Agenda

- Review: the Kevin Mitnick Attack
- The TCP Reset 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 ___.

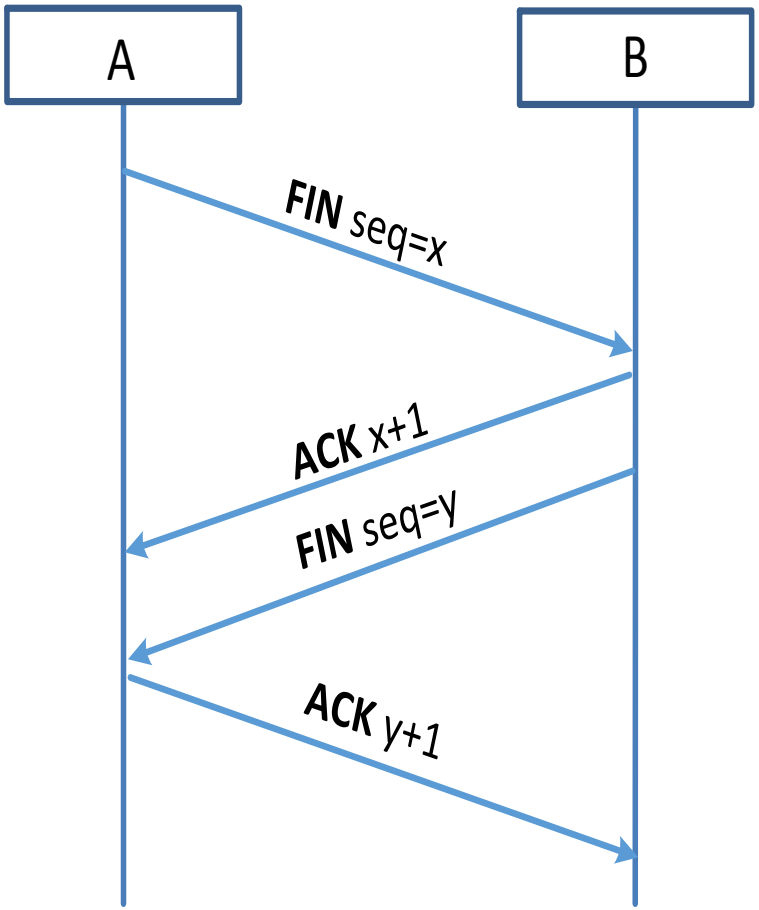
- A. A flood caused by the Hurricane Harvey.
- B. A technique used by attackers to make the target machine busy.
- C. A technique used to establish a TCP connection.
- D. A technique used to synchronize emails between Hillary Clinton's private email server and the government's official email server.

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.

Closing a TCP connection - Civilized Method

Two parties both say goodbye - following TCP FIN Protocol.



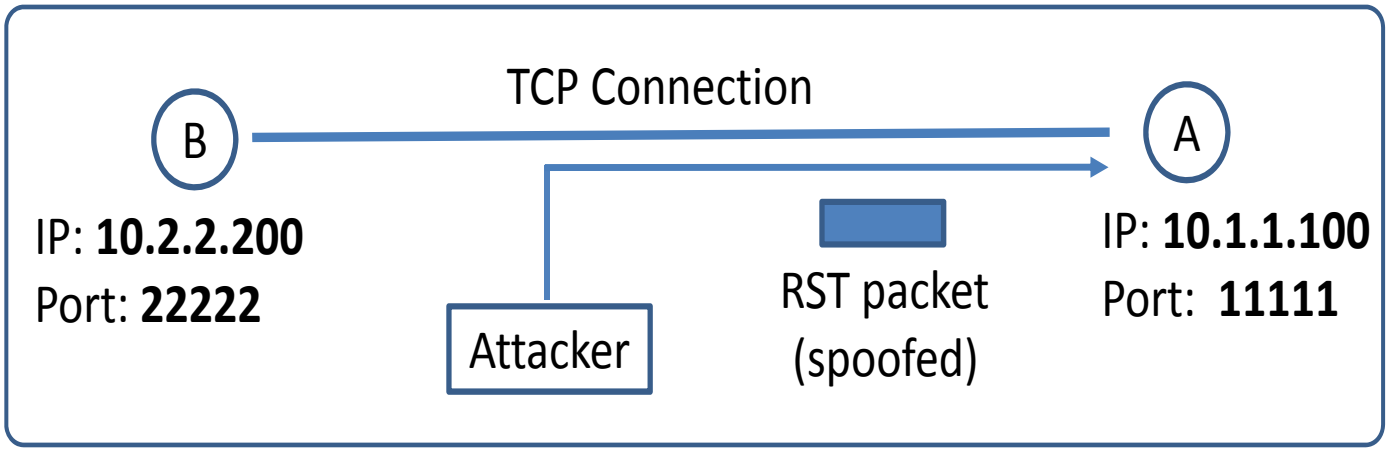
Closing a TCP connection - Rude Method

One party sends a single RST packet to the other; for emergency use only, e.g., when there is no time to do the FIN protocol, or when errors detected.

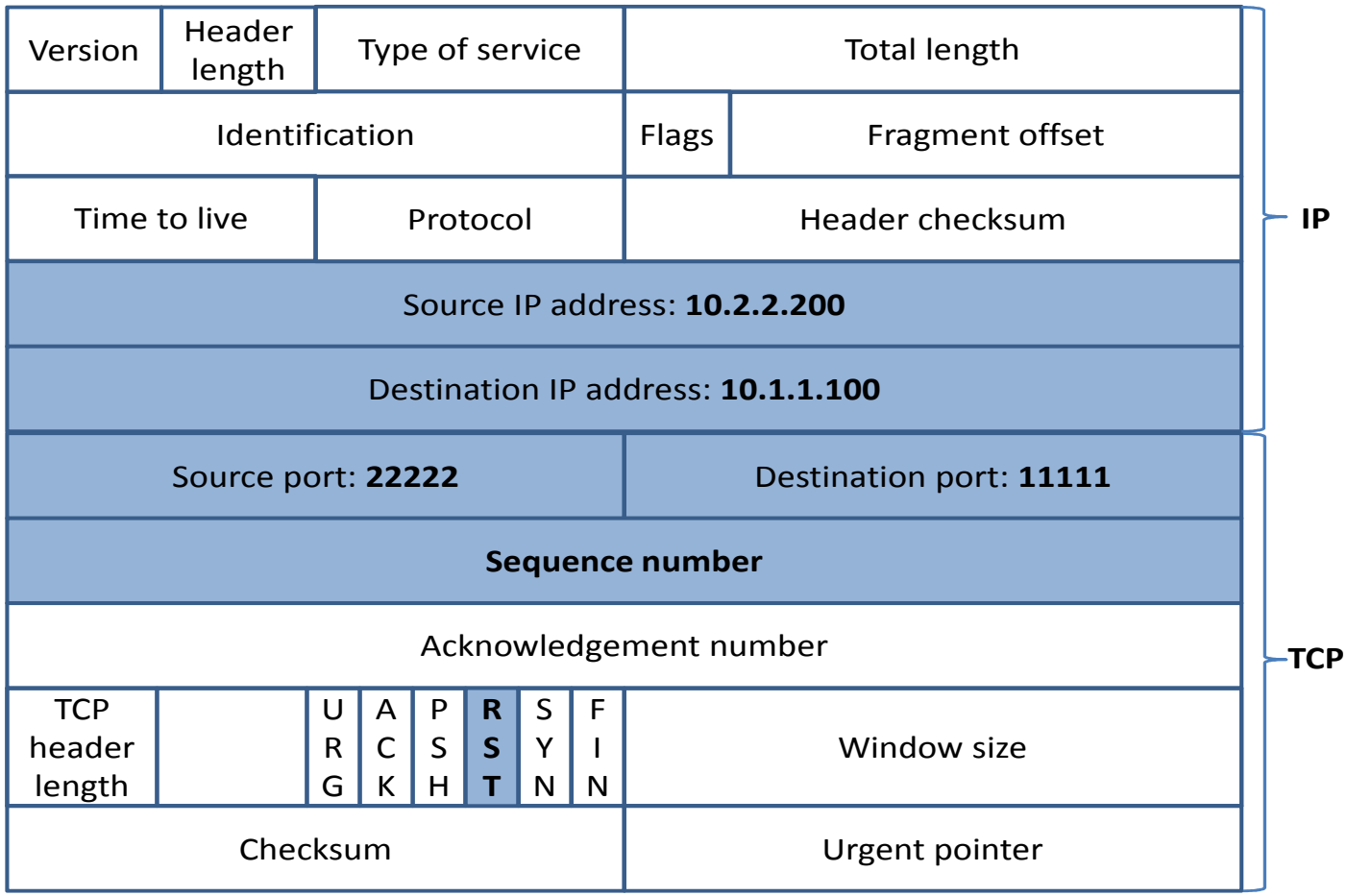
TCP Reset Attack

Attacker spoofs a TCP RST packet from A to B or from B to A, so as to close a TCP connection. A type of DOS attack.

TCP Reset Attack



TCP Reset Packet



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