Designing a Type-III Anonymous Remailer Protocol

Nick Mathewson
nickm@freehaven.net
Our Goals

- Fix holes in Mixmaster (Type-II) remailers
- “Conservative” design
- Working implementation; deployed network
Our Adversary

- Global passive adversary
- Owns some of the nodes
- Can generate some traffic

We are not real-time, packet-based, or steganographic.
Changes from Mixmaster...
Key Rotation/Replay prevention

- Type II has no automated key rotation
- Type II has sketchy replay prevention
- Solve them together: keep hash of all headers seen since last key rotation
Secure replies

- Cypherpunk has reply blocks, but is vulnerable to replay attacks (and everything else...)
- Mixmaster has no reply blocks; people who want replies must use Cypherpunk.
- Mixminion provides single-use reply blocks:
  - Indistinguishable from forward messages
  - ...even by the nodes!
Link Encryption

- Cypherpunk and Mixmaster use SMTP for transport
- Mixminion uses TLS over TCP
- Forward anonymity against future compromise
And more...

- Integrated directory service
- Integrated exit policies
- Nymservers with single-use reply blocks.
Read our papers
Play with our code

http://mixminion.net/

We’ll be at Oakland (IEEE Security and Privacy) in May