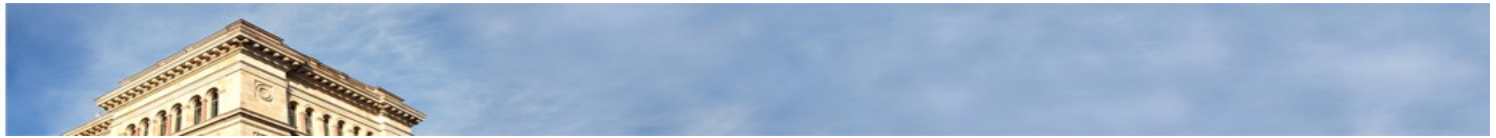
Technische Universität Berlin

Onion^{Core}

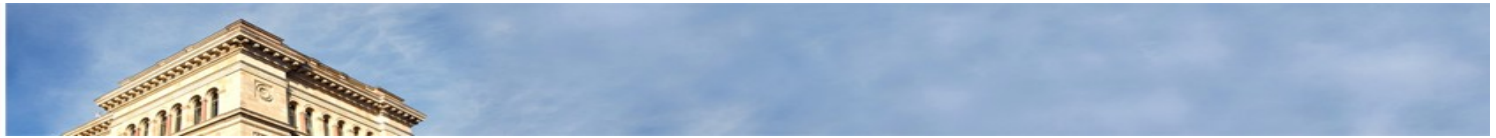
Social anonymous Filesharing

Tim Hinkes | Information Systems Engineering | Presentation Bachelor Thesis



Technische Universität Berlin

- Motivation
- State of the Art
- Basics
  - Tor
  - BitTorrent
  - DHT
  - Asymmetric Cryptography
- Goals
- Onion^{Core}
  - PeerGroups
- Experiments
  - Transfer Rates Tor ↔ Plain
  - Hybrid Filesharing
- Conclusion



Technische Universität Berlin

Motivation

- Sharing files playes major role in todays Internet
- Files often contain “unpleasant” data
  - Wikileaks
  - Critical speech

- Centralized Server-Client structure
  - Unpleasant data is easy to block

- P2P Client-Client structure
  - Hard to censor
  - Clients give out identity to everyone

Motivation

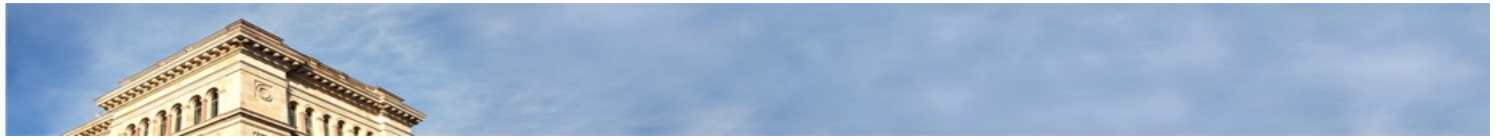
- Sharing files playes major role in todays Internet
- Files often contains “unpleasant” data
  - Wikileaks
  - Critical speech
- Centralized Server-Client structure
  - Unpleasant content is easy to block

- P2P Client-Client structure
  - Hard to censor
  - Clients give out identity to everyone

Motivation

- Sharing files playes major role in todays Internet
- Files often contains “unpleasant” data
  - Wikileaks
  - Critical speech
- Centralized Server Client structure
  - Unpleasant data is easy to block

- P2P Client Client structure
  - Hard to censor
  - Clients give out identity to everyone



Technische Universität Berlin

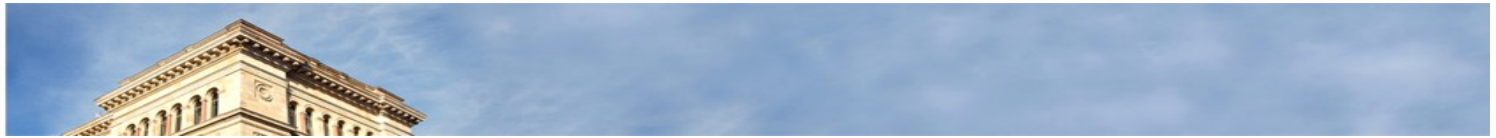
State of the Art

Transport-Layer anonymity

- Tor (The onion router)
- I2P (Invisible internet Project)
- ...

Torrent over Transport-Layer anonymity

- very slow for all peers
- Easy to set up



State of the Art

Transport-Layer anonymity

- Tor (The onion router)
- I2P (Invisible internet Project)
- ...

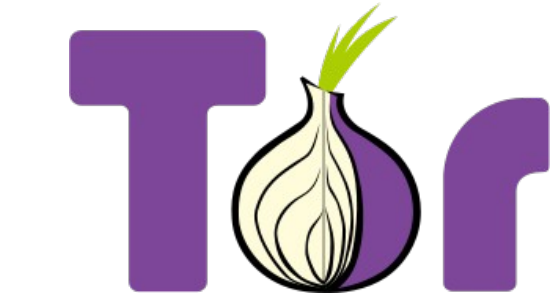
Torrent over Transport-Layer anonymity

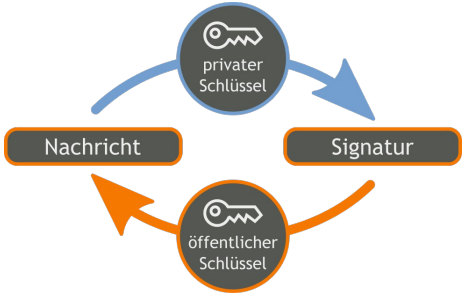
- very slow for all peers
- Easy to set up

Projects providing anonymous filesharing infrastructure

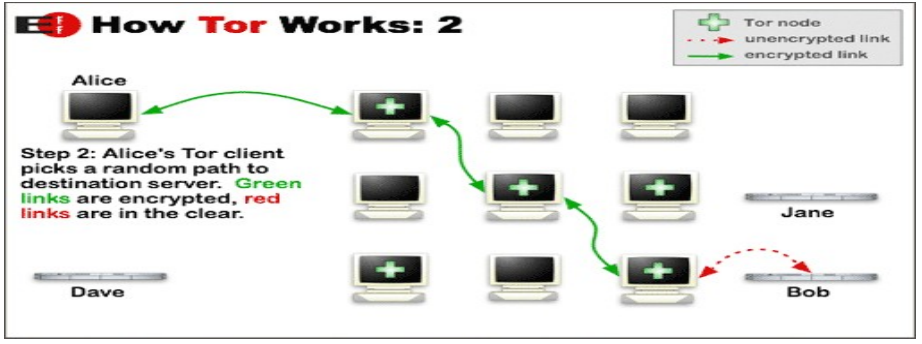
- BitBlender
  - Tor-Style Routing over BitTorrent
- Freenet
  - Closed virtual Network
  - “persistent” storage on P2P architecture

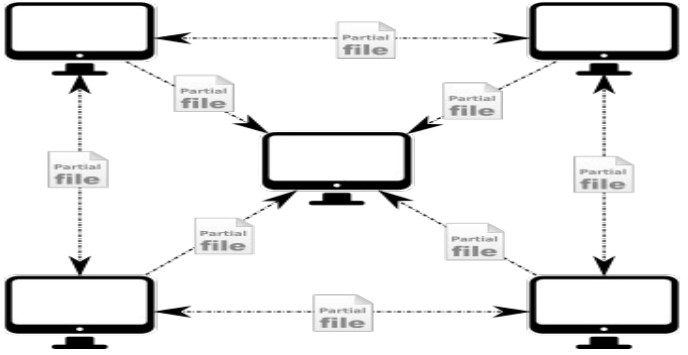
Basics

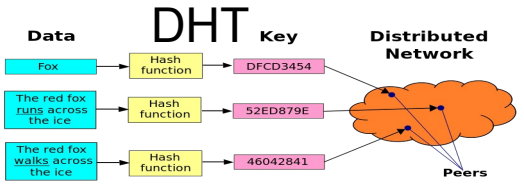


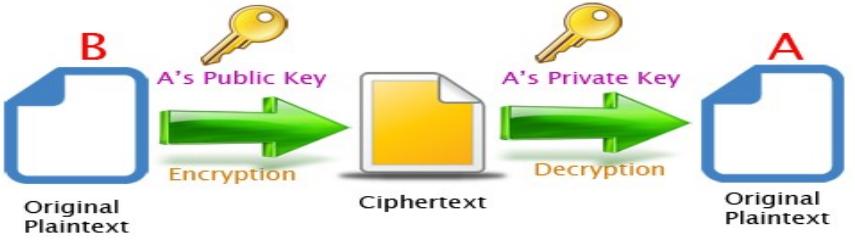


Basics

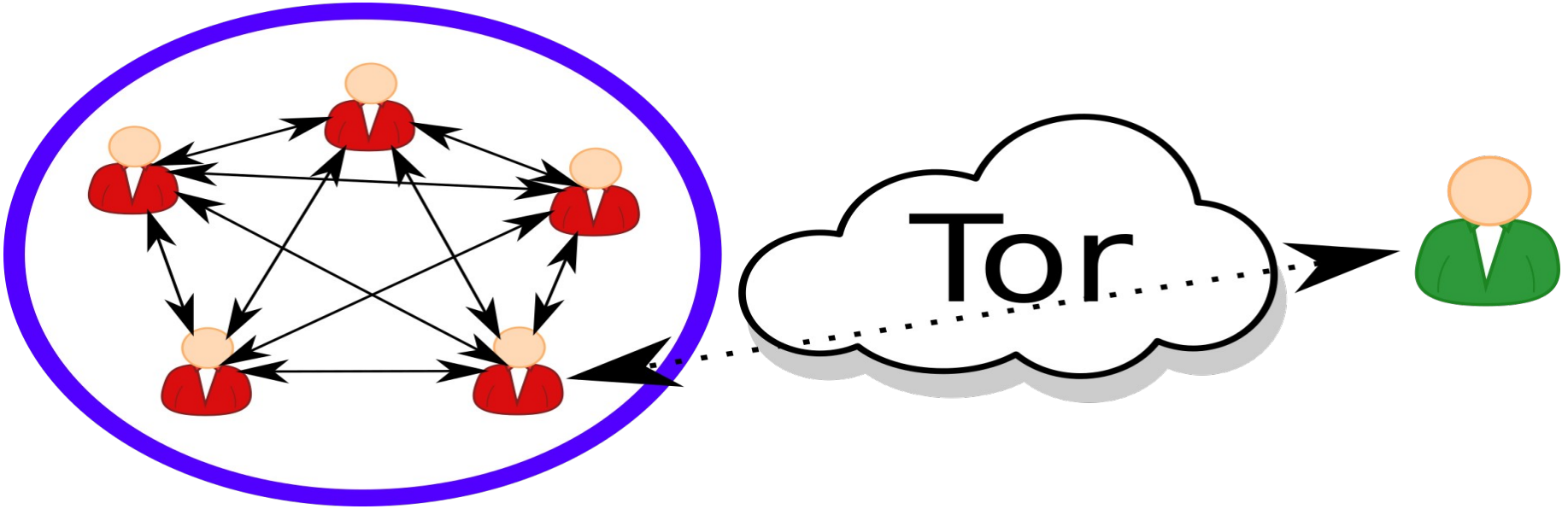




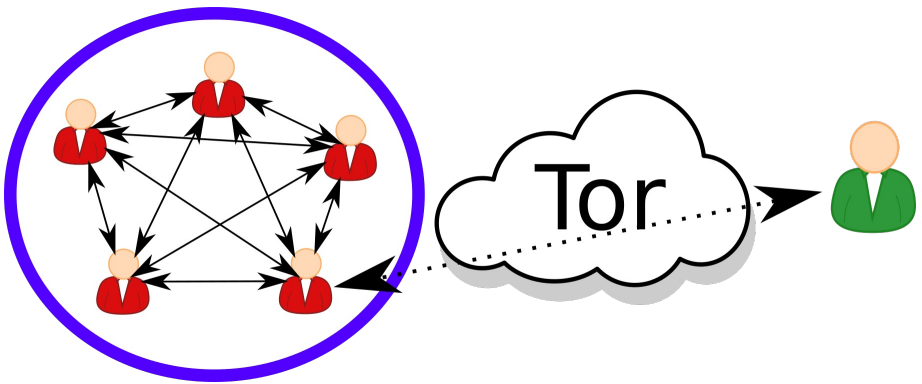




Goals



Goals



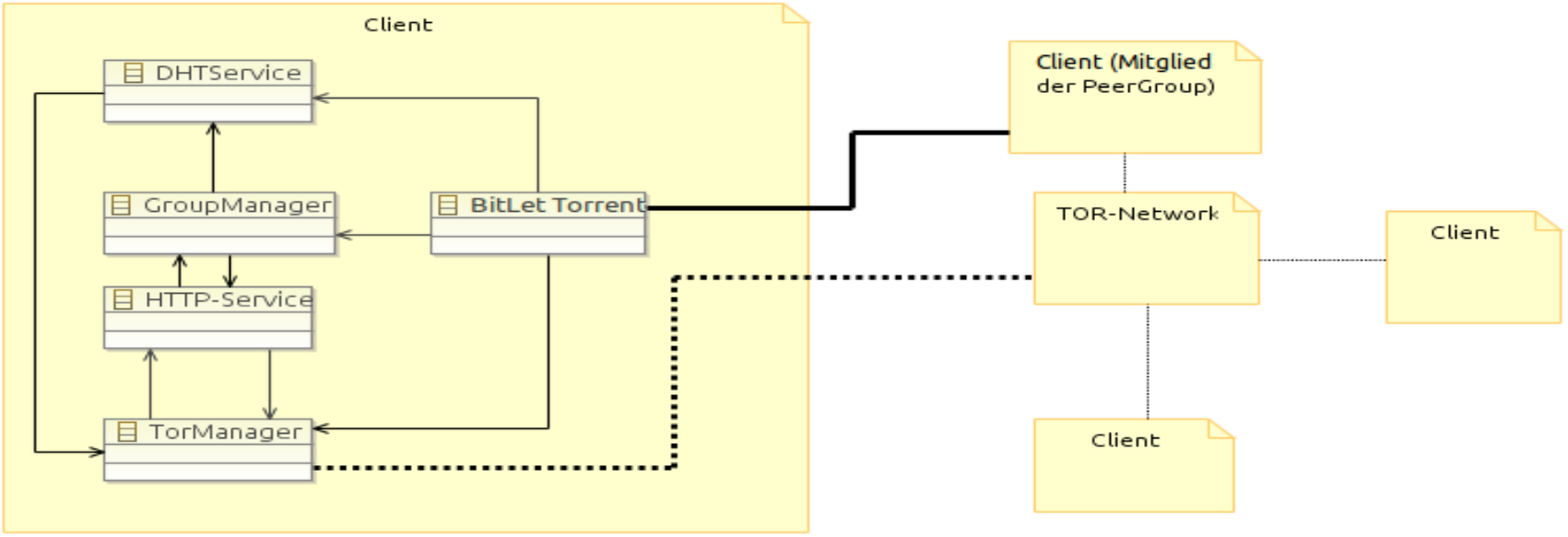
Hybrid sharing

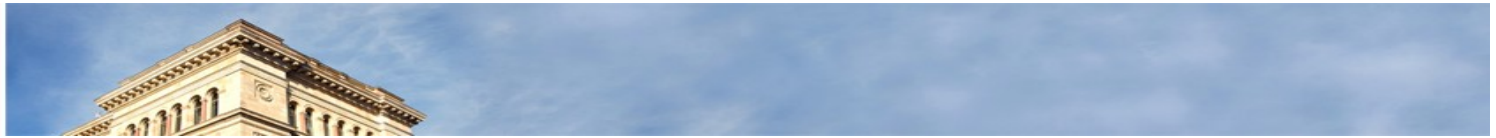
- Plain connection within PeerGroup
  - Very fast
- Anonymous connection to everyone else
  - Slow

Ease of use

- Reduces human error in crypto/trust

Onion[Core]



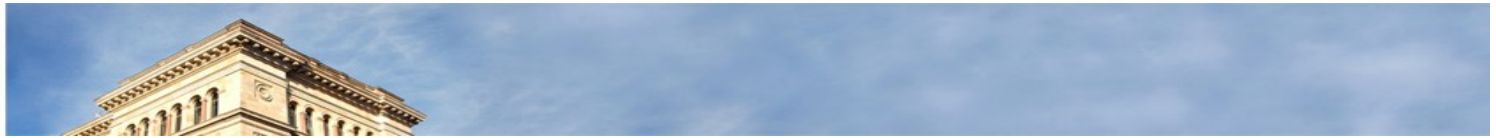


Technische Universität Berlin

Onion^{Core} PeerGroups

PeerGroupMember

- Authenticated by Public-Key
- Addressed by Tor-HiddenAddress
- Authorization by known Public-Key



Technische Universität Berlin

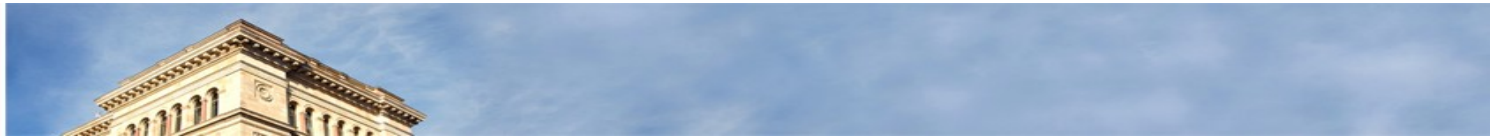
Onion^{Core} PeerGroups

PeerGroupMember

- Authenticated by Public-Key
- Addressed by Tor-HiddenAddress
- Authorization by known Public-Key

PeerGroup

- Identified by UUID
- Contains list of trusted Public-Keys



Technische Universität Berlin

Onion^{Core} PeerGroups

PeerGroupMember

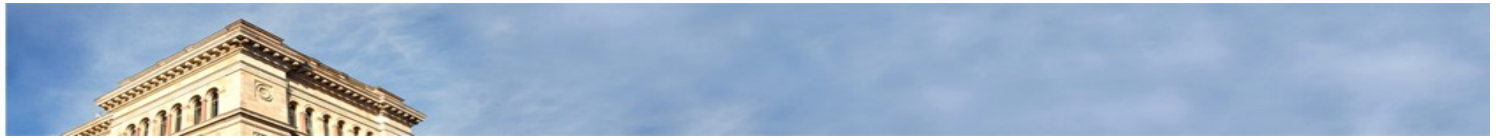
- Authenticated by Public-Key
- Addressed by Tor-HiddenAddress
- Authorization by known Public-Key

PeerGroup

- Identified by UUID
- Contains list of trusted Public-Keys

PeerGroup Features

- No hierarchy between Members
- No removal of Members
- Full trust once accepted into Group



Onion^{Core} PeerGroups

PeerGroupMember

- Authenticated by Public-Key
- Addressed by Tor-HiddenAddress
- Authorization by known Public-Key

PeerGroup

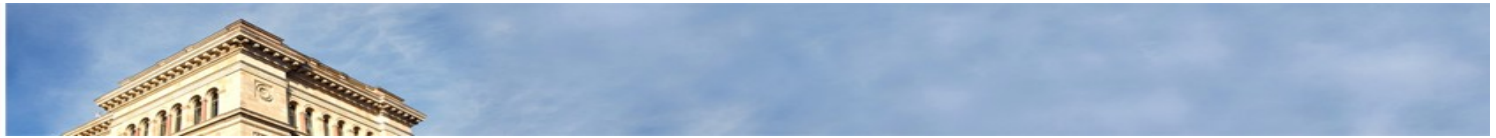
- Identified by UUID
- Contains list of trusted Public-Keys

PeerGroup Features

- No hierarchy between Members
- No removal of Members
- Full trust once accepted into Group

PeerGroup Invitation

- Member must initiate a invitation
- Minimal User interaction
  - User needs to communicate nonce



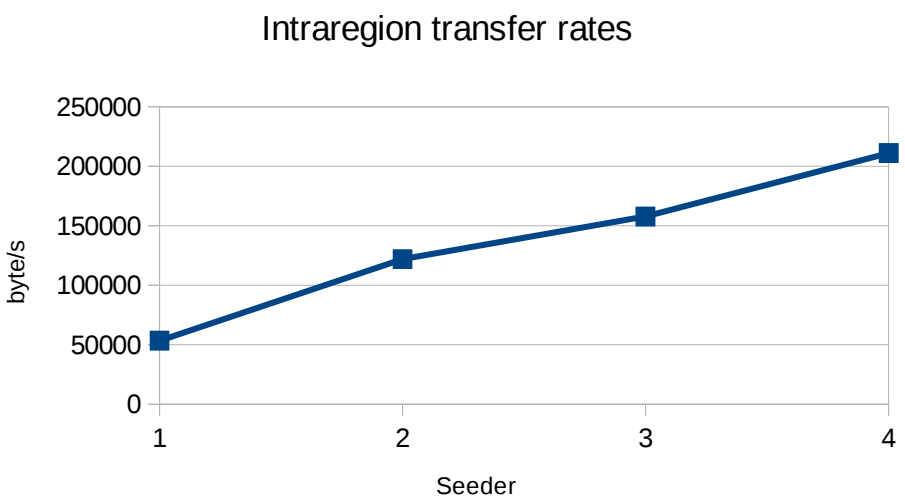
Technische Universität Berlin

Experiments

Setup

- Amazon EC2 instances
  - Distributed across regions
- Test over different times of the day
  - Compensating for fluctuation
- At least X runs per experiment
  - Consistent Data

Results Transfer Rates Tor ↔ Plain

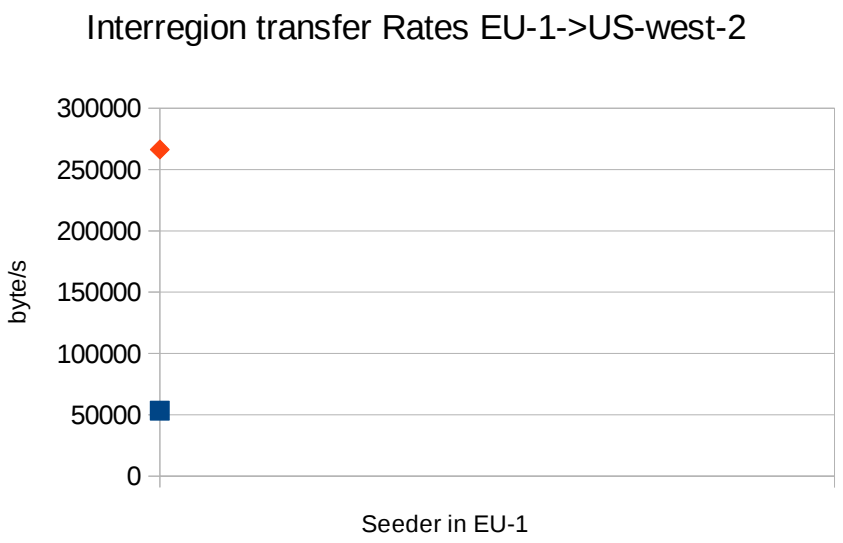


Plain transfer rates ~ uplink speed

Tor rates VERY inconsistent

- Slow links 16kb/s
- Fast links 80/kbs
- Rates are varying

Results Transfer Rates Tor ↔ Plain (Geodistribution)

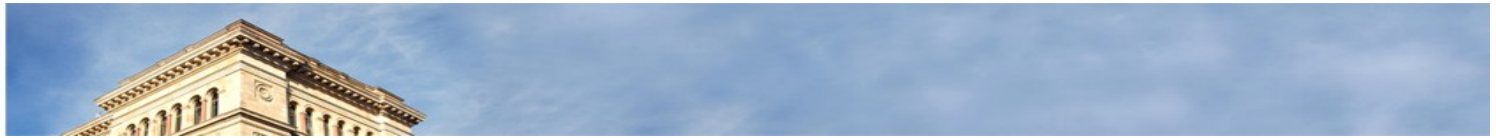


What changes in transfer rates when Peers are geodistributed

- AWS EU-1
- AWS US-west-2

No change visible in Tor traffic

- Traffic is routed around the globe anyways
- Plain rates went down



Results hybrid sharing

No data available

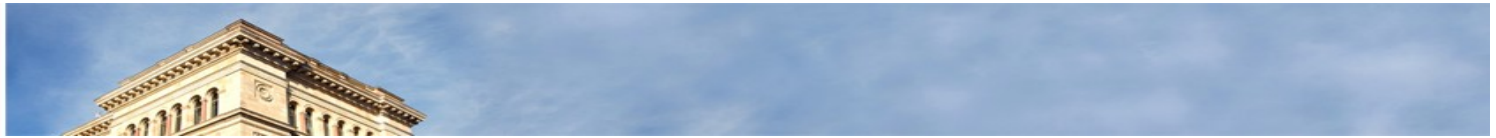
- Instabilities in underlying Libraries
- Worked once during testing

Practical Test of sharing a file with trusted and untrusted Peers

- 1 trusted Peers
- 2 untrusted Peers

Hybrid sharing can work

- Viable approach if no trusted peer in own region



Conclusion

With different anonymity layer the System could be used to circumvent censorship (BitBlender)

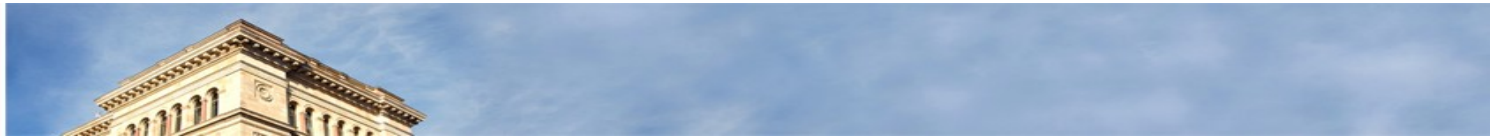
Transfer rates of Tor connections are not highly related to location of the endpoints

Distributed Systems are a lot of work

- > 8.000 lines of code

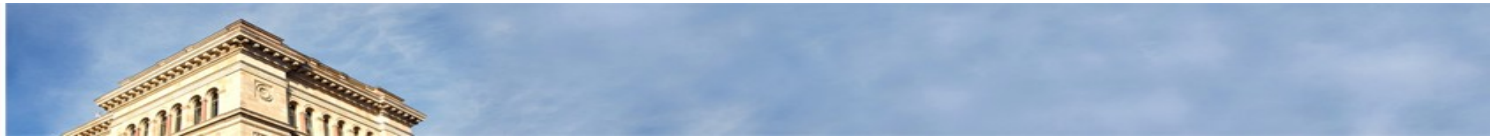
Reliance in not well known libraries can lead to problems

- Silvertunnel (tor library) seems not very stable
- Torrent library had design issues
  - Only using *Object* and *instanceof* in return types and handling



Technische Universität Berlin

¿Questions?



Technische Universität Berlin

Thank you

Appendix SeqDiagram PeerGroupApplication