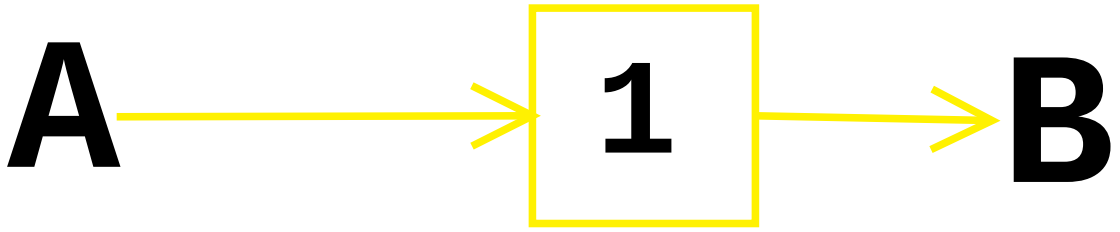
Mixminion: Design of a Type III Anonymous Remailer Protocol

Roger Dingledine
The Free Haven Project

Threat Model (what we aim to defend against)

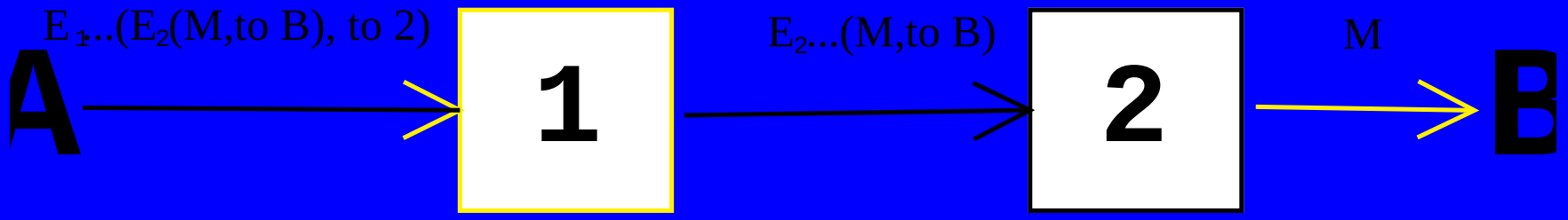
- Global passive adversary – can observe *everything*

Direct Forwarder



But: an observer of Alice can just read M and know it's going to Bob

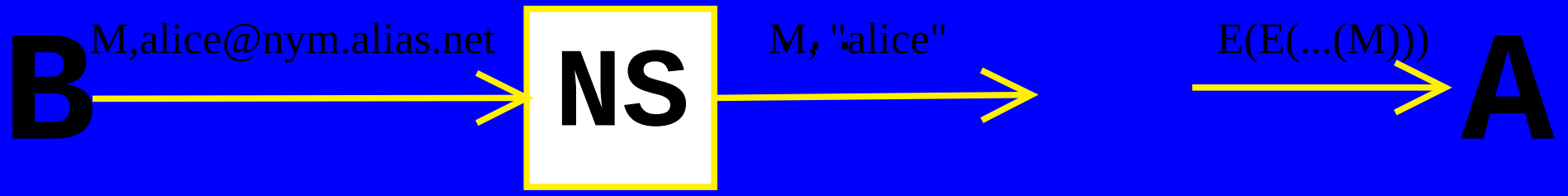
Multiple Hops



Assume: Not all hops wis21IT.hops and1IT.hops Howouw

Direct Reply

Nymserver



NS knows **A**'s reply block but not her location.

Replay cache

- When a message comes in, hash it and add it to the replay cache.

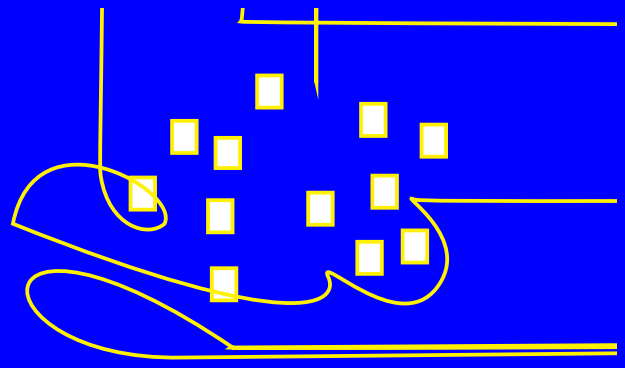
- If it's already in the cache, drop it.

But: you have to remember all the hashes forever!

Expiration dates

- Exp date is chosen randomly between 3 days ago and 3 days from now.
- Each node checks exp date; if more than 7 days old, drop.
- Now adversary can’t tell when the message was

Pooling



- Not all messages come out at each flush. Keep a minimum num/er in the pool, always.
- Now it's harder to target an individual message.

Dummy messages

- Users sometimes send decoy messages even if they have nothing to send.
- Hopefully there will be enough messages that the adversary will be confused.
- Dummies go several hops and stop (hard to -ecide convincing destinations).
- If you stop aere, you get type 2 (Mixmaster) remailers.

Passive subpoena attack

- Eve can record messages for later subpoena
  She can also recognize her own messages, which helps with flooding attacks

- Fix: Link encryption with ephemeral keys (rekeyed every message / few minutes)

Active subpoena attack

- Mallory can still record messages from the node she runs, and arrive later with a subpoena.

- Fix: Periodic key rotation

Partition attack on client knowledge (1)

- Adversary can distinguish between clients that use static node lists and clients that frequently update

Partition attack on client knowledge (2)

- Directory servers can be out of sync; evil directory servers can give out rigged subsets to trace clients.

- Fix: DSs must successively sign directory bundles; a threshold of servers is assumed good.

Partition attack on message expiration date

- Delaying a message a few days will push its exp date to one end of the valid window – so they won't be uniformly distribu1(e)-601(d.)TET1001-47.82

Tagging attack on headers

- Mixmaster headers have a hash to integrity-check the fields for that hop. But it -oesn't check the rest of the header.
- So we can flip some bits later in the header, and if we own the node later in the path that corresponds to the header we just broe, we can recognize the message.
- We must make the hash cover the entire header.

We’re still using Cypherpunk replies

- No replay protection

We support three delivery types

- Forward messages, only Alice remains anonymous
-

Replies are anonymous:

Open problem: reputatioT17L0ee17L0di p

Open probleOpen prok10Td5(long-termp)-35(

Privacy Enhancing Technologies workshop