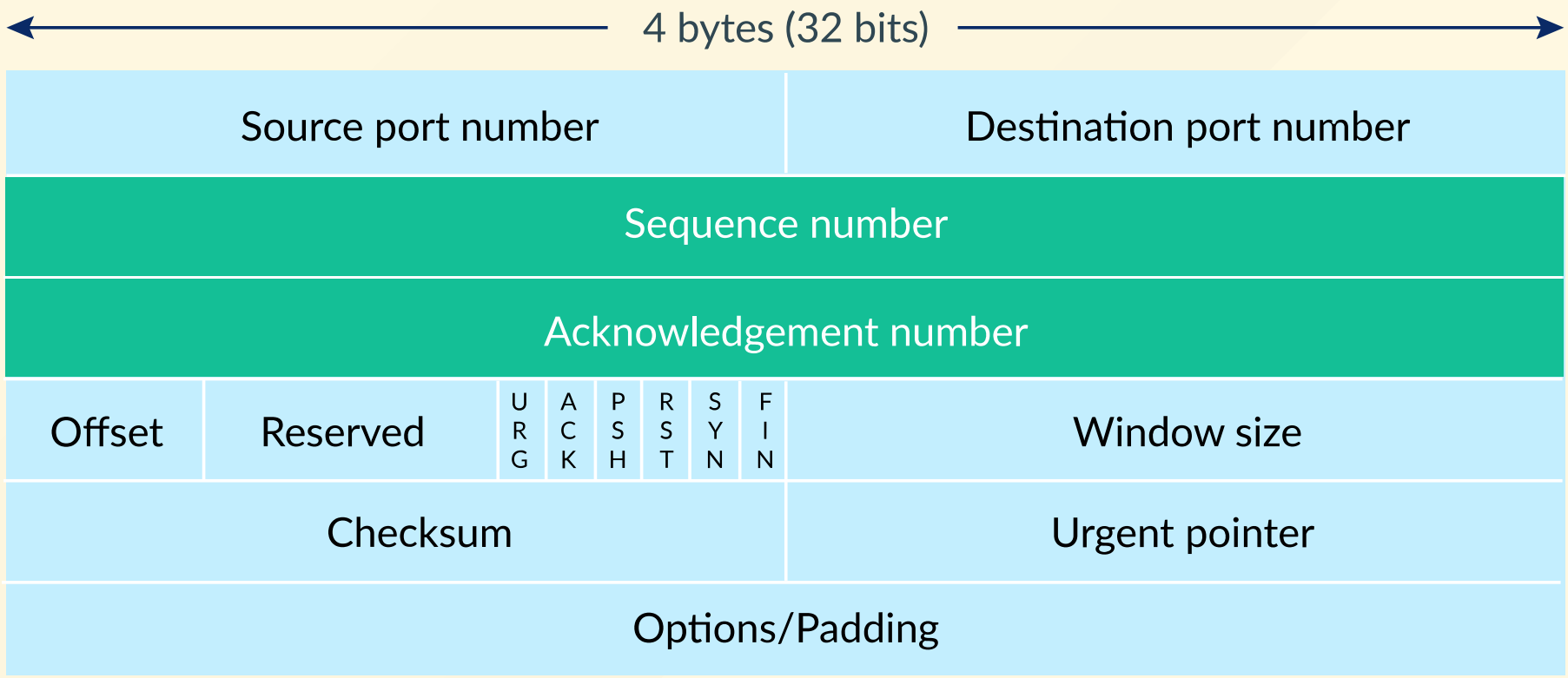
TCP Reset Attacks

- CEG 6430/4430 Cyber Network Security
- Junjie Zhang
- junjie.zhang@wright.edu
- Wright State University

TCP Packet Header



How to Close TCP Connections?

- The "Civilized" Approach: FIN
  - A sends B a FIN and B replies A with an ACK
    - The A-to-B connection is closed but the B-to-A one is open
  - B sends A a FIN and A replies B with an ACK
    - The B-to-A connection is closed
- The "Non-Civilized"/"Emergency" Approach: RST
  - Either A or B sends a single TCP RST packet to the other side
    - Immediately breaks the connection.

RST Can Be Helpful

- No time to do FIN
- A system receives an SYN-ACK packet without sending a SYN packet
  - The server is likely under an SYN flood attack
  - The system can send the server an RST packet to close the half-open connection

TCP RST Attack

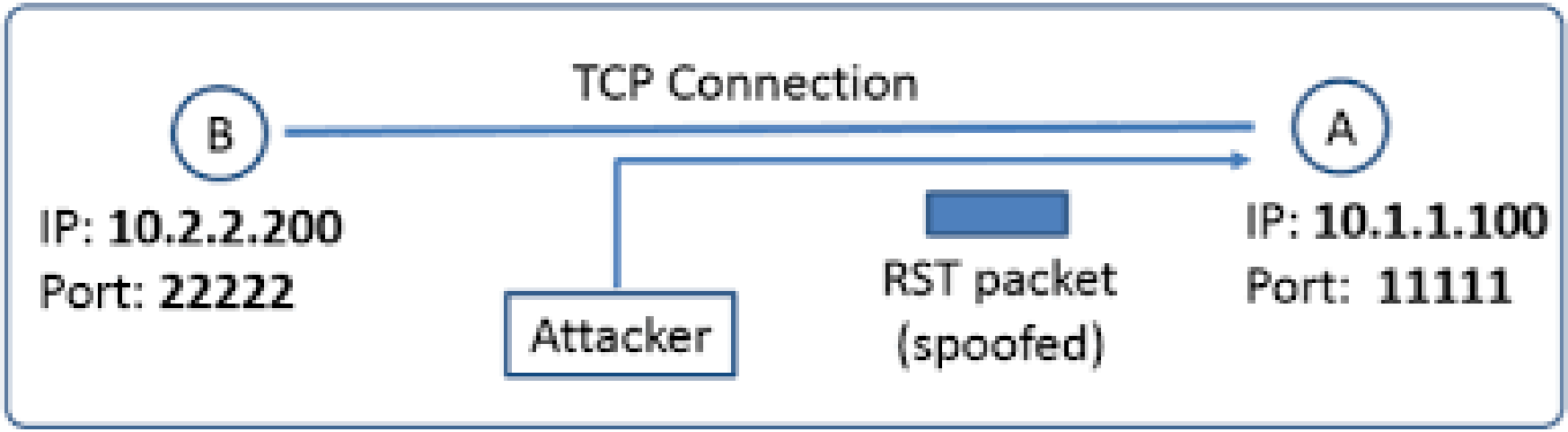
An attacker, say Eve, wants to spoof an RST packet to discrupt an TCP connection between Alice and Bob. This RST packet has to be ***correct***:

- Correct Src & Dst IPs
- Correct Src & Dst Ports
- Correct Sequence Number
  - The sequence number matches the one expected by the receiver.

TCP RST Attack

- Eve is off-the-path: Eve cannot observe packets exchanged between Alice and Bob
  - It is very challenging to launch TCP RST Attack in this case.
- Eve is in-the-path: Eve can observe packets exchanged between Alice and Bob
  - It is much easier to launch such attack since
    - IPs and Ports are readily available from the observed packets.
    - Correct sequence numbers can now be predicted (but the race-condition challenge is still there)

TCP RST Attack



TCP RST Attack Using netwox 78

In console 1, connect to bender using ssh

```
ssh w077jxz@bender.cs.wright.edu
```

In console 2, launch TCP reset attack against this ssh session. 120 is my IP address and 150 is bender's IP address

```
sudo netwox 78 -d eth0 --filter "tcp and src host 172.20.135.210 and dst host 130.108.5.150"
```

```
[w077jxz@head ~]$ tclient_loop: send disconnect: Broken pipe
```