How to extract repeated random numbers used in the Bitcoin blockchain

Jason Papapanagiotakis

This document is a step-by-step tutorial on how to extract random numbers used more than once for the elliptic curve digital signature in the Bitcoin blockchain.

Introduction

Randomly choose the same 32-byte long number more than once should happen only with negligible probability but due to various reasons this phenomenon can be observed in the public Bitcoin ledger. This can lead to different types of attacks as described by Courtois [1] where some or all users can steal the contents of a wallet that used one of those "bad randoms". This makes the discovery of those numbers and the study of the way they appear a worthwhile goal.

Prerequisites

In order to recover all reused random numbers, the complete Bitcoin blockchain is needed in a database. To do this follow the instructions found here. Once you have completed those steps you should add two extra columns, the inputscript and the scripted and then proceed to the next section.

Extracting reused random numbers

In this step you are going to create two additional tables in the database that was previously created. The first table will be called *Randoms* and contain a list of all random numbers used together with the ID of the *inputscript* in which they appeared, finally, the second table will be called *BadRandoms* and will store all random numbers that appeared more than once together with a counter of how many times they have been used.

[1] Courtois, N.T., Valsorda, F. and Emirdag, P., 2014. Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events.

In order to create the two tables mentioned, you will need Microsoft SQL Server Management Studio that should have been installed together with SQL Server, if not, download and install the corresponding version for your database, this software is free.

The next step is to download the *RandomsToTables.sql* script from here open it with SQL Server Management Studio and execute it (F5), this will take up to 3 hours depending on the hardware and the load of the machine. Once the query is completed you can look at the two new tables.

Generating webpage with reused random numbers

The final step of this tutorial is about how to generate a webpage that contains the random numbers used more than once together with the transactions in which they appeared.

1. Download and install Python 2.7
2. Next you will need *pymssql*, a Python module that makes the connection to SQL Server very easy.
    a. Download it from here and place the file into C:/Python27
    b. Now install it using pip command line, cd into C:/Python27 and run the following: pip install pymssql-2.1.1-cp27-none-win_amd64.whl
    c. Instructions to enable the use pip can be found here
3. Download the python script db2wb.py from here
4. Edit the 6th line of the file and insert the details of your database (user/password)
5. Run the script from command line: *python db2wb.py*

After those steps a file named index.html should appear on the same directory as the python script. Open it with any web browser. You can download the final result from here based on data collected the 07/03/2016.