Review for Final

Of content that came after the midterm
Final Exam Overview

- Thursday 12/11 2:30 - 4:20PM
- **Bring your router**, its power supply, ethernet cord, etc
- Closed book
- Calculators encouraged (nothing fancy)
- Essay questions
- Don’t Cheat
Final Exam Overview

• Material not mentioned in the lectures will not appear
  • Exam weighted towards post-midterm material
  • 25% pre-midterm, 75% post-midterm
• You are responsible for Chapters 1-6, 8, 9
• Subsections of interest for post-midterm content: 4.3; 5.1, 2; 6.1, 2, 3; 8.1, 2, 3, 4, 5; 9.1, 4
TCP (part3)

- Nagle’s Algorithm, Delayed acknowledgements
- Congestion and fairness
  - Implicit congestion feedback
  - Slow start
  - AIMD
- Fast retransmit, Fast recovery
Inter-domain Routing

- Hierarchical addressing and Route aggregation
- IP forwarding based on Prefix matching
- Autonomous System (AS) structure of Internet
  - Hierarchy and coordination through border routers
  - AS relationships (Peer, Provider, Customer), router export policies
  - Inter-domain (AS) paths (quality vs. price)
- BGP-4
- Multi-homing
DNS

• Problems with using HOSTS.TXT
• DNS hierarchy, namespace distribution
  • Query/Response protocol
  • Recursive and Iterative lookups
  • Bootstrapping
• Caching
• DNS resource records (RR)
• DNS’ vulnerability to attack
HTTP

• Request\Response protocol
• Why is HTTP 1.0 performance so bad?
  • Interplay between TCP mechanisms and HTTP
• How does HTTP 1.1 improve things?
• Caching
Security (I)

- Security threats
  - Application vulnerabilities
  - ICMP attacks
  - TCP attacks
  - DNS attacks
  - Routing attacks
  - DoS attacks
- Firewalls, Network\App-layers security
  - Flow reconstruction in firewalls
Security (2)

- Network security goals and threats
- Encryption
  - Key integrity (message auth codes)
  - Challenge\Response authentication
  - Encrypting large messages (chaining)
- Public Key Encryption
  - For establishing sessions keys
  - Distribution (PKI, X.509), Revocation
  - Kerberos, Message Digests
- PGP, SSL/TLS, IPSEC
Privacy

- Anonymizing proxies
- MIX nets
- Tor (onion routing)
- SlyFi (you don’t have to know protocol details)
Peer-to-Peer Systems

- Benefits of P2P Systems
- Challenges for designing P2P Systems
- Napster, Gnutella and BitTorrent high-level protocol details
- Why are incentives necessary for P2P systems to be successful?
- BitTorrent tit-for-tat incentives strategy