CS 181AG
Lecture 23

Security & Wireless

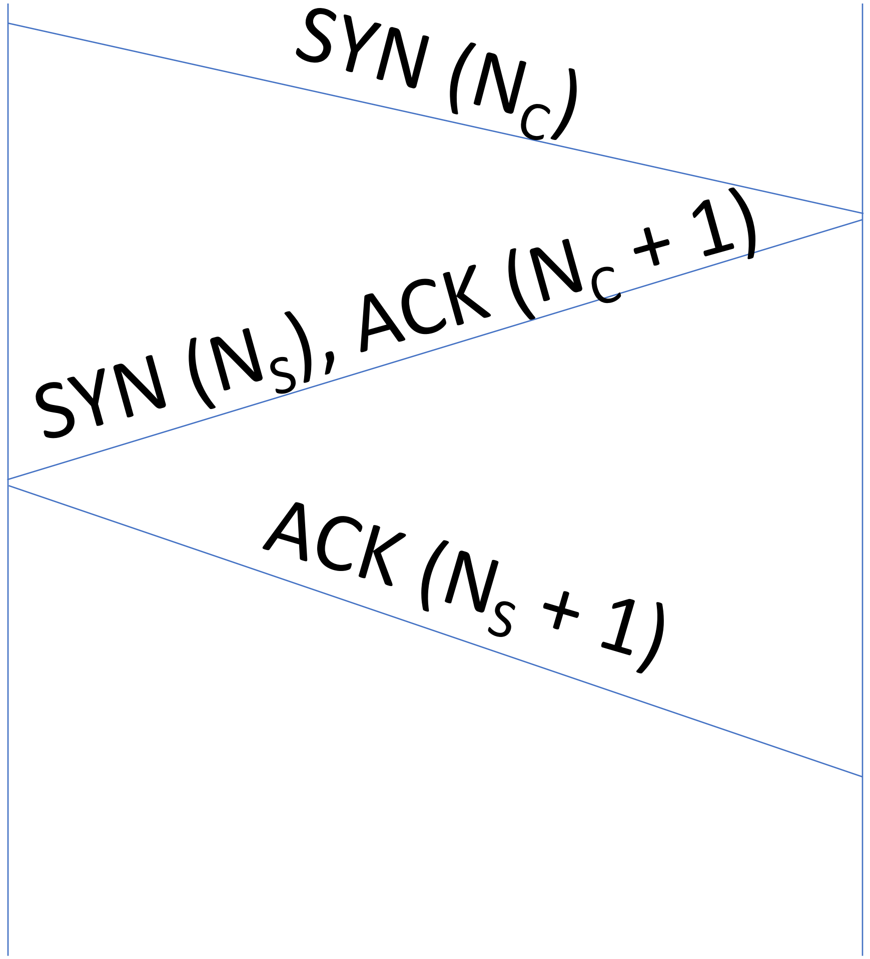
Arthi Padmanabhan

Dec 5, 2022

Today’s Plan

- Last lecture before final review (!!)
- Couple (unrelated) topics that I think are good for you to know before leaving the class :)
  - How can attackers take advantage of the protocols we’ve learned about recently to pretend to be someone else? What are the measures to stop or reduce the chances of that?
  - How do wireless networks and cell service work?

Network Security: TCP



Network Security: TCP

- If you can get server’s sequence number, you can start sending data to server
- Bad for:
  - Any IP-based authentication (SMTP)
  - Rlogin (now replaced by ssh)
  - Could send reset packets to disrupt someone else’s ability to interact with server
  - What about router-to-router communication (e.g., BGP)?

Network Security: TCP

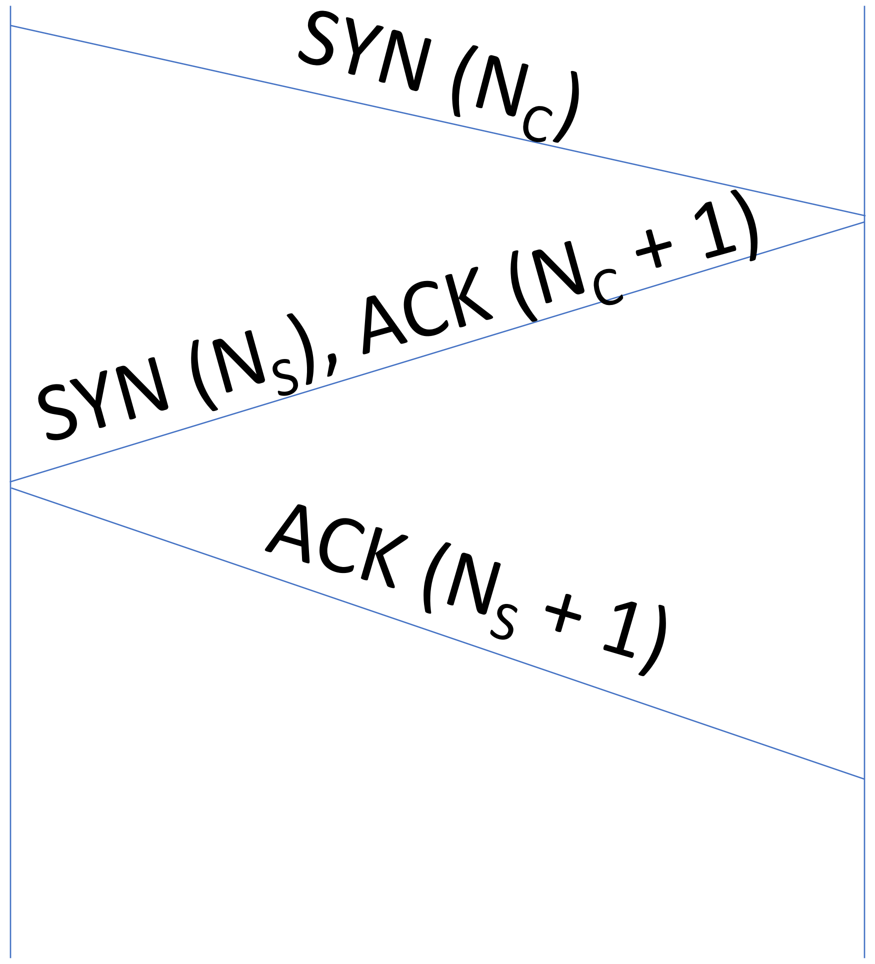
- Guessing server’s sequence number used to be easier
- Sequence number incremented by some value (e.g. 16k) for each new connection

Network Security: TCP

- Guessing server’s sequence number used to be easier
- Sequence number incremented by some value (e.g. 16k) for each new connection
- One fix: change sequence numbers per connection, not globally

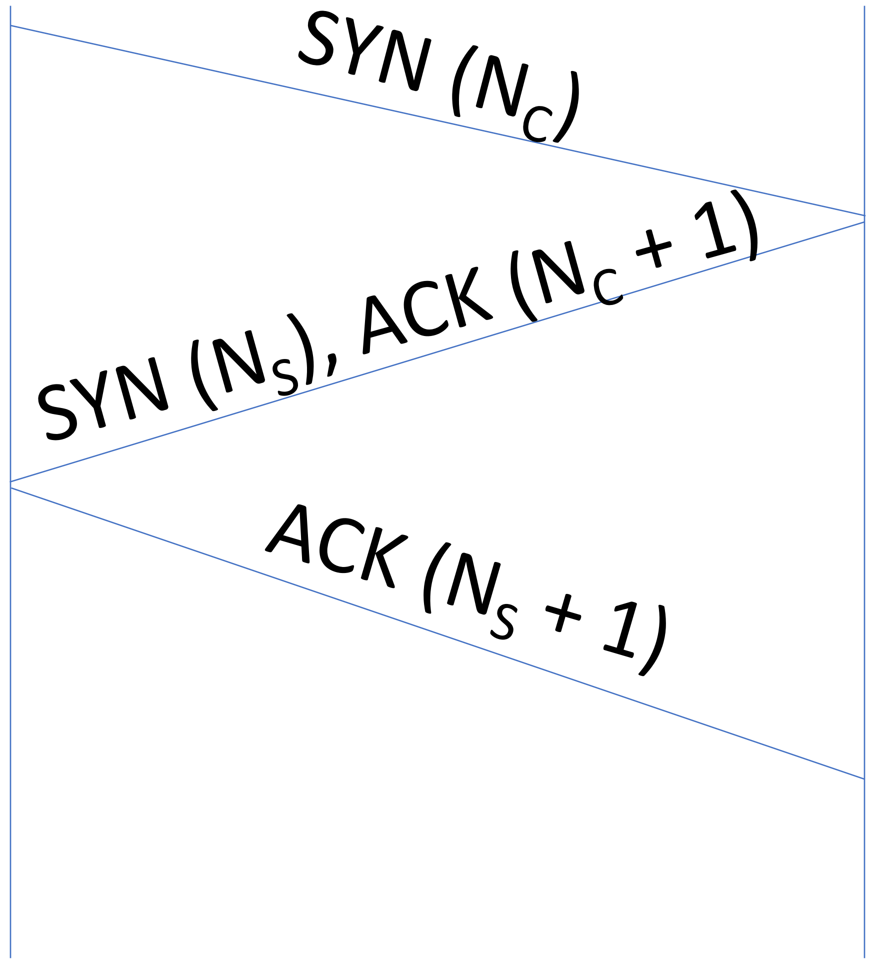
Revisiting DDoS on TCP

- Server must store state (client sequence number and its own sequence number) for each client
- Send flood of packets such that table overflows



Revisiting DDoS on TCP

- Solution: only keep state after client has echoed back a computable key



Network Security: DNS

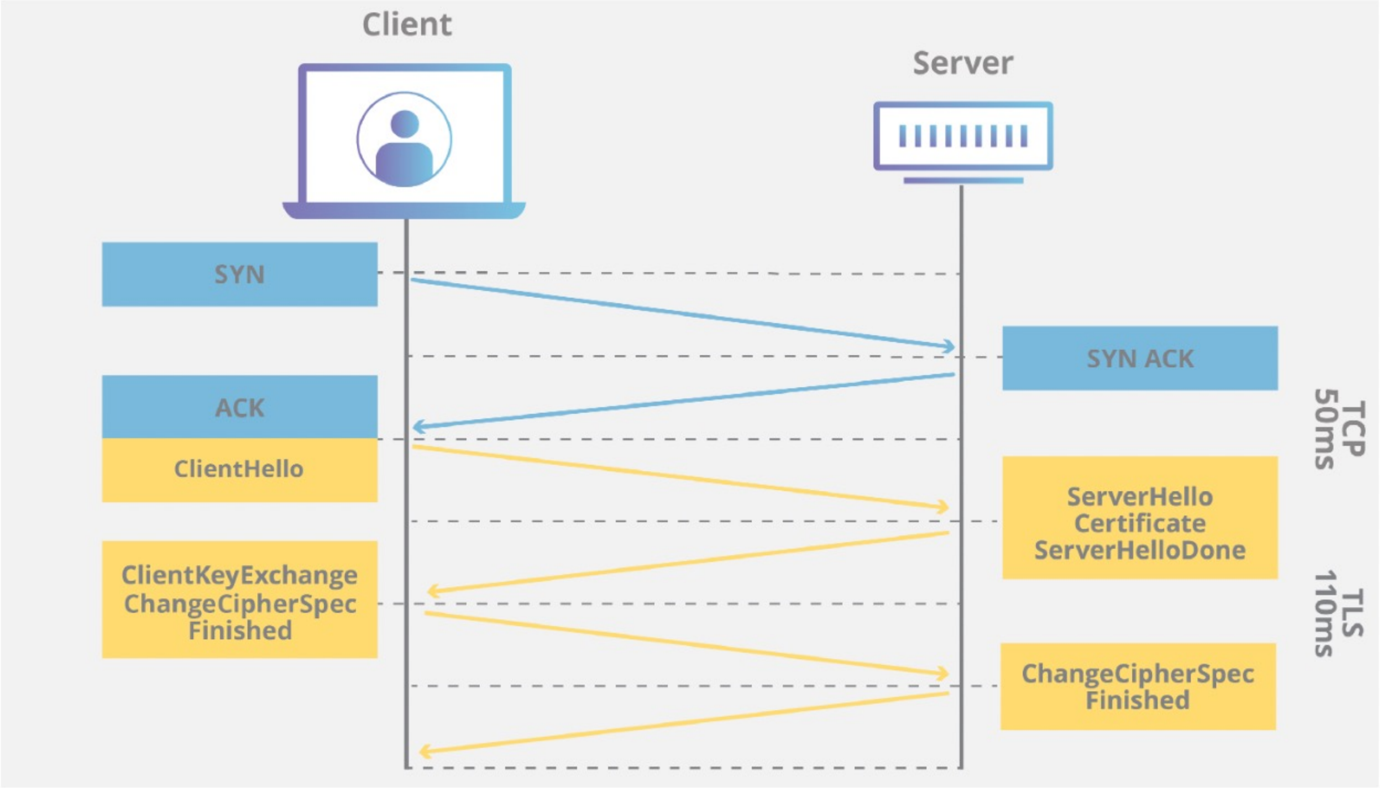
- DNS was particularly vulnerable to attacks
- Used UDP (no setting up connections)
- By convention, source and dest port were 53
- Why is this bad?

Network Security: DNS

- Places to inject randomness: source port, query ID
- Add security at application level – DNS responses should be signed
    - Gets complicated: how to sign that a response does not exist?

TLS

- When your browser runs https, it is using TLS
- TLS encrypts and authenticates data



Wireless Communication & Cell Service

- When we see colors, we’re seeing waves – tighter waves -> purples, looser waves -> red
- Much shorter = much more powerful -> x-rays
- Much larger = ultra-high frequency **radio** wave
  - Can travel large distances, bend around obstacles
  - Good for communication

Properties of Waves

- Amplitude
- Wavelength (corresponds with frequency)

Binary

- High amplitude = 1, low amplitude = 0
- OR high frequency = 1, low frequency = 0

Other Ways of Encoding with Waves

- Could also consider the wave going up vs wave going down
- Could also consider more than 2 “phases” – up to 8
- Could consider amplitude in addition

Code Division Multiple Access

- User 1: 11
- User 2: 01
- User 3: 10