1. Welche Arten von Sockets gibt es? Beschreibe in groben Zügen ihre Unterschiede!

Unix Sockets

Konzept von Unix - Unix System - Daten zwischen Rechnern hin und her zu schicken - keine IP sondern Localhost

Internet Sockets

UDP/Datagrammsockets

Schickt an Adresse aber überprüft nicht ob es erhalten wurde

Wie SMS

Streaming Sockets

Verbindungsaufbau - Socket - Kommunikation über Stream

Wie Telefonieren

Websockets

Bauen auf HTTP auf

Zustandslos - (Nur 1 request und 1 response)

Bauen permanenten HTTP stream auf (evtl mit session cookie)

1. Wozu dient ssh, was ist putty?

Secure Shell 🡪 dient zur sicheren Verbindung zwischen zwei Rechnern. Mehrere Nutzer können mit einem Rechner gleichzeitig arbeiten. Remote Linux Terminal 🡪 Verschlüsselt

Putty

Windows SSH client

1. Wie werden gemeinsame Ressourcen vor konkurrierenden Prozessen geschützt?

Mutex (schließt andere Prozesse von der Ausführung kritischer Abschnitte aus)

synchronized keyword (one Thread at a time)

Semaphoren

Man macht einen Atomaren Prozess. Dabei sagt man dem Betriebssystem, dass der Bereich bis auf wiederruf gesperrt werden soll.

1. Beschreibe das Konzept des Iot Brokers! Gib Beispiele für MQTT Broker an.

Mosquito Broker

Irgendwo rennt zentraler Service

1 publisht, 1 subscribed und alles rennt über Topics

QOS

0 egal bei publish ob jemand abholt

1 publish jemand kann öfters abholen

2 jeder subscriber bekommt es genau 1 mal

Retain

Broker muss meldung aufbewahren

Access Control

publisher publisht für bestimmten nutzer und dieser kann die daten mit dem richtigen passwort abholen

1. Wie kann man einen MQTT Broker aus js, java, C#, C verwenden?

Paho Bibliothek

Connect (mit hostname und clientid) - Client anlegen - Client hat methode publish und subscribe methoden (bei beiden muss der topic angegeben werden)

1. Was sind die GPIO Ports am Raspberry?

General Purpose Input Output Ports

Arbeiten mit 5 Volt

1. Mit welchen Spannungen arbeiten Microcontroller?

5 Volt oder 3.3 Volt logik

(0-3.3 = false 3.4-5 = true)

1. Was ist ein Sensor, was ein Aktor? Wozu benötigt man Vorwiderstände, was ist ein Relais?

Sensor liest physikalische Daten, die die Umwelt beschreiben ein (Input) z.B. Temperaturmesser

Aktor macht etwas (Output) z.B. Motor

Vorwiderstand reduziert die Stromstärke (Verhindert dass zu viel Strom durchfließen kann)

Relais (Kann mit kleiner Spannung z.B. 5V eine riesen maschine mit z.B. 10 KV bedienen)

1. Welche Vorteile und Nachteile hat der Raspberry gegenüber einem Arduino?

Raspberry ist ein voller Computer nicht nur ein Microcontroller

Hat LAN und WLAN

Nachteil: Viel Komplexer, Betriebssystem nicht Echtzeitfähig, Viele Tasks die Konkurrieren (Threads), Kein Analog Port

Vorteil Arduino: Simple Entwicklungsumgebung

1. Wie arbeitet der I2C Bus?

Primitiver Bus der mit 2 Leitungen arbeitet Clockleitung, Dataleitung

7 Takte Adresse, 8. Takt R/W, 8 Takte lesen oder schreiben

1. Wie ist ein Block der blockchain aufgebaut?

* Timestamp
* Hash vom Vorgänger
* Eigentliche Information
* Proof of Work
* Aktueller Hash
* Nonce (nuller)

1. Was ist der proof of work und welchen Sinn hat er?

Nonce wird durchvariiert

Hash muss bestimmte Voraussetzung erfüllen

Damit wird bewiesen, dass Arbeit reingesteckt wird

1. Wie werden Blöcke aneinandergereiht?

Über den Vorgängerhash

Bzw. Aktueller Hash ist vorgängerhash vom nächsten Block

Neuer Block wird nach richtigem hashen an den letzten block angehängt

1. Beschreibe das Konzept eines verteilten Medianfilters, wie erfolgt der Datenaustausch?
2. Wie werden Kennwörter in Datenbanken gespeichert, was sind salt und pepper?

Gehasht

Salt: Chars werden vor dem hashen vor das Password gereiht

Pepper: Am Server wird irgendwo noch ein Passwort gespeichert, mit dem man den hash vor dem speichern nochmals hasht

1. Was ist ein Zertifikat, wie arbeiten digitale Signaturen?

Zertifikat 🡪 ist ein digitaler [Datensatz](https://de.wikipedia.org/wiki/Datensatz), der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen [Authentizität](https://de.wikipedia.org/wiki/Authentizit%C3%A4t) und [Integrität](https://de.wikipedia.org/wiki/Integrit%C3%A4t_(Informationssicherheit)) durch kryptografische Verfahren geprüft werden kann.

Digitale Signaturen 🡪 Public-Key und private Key wird generiert. Der Sender behält den private Key und schickt den Public-Key zum Empfänger. Der Sender verschlüsselt seine Signatur mit seinem private Key und schickt daraufhin die Daten und die Signatur zum Empfänger. Dieser entschlüsselt die Signatur mit dem Public-Key. Wenn dies möglich ist geht es weiter sonst ist es eine falsche Nachricht.

1. Wie installiert man am Server das „s“ in https?
2. Was sind die Schutzziele der Informationssicherheit?

Authentizität

Vertraulichkeit

Integrität

Keine Wiederholung