WHY DO WE NEED ANONYMITY?

• Protect legitimate personal privacy concerns
  – Privacy in medical issues or psychological counseling
  – Allow for safe “whistle blowing”

• American Association for the Advancement of Science (AAAS) believes that privacy is a fundamental human right, and certainly a right guaranteed by the U.S. Constitution
PREVIOUS EFFORTS AT ANONYMITY

• Single Proxy
  – Pre-assigned machine forwards data for the network
  – Responder can determine Proxy but not Initiator
  – Disadvantage
    • Initiator not anonymous from Proxy
SINGLE PROXY

I - Initiator
R - Responder
P - Proxy
EXISTING ANONYMOUS PROTOCOLS

CROWDS

- Forward connection randomly through series of host-level proxies
- Should be a jondo to participate
- Anonymous as no proxy can determine if last hop was Initiator
EXISTING ANONYMOUS PROTOCOLS

CROWDS

I - Initiator
R - Responder
J - Jondo
EXISTING ANONYMOUS PROTOCOLS

ONION ROUTING

• Onion Routers added to network as special service
• Initiator connects to onion router
• Onion router encodes network path in packet
• Packet follows constructed path to R
EXISTING ANONYMOUS PROTOCOLS

ONION ROUTING

I - Initiator
R - Responder
O - Onion-router
DRAWBACKS

• Latency Issues
  – Crowds members located all over Internet.
  – Latency can be arbitrarily bad, depending on location of random members on path

• Traceback
  – When connection is active, follow flow of packets (active trace back)
  – When connection is inactive, examine internal state at each member (passive trace back)
OUR DESIGN GOALS

• Provide privacy for individual users
• No new network infrastructure
• Reduce latency
• Limit Traceback
• Forward path: Layered encoding, similar to Onion Routing, allows control of path
• Return Path: Use IP Multicast
• IP Multicast allows anonymous reception over shortest path
I - Initiator
R - Responder
O - Onion-router

HORDES
ADVANTAGES OF HORDES

• Uses existing network services
• No return path stored at intermediate hops - limits trace-back
• Multicast on return path - reduces latency
• Multiple receivers - provides anonymity
HORDES

• Work done
  – Implementation for HTTP protocol

• What’s next?
  – Modules for other protocols: FTP, Telnet etc
  – Real world testing and distribution
  – Interoperability across various platforms
  – Improved Key distribution and management