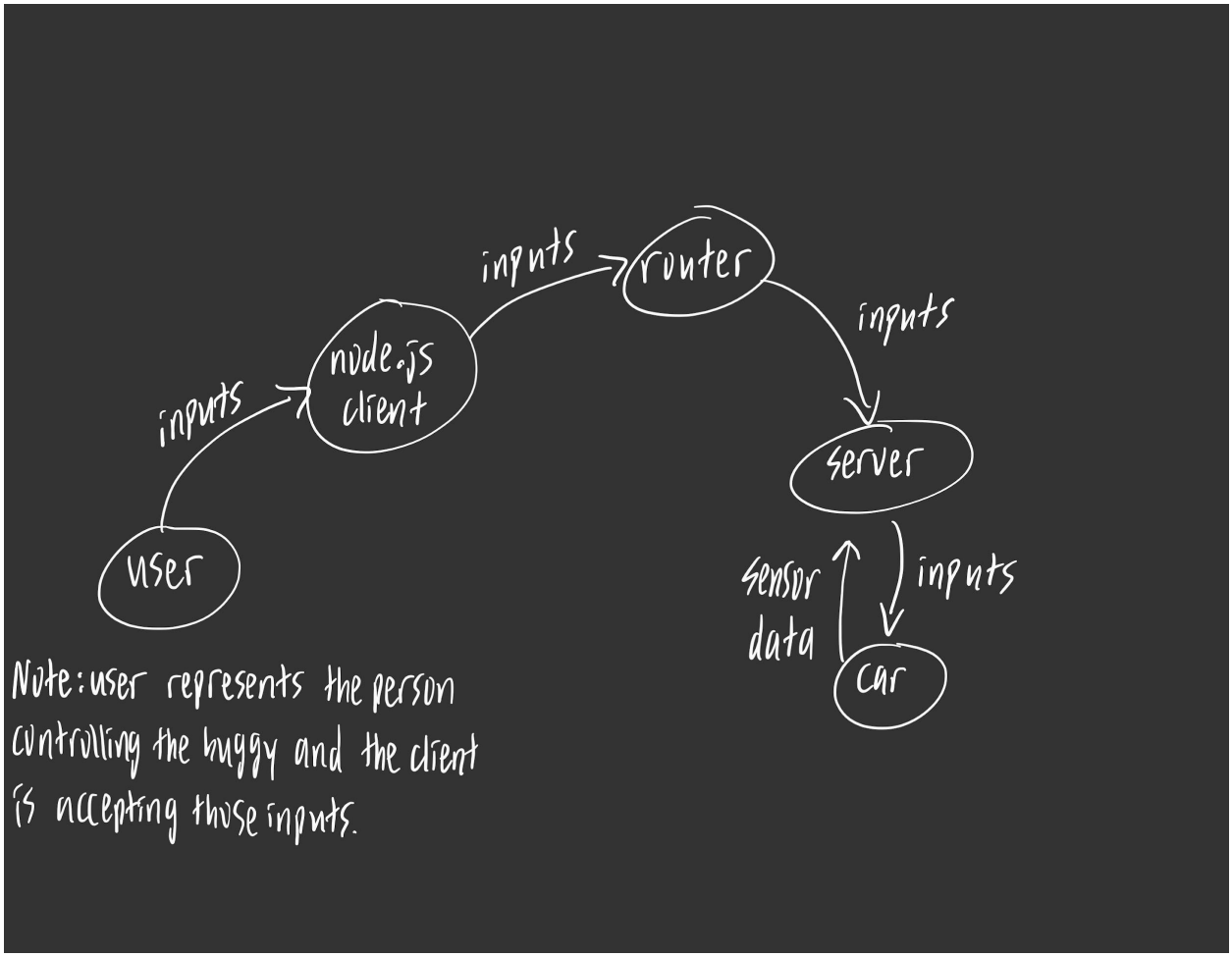
Suppose you are assigned the task of driving your car/robot via remote control over the internet. Based on the skills learned in the course, you should have a sense of what tools and network communication will be required to do this.

1. Sketch the overall flow of information to drive a car with remote control over the Internet.



2. Identify weaknesses in your overall system (client, local network, internet, server, node.js, ESP32) with respect to security compromise.
    - Client
        - User devices susceptible to malware attacks
        - Inadequate security on client devices
    - Local network
        - Insecure Wi-Fi configurations, such as using weak passwords or outdated security protocols (e.g., WEP), can allow unauthorized access to the local network
        - Inadequate monitoring of network traffic and activities may result in delayed detection of suspicious behavior or security incidents

- Internet
    - Unsecured data transfer
    - Vulnerability to DoS attacks
    - Reliance on insecure protocols, such as HTTP instead of HTTPS, can expose data to interception and manipulation
- Server
    - Security flaws in the server software could allow unauthorized access
    - Running outdated server software, including the operating system and server applications, may expose the server to known vulnerabilities
    - Inadequate authentication mechanisms and poorly configured authorization settings may lead to unauthorized access to the server
- Node.js
    - Reliance on external libraries and modules may introduce vulnerabilities if these dependencies have security issues
    - Improper handling of user input can lead to code injection vulnerabilities, allowing attackers to execute arbitrary code on the server
- ESP32
    - Using outdated or unsecure firmware versions on the ESP32 can expose it to known vulnerabilities
    - Transmitting sensitive data without encryption can expose it to interception
    - The physical exposure of the ESP32 may allow attackers to gain unauthorized access or manipulate the hardware

3. List at least five ways can a bad guy attack your specific system. Be very specific
    - Phishing attack on user devices where the attacker sends deceptive emails or messages to the user, tricking them into revealing sensitive information or installing malicious software
    - Man-in-the-Middle attack on wireless communication where the attacker intercepts and modifies communication between the user's device and the server, potentially altering control signals
    - Server code injection where exploiting vulnerabilities in the server, the attacker injects malicious code, gaining unauthorized access and manipulating control signals
    - ESP32 firmware manipulation where exploiting weaknesses in the ESP32 firmware, the attacker manipulates the microcontroller to execute unauthorized commands on the car/robot
    - Denial of service attack on the server where the attacker disrupts communication, rendering the remote control system unresponsive
4. Describe a way to mitigate each attack

- Implement email filtering, user education on phishing awareness, and use two-factor authentication to enhance user device security.
- Use secure, encrypted communication protocols (e.g., HTTPS) to protect data in transit, and regularly update Wi-Fi security protocols
- Conduct regular security audits, use secure coding practices, and apply patches promptly to prevent code injection vulnerabilities
- Regularly update and secure firmware, use secure boot mechanisms, and implement firmware integrity checks
- Implement rate limiting, use firewalls, and leverage content delivery networks (CDNs) to absorb excess traffic during a DoS attack