BLOCKCHAINS, CRYPTOCURRENCIES, AND SMART CONTRACTS CS 5433

CORNELL TECH

HOMEWORK # 3

Joe Abi Sleiman – jba68

05/11/2018

TABLE OF CONTENTS

Contents

Problem 1 – Tokens and Simple Smart Contracts

Deployed contract address: 0xc5f9f03f4f404d1564f0d587a34e4e92aab93f3c

Problem 2 - Gaming Contracts

Monster address: 0x02AC08Db45f5702AF1cF6cF50cFe3291b93DE552

Problem 3 - Rafael’s Gambit

(1) Master Key: A5E5597A41B3D86D5523D64BE9737E64C2EECCFEE8C5EEC3

(2) One potential vulnerability that the backdoor might succumb to is transactions getting reorder on the blockchain. For example if a user makes multiple transactions at the same time, these transactions might get pushed onto the blockchain in an order different than that by which the user made them. In this case, the scheme of the backdoor fails. One potential way to improve this is to force a delay between user transactions so that we preserve the order of transactions. Another vulnerability the backdoor has is that it can be exploited by someone other than the wallet owner, and potentially before them. One way to remedy this is to leak an encrypted version of the key rather than the key itself. Using a public key encryption scheme, we can leak a signed version of the key and then use the private key to reconstruct the original key (so we encrypt the cipher text and leak that encrypted version – then when we reconstruct that version we use the secret key to decrypt).

(3) One potential way would be to leak more than 1 bit per transaction. We can choose to leak 2 bits for instance and that would require half the transactions as the key length.

Problem 4 - What Anonymity?

The approach I used was based on comparing transaction amounts sent from input addresses and those amounts received at output addresses, and subsequently trying to link them. As the amounts sent and received were different, the mapping process at that point became quite straightforward.

Using blockchain.info, I summarized the input addresses and their corresponding transactions (bitcoins sent into the tumbler). The results can be found below:

Input	Bitcoin Sent
1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM	0.025
135g5Es7VXvbaAkwzguv7q7xaSSTifav5H	0.05
1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz	0.01
1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ	0.02

Similarly for the output addresses:

Output	Rceived
18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp	0.00987
1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7	0.024413
1BCaztysy2paguXjuC8c652vckNMks69ce	0.019865
13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT	0.04874

At this point, I looked for transactions of similar amount, taking into consideration a small delta that would correspond to the transaction fee. The results are below:

Input		Output
1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM	**Corresponds To**	1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7
135g5Es7VXvbaAkwzguv7q7xaSSTifav5H		13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT
1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz		18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp
1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ		1BCaztysy2paguXjuC8c652vckNMks69ce