Turtle: Safe and Private Data Sharing

Bogdan C. Popescu
Petr Matejka
Bruno Crispo
Andrew S. Tanenbaum

Vrije Universiteit, Amsterdam
Motivation

• Use p2p for safe sharing of sensitive data
  – an adversary (censor) attempts to prevent this

• Current solutions - anonymizing p2p networks
  – open connectivity => any 2 nodes may interact
  – good nodes interacting w. censor nodes => exposure
  – exposure => potential legal harassment
  – legal harassment => people don’t use it!

• Can we do better?
Solution - Turtle

• Create the P2P overlay based on social links

• Communication between links is encrypted
  – “Friend” nodes agree on keys out-of-band

• Both queries and results go hop-by-hop

Data exchanged only between trusted parties!
Security properties

- Only trusted and authenticated parties can interact
- Each user is his own trust root
- Interesting security properties
  - Node compromise causes localized damage
  - Immune to Sybil attacks
  - Good protection against DoS attacks
Current Status

• Prototype Turtle client software available
  – designed as a plug-in for the GiFT p2p daemon
  – http://www.nlnet.nl/project/turtle/

Thank you!