcement of an attack time is not instantaneous, and if two generals announce different attack times at close to the same time, some generals may hear one time first whilst other generals may hear the other time first.

Explain how a "proof-of-work" mechanism, like the one used in Bitcoin, can be used to solve the above problem. (Hint: the first problem to be solved should be based upon the attack time that has been heard).