TCP/IP
Security Attacks

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

These slides are available on-line at:

http://www.cse.wustl.edu/~jain/cse571-07/

1. TCP Segment Format, Connection Setup, Disconnect
2. IP: Address Spoofing, Covert Channel, Fragment Attacks, ARP, DNS
3. TCP Flags: Syn Flood, Ping of Death, Smurf, Fin
4. UDP Flood Attack
5. Connection Hijacking
6. Application: E-Mail, Web spoofing

TCP Segment Format

Source Port								Destination Port
Sequence Number								
Ack Number								
Data Offset	Res	Urg	Ack	Push	Reset	Syn	Fin	Window
Checksum								Urgent Pointer
Options								Padding
Data								

- Urgent: Deliver immediately at destination
- Push: Leave source immediately
- First data byte is ISN+1. Ack is next byte expected. Expecting Ack to Ack+window-1 next.