Digital tradecraft and the need for escrow in the counter-economy

Frank Braun

October 13, 2012

Who am I

- computer science background
- IT security consultant, will work for Bitcoin
- libertarian, pro free-markets
- interested in Austrian economics

$\Rightarrow$ *freedom technology*

What's up with the mask?

- privacy is necessary for liberty
- privacy is not granted, it has to be taken
- extreme surveillance requires extreme countermeasures

$\Rightarrow$ privacy extremist

Overview

Definitions

Tradecraft is skill acquired through experience in a (typically clandestine) trade.

Digital tradecraft is tradecraft in the virtual (digital) realm.

Counter-econonmy (a.k.a the informal economy) is all economic activity which is not fully official, registered, regulated, or taxed.

Formal vs. informal economy

- formal economy:
  - rests heavily on state-issued ID
  - cost of enforcement is externalized

  $\Rightarrow$ a higher risk of attacks can be tolerated
- informal economy:
  - typically uses pseudonyms
  - cost of enforcement cannot be externalized

  $\Rightarrow$ probability of attack must be reduced

Areas of attack

1. communication
2. record keeping
3. fraud

Digital tradecraft reduces all this risks.

Escrow deals with risk 3.

Areas of digital tradecraft

1. secure IT infrastructure
2. pseudonyms, reputation, and community
3. protocols

Secure IT infrastructure

1. secure communication
   - who talks to whom? (context)
   - what do they talk about? (content)
2. secure record keeping

Encryption: Introduction

- "conventional" symmetric encryption uses one key for encryption and decryption (secure channel needed for key exchange)
- in contrast, public-key encryption is *asymmetric* and uses *key pairs* (a public and a private key)
- something encrypted for a given *public key* can only be decrypted by the corresponding *private key*
- the reverse operation is a digital signature: something encrypted (*signed*) by a private key can only be decrypted (*verified*) by the corresponding public key

$\Rightarrow$ public-key encryption solves the key exchange problem

Encryption: Applications

symmetric encryption: hard disk encryption
$\Rightarrow$ secure record keeping
e.g., use dm-crypt, eCryptfs, or TrueCrypt

asymmetric encryption:

- e-mail (use GnuPG)
- chat with off-the-record (OTR) messaging (e.g., use Adium or Pidgin)
- VoiP with ZRTP (e.g., use Jitsi)

Anonymization: Introduction

anonymization is based on *mixing* & *relaying*

mixing content from multiple users together

relaying the content through multiple hops

$\Rightarrow$ it is not possible[1] to determine what content is from whom

[1] correlation attacks aside

Anonymization: Applications

your IP address connects your online activities to your real identity

$\Rightarrow$ anonymizing your IP address is mandatory

e.g. with

- I2P (the recommended free choice)
- TOR
- commercial *multi-hop* VPN providers (e.g., Cryptohippie)

Mobile phones

- they track your location all the time
- can be activated as a remote bug
- all your call information and text messages are recorded permanently
- reveals your social graph
- the actual content of your calls is stored or will be shortly
- anonymous phones do not help against voice recognition

$\Rightarrow$ Do **not** use mobile phones!

$\Rightarrow$ Do use secure laptops and tablets instead!

Bitcoin

- IMHO the best online payment method we currently have
- **not** anonymous (but can be used pseudonymously)
- fully traceable
- buy your Bitcoin at an over-the-counter (OTC) exchanger
- e.g., use `bitcoin-otc.com` or `localbitcoins.com`
- do **not** use online wallets

Secure IT infrastructure conclusion

- get the basics down, use *at least*:
  - IP address anonymization
  - hard disk encryption
  - email and chat encryption
- secure IT infrastructure has compounding interest
- continuously educate yourself
- build mental models, know the limits of the technology
- there is no silver bullet
- never forget the human factor

$\Rightarrow$ without secure IT your are toast

Digital Tradecraft

Digital tradecraft is more than secure IT infrastructure:

- pseudonyms
- reputation
- community
- protocols

Formal economy: state-issued ID, externalization of enforcement cost

Informal economy: (multiple pseudonyms), reduction of risk and enforcement with reputation and protocols

Pseudonyms (nyms for short)

- use pseudonyms instead of name given at birth
- bind your pseudonym to a GnuPG key-pair
- $\Rightarrow$ allows to prove ownership of pseudonym
- e.g., I own the key `0xCEC00E94` and can prove that with a digital signature
- nyms are free, you should use multiple ones if appropriate

$\Rightarrow$ get an online pseudonym today and generate a key-pair

Reputation

- as with your real name, pseudonyms aquire reputation if people get to know you and you act honoroable
- reputation represents an economic value
- high reputation allows deals and roles which would otherwise be impossible
- reputation can be transferred (to a certain extent, more on that later)

$\Rightarrow$ don't be an ass and keeping your word is good for business

Community

- community is the place where nyms interact and reputation is build
- modern digital tribes are the analog to ancient clans
- community happens online (Libertopia) and offline (`#agora`)
- do not underestimate the power of digital tribes
- strongly hierarchical organizations are for corporate drones

$\Rightarrow$ invest in relationships

Protocols: Introduction

Pseudonyms + Reputation + Community $\Rightarrow$ Protocols

A **protocol** is a set of rules/customs to solve a defined problem.

Tradecraft comprises the knowledge and proper use of the appropriate protocols.

Digital protocols are often similar to their physical counterparts.

Protocol: Introducer

problem: nym with low reputation wants to do business which requires higher reputation

solution: nym with high reputation vouches for nym with low reputation

$\Rightarrow$ get to know people well with high reputation

$\Rightarrow$ use introducer protocol to employ multiple nyms! (better security via separation of concerns)

Protocol: Contract with mediator

problem: two nyms want to enter into a contract and need a way of enforcing it

solution: they decide on a (high reputation) mediator beforehand

- dispute handling is decided on beforehand
- if at least one party complains dispute resolution is started
- parties give evidence/information to mediator
- mediator arbiters
- if one party does not accept arbitration contract might become public (reputation penalty)

Protocol: Authenticated anonymous groups

problem: a group of nyms wants to start joint-venture but decisions should remain anonymous

solution: create an authenticated anonymous group

- each nym creates a list of new key-pairs and writes IDs on paper
- each nym puts one ID into box
- all IDs are put on the table
- each nym confirms that his ID is contained in the IDs on the table
- $\Rightarrow$ group formed
- group uses new nyms for decisions
- $\Rightarrow$ it is not possible to say who decided

Remaining area of attack

1. (communication)
2. (record keeping)
3. **fraud**

Digital tradecraft greatly reduces risks 1. and 2., but a significant fraud risk remains

Escrow deals with that.

Escrow: Introduction

risk of fraud:

- reduction with reputation (problematic)
- mitigation with escrow

escrow typically is the use of a third party to hold funds until transfer of goods is completed

example: alice wants to buy goods from bob

1. alice gives money to escrow
2. bob gives/sends goods to alice
3. alice confirms receipt of goods to escrow
4. escrow gives money to bob

Escrow: How to use it

- escrow should have high reputation and be auditable
- escrow is not part of the deal
- terms clearly agreed upon in advance
- use *fair witness* (e.g., to judge the quality of goods)
- (group of) mediators is known in advance

possible selection of mediators and arbitration procedure:

- each party selects a mediator
- the two mediators agree upon third mediator
- all five vote

Over-the-counter (OTC) Bitcoin exchange

depending on amount and trust an OTC needs more or less tradecraft:

- deal is agreed upon in advance, do not deviate
- escrow might be useful
- (from *Theory and Practice of Black Market Business* talk):
  - brush
  - drop/cache
  - ...

see `http://shadowlife.cc/files/btcotc.pdf` for details

Conclusion: Fork in the road

- The material in *Theory and Practice of Black Market Business* and this talk basically contains everything which is necessary to build an international covert organization with the potential to undermine and subvert monopolies and give us more personal liberty in our lifetime.
- Of course, nobody wants that here.
- Alternative: The heavily regulated total surveillance state which keeps you safe and secure.
- As a good citizen, you know what to vote for.
- Please smile when you are taking a walk... you're on camera!

Conclusion

To ensure liberty we need a thriving counter-economy.

- Appeal: Stop talking, start acting.

$\Rightarrow$ Trade securely in the counter-economy!

Acknowledgments: Jonathan Logan

Contacts:

- #agora IRC channel / community: `https://anarplex.net/` (under *contact*)
- For all things privacy: `http://shadowlife.cc` (Oct 2012)
- Mail: `frank@shadowlife.cc` (please use GnuPG)
- Key: `0xCEC00E94` (can be found on the keyservers)

Thank you for your attention! Questions?