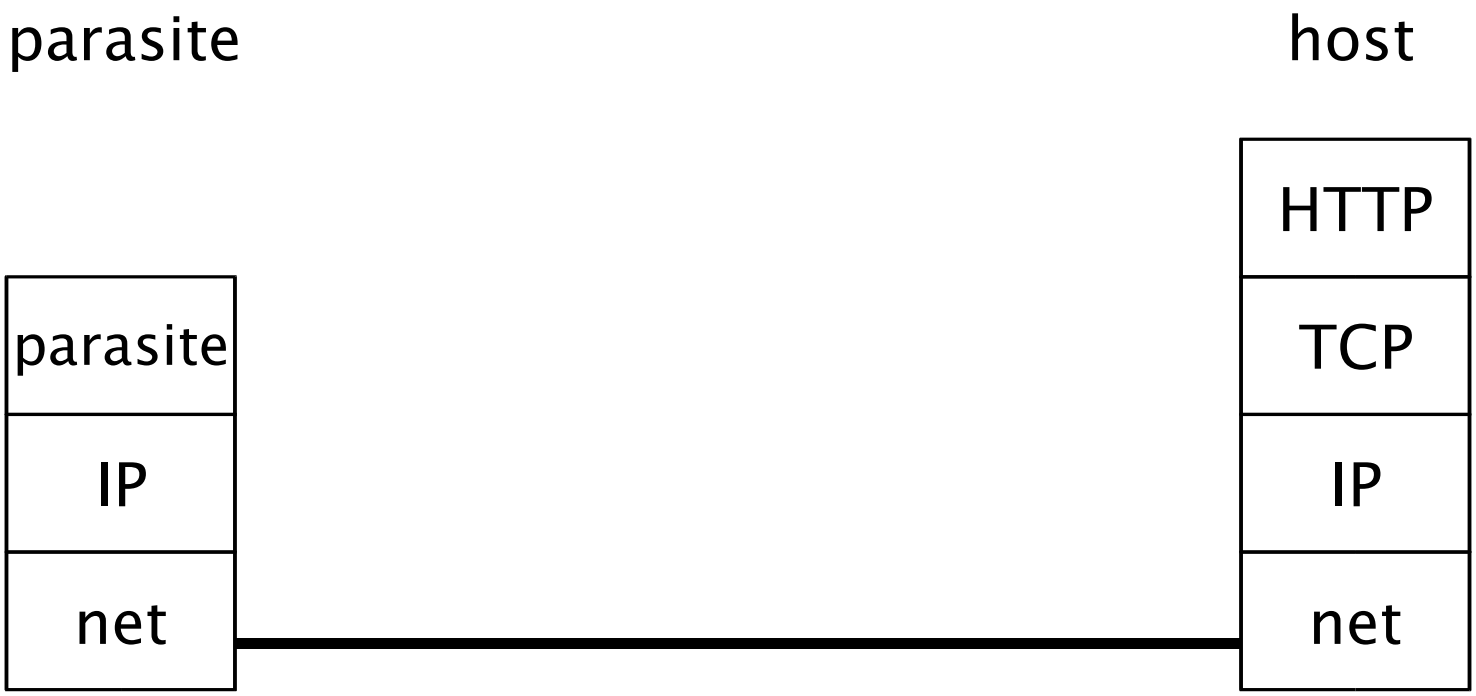
Parasitic Computing Example

Initial configuration



Step 1: Open "modified" TCP connection

- Actions
  - Open TCP connection from parasite code
  - Exchange three messages
  - Extract sequence number
    - from SYN received from host
    - needed for further communication

Step 1: Open "modified" TCP connection

1a) Send SYN message

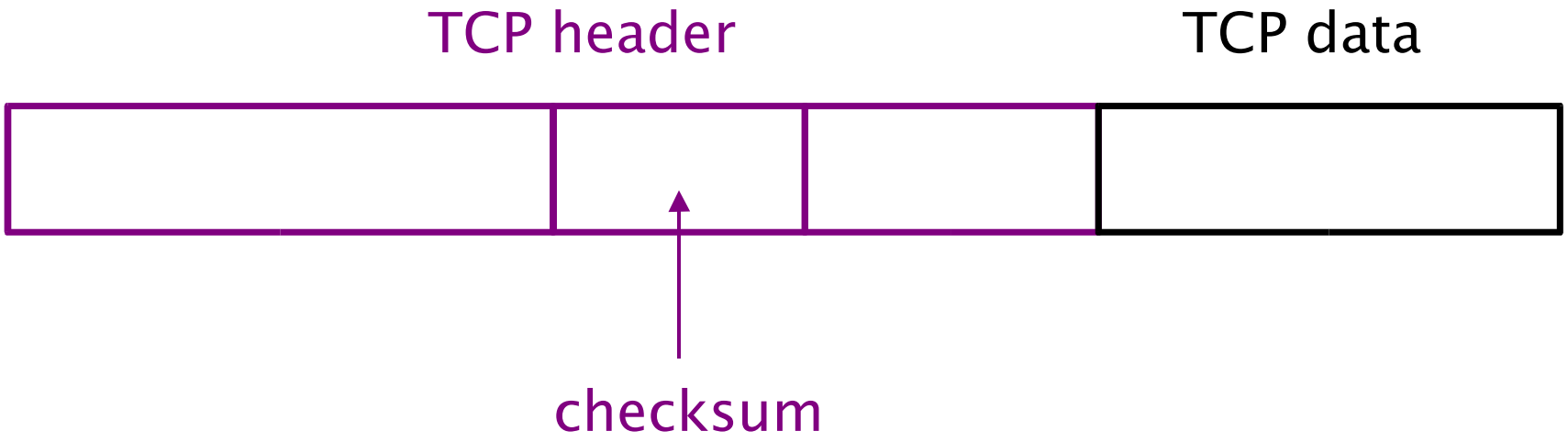
Step 1: Open "modified" TCP connection

1b) Receive SYN message,
extract host sequence number

Step 1: Open "modified" TCP connection

1c) Send ACK message,
connection open, ready for data

Step 2: Prepare TCP segment



- Checksum
  - Determined by SAT equation
- Data
  - Values of variables for this test

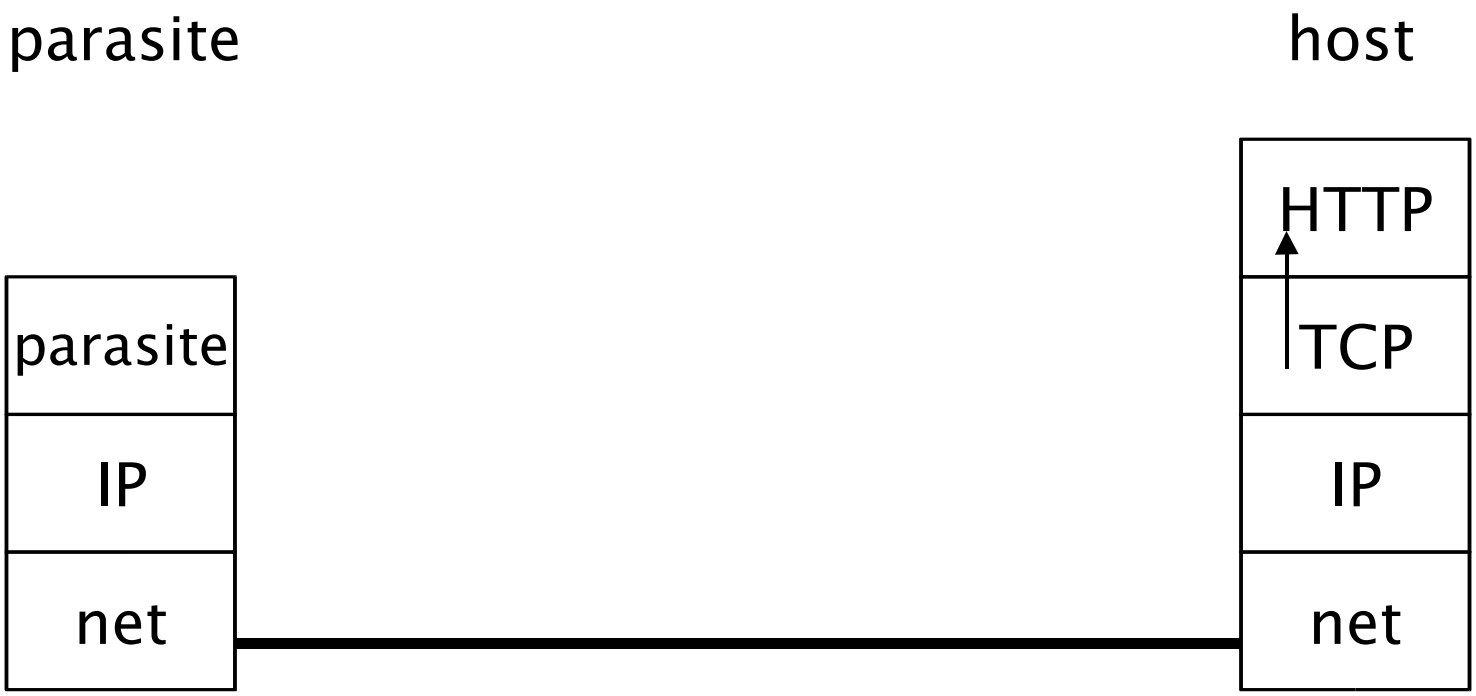
Step 2: Prepare TCP segment

- Compute checksum
  - Normally
    - Put 0's in checksum field
    - Sum segment (add each 16-bits)
    - Insert complemented sum into checksum field
  - Modified (for our exploit)
    - Put 0's in checksum field
    - Put "answer" in data field, padded to proper length
    - Sum segment (add each 16-bits)
    - Insert complemented sum into checksum field

Step 3a: Compute (positive answer)

3.a.1) Send modified TCP segment

Step 3a: Compute (positive answer)



3.a.2) TCP segment is valid, pushed up to HTTP

Step 3a: Compute (positive answer)

3.a.3) Receive HTTP reply
interpret this as a positive answer

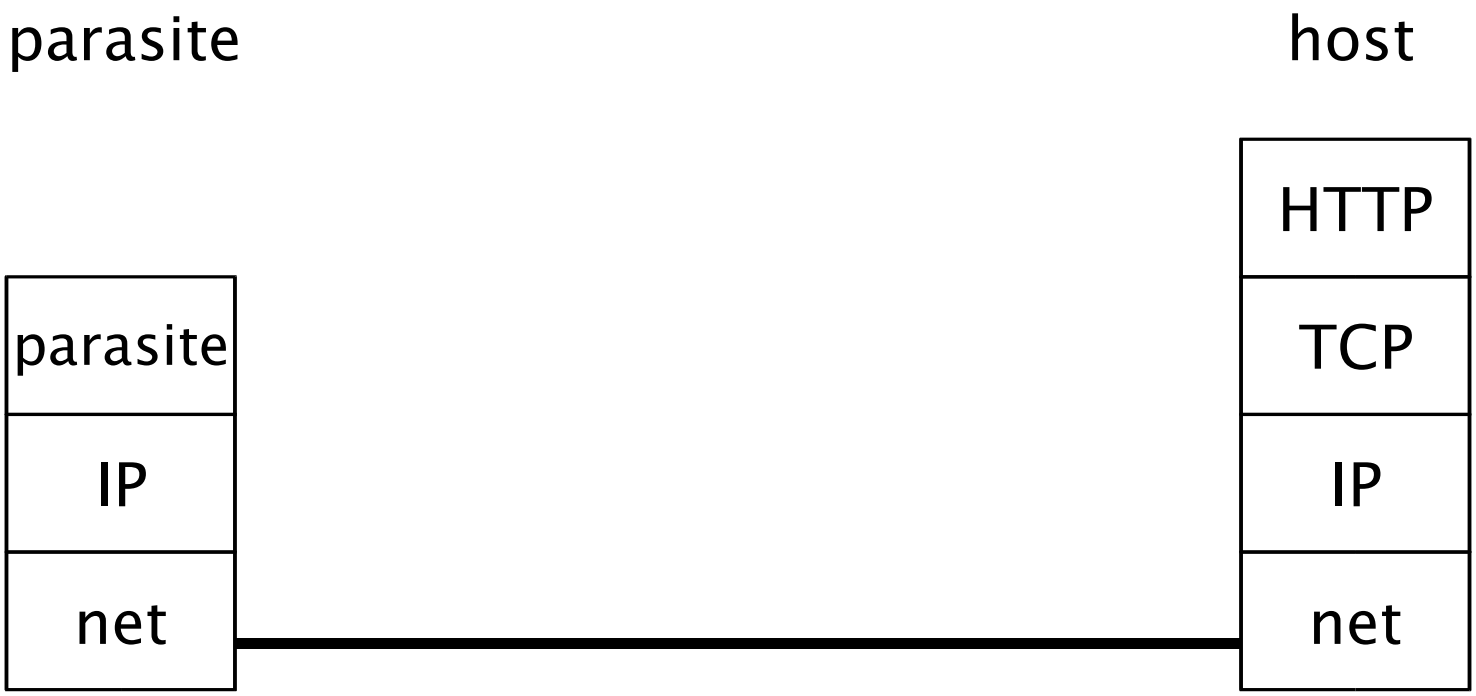
Step 3b: Compute (negative answer)

3.b.1) Send modified TCP sement

Step 3b: Compute (negative answer)

3.b.2) Invalid segment dropped by TCP

Step 3b: Compute (negative answer)



3.b.3) Parasite times out,
interprets that as negative answer