The Bright Side Of Darknets

Athanasios Kostopoulos

FOSSCOMM Patras May 2011

Introduction

- Assumes NO previous familiarity with ”Darknet” concepts
- This will NOT be a tech-heavy presentation
- Just the technical facts ma'am (no arguments for/against (pseudo-)anonymous networks)
- Focus on I2P
- 1st public presentation so thanks in adv...

Current (mis)-definition I

- ACM 2002 DRM Workshop

”We investigate the darknet – a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks.”

Current (mis)-definition II

- Tor: ”Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis”
- Freenet: ”Freenet is free software which lets you anonymously share files, browse and publish "freesites" (web sites accessible only through Freenet) and chat on forums, without fear of censorship.

Why go ”Dark”?

- Firewalls (China)
- Monitoring (every commercial and state actor that can perform it, perform it)
- Activism (Egypt, Libya, Iran)
- Privacy (Canada)
- ”cool” factor

The (Non-?)Controversy

- Copyright Infringement (e.g. Warez)
- Political Extremist content
- Other nefarious extreme content

But are there Darknet-only specific issues?

Are current Darknets ideal for mass copyright infigement? (speed issues)

Personally, I was not looking for it thus haven't seen any.

Common Darknet Implementations

- Tor (the poster boy)
- Freenet
- I2P
- Waste (R.I.P)
- …
- Roll Your Own

The Onion Router (Tor) I

- Perhaps the most famous and widely deployed anonymity network
- Based on Onion Routing
- Open Source (written in C)
- Available for Windows/OSX/GNU/Linux

The Onion Router (Tor) II

- Provides exit points from the darknet *
  - Used even by Law Enforcement Agencies
  - Vulnerable to sniffing, once data leaves the darknet (ask Dan Egerstan)
- Provides hidden services (.onion TLD) within the darknet

Onion Routing I

- Anonymous Communications over a public network
- Patented by US Navy in 1998
- ”Onion”: Plaintext message encrypted multiple times (onion layers)
- Source routed protocol (Tor Circuit)

Onion Routing II

- Sender determines path to recipient using a central directory service
- Sender retrieves public keys for all the intermediary nodes and encrypts in reverse order
- Each layer contains the cryptogram and next node information
- Once an intermediary receives the ”onion” it peels off its own layer and forwards

Freenet I

- Again, Freenet can be regarded as a distributed, anonymous data store.
- Free Software (Windows/OSX/GNU/Linux)
- Claims more than 2 million Downloads
- Significant Research Work Behind It
- Storage Oriented, as opposed to Message oriented.

Freenet II

- Users contribute both bandwidth and **encrypted** storage space.
- Content is kept on a popularity basis (unpopular content is deleted in order to make space for more popular content)
- Content published can survive long after the original publisher is gone.
- No personal experience with it so YMMV.

What is I2P? I

- I2P in its own words:
  - ”I2P is an anonymizing network, offering a simple layer that identity-sensitive applications can use to securely communicate. All data is wrapped with several layers of encryption, and the network is both distributed and dynamic, with no trusted parties.”
- Started 2003 – forked from Freenet
- Still WiP but quite usuable

What is I2P? II

- Free and Open Source Software
- Written in Java (!)
- Runs on Windows/OSX/GNU/Linux
- 0.8.5 is the latest version at time of writing
- Designed from the ground up to address privacy and security shortcomings of other similar solutions

But I have Tor Already!

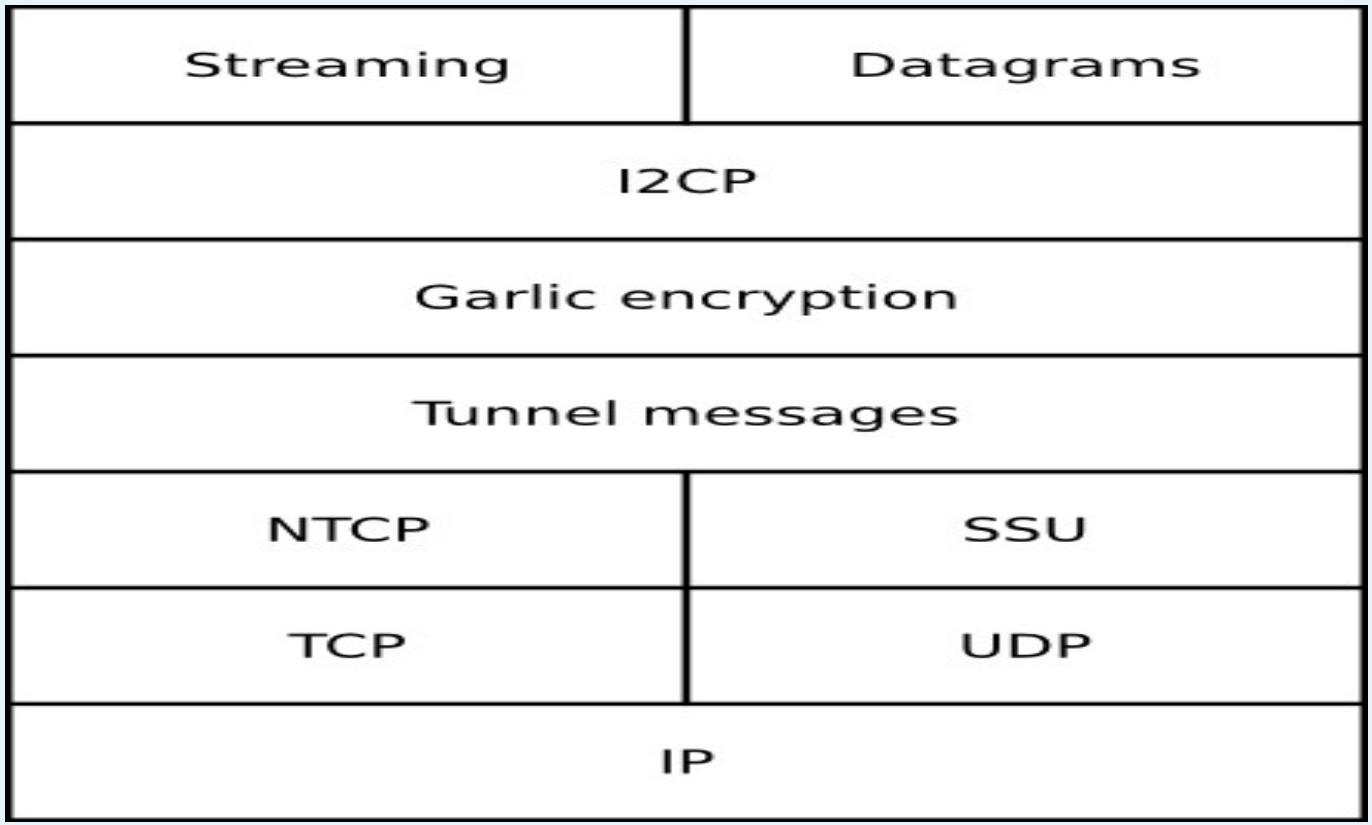
- Focus on operations within the Darknet
- Packet Switched
- Less Trust, more verification (directory servers/actual peer capabilities)
- Short Lived Tunnels (more on this later)
- No centralized resources per-se (which can be both good and bad)

I2P Building Blocks

- I2P is designed to be used on top of an existing, insecure packet switched network.
- Transport Layer
  - NTCP is I2Ps equivalent to TCP
  - SSU us I2Ps equivalent to UDP
- Tunnel Layer (on top of Transport)
  - Encrypted end-to-end
- Garlic Layer (on top of Transport)
  - Encrypted messaging *

I2P Building Blocks

- A picture is worth ...



Garlic Routing

- Yet another vegetable?
- Routing wise, I2P garlic routing is identical to Tor's onion routing*
- Message wise, garlic extends onion by bundling different messages together (can be any number of messages)
- All messages are exposed at endpoint, with each message containing different routing directives

I2P Tunnels I

- ”Garlics” travel through ”Tunnels”
- Tunnels are unidirectional (thus 2 parties require 4 tunnels)
- Tunnels can be exploratory or client (more on this later)
- Tunnels expire after a predefined amount of time
- Tunnel hop length varies (0 unsafe, def is 2)

I2P Tunnels II

- Exploratory Tunnels
  - ”Internal” I2P tunnels, selecting random peers and promoting appropriate ones.
- Client Tunnels
  - Used for end-to-end communication, selecting high-yield peers.
- Tunnels are tested periodically. Tunnels that fail testing are removed.
- Default Tunnel lifetime is set to 10 mins.

Crypto Algorithms Used I

- Algorithms by themselves are not a guarantee for the overall strength of the cryptosystem but are essential for it.
- Each transport packet is encrypted with AES256/CBC Mode, using explicit IV and MAC (HMAC-MD5-128) using ephemeral session key, created by 2048 Diffie-Hellman.
- Each Tunnel message uses AES256/CBC with explicit IV and SHA256 hash.

Crypto Algorithms Used II

- ”Garlics” are encrypted using AES256/CBC/each individuals hosts ElGamal public key.
- Upon decryption I2P Router honors certain message instructions, including the addition of time delays
- But where does that traffic go to?

I2P Destinations

- Destination is I2P-speak for ”host:port” appx
- Cryptographically unique *mobile* endpoint
- A destination is composed of
  - 2048-bit ElGamal for encryption
  - 1024 DSA for signing
  - Assorted variable size certificate data
- Much larger than IP:PORT so?

I2P Naming Scheme

- A handy way for humans is to short names to mnemonic forms (i.e. anonymous.i2p)
- I2P has no central DNS resources
- Network-wise: Enter netDb
- A small percentage of high-bandwidth peers is used as ”floodfill peers”
- Floodfills stores both signed I2P router info and signed leaseSet info

I2P Naming Scheme

- Floodfills are queried fron individual I2P routers
- A request in ALWAYS answered by the floodfill asked (no propagation)
- I2P routers can (and will) put assorted data into floodfills
- Since all nodes are transient, when the number of floodfills drops, new ones are created.

/etc/hosts on steroids

- Each client is saving his own addressbooks
  - An addressbook allows for human readable (and memorable names)
  - Each client maintains its own:
  - privatehosts.txt
  - userhosts.txt
  - hosts.txt

/etc/hosts on steroids

- A client can subscribe to other public address book repositories
- *Cryptographic uniqueness is lost*
- First match found is used
- Conflicts are ignored
- Now you can see eep-sites

Eep-what?

- Eepsite is I2P-speak for sites available only within I2P
- TLD is i2p
- Every I2P router starts a web server by default so start publishing content!
- From an application perspective, eepsites can match what you meet on the traditional WWW, including complex, interactive websites

P2P and Distributed

- Tunnel Model does not scale well for P2P and distributed computing systems
  - Number of tunnels grows
  - Tunnel creation is expensive
  - A need for agreement arises
- Luckily, I2P provides with an SDK which allows distributed and P2P applications to be written for use within I2P

Not Covered

- This was only a short presentation of what Darknets in general and I2P in particular are.
- This is an active research field, with each branch deserving studying on its own.
- Possible attacks and countermeasures have not been covered
- The protocol/application stack is much, much, much, much more extensive.

Contribute

Whoa, I'm sold. How can I contribute?

- Easiest way? Use it!
- Do you like it? Advocate it!
- Donate money (Bitcoins accepted too!)
- Donate your skills:
  - Translations
  - Coding
  - Security review

Discussion

- Questions?
- Ideas?

Thank you!

Feedback is more than welcome :-)

Drop me a line: akostopoulos@acm.org

Ask for social networking info

Web Resources

- TOR: https://www.torproject.org/
- Freenet: http://freenetproject.org/
- I2P: http://www.i2p2.de/

Thanks to all the teams for their hard work, GFX and documentation.