CS 5433 – Blockchains, Cryptocurrencies, and Smart Contracts

Assignment 3

Name: Sunny Ladkani *Spring 2020*

Q 3.2 What vulnerability or vulnerabilities does our backdoor have? Provide a scenario in which the backdoor can fail despite a user actively using our backdoored wallet. How might it be improved?

Answer Now that we can capture the secret key by looking at the transactions, this opens us to - watch the balance in the account, transfer all the money from Ari's wallet to any wallet of our choice.
This can fail if the wallet can have multiple secret keys.
One way to improved this is to use the secret key XOR with transaction number to switch the signature key to 1. This provides randomness to the attacker, but is completely controlled by the owner of the secret key.

Q 3.3 How might the scheme be modified so that a seed can be exfiltrated from a wallet using fewer transactions?

Answer We can reduce the number of transactions by trying few combinations of key using brute force. Suppose we have 191 transactions, we can use 2 different bit values at beginning and end to get the secret key.

Q 4 Deanonymize the mixers

Answer By looking at the amount recieved by the output, we can figure out what is the only possible input in the transaction that can support the output. For example, an output of 0.01 is only possible by an input of 0.01. Using the proximity approximation, I was able to match the input with output transaction.

Inputs	Outputs (Matched)	Outputs	Sent	Recieved	Recieved Back
1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM	1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7		0.025		0.025
135g5Es7VXvbaAkwzguv7q7xaSSTifav5H	13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT		0.05		0.05
1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz	18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp		0.01		0.01
1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ	1BCaztysy2paguXjuC8c652vckNMks69ce		0.02		0.02
		18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp		0.01	
		1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7		0.0244	
		1BCaztysy2paguXjuC8c652vckNMks69ce		0.0199	
		13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT		0.05	