



BIKEBEACON

Geo-Tracking für Arme (und arm gebliebene)

KNF Kongress, 24.11.2019

Problem

- Wertvolle Anschaffungen sollen nicht spontan einen neuen Besitzer finden
- Nicht jeder mobile Gegenstand rechtfertigt einen GPS-Tracker mit GSM-Anbindung
 - hohe Anschaffungskosten (Teltonika FMB120 ~60 Euro)
 - hohe Betriebskosten (SIM-Karte ~10 Euro / Jahr)
 - evtl. Probleme beim Einbau (z.B. GPS-Antenne sollte den Himmel "sehen")



Inspiration

- Bluetooth Schlüsselfinder
 - geringe Reichweite
 - notwendige Batteriewechsel
 - vergleichsweise teuer
 - wenig Nerdfaktor
- aus früheren Experimenten ist bekannt, daß eigentlich überall WLAN vorhanden ist
- ESP8266 als Bastelplattform sehr bewährt – ESP32 noch besser

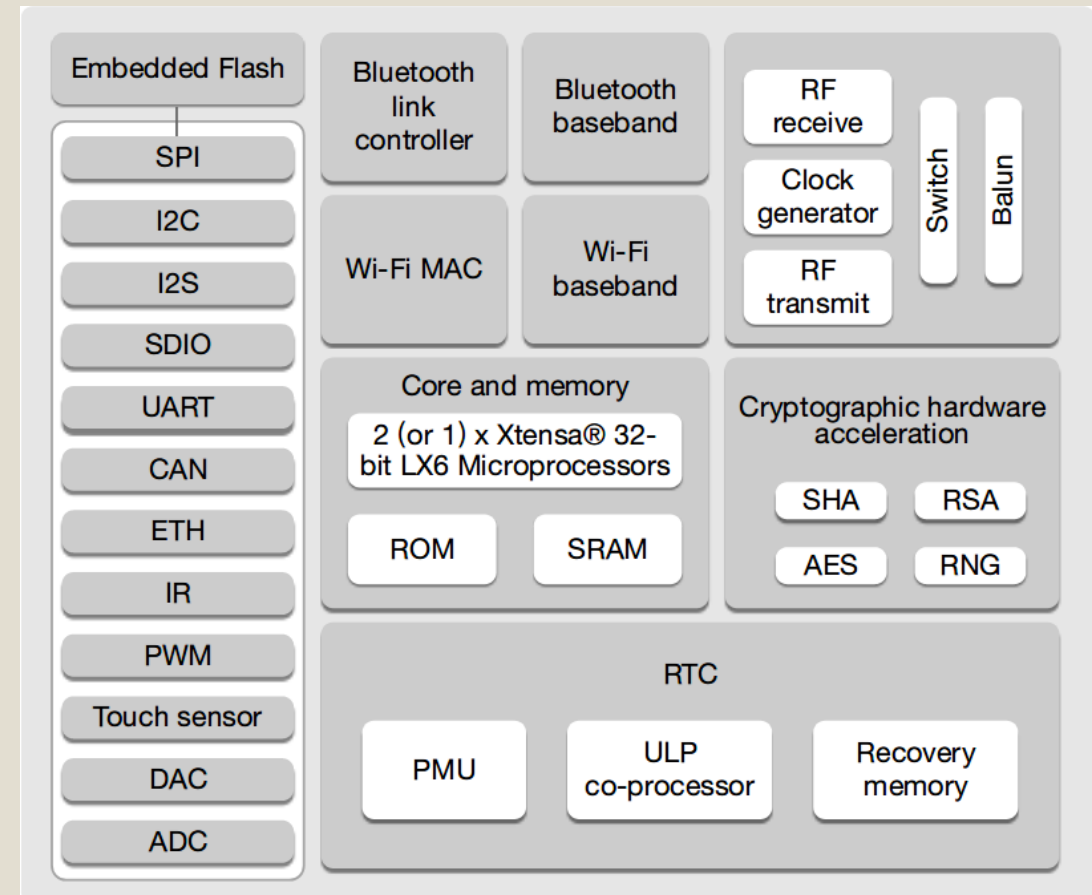




UMSETZUNG

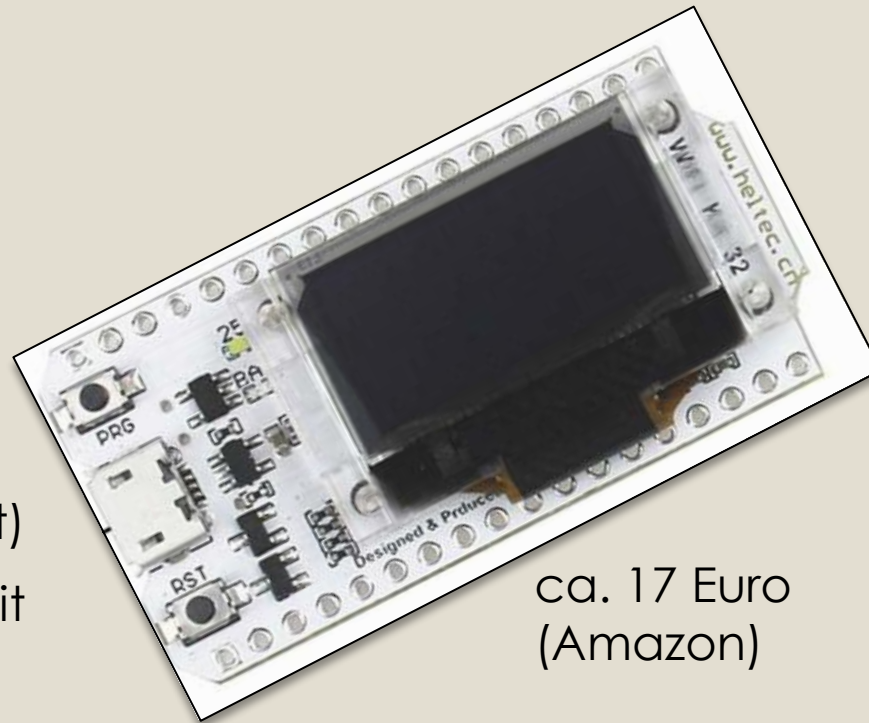
ESP32 CPU

- 240MHz Xtensa 32bit LX6 dual-core
- 520kBytes SRAM
- 448kBytes ROM
- externes SPI-Flash (memory mapped)
- 802.11b/g/n Wifi
- Bluetooth 4.2 und BLE
- diverse Peripherie
 - SPI, I2C, I2S, SDIO, UART, CAN, Ethernet, RTC, DAC, ADC, usw.
- Compiler und Bibliotheken liefert der Hersteller gratis

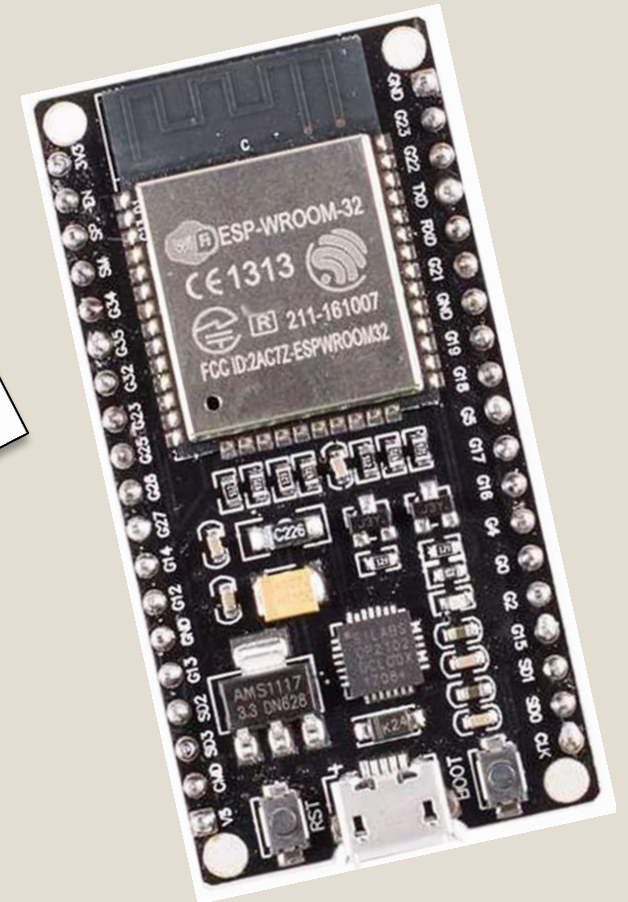


Module mit ESP32

- große Auswahl an Modulen (einfach nach "ESP32" suchen)
- üblicherweise Stromversorgung und Programmierung über USB (USB-Seriell-Wandler integriert)
- manche Module kommen mit Lithium-Ladecontroller
- Varianten mit Display
- alle Module haben SPI-Flash im Megabyte-Bereich

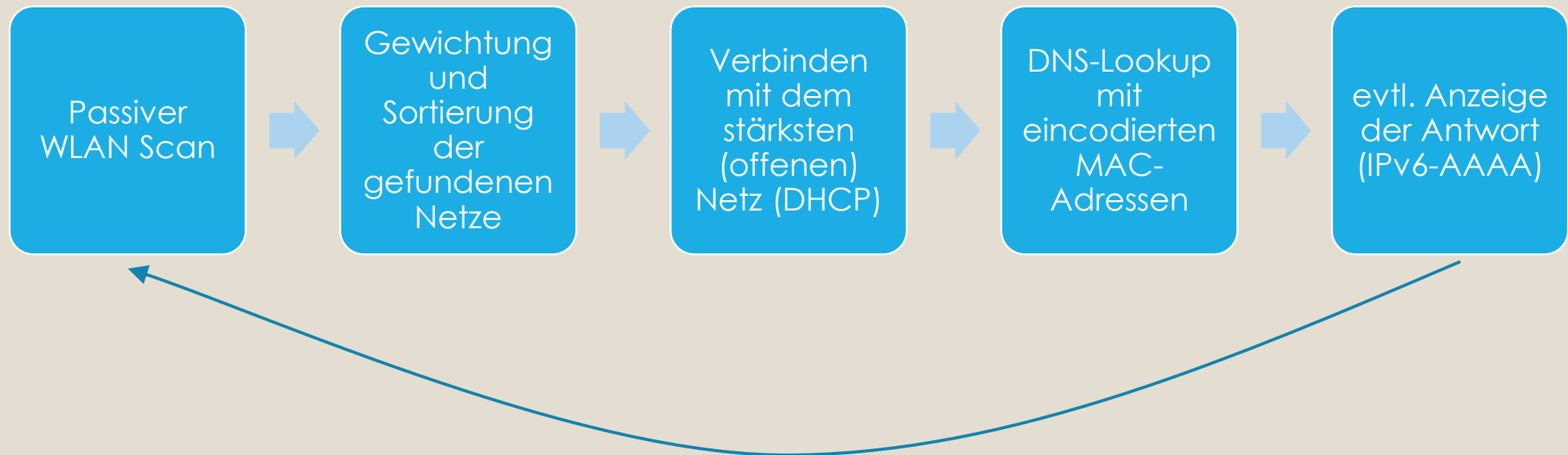


ca. 17 Euro
(Amazon)



ca. 8 Euro (Amazon)

Umsetzung (Firmware)



DNS-Lookup

- DNS-Tunnel sind bewährte Technologie ;-) (siehe nionet-Vortrag von 2005)

```
IP 83.169.184.227.62805 > 90.213.10.221.53: 47097 [1au] AAAA?  
nkvysrscg3wszr5u8kwakp488wctxlckgwgubqcb28pgs4bhb9sfzpbz4gubtu.kz44  
ntre9n73wn7bk6uc7jdacutf96mptjf7eu6k6wddfpbwr7szyxhqrnj6p28.ntsraap9  
9xk4s5kzchrletabjj4qts.t.aineko.org. (200)
```

```
IP 90.213.10.221.53 > 83.169.184.227.62805: 47097* 1/0/0 AAAA  
3136:3a30:383a:3430:2320:2033:3638:3938 (217)
```

- t.aineko.org ist die Zone des Nameservers
- Base32-Encoding, da viele Server die Anfrage in Großbuchstaben umwandeln
- Antwort als IPv6-Adresse (16 Bytes)

Inhalt des Lookups

- Geräte-ID (32 Bit)
- bis zu drei MAC-Adressen (BSSIDs) von gefundenen WLAN-Netzen
- SSID des verwendeten Netzes für den Lookup

- ein Authentikator, damit mit nicht jeder den Server verwendet
- Alles ist komplett verschlüsselt (Curve25519 bzw. libsodium crypto_box_seal, Public-Key des Servers ist im Gerät hinterlegt – dauert bei 160MHz ca. 100ms)

Arbeit des Servers

- entschlüsseln und Berechtigung prüfen
- MAC-Adressen via Google-Location-Service in eine Koordinate umwandeln (Mozilla bietet eine kompatible Datenbank, Apple hat einen ähnlichen Dienst)
- Ergebnisse in einer Datenbank speichern

```
{  
  "wifiAccessPoints": [  
    {"macAddress": "'$1'"},  
    {"macAddress": "'$2'"},  
    {"macAddress": "'$3'"}  
  ]  
}
```



```
{  
  "location": {  
    "lat": 49.7361705,  
    "lng": 9.95915619  
  },  
  "accuracy": 150  
}
```

<https://www.googleapis.com/geolocation/v1/geolocate?key=abcdefghijklmnopqrst...>



AUSBLICK

Server-Software und GUI

- Server-Software aktuell in C++ mit Qt geschrieben – evtl. Python-Implementierung?
- Qt-GUI mit verschiedenen Auswertungs- und Exportfunktionen
- evtl. Webseite mit Live-Tracking

Funktionalität

Übertragung längerer Nachrichten (gestückelt) vgl. CAN ISO-TP

Pager-Funktionen

Schaltfunktionen

großes Display (TFT)

Bewegungserkennung (Energiesparmodus)

ESP32-Module mit LoRa sind verfügbar – evtl. Verbindung

GPS-Input (genaue Koordinaten)

GPS-Output (simuliertes NMEA)

Low-Bitrate-Audio-Codec (codec2) -> DNS-Phone

Veröffentlichung

- Die komplette Software wird mit Sourcen veröffentlicht
 - evtl. Github-Seite
 - GPLv2
- noch nicht ganz fertig bzw. Aufräumen dringend notwendig

◦ Mail an **bikebeacon@castleturing.net**

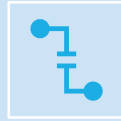


WARNUNG DISCLAIMER

WARNUNG



Man sollte Experimente dieser Art nur mit eigenen WLAN-Netzen machen oder mit Netzen, von denen man weiß, daß es in Ordnung geht.



Bei den haufenweise zu findenden DSL- und Kabel-Router-Hotspots (Telekom_FON, Vodafone Hotspot, Vodafone Homespot, etc.) kann man von einem Einverständnis vermutlich nur schwer ausgehen.



Ganz besonders bevor man ein Produkt mit der beschriebenen Funktionalität auf den Markt bringt (Stichwort Fahrradalarmanlage), sollte man mit einem Anwalt reden.



Im Zweifelsfall dürfte es einem dieser Provider leidlich leicht fallen, die entsprechende Domain auszufiltern.



Alle getrackten Leute sollten davon wissen und zugestimmt haben. Andernfalls greift das Strafrecht.



DANKESCHÖN!
FRAGEN? IDEEN?

bikebeacon@castleturing.net