1 Threats to Privacy and Personal Freedom

1.1 Media Threats

- RIAA
- MPAA

1.2 Government Threats

- Department of Homeland Security
- Federal Bureau of Investigation
- Patriot Act

2 How Lawsuits Happen in Standard P2P

- Search results contain IP addresses
- Downloads use IP addresses for direct connections (fast downloads)
- RIAA uses IP addresses to file lawsuits
- We could prevent these kinds of suits if we had anonymous communication.

3 Anonymous Communication in the Real World

- Alice an Bob are in a crowd
- Alice doesn't know who or where Bob is, and Bob doesn't know Alice either.
- Alice wants to get a message to Bob without revealing her identity to Bob or to anyone else.

4 The Crying of Lot 49

- An underground postal system for paper messages
- Senders and receivers are anonymous
- Not clear from the book how the routing works

5 The Message's Point of view

- Message must go from source to destination
- Message cannot have global information about where destination is
- Message must not carry global information about where it is coming from.

6 Ants do this

- Ants travel from their nest to food (and back) with no global information about their environment
- How? By using local routing cues
- Mark ground with chemical scents called pheromones
- Explore randomly, leaving pheromones behind
- Follow the strongest pheromone trails

7 Improving the Ant Model

- Pheromones are non-directional
- An ant may follow a trail backwards by accident
- Physical limits
- Network algorithms are not limited in the same way
- Two pheromone types:
  - "coming from home" pheromone
  - "coming from food" pheromone

8 Back to the Crowd

- Alice passes messages "From Alice, To Bob" to her neighbors
- Message spreads through crowd
- Each person remembers who they first got a message "From Alice" from (like a "coming from Alice" pheromone being left in the crowd)
- Message flood eventually reaches Bob

- Bob can send a message "From Bob, To Alice" back into crowd
- Message back to Alice can follow the "From Alice" trail, leaving a "From Bob" trail as it goes
- A two-way communication path has been established in the crowd
- None of the other crowd members know who Alice and Bob are

9 In a Network

- People in crowd become network nodes
- Neighbors are the small set of nodes that each node maintains connections to (sockets)
- Passing a message means sending a message through one of these neighbor connections
- Each node maintains a table of pheromone scents that track which neighbor messages *from* Alice are coming from
- When a node sees a message to Alice, it sends the message back through the appropriate neighbor

10 MUTE Virtual Addressing

- Random 160-bit numbers (encoded as 40-character hex strings) used as virtual addresses
- Virtual addresses picked using a cryptographically sound random number generator
- Extremely small chance of collision (addresses are effectively unique)
- Nodes keep their virtual addresses secret: they grab messages addressed to them, but they never divulge their addresses to other nodes.

11 MUTE Routing as a Black Box

- Routing layer supports delivering message from one virtual address to another anonymously
- We can build all sorts of services on top of MUTE routing (examples: chat, web browsing, and email)
- Main example: file sharing.

12 MUTE File Sharing

- Downloads are routed based on virtual addresses
- RIAA node learns nothing about the identity of the uploader or downloader
- RIAA learns nothing by performing a search

13 MUTE Neighbor Link Encryption

- What about an RIAA spy sniffing packets on the local network?
- Encryption used to secure each neighbor link:
  - AES 128-bit stream ciphers
  - RSA Public Key System (1024-bit default) to exchange secret AES keys
  - Fresh AES key used for each stream
  - Separate key used for each stream direction

14 Open Source Tools Used

- Graphics: Dia, The GIMP (including logo and slides)
- Slide typesetting: LaTeX
- GUI: wxWindows (now called wxWidgets)
- Cryptography: Crypto++
- All development tracked via SourceForge

15 The Future; More Info

- MUTE has been very popular so far (270,000 downloads in less than 6 months)
- More details at the MUTE website