Heresy in the Church of Anonymity

langos@inf.fu-berlin.de

Given

- Anonymous Web Browsing
  - Mix based
  - Perfect anonymity in user set
  - No logs at Mixes
  - …
  - Everything peachy

Given

- Anonymous Web Browsing
  - Mix based
  - Perfect anonymity in user set
  - No logs at Mixes
  - …
  - Everything peachy
- Retro fitting tracebility

Why should I?

- Required to by law
  - Some anonymity better than none
- Deployment
  - Law enforcers run nodes,
  - or pay inepentent operators
- Easier to sell socially
- Public/free service
  - Finally: USERS!

Requirements

- Don’t change the attacker/trust model
- Pure retrival stays anonymous
- Transmissions recoverable
  - Clear regulations on recovery
  - Judge signed warrant
- Logs unavoidable?
  - Yes, but not centralized.

Transport

- Tag message at first Mix
  - E.g. IP Number
- Encrypt tag at every Mix

  (while the message gets decrypted)
- At last Mix
  - If retreiving forget tag
  - If transmitting send tag along and forget
- Receiver
  - Standard log entry

Recovery

- *Show me a warrant and the tag*
- *I'll show you some decrypted bits (no keys)*
- *Go to previous Mix.*
- *Finally recover the tag.*

Tons of Problems

- Distinguishing retrival / transmission
  - SSL
- No message logs but key logs
  - Warrant for the keys?
    - Key decay
- Make tag small enough to fit in log lines
- Special requirements for first / last Mix
  - Have it anyway
- Where's the big catch?