Agenda

- Review: the Kevin Mitnick Attack
- The TCP Protocol (Basics) and SYN Flood Attack

Kevin Mitnick is ___.

- A. A hacker who hacked into Jennifer Lawrence's iCloud account and released her nude photos online.
- B. A professor at BSU.
- C. A hacker who was on the FBI's most wanted list.
- D. Kim Kardashian's husband.

Kevin Mitnick is ___.

- A. A hacker who hacked into Jennifer Lawrence's iCloud account and released her nude photos online.
- B. A professor at BSU.
- C. A hacker who was on the FBI's most wanted list.
- D. Kim Kardashian's husband.

The Kevin Mitnick attack was against the ___.

- A. TCP 1-way handshake
- B. TCP 2-way handshake
- C. TCP 3-way handshake
- D. TCP 4-way handshake

The Kevin Mitnick attack was against the ___.

- A. TCP 1-way handshake
- B. TCP 2-way handshake
- C. TCP 3-way handshake
- D. TCP 4-way handshake

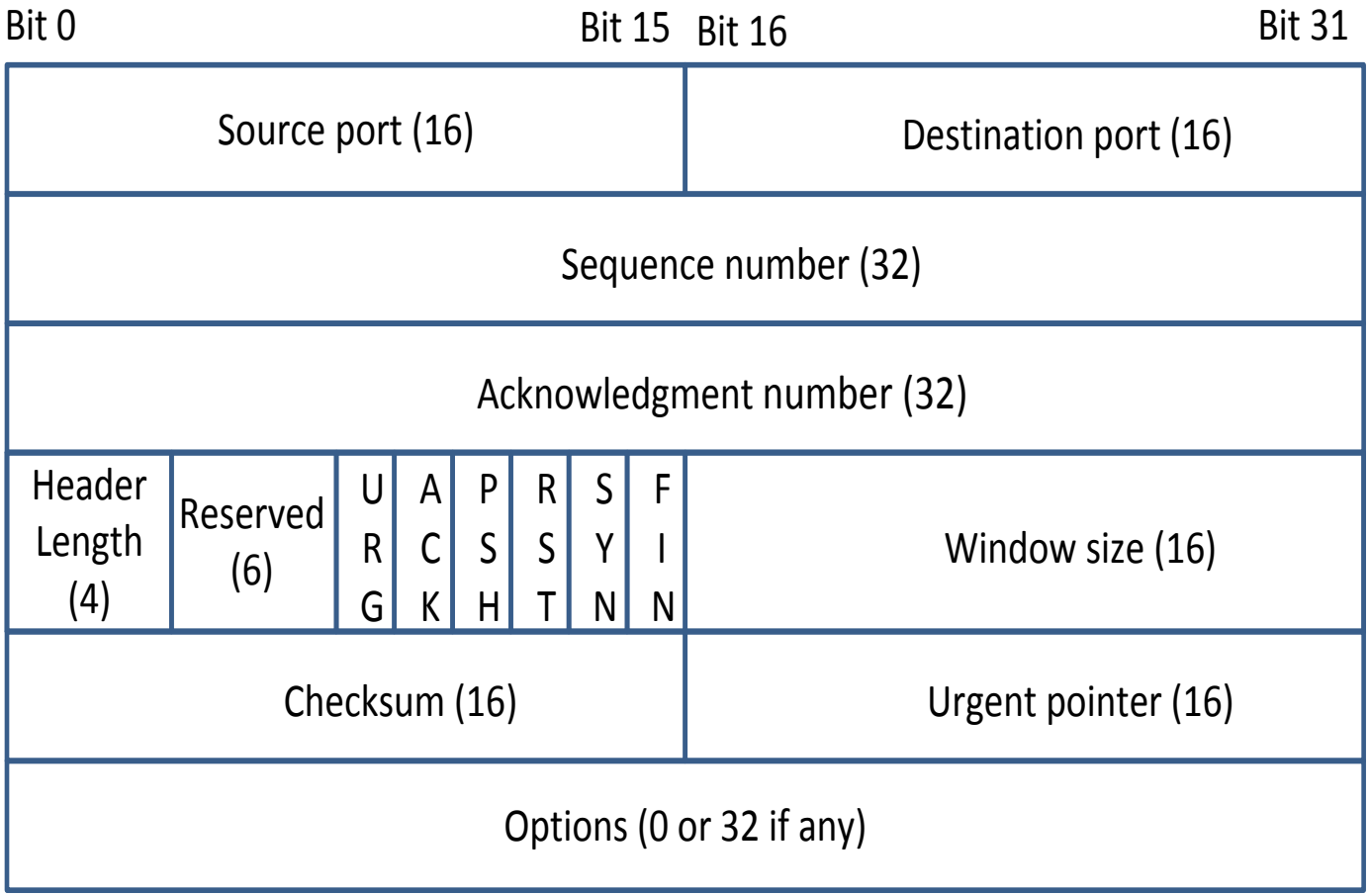
SYN flood is __.

- A. A flood caused by the Hurricane Harvey.
- B. A technique used by attackers to make the target machine busy.
- C. A technique used to establish a TCP connection.
- D. A technique used to synchronize emails between Hillary Clinton's private email server and the government's official email server.

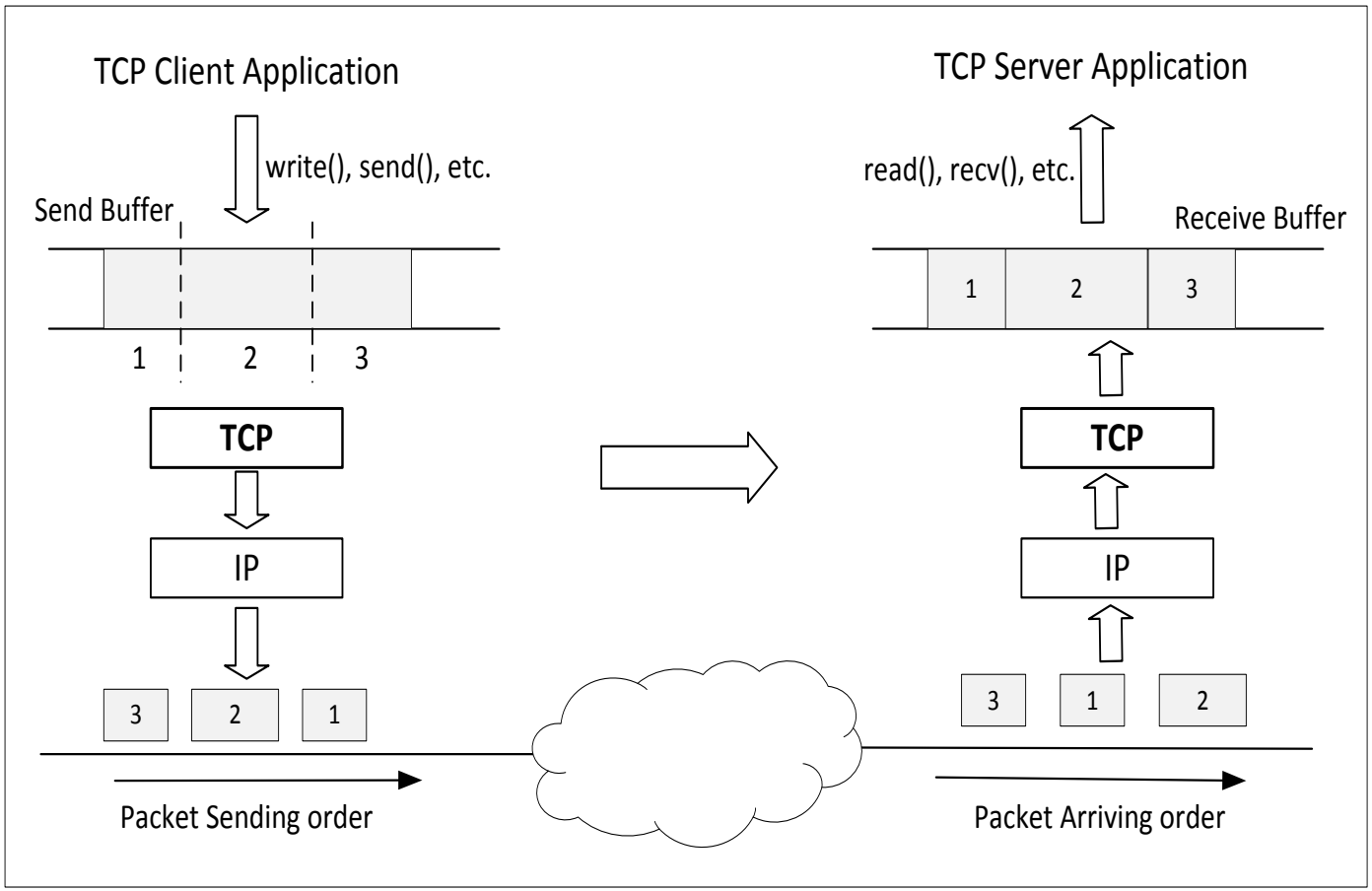
SYN flood is __.

- A. A flood caused by the Hurricane Harvey.
- B. A technique used by attackers to make the target machine busy.
- C. A technique used to establish a TCP connection.
- D. A technique used to synchronize emails between Hillary Clinton's private email server and the government's official email server.

Transmission Control Protocol (TCP) Header



TCP Data Transmission



Establish a TCP connection - Client Side Program

- create a socket
- set the destination information
- connect to the server
- send and receive data
- close the connection

Demo code:
http://cs.boisestate.edu/~jxiao/cs333/code/tcpclient.c

Establish a TCP connection - Server Side Program

- create a socket
- bind to a port number
- listen for connections
- accept a connection request
- send and receive data
- close the connection

Demo code:
http://cs.boisestate.edu/~jxiao/cs333/code/tcpserver.c

Denial of Service (DoS attack)

Traffic into and out of a network blocked when servers flooded with malformed packets that contain false IP addresses, other harmful data, or other fake communications.

SYN Flood

Network overloaded with packets that have the SYN flag set.
Servers overloaded with requests for connections and unable to respond to legitimate requests.

Reference

A large portion of the material is adapted/copied from:

- Computer Security - A Hands-on Approach by Wenliang Du
- Guide to Network Defense and Countermeasures - Randy Weaver, Dawn Weaver, Dean Farwood