# Wifi µDucky

## Introducere

Emuleaza o tastatura generand input primit de la un client conectat pe propria retea wireless. Inspiratia a fost USB Rubber Ducky.

## Descriere generală

Initial ESP-ul creaza o retea wifi fantoma si astapta sa fie activat printr-o transmisie speciala. Odata activat porneste o retea ascunsa si permite prin intermediul ei accesul sa un server de comanda si control. Folosind server-ul se controleaza ce apasari de taste va trimite la calculatorul conectat.

ESP-ul transmite direct comenzile de la utilizator, urmand sa fie decodificate si executate pe Arduino. Comenzile sunt ingradite de '#'(”#sleep20#” ⇒ wait for 20 ms) si respecta urmatorul set de reguli

```
##                                      =>        #
#SLEEP[0-9]+#                           =>         wait for

 #P:WIN#r#R:WIN##sleep20#cmd /c color 02  && tree && color#ENTER#

ms                          max 65536
#($ACTION:)?$SPECIAL_KEY#               =>        specific key
#($ACTION:)?0x[09a-fA-F]+#              =>        raw send

 BCD#P:CTRL##LEFT##sleep20##R:CTRL#A

:                                      =>

 #P:WIN#r#R:WIN##sleep20#notepad
 #sleep250#
 You Got hacked



ACTION:
T                                 =>        tap
DEFAULT
P                                 =>        press
R                                 =>        release
```

Exemple:

```
#P:WIN#r#R:WIN##sleep20#cmd /c color 02 && tree && color#ENTER#
```

```
BCD#P:CTRL##LEFT##sleep20##R:CTRL#A
```

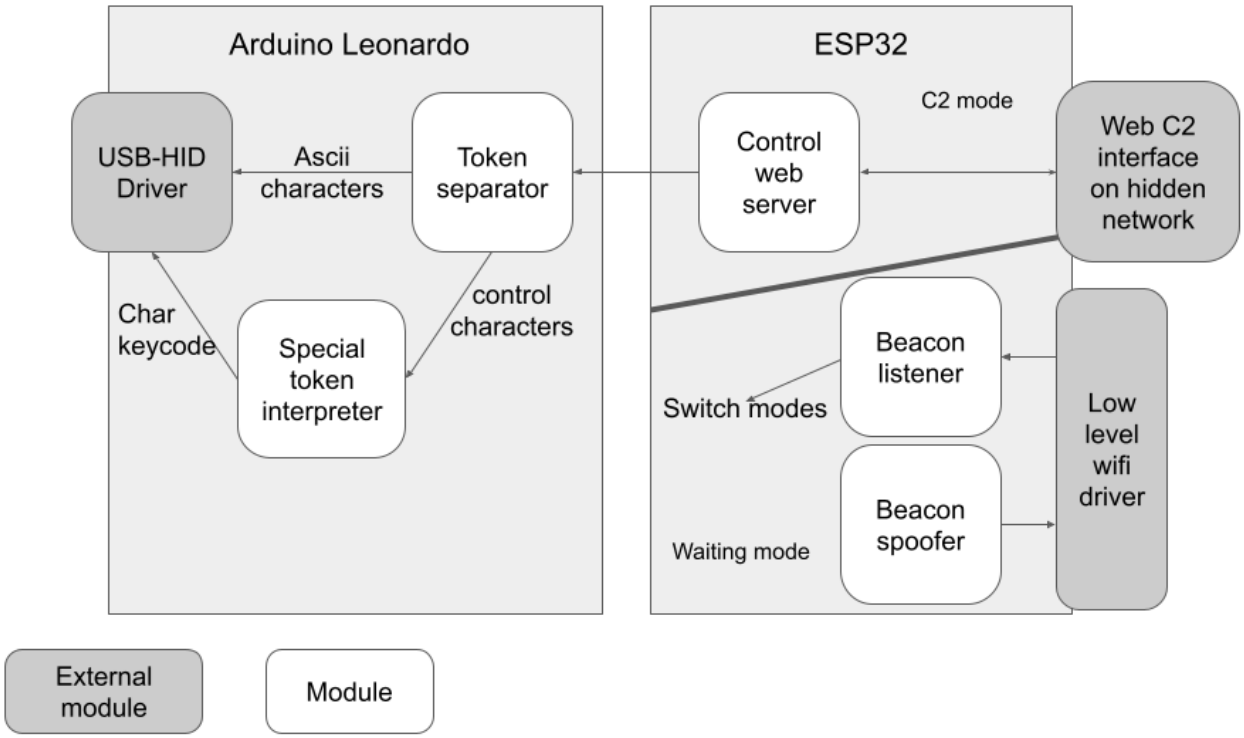
```
#P:WIN#r#R:WIN##sleep20#notepad #sleep250# You Got hacked
```

## Hardware Design

Componente:

- ESP8266
- Beetle Board(miniatured Arduino Leonardo)
- Modul translator de tensiune

## Software Design




Pe ESP, odata primit un beacon cu un SSID specific ESP-ul trece in modul de Comand&Control.

Mediu de dezvoltare: Arduino IDE

Librarii: Arduino ESP8266

cateva functii ESP:

- void send_fake_beacon()
- void build_fake_beacon(const char *ssid, byte channel)

cateva functii Leonardo:

- void handle_special(const char *token)
- const char *get_next(uint8_t *ret_is_special)
- void append_char(const char new_keystroke)

## Rezultate Obţinute

Care au fost rezultatele obţinute în urma realizării proiectului vostru.

## Concluzii

## Download

Surse

## Jurnal

Capsula cu ESP-07S pe care voiam sa il folosesc nu functiona pe partea de WiFi, din motive de timp am trecut pe un modul cu ESP8266.

## Bibliografie/Resurse


- Arduino Beetle
- ATmega16U4 Datasheet
- ESP32Marauder (a collection of wifi pentesting tools)
- ESP8266 API Reference
- Arduino ESP
- Arduino Keyboard Special Keys Reference


Export to PDF