Midterm Project Presentation
Tor Fingerprinting Attack

Wooyoung Chung – George Karavaev – Nathan Dautenhahn

Computer Security II
University of Illinois Urbana-Champaign

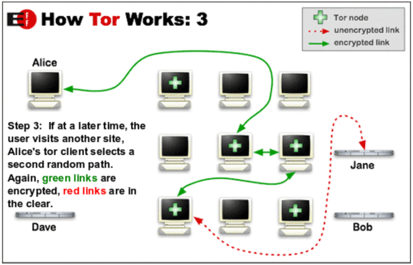
October 29, 2009

Outline

- Tor Background
- Current Status
- Future Agenda

Background

- Tor is an online anonymity tool
- Works for a few applications: browsing, chat
- Defends against global advesary
- Attacks attempt to gain information as to what content a given client is viewing
- All data sent in fixed cell sizes and encrypted
- Fingerprinting attack: adversary listens to Tor Proxy and uses pattern recognition to identify a website



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Current Status

- Fingerprint Development
  - Use number of packets for fingerprint
  - Packets with data are approximately 650 bytes long
  - Collect unique data about each website
- Initial Fingerprint Results
  - Appears as though entry nodes can use whatever port they choose as long as it uses TLS
  - Used Ports: 443, 1443, 9001
  - SHOW HERE IMAGE OF INITIAL PACKET ANALYSIS

Future Agenda

- Fingerprint Refinement
- Implement attack to detect single request per stream
- Analyze results from implementation
- Refine fingerprint and/or recognition software
- Implement detection for multiple requests per stream