Raluca Ada Popa
Spring 2018

CS 161
Computer Security

Discussion 12

Week of April 23, 2018

Question 1 ***Mining Pools*** **(20 min)**

On April 20th, 2018, the estimated hash rate of the bitcoin network was $\approx 3\times10^{19}$ hashes/sec. The DragonMint 16T, one of the most powerful ASIC miners in the world, can do $\approx 1.5 \times 10^{13}$ hashes/sec.

(a) Alice has just purchased a DragonMint 16T and wants to start mining. Given that a block is mined by the whole network every 10 minutes on average, how long does Alice expect to wait until she mines a block?

(b) Why might Alice want to form a pool with other individuals like her, even though her expected income from bitcoin mining will go DOWN due to the cost of pool overhead?

(c) Alice wants her pool to mine at least a block per week on average. How many DragonMint 16T's would need to join her pool to accomplish this?

(d) Some members of Alice's pool are using slower hardware, and some only wish to mine at night when electricity is cheap. How should Alice fairly distribute the pool's income amongst the members, when some are contributing more than others? How can she efficiently estimate how much each member contributed?

(e) Alice's pool pays proportionally, but Bob tells Alice that he thinks this is a bad idea. Bob says that mining for her pool becomes less profitable when they haven't found a block in a while. Why might this be, and how could Eve take advantage of pools like Alice's to make more profit than someone who simply mines for one pool forever. Also, what are some ideas for how Alice could resolve this issue?

Question 2 ***Consensus*** **(10 min)**

(a) Eve is buying a penguin from Alice. Eve generates and then sends Alice a valid transaction message, which transfers 100BTC to Alice's wallet. The signature is correct, and Eve has enough funds to make this transaction. Upon receiving and verifying the transaction, Alice gives Eve the penguin. What attack could Eve do to avoid paying Alice the 100BTC?

(b) What can Alice do to make sure she's actually received the money?

(c) Alice tells Eve she will wait until the next block is mined to determine if the transaction went through. Given that the last block was mined 9 minutes ago, and a block is mined every 10 minutes on average, how long does Eve expect to wait?

(d) Alice is unsure if waiting for the next block is secure enough. Let's say Eve controls a mining pool with a large fraction of the total network hash rate, and is trying to perform an attack similar to the one from part 1, even though Alice is now waiting for the next block to be mined with her transaction in it before releasing the penguin. What does Eve need to do to pull off the attack?

Question 3 ***Bitcoin Potpourri*** **(15 min)**

(a) Tired of generating new addresses for every transaction, Bob decides to use the same address over and over again for his transactions. Why might this be a bad idea?

(b) Alice wants to "anonymize" her bitcoin by moving them to new addresses without them being traced (for totally benign reasons). How can Alice, and many other users like her, accomplish this together?

(c) Alice currently uses a wallet application on her laptop to store her bitcoin. Alice is concerned about malware on her computer making her bitcoin vulnerable. She wants to use her laptop to send bitcoin, but doesn't want her bitcoin to be stolen even if her laptop is compromised. What are some ways she could accomplish this?

(d) Alice decides to use a hardware wallet to store her bitcoin. Her wallet looks like a usb drive with one button on the side. When she wants to send bitcoin, she inputs the transaction details into an application on her computer, and then presses a button on her wallet to confirm the transaction. When the button is pressed, it signs the transaction proposed to it by the computer. The button ensures transactions are only signed when Alice intended them to be, and the wallet's internals ensure no information about her private keys are ever leaked to the computer, only signatures. Is this scheme secure? How could attacker that compromised Alice's computer steal her bitcoin? What can Alice do to prevent this?

Question 4 ***Review: Crypto*** **(10 min)**

(a) Let E_0 be the AES block cipher with a key of all zeros. What property is E_0 missing to be a hash function?

(b) What is one advantage of CTR over CBC mode?

(c) Say RSA signatures are used with a secure hash function to create a signature S on the message M. What property of the hash function prevents an attacker from creating another message M' such that S is a valid signature on M'?

(d) Alice decides that she will generate her password by finding the SHA256 hash of an English word. True/False: this new password is more secure.

(e) Boogle decides to add client-side password hashing to all their login forms, using Javascript. This way, even if a TLS connection is compromised, the attacker will still not be able to login as that user. What is wrong with this scheme?