



Anomos

Pseudonymous, Encrypted BitTorrent

by: Rich Jones, John Schanck

What is Anomos?

- Anomos is an encrypted, pseudonymous multi-peer-to-peer file sharing protocol, based on BitTorrent.
- The current code in the git repository is based of a fork of the official BitTorrent tracker/client, version 4.0.

What pros and cons of BitTorrent?

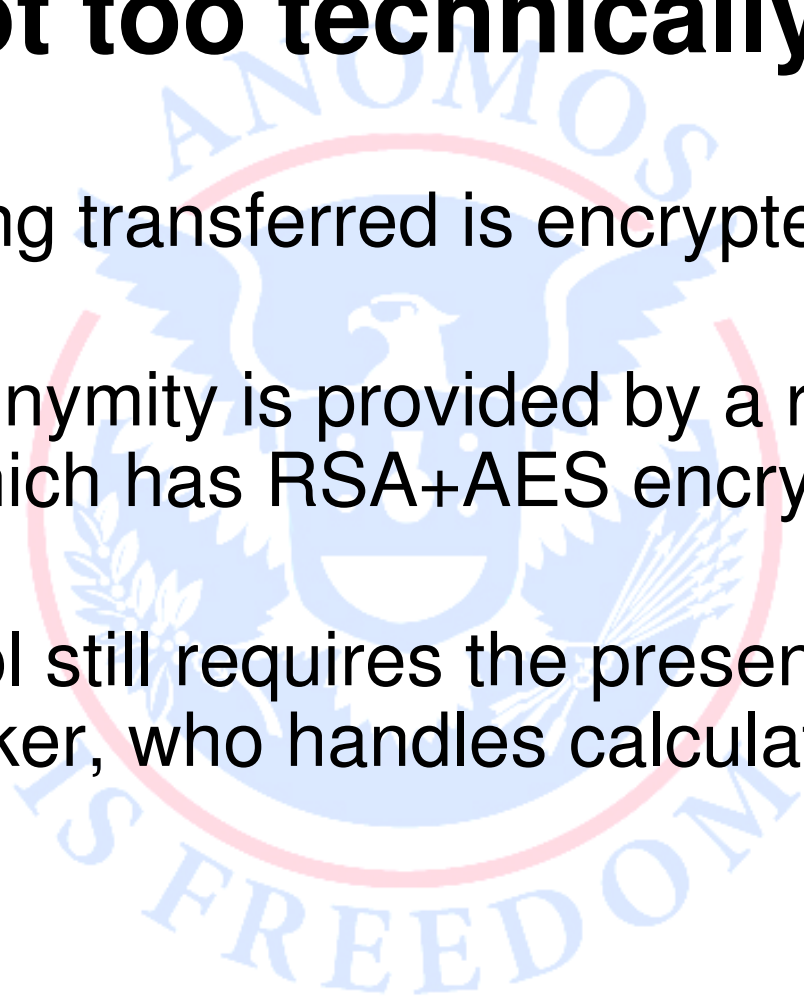
- + FAST (Multi-peer2peer, as opposed to old, directly connected p2p such as Napster).
- + Widely Used
- - Unencrypted
- - Onymous
- - Traffic is deliberately sniffed by companies playing detective, such as MediaSentry
- - This means that users can be tracked, and some will be prosecuted.
- - Traffic may be tampered with by ISPs

What are the pros and cons of current encryption/routing schemes?

- + Routing traffic is encrypted
- +/- Encrypted traffic (and unencrypted traffic without identifiable information) is pseudonymous
- - Less widely used
- - Typically slow(er)

How does Anomos work? (Not too technically..)

- The file being transferred is encrypted with 128-bit AES.
- The pseudonymity is provided by a routing mix network, which has RSA+AES encrypted peer to peer links.
- The protocol still requires the presence of a trusted tracker, who handles calculating the data paths.

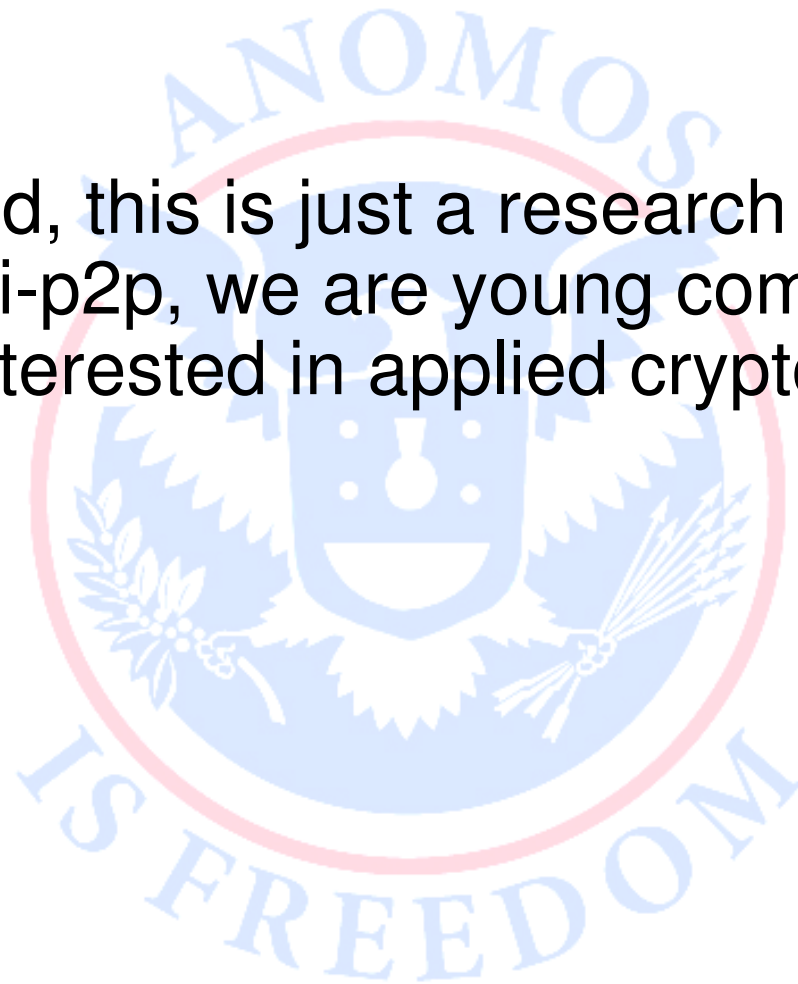


What are the pros and cons of Anomos?

- +Encrypted end to end
- +Pseudonymous Mixnet
- +Fast speeds of Multi-P2P (Though not as fast as normal BT)
- +Based on popular, familiar technologies
- -Use of a centralized tracker

Why is it important?

- On one hand, this is just a research exercise into secure multi-p2p, we are young computer scientists interested in applied cryptography and anonymity.



Why is it important?

- But, on the other hand, we believe this tool is necessary to the current and future security of free information.
- Internet users are being prosecuted by draconian laws, passed by a corrupt government funded by large media companies.
- At the same time, all other BT and internet users are being tracked by their ISPs and governments.
- Anomos prevents this and provides a platform into research for ways to continue to prevent this.
- This is important for the future of free information.

Vaguely Related Quote

- "The American public has proven remarkably susceptible to the manipulation of truth, which increasingly dominates the country's political discourse. Indeed, a whole network of publications, some of which manage to parade as mainstream media, is devoted to the task. Yet I believe that it is possible to inoculate the public against false arguments.. Now is an ideal time to begin that effort."
- George Soros 'From Karl Popper to Karl Rove – and Back', 2007

Tying it in..

- The internet is, of course, an open broadcast medium, the meta-media, and is rapidly changing the face of truth and accountability in politics. This protocol ensures the freedom to continue to pursue this accountability without fear from prosecution by corporate governments.
- Censorship-resistant outlet for independent news media.
- (Wikileaks, LiveLeak, etc)

Cryptoanarchizing Tools

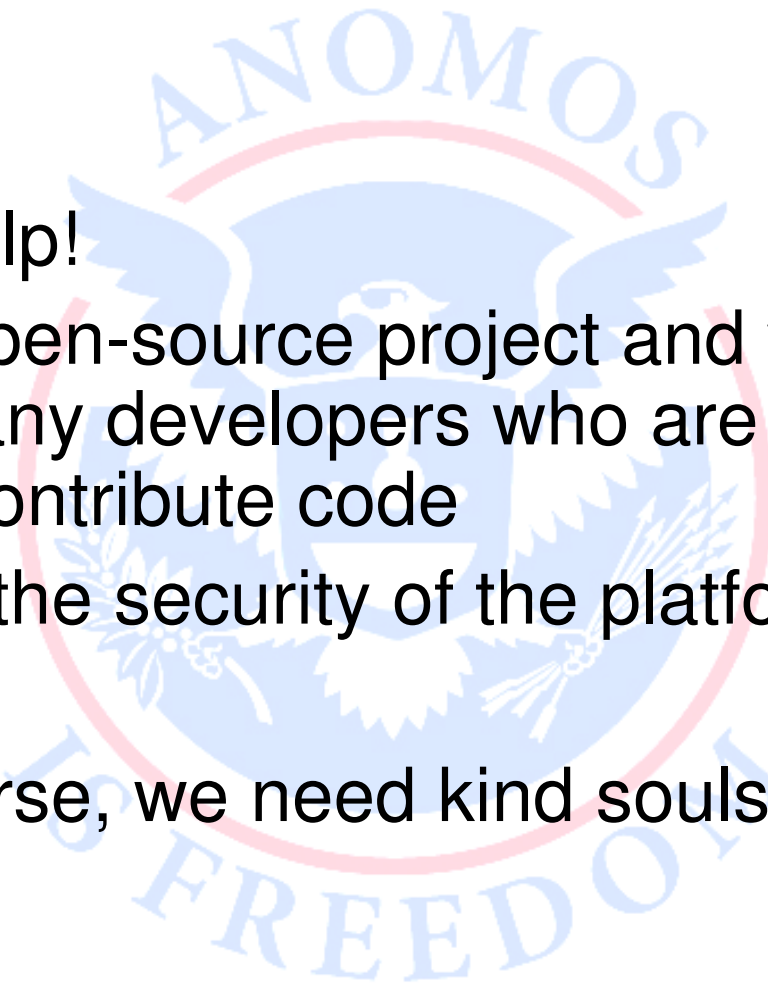
- A lot of people have talked about the internet as a 'democratizing' tool.
- But, they have seemed to missed the point.
- Rather, the internet is a brilliant ***anarchizing*** tool, as no power has to be relented to anybody in order to spread any type of information.
- Anomos ensures this in a practical sense.

Drawbacks

- - Requires use and trust of a central tracker.
- - Hosting should probably be in a copyright haven.. Sweden?
- -Still in the early stages.

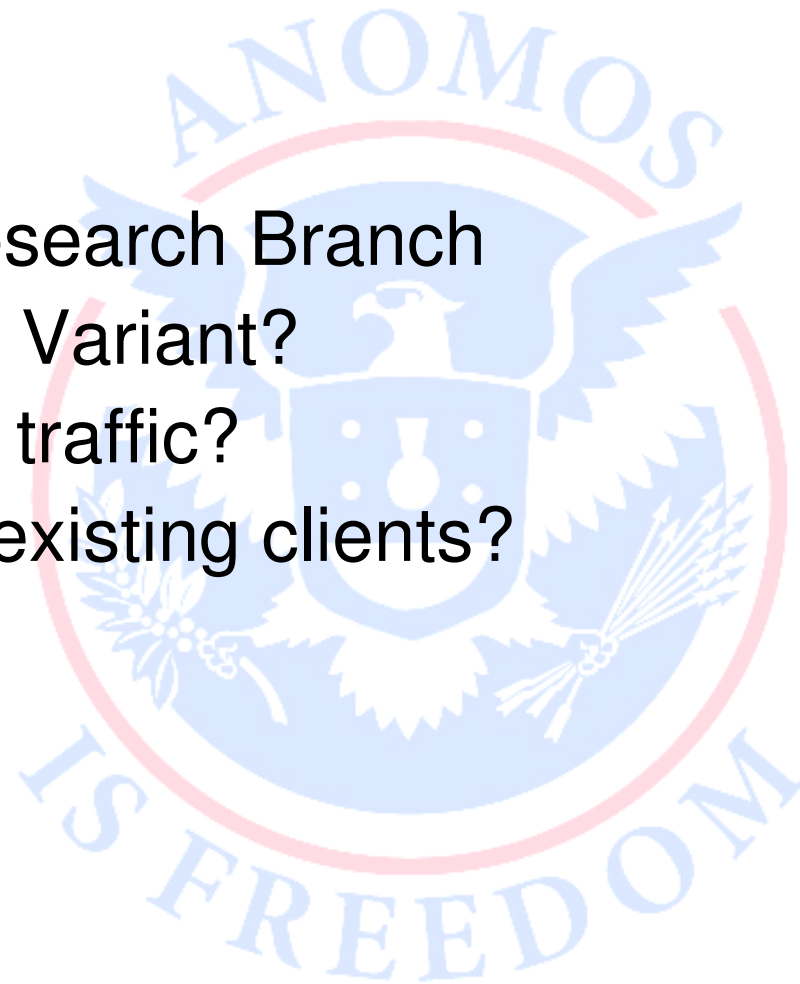
Help Wanted!

- We need help!
- This is an open-source project and we are looking for any developers who are interested to come and contribute code
- or help test the security of the platform.
- Also, of course, we need kind souls to run some trackers!



The Future..

- Anomos Research Branch
- Trackerless Variant?
- Obfuscated traffic?
- Plugins for existing clients?



More info

- Website: <http://www.anomos.info>
- Git: <http://anomos.info/git/>
- Rich: **miserlou@gmail.com**
- John: **jms07@hampshire.edu**
- To help: participate@anomos.info

