# Onion Routing

**Yanyan Zhuang**

Department of Computer Science

http://www.cs.uccs.edu/~yzhuang/

# Tor History

- **1996**: “Hiding routing information”, by David Goldschlag, Michael Reed and Paul Syverson, International Workshop on Information Hiding
- **1997**: “Anonymous connections and onion routing”, by Michael Reed, Paul Syverson, and David Goldschlag, IEEE Symposium on Security and Privacy
- **1998**: Distributed network of 13 nodes at Naval Research Lab (NRL), UMD
- **2000**: “Towards an analysis of onion routing security”, Paul Syverson, Gene Tsudik, Michael Reed, and Carl Landwehr, Designing Privacy Enhancing Technologies

# Tor History

- **1996**: “Hiding routing information”, by David Goldschlag, Michael Reed and Paul Syverson, International Workshop on Information Hiding
- **1997**: “Anonymous connections and onion routing”, by Michael Reed, Paul Syverson, and David Goldschlag, IEEE Symposium on Security and Privacy
- **1998**: Distributed network of 13 nodes at Naval Research Lab (NRL), UMD
- **2000**: “Towards an analysis of onion routing security”, Paul Syverson, Gene Tsudik, Michael Reed, and Carl Landwehr, Designing Privacy Enhancing Technologies
- **2003**: Tor network deployed (12 US nodes, 1 German), Tor code released by Roger Dingledine and Nick Mathewson under free MIT license
- **2004**: “Tor: The Second-Generation Onion Router”, by Roger Dingledine, Nick Mathewson, and Paul Syverson, USENIX Security Symposium
- **2006**: The Tor Project, Inc., as a non-profit

# Hiding Routing Information

- Onion routing: Why encryption alone is not enough?
  - Headers can't be encrypted
- Advantage
  - Well-written
- Disadvantage
  - Need to know all routers
  - Attacks not in details
  - One-way anonymity
  - Padding

# Hiding Routing Information

- Issues
  - Computationally expensive: public key encryption
  - Padding wastes bandwidth
  - Network congestion
  - Hostile proxy
  - Once a circuit established, can’t change the circuit
- What’s missing?
  - How to find proxy servers?
  - What if the server wants to be hidden? You can DDoS a server