How to use Silk Road for ~~fun and profit~~

EDUCATIONAL PURPOSES ONLY

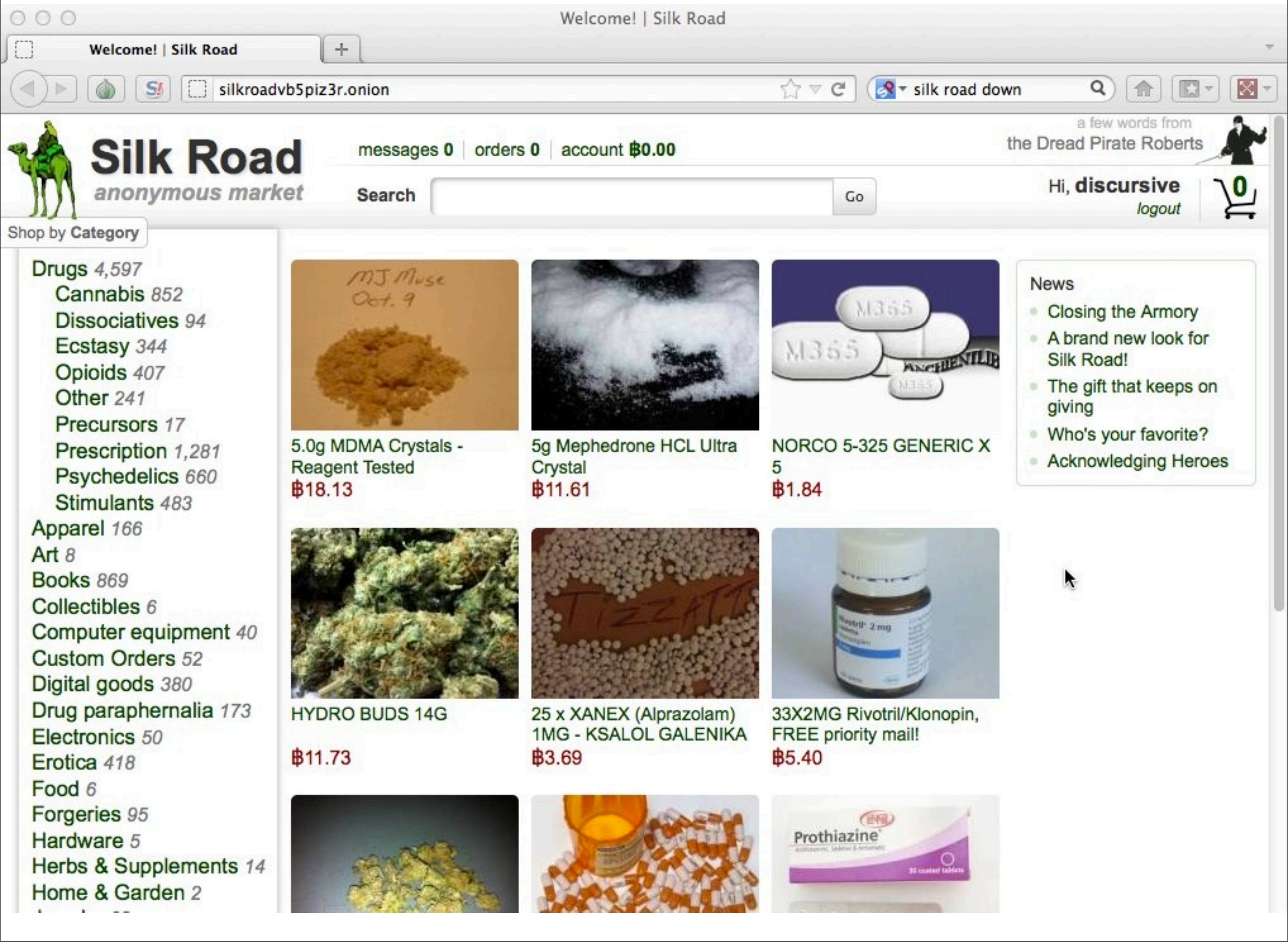
Building systems using open source cryptographic primitives

Who am I?

- garrettr@riseup.net
- @garrettrobin
- honestappalachia.org
  - Anonymous document submission platform for whistleblowers
  - Similar design strategies

What is Silk Road?

- An online marketplace specializing in contraband



Silk Road
anonymous market

messages **0** | orders **0** | account **฿0.00**

a few words from
the Dread Pirate Roberts

Search [ ] Go

Hi, **discursive**
logout
0

Shop by **Category**

- Drugs *4,597*
  - Cannabis *852*
  - Dissociatives *94*
  - Ecstasy *344*
  - Opioids *407*
  - Other *241*
  - Precursors *17*
  - Prescription *1,281*
  - Psychedelics *660*
  - Stimulants *483*
- Apparel *166*
- Art *8*
- Books *869*
- Collectibles *6*
- Computer equipment *40*
- Custom Orders *52*
- Digital goods *380*
- Drug paraphernalia *173*
- Electronics *50*
- Erotica *418*
- Food *6*
- Forgeries *95*
- Hardware *5*
- Herbs & Supplements *14*
- Home & Garden *2*

5.0g MDMA Crystals - Reagent Tested
฿18.13

5g Mephedrone HCL Ultra Crystal
฿11.61

NORCO 5-325 GENERIC X 5
฿1.84

HYDRO BUDS 14G
฿11.73

25 x XANEX (Alprazolam) 1MG - KSALOL GALENIKA
฿3.69

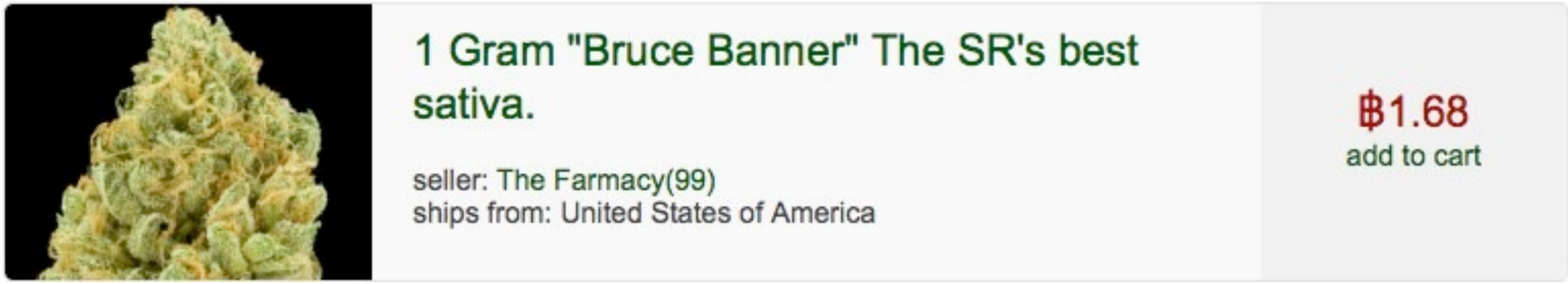
33X2MG Rivotril/Klonopin, FREE priority mail!
฿5.40

News

- Closing the Armory
- A brand new look for Silk Road!
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes

Price

- Prices on Silk Road are listed in Bitcoin
- Depends on value of Bitcoin, which tends to fluctuate (sometimes wildly)
- Currently $11.88 to 1 BTC (Sun Oct 14 15:35:25 PDT 2012)



1 Gram "Bruce Banner" The SR's best sativa.

seller: The Farmacy(99)
ships from: United States of America

฿1.68
add to cart

฿1.68 * $11.88 = **$19.9584**

What is Silk Road?

- Goal is to allow users and site operators to avoid investigation from law enforcement
- So far, so good (AFAWK)
  - CMU researcher estimates $1.9 million in sales/mo., steady growth
  - Recent FOIA requests denied (unclear if it is a target)
  - Other, similar sites have been taken down

Case Study: Farmer’s Market

- Similar site to Silk Road
- Also used Tor hidden service
- Investigation not discussed in indictment, but likely due to their use of PayPal, Western Union, etc.
- http://nakedsecurity.sophos.com/2012/04/23/farmers-market-tor-narcotics/

Design Goals

- Client
  - Communicate anonymously
  - Pseudo-identity for trust
  - Transact anonymously
- Server: site operators
  - Don’t get shut down

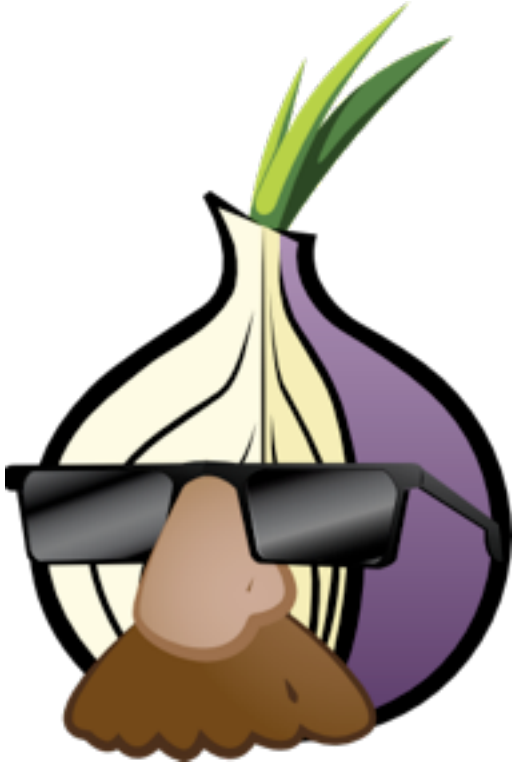
Design Goals

- Client
  - Communicate anonymously → Tor
  - Pseudo-identity for trust → GPG
  - Transact anonymously → Bitcoin
- Server: site operators
  - Don’t get shut down

Adversary

- Law Enforcement
  - US: FBI, DEA
  - https://www.eff.org/pages/tor-and-https

http://silkroadvb5piz3r.onion/



.onion?

- Tor Hidden Service
- Only accessible over Tor
  - Or clearnet Tor proxy like onion.to, tor2web (this does *not* provide client anonymity)
- Provides anonymity for the client **and** server. Bonus: end-to-end encryption
- https://www.torproject.org/docs/hidden-services.html.en

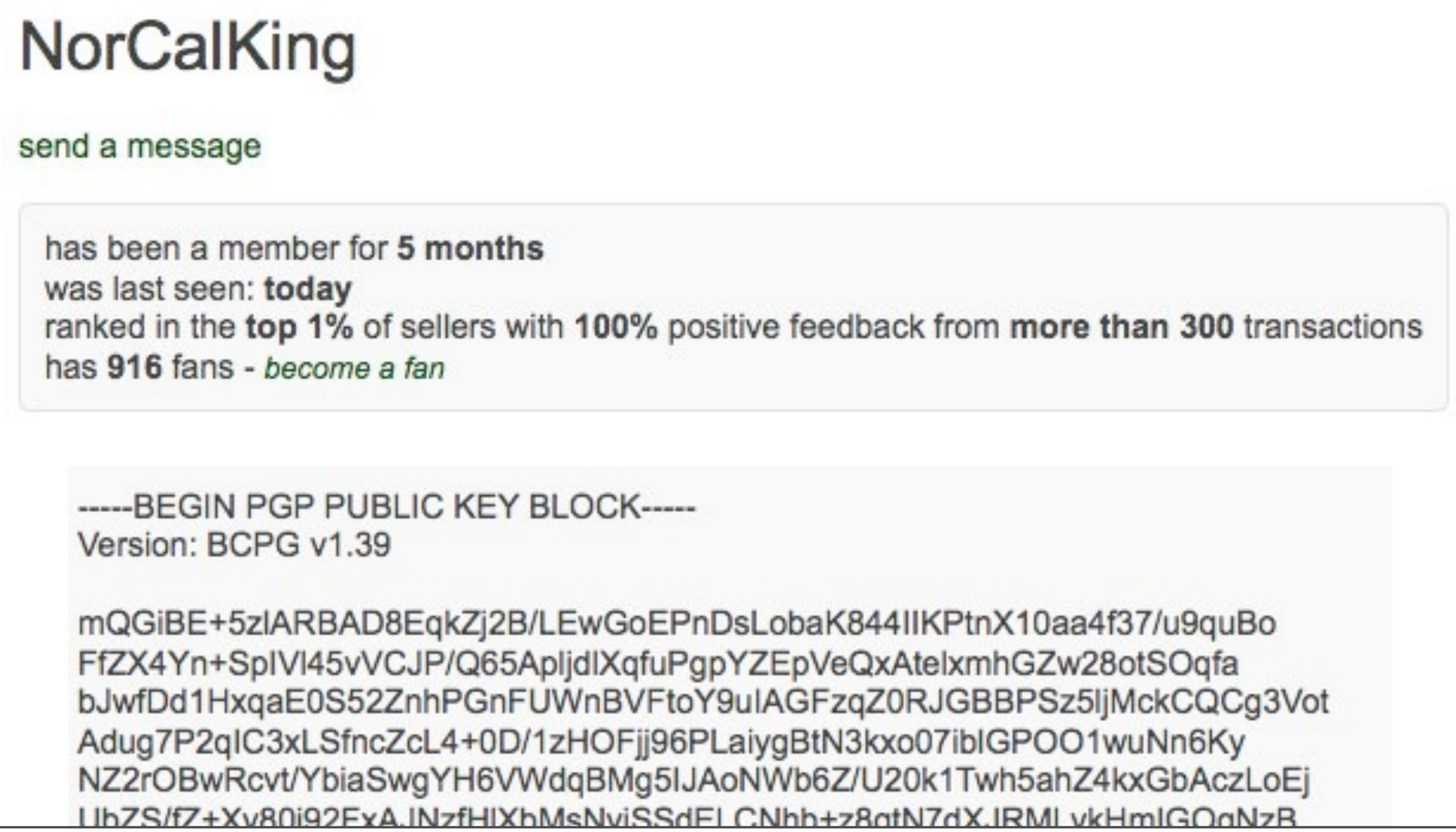
Attacking hidden services Part 1: the protocol

- Original hidden service protocol was flawed.
- “Locating Hidden Servers” (Øverlier and Syverson 2006)
- (Partial) Solution: entry guards. Open problem.

Attacking hidden services Part 2: the hidden service

- Ultimately a hidden service is any TCP-based service. Commonly a web server, can have fun with SSH etc.
- Traditional website vulns. apply: PHP exploits, SQL injections, etc.
- DDoS is not so useful: "attackers forced to attack the onion routing network because they do not know Bob's IP address"

- 2 purposes: encryption and signatures
- See something you like? The vendor’s page usually has their public key on it.



NorCalKing

send a message

has been a member for **5 months**
was last seen: **today**
ranked in the **top 1%** of sellers with **100%** positive feedback from **more than 300** transactions
has **916** fans - *become a fan*

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG v1.39

mQGiBE+5zIARBAD8EqkZj2B/LEwGoEPnDsLobaK844IIKPtnX10aa4f37/u9quBo
FfZX4Yn+SplVl45vVCJP/Q65ApljdlXqfuPgpYZEpVeQxAtelxmhGZw28otSOqfa
bJwfDd1HxqaE0S52ZnhPGnFUWnBVFtoY9uIAGFzqZ0RJGBBPSz5ljMckCQCg3Vot
Adug7P2qIC3xLSfncZcL4+0D/1zHOFjj96PLaiygBtN3kxo07ibIGPOO1wuNn6Ky
NZ2rOBwRcvt/YbiaSwgYH6VWdqBMg5IJAoNWb6Z/U20k1Twh5ahZ4kxGbAczLoEj
UbZS/fZ+Xv80i92ExAJNzfHIXbMsNviSSdELCNbb+z8qtN7dXJRMLvkHmIGOqNzB
```

GnuPG

- Encrypt message using their public key, send it to them (via Silk Road's internal messaging system) with your public key
- Achieves both goals:
  - Only you and the vendor and read the messages you send back and forth (not even Silk Road can read them)
  - Gives a degree of verification of vendor

Bitcoin

- Online transactions with national currencies using established payment providers (such as Paypal, Google Checkout, Amazon, etc.) are extremely easy for law enforcement to track.
- Bitcoin is used as a (possibly) anonymous and decentralized currency for transactions on Silk Road.

How's it work?

- A "coin" is a chain of digital signatures
- Every user has a public key and a private key.
- To exchange a coin:
  - Digitally sign the hash of the previous transaction and the public key of the next owner, add to the end of the coin

Double-spending

- Problem - payee can’t verify they’re the only person who received the coin.
- Double-spending is a fundamental problem in distributed electronic currencies.
- Old solution: central bank or “mint”
- New solution: distributed timestamp server and proof-of-work

Privacy with Bitcoin

- All transactions are public!
- Bitcoin is anonymous *if your public key is anonymous*.
- This is hard - who do you trust? If you send or receive money from anyone, they will learn your public key.

Privacy with Bitcoin

- Furthermore, if *any* public key of a recent transaction in the block chain has been compromised, can try to work through transactions to identify others as well.
- Sometimes people accidentally (or intentionally) publish their public keys online. That's ok as long as you're not concerned about anonymity.

Privacy with Bitcoin

- First step: try to keep your public key anonymous
- Second step: don't reuse the same keypair. Generate a new one for each transaction.
  - If one public key is compromised, only one transaction is compromised (instead of all of them)

Bitcoin “mixing”

- also called a tumbler service
- Put your not-so-anonymous bitcoins into a big pool with other people’s bitcoins
- Withdraw the same amount you put in (minus a transaction fee, of course) of random coins
- eWallet is one such service. Silk Road runs its own - unknown how good it is

Problems

- If you try to anonymize more than about 10% of the coins total in the mixing service, you're going to increase the probability of getting your own coins back.
- Ultimately, we're back to needing a trusted third party.

Bitcoin Applications

- Connections to peers are unencrypted by default. Vulnerable to network surveillance.
- Even if using Tor or similar encryption layer, attacker can try to do timing/ correlation attacks.

Getting Bitcoins

- is hard. Options
  - Mine them (late to the game)
  - Do stuff for people who will pay you in Bitcoin
  - Exchange official currency for Bitcoin

Exchanges

- Mt. Gox is the most well known one.
  - Silk Road derives its prices from Mt. Gox
  - Been hacked numerous times, passwords compromised, lots of Bitcoin stolen

Exchanges

- AFAIK, it's pretty hard to get real money into an exchange anonymously.
- Doesn't seem to be a way to make a deposit from a prepaid credit card
- BitInstant is what I tried - could be ok but a lot of hoops. Can deposit cash via MoneyGram.

Questions?

garrettr@riseup.net
@garrettrobin