Security of Networks, Services, and Systems

TCP Vulnerabilities

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC

TCP Vulnerabilities

- TCP SYN flooding – already seen this, simplest
- Other vulnerabilities rely on guessing the sequence number
  - TCP session establishment spoofing
  - TCP session hijacking
  - TCP session reset

Spoofing TCP session establishment

Guessing the initial sequence number

"A Weakness in the 4.2BSD Unix TCP/IP Software", Robert T. Morris, AT&T Bell Laboratories

- Use IP source spoofing to bypass firewall, ok to send packets
  - But responses are sent to spoofed address and lost
- Simple for UDP, more challenging for TCP: 3-way handshake
  - **1. A->B:** SYN seq=x ; **2. B->A** (LOST)**:** SYN seq=y, ACK x+1; **3. A->B:** ACK y+1
  - Need to build an ACK packet (3.) without seeing the SYN/ACK packet (2.)
  - Need to guess the initial seq. number y so we can send the ACK packet (3.)

Spoofing TCP session establishment

Guessing the initial sequence number

"A Weakness in the 4.2 BSD Unix TCP/IP Software", Robert T. Morris, AT&T Bell Laboratories

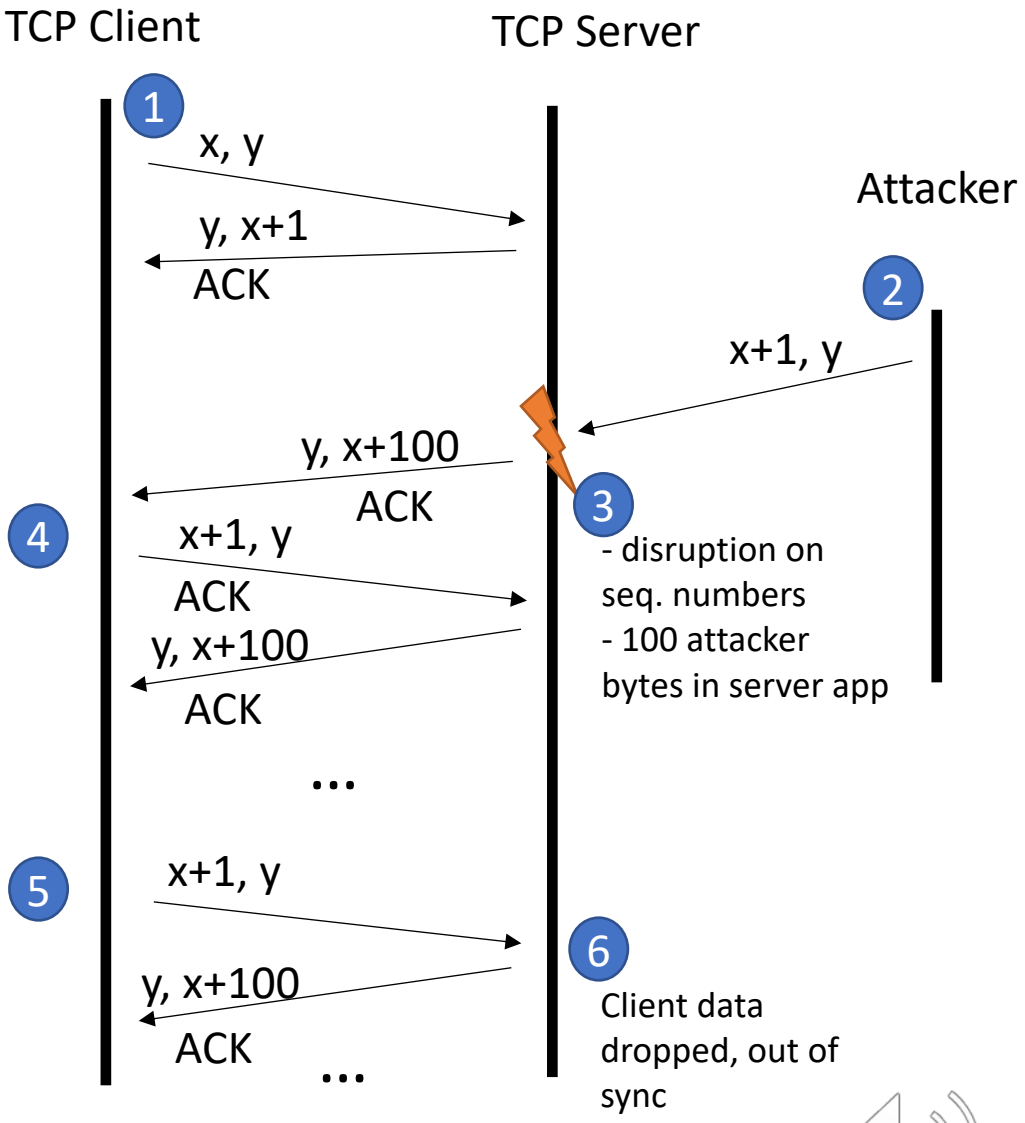
- How are initial sequence numbers generated?
  - 4.2 BSD Unix: +128 every new second, and +64 after each new connection
  - Solution: get seq. number from legitimate TCP connection, add 64 to get y
- Spoofed IP address must not be in use
  - Otherwise spoofed host sends RST packet to server and attack fails

TCP session hijacking

- Goal: inject packets on a TCP connection
- Successful injection causes loss of synchronism
- Hijacking vs. spoofing new session

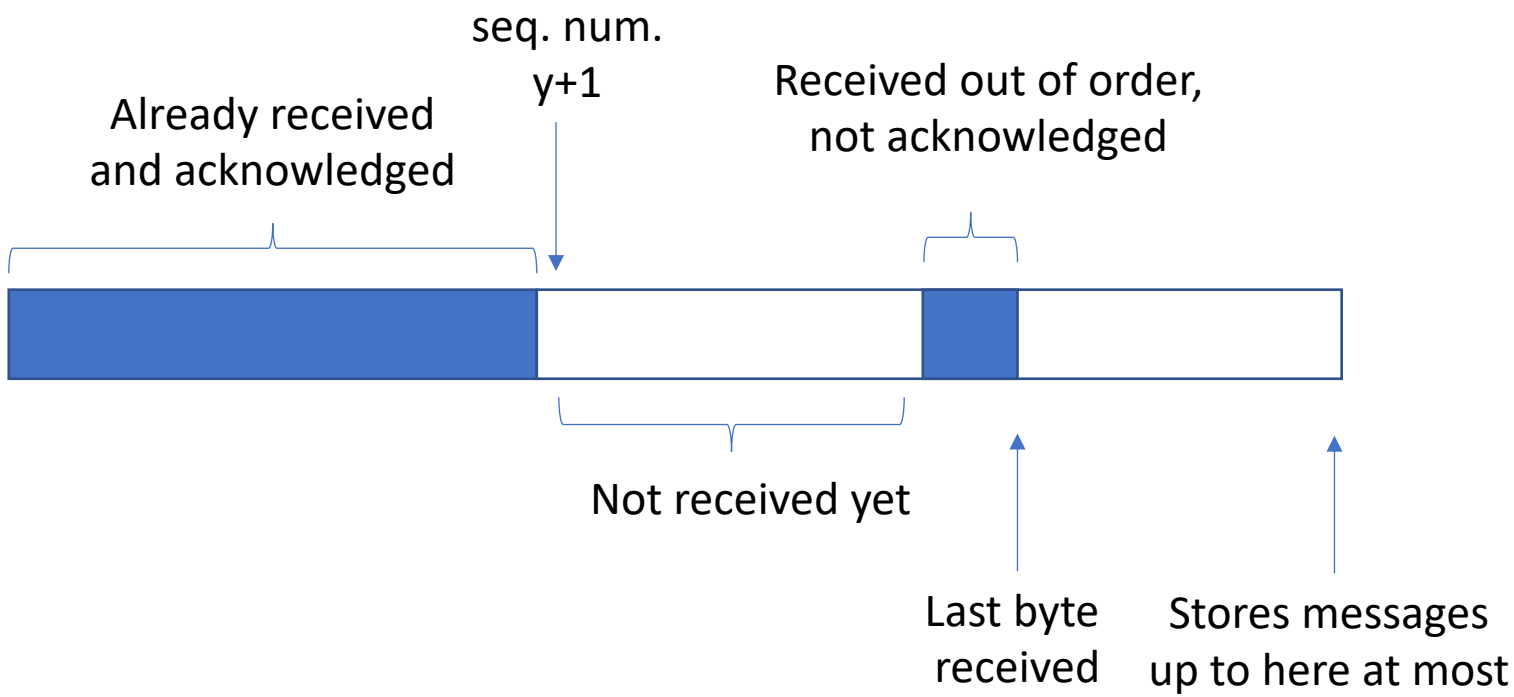
TCP session hijacking

- Spoofed packet with data and expected sequence number **(2)**
- Data delivered to application, sequence number updated **(3)**
- Client expects sequence number not to have changed
  - Responds with ACK to out of sync ACK **(4)** causing ACK storm
  - Sends data with wrong seq. number **(5)** causing server to drop the data

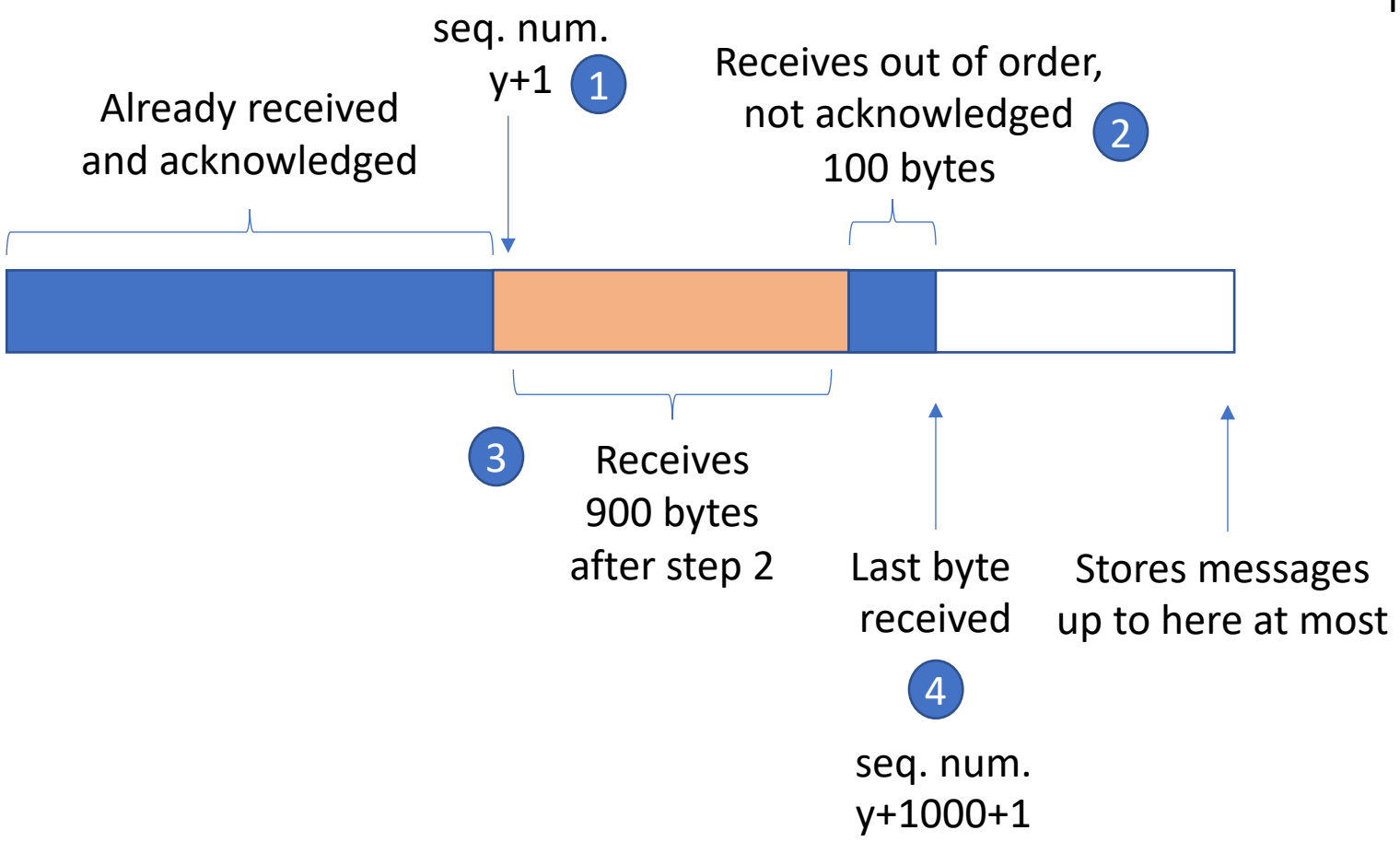


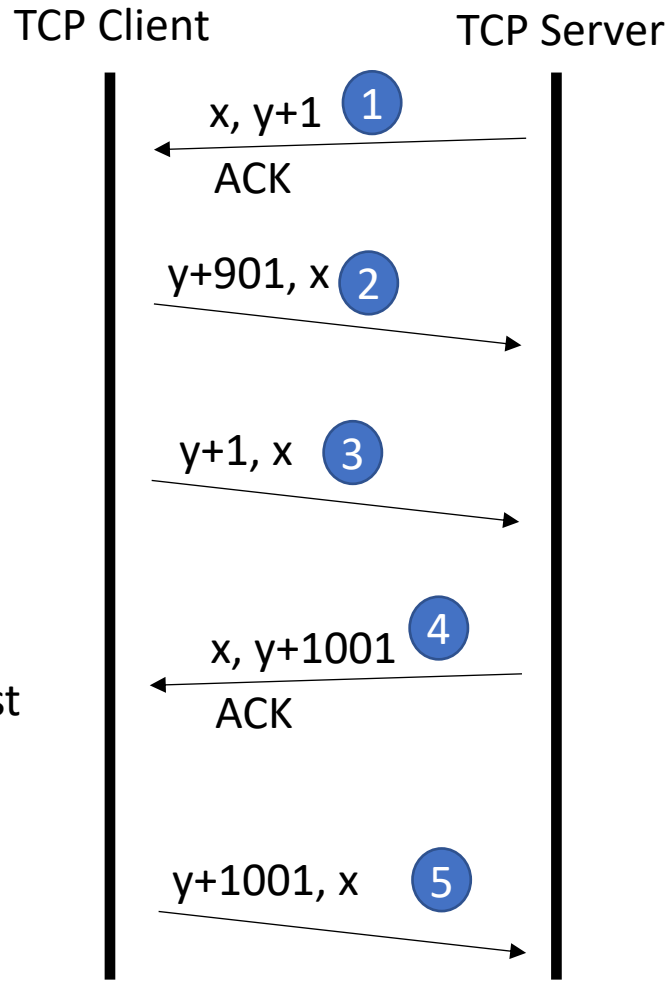
Accepted range of sequence numbers

- Out of order arrival supported
- Limited to receiver buffer

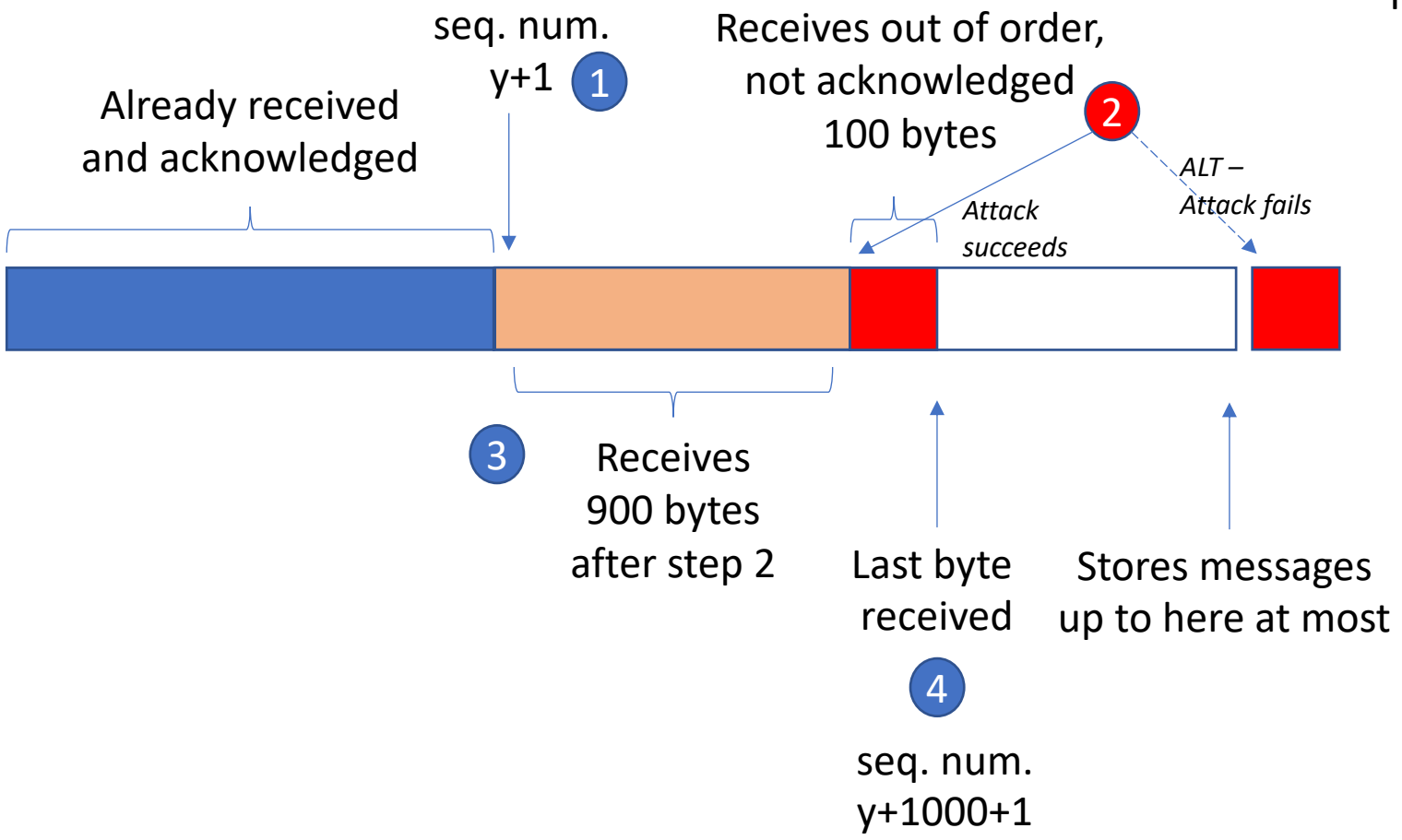


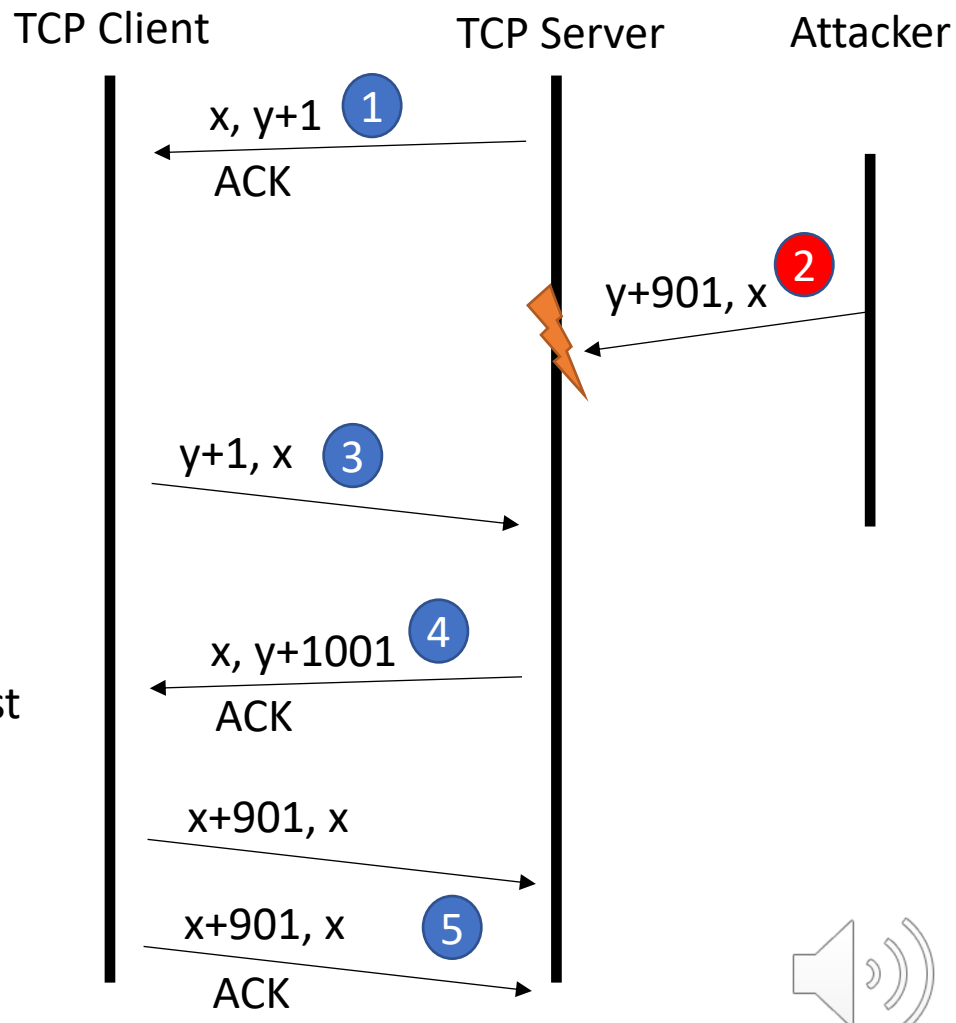
Accepted range of sequence numbers





Accepted range of sequence numbers





TCP reset

- The goal of a TCP reset attack is to break an existing TCP connection
  - The victims are the TCP server, the TCP client, or both
- Civilized tear down of a TCP connection
  - Like the three-way handshake
  - **A->B:** FIN seq=x ; **B->A:** ACK x+1 , FIN seq=y ; **A->B:** ACK y+1
- Uncivilized tear down
  - **A->B:** RST seq=x
  - Done even if A does not reply back to B with final ACK
  - Designed to be used in situations of error

TCP Reset – sequence number

- RST packet
  - Spoof source and destination IP addresses and port numbers
  - Guess the sequence number
- Problem for the attacker:
  - Finding out the value of x in **A->B:** RST seq=x
  - x should be within receiver's window size
  - using the exact sequence number expected by the victim is more robust
- Depends on the topology of the victims and attacker
  - Assume attacker on same network as one of the victims and **can sniff packets**
- Depends on how slowly the sequence numbers change
  - And how fast you can sniff the sequence number and spoof the RST packet

Security of Networks, Services, and Systems

TCP Vulnerabilities

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC