Hacking the Global Economy with GPUs

or How I Learned to Stop Worrying and Love Bitcoin

By Skunkworks

-First time DEFCON speaker and attendee
-Electrical Engineering Undergrad at a Major University
-Hardware Geek with diverse interests
-Not affiliated with Lockheed-Martin!
-Not affiliated with Bitcoin!
-Basic introduction with in-depth portion

-This talk may have been updated!

WHY was Bitcoin created?

- High fees with current e-payment solutions
- Paypal (and others) playing big brother
- Increase in decentralized digital technologies, eg torrents

WHAT is Bitcoin and WHO made it?

- A decentralized Peer-to-Peer currency
- No central authority
- Transactions verified by peers
- Over $100,000,000 US in value
- “Money” printed by GPUs
- Enigmatic developer Satoshi Nakamoto who left in 2010

The Economics of Bitcoin

Hackers? In *my* Economy? It's more likely than you think!

- Bitcoin is Fiat currency, just like USD
- It has built in deflation, never more than 21,000,000 BTC
- Can be traded down to 0.00000001BTC
- Generated by GPUs (or ASICs?), backed by the marginal utility of a Semi-Anonymous virtual currency
- Not a Ponzi Scheme, but the early adopters got rich
- Price up over 200,000%, rampant speculation due to media coverage and novelty of currency type
- Will likely find an equilibrium price due to many factors

A chart is fine too...

- $0.06 to $30 in a few months, this scale is logarithmic!
- Who made big bucks?

SHA-256, the block chain and GPUs

- Bitcoin algorithm based on SHA-256
- GPUs are hundreds of times faster than CPUs
- Every transaction is hashed and becomes part of the “block chain”
- Coins stored in a wallet.dat file
- The entire network is many times more powerful than folding@home or the RIEKN supercomputer
- Mining pooled to a large degree, fees are making top pool operators rich

Attack Vector: Botnets and Bitcoin

- These attacks rely on overwhelming the network with illegitimate clients or a lot of hashing power
- Forking the block chain if you control over 50% of the network hashing power
- “Cancer nodes” refusing to relay blocks and process transactions, allowing double-spending and network stoppage
- Half of the hashing power would represent over $120,000 per day for the attacker, making an attack attractive
- A botnet for financial gain that doesn't harm the network could be running today
- A supermassive botnet can create total market-power

Attack Vector: Botnets and Bitcoin

- “Timejacking” a node requires a fairly small botnet
- Bitcoin will drop a connection to a peer sending too much data, making DoS a bit harder, at least requiring more nodes.
- No way to tell the difference between a botnet that “plays by the rules” and a bunch of legitimate users
- The most lucrative use of a botnet in the long term may not be attacking the network, but contributing to it
- “Rule abiding” botnets could represent a significant fraction of today's hashing power and we wouldn't know

Attack Vector: Pickpocketing wallet.dat

- Not all users are level 31337 computer scientists
- wallet.dat is unencrypted
- Many daytraders and speculators, a few dimwits
- Specialized Trojan Horses target Windows
- Limewire. Wait, Limewire!?
- Don't put all your eggs in one unprotected basket, just ask “Allinvain” who lost $500,000 in a single wallet.dat file
- See en.bitcoin.it/wiki/Securing_your_wallet

Attack Vector: Third Parties

- Third-parties such as currency exchanges and giftcard services provide fertile attack ground, each attack would be site specific
- Mt. Gox 0wned, had old unsalted password hashes, $9 million attempted sell off of compromised accounts crashed market, forced a freeze on trading for almost a week
- Deepbit.net 0wned, unspecified amount taken when payout addresses changed, cost eaten by site admin
- Many bitcoin related sites don't yet take as security-conscious a view as established banks

Attack Vector: The Gullible Users

- Bitcoin 419 Scams
- Fake Giftcard payouts
- Fake investment sites
- Fake currency exchanges
- “I'm a Nigerian Prince who has won 89 Million Bitcoins and I just need you to pay my Bitcoin transfer fee so you can claim 10%”
- There is no patch for human stupidity, a fool and their bitcoins are soon parted

Attack Vector: High Frequency Trading

- Constant computerized trading of a financial holding based miniscule market fluctuations with the intent to turn a small profit thousands of times
- “High rollers” can assert partial market power, execute high frequency trading with good results by single handedly moving the market
- High Frequency Trading is quite slow on the actual Bitcoin network, would be carried out through third parties

Attack Vector: The “Finney” Attack

- Accepting a 0-confirmation transaction creates the problem
- Attacker sends coins to himself in an unbroadcasted block, “spends” coins, the coins sent to the attacker's own address take precedence
- The problem with a bitcoin vending machine

Drugs, Weapons and Money Laundering
Oh, so that's where the bad press is from?

- Silkroad marketplace trades in (mostly) illegal wares, relies on the supposed anonymity of Bitcoin for plausible deniability of financial transfers proceeding shipment
- Money laundering is trivial with Bitcoin, again relying on the supposed anonymity of the network
- Represents a nice shiny object for the media to peck at

P.W.N.T. by a L.E.A.: So maybe Bitcoin isn't so anonymous after all...

- It is public information what address has what bitcoins, and from who they were received
- If you can tie a few addresses to a few people, and people use only one address, anonymity is out the window
- High level network monitoring can possibly identify many bitcoin users
- eWallet providers are somewhat of a solution, but introduce third party issues

ASICs: The Darkhorse

- A few watts per chip, versus 100+ for a GPU
- Very high upfront development costs and effort
- Possibility to create network-scale hashing capability with millions in investment
- Already deployed in at least one mining operation
- May already represent a substantial portion of network hashing power in relative secrecy

I accidentally the GPU market...

- Global shortages of AMD Radeon HD 5000 series GPUs
- Best price/performance GPUs selling used for upwards of 150% retail on ebay, craigslist, etc
- Individual buyers hoarding dozens of GPUs for resale or mining
- Sellouts within minutes of restocking on Newegg
- Radeon HD 6000 series and Nvidia are lower performing
- Radeon HD 7000 series leaked specs reveal rough comparability with 5000 series for bitcoin mining

Miscellaneous

- “But I'm growing currency, officer” - high power bill leads to fruitless raid of suspected weed growing operation
- buttcoin.org, humorously pointing out flaws in Bitcoin
- bitcoinminingaccidents.com, heat stroke case

THE END

- Questions?