Bruce

Cheap Yellow Display (CYD-2432S028)

Descripción general:

Esta placa de desarrollo combina un potente microcontrolador ESP32 con una pantalla táctil TFT LCD de 2,8 pulgadas, ofreciendo una plataforma versátil para proyectos de IoT (Internet de las cosas) y aplicaciones de interfaz gráfica de usuario (GUI).

Componentes clave:

- **Microcontrolador ESP32:**
  - Procesador de doble núcleo de 32 bits que ofrece un alto rendimiento.
  - Conectividad Wi-Fi y Bluetooth integrada, lo que facilita la comunicación inalámbrica.
  - Amplia gama de periféricos, incluyendo UART, SPI, I2C, PWM y ADC.
- **Pantalla TFT LCD de 2,8 pulgadas:**
  - Resolución de 240x320 píxeles, que proporciona imágenes claras y nítidas.
  - Tecnología TFT (Thin-Film Transistor) para una buena calidad de color y ángulos de visión.
  - Pantalla táctil resistiva o capacitiva, que permite la interacción del usuario.

- **Compatibilidad con Arduino y LVGL:**
    - Soporte para el entorno de desarrollo Arduino, lo que facilita la programación y el uso de bibliotecas existentes.
    - Compatibilidad con la biblioteca LVGL (Light and Versatile Graphics Library), que permite crear interfaces gráficas de usuario complejas y atractivas.

Características y funcionalidades:

- **Conectividad inalámbrica:**
    - Wi-Fi: Permite la conexión a redes Wi-Fi para acceder a Internet y comunicarse con otros dispositivos.
    - Bluetooth: Permite la comunicación con dispositivos Bluetooth, como teléfonos móviles y sensores.
- **Interfaz de usuario gráfica:**
    - La pantalla táctil permite crear interfaces de usuario interactivas para controlar dispositivos y mostrar información.
    - La compatibilidad con LVGL facilita el desarrollo de interfaces gráficas con elementos como botones, gráficos y texto.
- **Versatilidad:**
    - Adecuada para una amplia gama de aplicaciones, incluyendo:
        - Sistemas de control doméstico inteligente.
        - Dispositivos de monitorización y visualización de datos.
        - Interfaces de usuario para dispositivos electrónicos.
        - Proyectos de IoT que requieren interacción con el usuario.
- **Facilidad de programación:**
    - La compatibilidad con Arduino simplifica el proceso de programación, incluso para principiantes.

Especificaciones técnicas generales (pueden variar según el fabricante):

- **Procesador:** ESP32 de doble núcleo.
- **Pantalla:** TFT LCD de 2,8 pulgadas, 240x320 píxeles.
- **Táctil:** Resistivo o capacitivo.
- **Conectividad:** Wi-Fi, Bluetooth.

- **Interfaces:** UART, SPI, I2C, PWM, ADC.
- **Alimentación:** 5V (a través de USB).

Consideraciones:

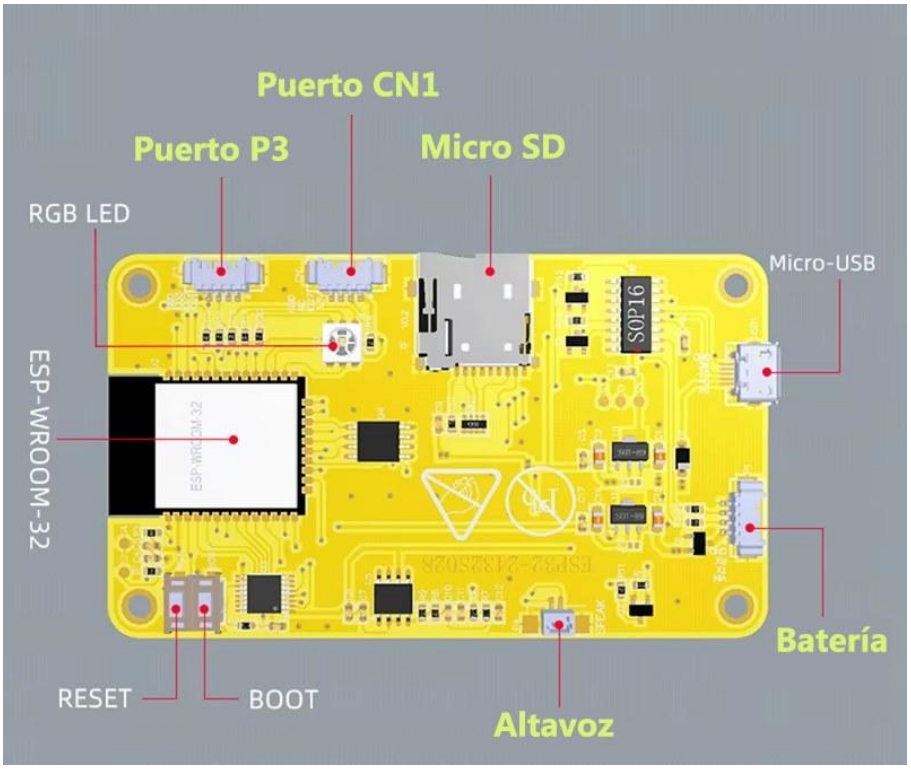
- Al elegir una placa de este tipo, es importante verificar las especificaciones detalladas del fabricante, ya que pueden existir variaciones entre modelos.
- Es importante saber que la tecnología táctil resistiva es mas antigua y menos precisa que la capacitiva.

Proyectos disponibles

La comunidad CYD ha desarrollado una amplia gama de proyectos, desde pantallas simples hasta aplicaciones complejas de IoT. Algunos proyectos notables incluyen estaciones meteorológicas, sistemas de domótica, consolas de juegos portátiles e instalaciones de arte interactivo. Estos proyectos muestran la versatilidad del dispositivo y la creatividad de sus usuarios.

Dónde comprar

Puede comprar el CYD de varios minoristas en línea. AliExpress es típicamente la opción más asequible, con precios de alrededor de 12€.



M5Stick-Launcher

Lanzamiento de aplicaciones para dispositivos M5Stack, Lilygo, CYDs, Marauder y ESP32.

Con Launcher podrás:

Actualización de *la OTA* OTA

- Instale binarios del repositorio M5Burner (sí, en línea, sin necesidad de un cable USB)
- Instale binarios desde una WebUI, que puedes empezar desde la opción CFG, instalando binarios que tienes en tu computadora o smartphone
- Instale binarios de su tarjeta SD

Gestión *SD*de tarjetas SD SD

- Crear nuevas carpetas,
- Borrar los archivos y carpetas,
- Nombrar archivos,
- Copia y pegue archivos,
- Instalar binarios

Interfaz de usuario web *de WUI*

Configuraciones *de CFG* (Personalización)

- Modo de carga
- Cambiar brillo
- Cambiar la hora dim
- Cambiar el color de la interfaz de usuario
- Evite/Pregunte Spiffs (Cambiar de no pedir instalar el sistema de archivos Spiffs, sólo Orca One utiliza esta característica)
- Cambio de rotación
- Todos los archivos / solo Bins (ver todos los archivos o solo .bins - por defecto)
- Cambiar el Plan de Partición (permite instalar aplicaciones grandes o UiFlow2, por ejemplo)
- Lista de las Particiones
- Despejar la partición FAT
- Guardar SPIFFS (Guardar una copia de la partición SPIFFS para restaurar cuando sea necesario)
- Guardar FAT vfs (Guardar una copia de la partición FAT para restaurar cuando sea necesario)
- Restaurar SPIFFS
- Restaurar FAT vfs

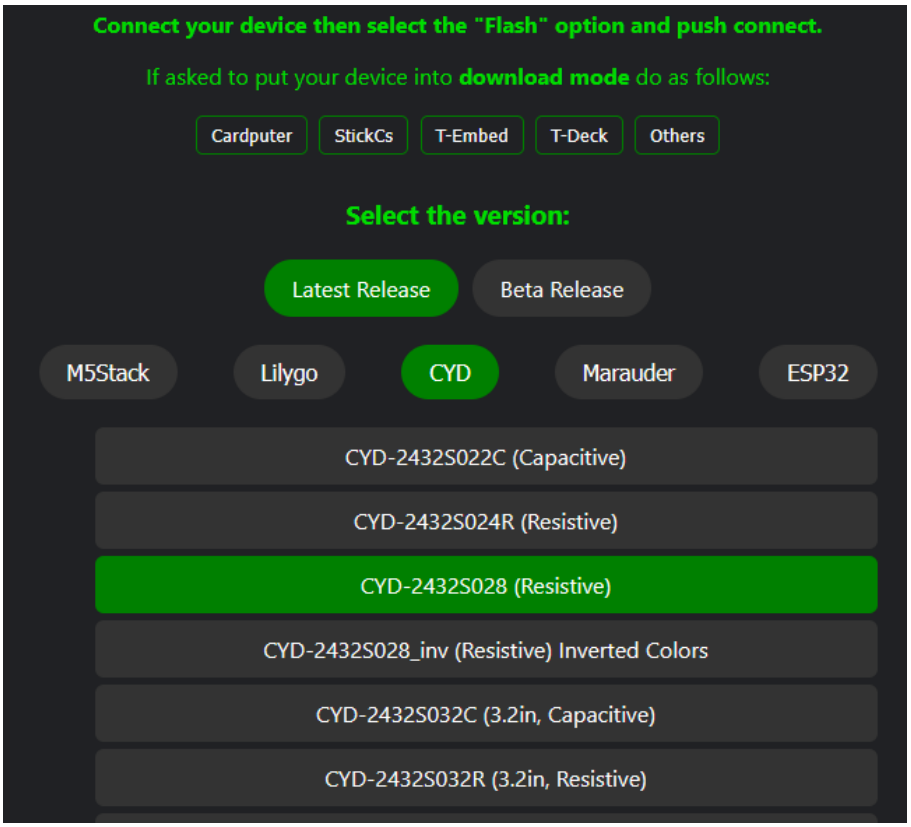
consejos

- Tener una tarjeta SD es bueno para una mejor experiencia, pero no es realmente necesario. SDCard Hat para M5StickCs
- Usted puede aprender más sobre cómo funciona o Launcher Wiki.
- Dónde/Cómo encuentro Binarios para lanzar - Obtención de binarios para lanzar
- Ahora puedes descargar binarios de AQUI.

Cómo instalar

- Utilice el Flasher: Lanzador Flasher.
- Utilice M5Burner, o
- Descargue el archivo .bin de Releases para su dispositivo y utilice https://web.esphome.io/ o esptool.py y flashe el archivo: Launcher-{ver}-{YourDevice}.bin en tu dispositivo.

https://bmorcelli.github.io/M5Stick-Launcher/



Cómo usar

- Enciende tu dispositivo.
- Pulse M5 (entrada) en la pantalla de inicio de inicio de lanzadera para iniciar el lanzador
- Elija OTA para instalar nuevos binarios de M5Burner repo
- Después de instalarse, al encender el dispositivo, si no presiona nada, se lanzará el programa instalado.

Cuestiones conocidas

- UiFlow 1 no trabaja con Launcher.. utiliza un viejo distro de MicroPython, que utiliza una distro vieja de ESP-IDF con muchos secretos que no podría averiguar.

M5Stick-Launcher:

Archivos binarios para CYD:

https://github.com/bmorcelli/M5Stick-Launcher/releases

ESP32Marauder:

Archivos binarios para CYD:

https://github.com/justcallmekoko/ESP32Marauder/releases

Ghost_ESP:

Archivos binarios para CYD:

https://github.com/Spooks4576/Ghost_ESP/releases

Proyecto Bruce

Bruce es un escáner y analizador de Bluetooth Low Energy (BLE). Este proyecto permite a los usuarios escanear dispositivos BLE, analizar sus datos e interactuar con ellos. Es particularmente útil para los desarrolladores que trabajan en aplicaciones BLE y proyectos de IoT. Bruce aprovecha las capacidades de Bluetooth de CYD para proporcionar una herramienta integral para el desarrollo y pruebas de BLE. Los usuarios pueden explorar el entorno BLE a su alrededor, recopilar datos de varios dispositivos e incluso desarrollar nuevas aplicaciones BLE.

https://github.com/pr3y/Bruce

Bruce es un firmware ESP32 diseñado para operaciones de seguridad ofensivas, soportando varios dispositivos incluyendo la pantalla CYD-2432S028. Here es una guía completa sobre cómo instalar, ejecutar y utilizar Bruce en esta pantalla.

Bruce está destinado a ser un firmware versátil ESP32 que soporta una tonelada de características ofensivas que se centran para facilitar las operaciones del Equipo Rojo. También soporta productos m5stack y funciona muy bien con Cardputer y Sticks.

Bruce proviene de una aguda observación dentro de la comunidad enfocada en dispositivos como Flipper Zero. Si bien estos dispositivos ofrecían un vistazo al mundo de la seguridad ofensiva, había una sensación palpable de que algo más se podía lograr sin ser eso sobreprecio, particularmente con el ecosistema de hardware robusto y modular proporcionado por los productos m5stack.

Instalación

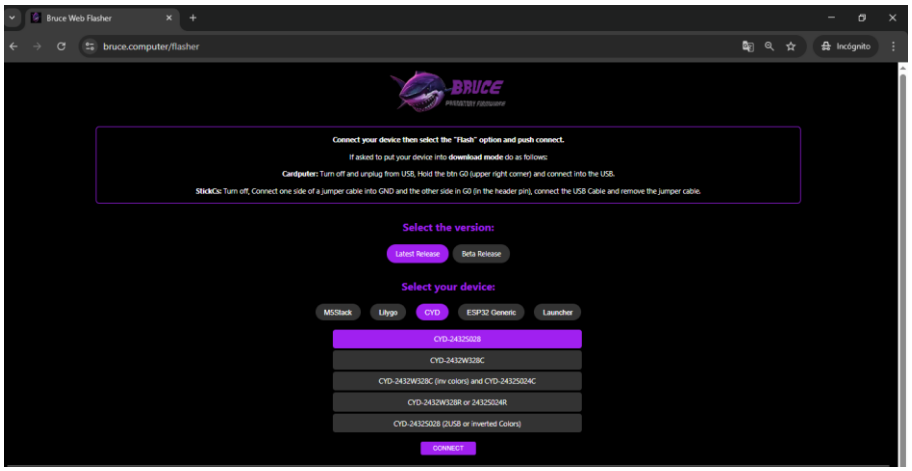
La forma más fácil de instalar Bruce es usando el Web Flasher oficial. Esta herramienta te permite flashear el firmware directamente desde su navegador, simplificando significativamente el proceso.

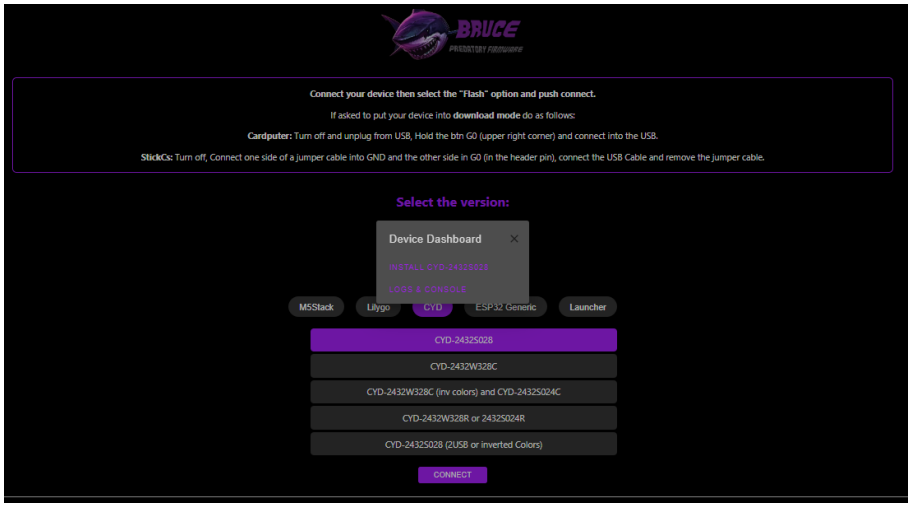
O si ya usas M5Launcher para administrar tu dispositivo m5stack, puedes instalarlo con OTA.

También puedes quemarlo directamente desde la herramienta m5burner, sólo tienes que buscar 'Bruce' en la categoría de dispositivo que desea y haga clic en la grabación

Sigue estos pasos:

1. Abre tu navegador web (preferiblemente Chrome) y ve al Bruce Web Flasher.
2. Conecta tu pantalla CYD-2432S028 a tu computadora a través de USB.
3. Sigue las instrucciones en pantalla para seleccionar el archivo de firmware apropiado y flashearlo en tu dispositivo.





Una vez instalado, Bruce comenzará a ejecutarse automáticamente en su pantalla CYD-2432S028. Puedes interactuar con él a través de varias interfaces dependiendo de tu configuración:

- **WiFi:** Conéctese a la red WiFi del dispositivo para acceder a su interfaz web.
- **Monitor serie** : Utilice un monitor serie para ver los registros e interactuar con el firmware directamente.

BLE

Desconectar BLE

Si BLE está activo actualmente, utilice esta opción para desconectar. No se necesita más explicaciones.

Comandos de medios

Controla las funciones multimedia de tu smartphone (trabaja con todos los dispositivos Android):

- Toma capturas de pantalla
- Reproducir/pausa música
- Deja de reproducir, y más.

BLE Scan

Escanee dispositivos cercanos Bluetooth Low Energy (BLE) sin esfuerzo.

BadBLE

Simula un teclado para implementar DuckScripts en dispositivos emparejados. **Nota:**

- El dispositivo **debe estar previamente emparejado** para que esta característica funcione.
- Después de desconectar BLE, necesita reiniciar el dispositivo para activar esta funcionalidad de nuevo.

Características del juego BLE

Spams iOS

Envía un maridaje de dispositivos bluetooth siguiendo muestras de paquetes de AppleJuice y SourApple

- AppleJuice: El spam combinando iOS Bluetooth.
- SourApple: Echacanazo de choque Bluetooth iOS.

SwiftPair Spamming

Enviar notificaciones de emparejamiento de dispositivos Bluetooth para Windows (SwiftPair)

Spam para Android

Bluetooth pairing de notificación de patinaje para dispositivos Android *(añadido en versión 1.0.*0).

Dispositivos de Samsung

Spamming de notificación Bluetooth para dispositivos Samsung *(añadido en la versión 1.0.*0).

Spam todo

Una opción universal para spam todos los dispositivos compatibles simultáneamente, es más eficaz en entornos controlados)

IR

Infrared Emitter: La mayoría de las tablas M5Stack vienen equipadas con un emisor de IR incorporado.

Características

• TV-B-Gone: Envía señales infrarrojas para apagar varias pantallas.

• IR personalizado: Permite el envío de códigos IR personalizados de archivos almacenados en LittleFS o en una tarjeta SD.

• IR Read: Capaz de leer y decodificar señales IR entrantes.

Replay Payloads Like Flipper.

Acceso .irArchivos, visita: Infrared Payloads.

https://github.com/Lucaslhm/Flipper-IRDB también tiene tantas cargas útiles que puedes usar

Métodos para la transmisión .irArchivos

1. **Aplicación IR personalizada** : Seleccione comandos individualmente en el menú "IR".
2. **Administrador** de **archivos SDCard/LittleFS** : Acceso bajo el menú "Otros" (envía todos los comandos).
3. **WebUI** : Haga clic en el botón de antena junto al archivo (envíe todos los comandos).
4. **Comando serie:** Por ejemplo, utilizar ir tx_from_file AC_LG_SX122CL_off.ir. Para más detalles, consulte la Guía de Comando Serial (envíe todos los comandos).

RF

Escaneo/Copiar

Escanee y copiera las señales de RF en la modulación de ASK/OOK. Comenzará con la frecuencia por defecto (433Mhz, común para los módulos M5 RF433R y FS1000A).

Modo

Decode : trata de decodificar la señal con decodificador RCSwitch **RAW** : Mostrará señales RAW obtenidas de la biblioteca RCSwitch.

Filtro

Código : En el modo Decodificación, sólo mostrará señales decodificadas. más confiable en entornos ruidosos **Todo:** capturará señales decodificadas y RAW

Replay

Envíe la última señal capturada por Bruce.

Salvar

Almacena la señal en . /BruceRF de su tarjeta SD o LittleFS**

CC1101 sólo menú

Rango

Elija la frecuencia de escaneo o un rango para detectar la frecuencia

Urea

Elija la sensibilidad del escáner. -60 a una frecuencia de error más estricta (más precisa) -80 a una frecuencia más amplia (error mayor, menos preciso)

Grado de crudo

Registra la señal RAW usando el controlador ESP32 RMT, mostrando la señal cruda obtenida en pocos segundos de captura. La grabación comenzará una vez que detecte una señal

mínima en la entrada. Si usa CC1101, puede elegir la frecuencia que desea registrar. En esta función puedes Guardar y reproducir señales.

SubGhz personalizado (compatibilidad limitada)

Transmite las señales almacenadas en archivos **.sub**, pueden ser los guardados por Bruce en la carpeta Bruce u otros descargados de internet.

Análisis del espectro

Muestra señales de forma de onda si se detectan frecuencias RF.

Spectrum de ola cuadrada

Cuando se detectan señales, muestra una onda cuadrada en función de los tiempos de la señal.

Jammer lleno

Inicia una señal cuadrada completa en la salida, interfiriendo el espectro RF en el área 433Mhz, o en el conjunto de **frecuencias RF** en el menú Config (si se utiliza CC1101)

Jammer Intermitente

Comienza una señal de PWM en la salida, interfiriendo la señal, no dañando al transmisor, si escucha la frecuencia con una radio, yo será capaz de escuchar un sonido de "weeeooooooooooeoeeee"

Config

RF TX Pin y RF RX Pin

Si utiliza M5Stack, FS1000A u otro módulo de pin único para transmitir la señal, aquí es donde puede elegir el pin

Módulo RF

M5 RF433T/R

Módulos M5 RF433T/R o módulos no oficiales.

CC1101

Si estás usando un StickCPlus (1.1 o 2), te presentarás a dos opciones de CC1101

CC1101 (legado)

Esta configuración está diseñada para utilizar sólo el CC1101 en el autobús, utilizando ESTA configuración

CC1101 (Shared SPI)

Esta configuración está diseñada para compartir el autobús SPI con la tarjeta SD, pero en este caso usted ned para añadir un transistor en el circuito, utilizando ESTA Configuración

RFID

Resumen RFID y NFC

RFID (Radio Frequency Identification) es una tecnología que utiliza campos electromagnéticos para identificar y rastrear automáticamente las etiquetas conectadas a los objetos. Estas etiquetas almacenan información codificada electrónicamente que puede ser leída por un lector RFID. La RFID se emplea comúnmente en diversas aplicaciones, incluyendo la gestión de inventarios, el control del acceso y los sistemas de transporte.

NFC (Near Field Communication) es un subconjunto de tecnología RFID que opera en distancias más cortas, normalmente a pocos centímetros. NFC permite a los dispositivos comunicarse poniéndolos cerca, haciéndolos ideales para pagos sin contacto, intercambio de datos entre dispositivos y sistemas de acceso inteligente.

Tipos de Etiquetas RFID: Escrito Vs. Clonable

Escritos RFID Escritos

Las etiquetas RFID correctas permiten a los usuarios modificar los datos almacenados en la etiqueta, facilitando actualizaciones de información dinámicas. Sin embargo, estas etiquetas normalmente no permiten escribir a **Block 0**, que generalmente contiene datos del fabricante o identificadores únicos.

Tazas Clonables RFID

Las etiquetas RFID Clonables representan un riesgo para la seguridad, ya que la clonación implica crear un duplicado de la información de la etiqueta. Esto puede conducir a acceso no autorizado o actividades fraudulentas. La clonación a menudo requiere escribir al **Bloque 0**, lo que requiere un tipo especial de etiqueta que soporta esta capacidad.

Tipos comunes de cintas RFID y NFC

- **MIFARE Classic 1k/4k** : Opera a 13.56MHz y ofrece 1KB o 4KB de almacenamiento de memoria. Se utiliza comúnmente en sistemas de control de acceso, programas de transporte y lealtad. Puedes encontrar versiones clonables de estas etiquetas aquí.
- **Serie NTAG:** Los tipos de etiquetas NFC populares, como NTAG213 y NTAG215, operan a 13.56MHz y son conocidos por su compatibilidad con una amplia gama de dispositivos y aplicaciones habilitados para NFC. Estas etiquetas admiten registros NDEF que pueden ser interpretados por smartphones.

- **EM4100 y T5557** : Protocolos RFID que funcionan a 125kHz, comúnmente utilizados para sistemas de control de acceso de baja frecuencia, placas de identificación, llaveros, seguimiento de activos y otras aplicaciones de identificación basadas en la proximidad.

Módulos compatibles

- **13.56MHz**

ML.M.M.M.M.M. MAFTA

MFRC-522 - vía I2C (Seleccione M5 RFID2en el menú de configuración)

PN532 - a través de I2C, SPI o BLE

- **RFID 125kHz**

RDM6300 (Esquema de conexión)

Características

13.56MHz

- Lea
- Escribir
- Clon
- Escribe NDEF Records (sólo etiquetas NFC)
- Borrar
- Guardar archivo
- Cargar archivo

RFID 125kHz

- Lea
- Guardar archivo

WiFi

Conéctese Wifi

Se conecta a una red elegida, le permitirá utilizar **funciones TCP Listener**, **ARP Poisoning**, **Station Deauth**, **TelNet**, **SSH** y **Scan Hosts**.

WiFi AP

Lanza un punto de acceso, para que puedas conectarte hasta 4 huéspedes para compartir información entre sí.

Wifi apuestas

Atracs de destino

Escáneres para un AP WiFi a ambos:

- obtener más información de la misma (MAC y canal),
- Envía marcos Deauth,
- Clone AP nombre y hacer un Portal del Mal,
- Deauth . Cintón
- Deauth . Clon y verifica, en caso de que estés tratando de obtener contraseña de una red WiFi.

Spam de faro

Spams marcos SSID en el aire.

Divertido SSID

Spams una lista de nombres de SSID pelados.

Rick Roll

Spams Rick Roll lyrics en nombres de SSID.

SSID aleatorio

Spams al azar SSID, compuestos por números y letras aleatorios.

Adueño SSID

Spams una lista de los SSID escritos en un archivo **.txt**. Debe haber

- Un SSID por línea
- Hasta 32 caracteres por SSID
- como muchos SSID que quieres

My SSID

Your SSID

His SSID

etc...

Deauth se deleganta

Paquetes de Foods Deauth a todos los Puntos de Acceso que puede encontrar.

Mal Portal

En modo EVIL Portal, BRUCE lee la entrada del teclado para el SSID y activa un WiFi abierto, con servidores DNS, DHCP y Web activados.

- EVIL Portal sirve una página de inicio de sesión falsa que pretende proporcionar acceso a Internet si inicia sesión.
- Este es un ataque de ingeniería social, y registrará el nombre de usuario y las contraseñas introducidos en la página.
- Puedes escribir el ssid antes y cambiar el SSID actual conectándote al portal desde tu propio dispositivo y navegando a http://172.0.0.1/creds o http://172.0.0.1/ssid
- Si tu dispositivo tiene un lector de tarjetas SD con una tarjeta formateada FAT insertada, los nombres de usuario y contraseñas se registrarán en Bruce.creds.csv en la tarjeta SD para que puedas leer más tarde.
- El soporte de tarjeta SD solo está habilitado por defecto en la plataforma M5Stack Cardputer. Se puede activar en dispositivos M5Stick, pero un lector de tarjetas SD debe ser construido y unido a la cabecera de pin del panel delantero. Nuevas características, SPIFFS y SDCard
- Para ejemplos de portales puede consultar https://github.com/pr3y/Bruce/tree/main/sd.files

Configuración de AP Nombre de HTML

Resumen

El EvilPortalEl sistema ahora admite la capacidad de definir un nombre de Access Point (AP) directamente dentro de sus archivos HTML. Al incluir una etiqueta específica en la primera línea de su archivo HTML, el sistema extraerá y establecerá automáticamente el nombre de AP, racionalizando el proceso de configuración.

Cómo funciona

1. Añada la siguiente etiqueta en la **primera línea** de su archivo HTML:

<!-- AP="YourCustomAPName" -->

Sustituir YourCustomAPNamecon el nombre deseado para su Punto de Acceso.

1. Cuando el archivo HTML se cargue, el sistema:
    a. Parse la primera línea del archivo.

b. Detectar el AP="..."tag.

c. Extrae el valor y confiéquelo como el nombre de AP.

2. Si la etiqueta no está presente le pedirá el nombre de AP (como de costumbre).

Ejemplo de archivo HTML

```
<!-- AP="MyCoolNetwork" -->
<!DOCTYPE html>
<html>
<head>
  <title>EvilPortal</title>
</head>
<body>
  <h1>Welcome to EvilPortal!</h1>
</body>
</html>
```

- En este ejemplo, el nombre de AP se configurará automáticamente en **MyCoolNetwork**.

Beneficios

- **Configuración dinámica** : Túscula fácilmente los nombres de AP sin modificar el código.
- **Facilidad de uso:** Configure los nombres de AP directamente en sus archivos HTML para una implementación más rápida.

Notas

- Asegurar el <!-- AP="..." -->La etiqueta está en la **primera línea** del archivo.
- La función no afecta a la funcionalidad de otros contenidos HTML.

Escucha TCP

Escuche las conexiones TCP entrantes en un puerto especificado. Espera a conexiones de clientes, permitiendo que el dispositivo actúe como servidor y maneje la comunicación con clientes conectados.

TCP Cliente

Permite que el ESP32 se conecte a un servidor remoto como cliente a través de TCP. Puede configurar la dirección IP y el puerto del servidor de destino, permitiendo la transmisión de datos hacia y desde el servidor.

TelNet

Conéctese a los servidores TelNet y ejecute comandos remotos.

SSH

Conéctese a servidores SSH y ejecute comandos remotos.

DPWO-ESP32

Búsqueda credenciales por defecto para algunos operadores de router más información aquí

RAW Sniffer

Guarda .pcap a la tarjeta SD con monitoreo crudo, también puede seleccionar para que guarde solo EAPOL/HandShakes y deje de poner spamming de deauth a las balizas detectadas previamente detectadas.

Azafatas de escaneo

Hace un escaneo ARP en la red actual basado en la máscara (equivalente a arp -a), después de que listará cada host en línea, entonces puede seleccionar un host para hacerse un toque de puerto TCP en puertos seleccionados (20, 21, 21, 22, 23, 25, 80, 137, 139, 443, 3389, 809, 8080, 8443, 9090 y más), como se ve en "ports" variable en scan-hosts.cpp y le permite elegir un ataque de host objetivo como:

Anfitrión de información

Descubre los puertos abiertos (20, 21, 22, 23, 25, 80, 207, 139, 443, 3389, 8080, 8443, 9090 y más) en la Hostia

SSH Connect

Intenta conectarse al Host usando SSH.

Estación Deauth

Los marcos Spams deauth apuntados a este dispositivo en particular

ARP Spoofing

- Envía falsas Resones ARP al anfitrión y a la pasarela, provocando la interrupción de la comunicación.Este es el paso de un ataque de Man-In-The-Middle usando la vulnerabilidad de la segunda capa OSI.

Envenenamiento de ARP

Envía las respuestas de Fale ARP a todos los hosts y a la puerta de entrada con direcciones aleatorias MAC. Posiblemente puede causar CAOS en la red, ya que todos los dispositivos no encontrarán la puerta de entrada para comunicarse.

Túnel de guardaespaldas

Para poder conectarse a un túnel de alambre con su cardputador fácilmente, necesita tener su archivo .conf y colocar en el directorio raíz de la tarjeta SD llamado "wg.conf" Si usted no sabe cómo generar un archivo .conf para el guardablo leída aquí

Brucegotchi

Esta característica hace muchas cosas al mismo tiempo, tales como:

- Espuma pwngrid
- Deauth redes WiFi cercanas en diferentes canales
- Recoger y guardar HandShakes (EAPOL)

Config

Añadir el mal Wifi

Añade un SSID en la lista para que puedas elegirlo con facilidad al abrir un Portal del Mal

Eliminar mal Wifi

Elimina un SSID previamente añadido.

FM

Juega en 76-108 MHzfrecuencias con un módulo Si4713.

Reportaje añadido en https://github.com/pr3y/Bruce/pull/195

Módulos compatibles

Necesita un Si4713. Esos módulos se apoyan por ahora:

1. Adafruit Si4713
2. CJMCU-4713

Alambre

Escálsamo


GND
5V
G26
G36/G25
G0
BAT
3V3
5V
M5StickC
PLUS2
BTN B G39
BTN A G37
BUZZER G2
IR G19
LED G19
ESP32-PICO-V3-02
LCD
1.14 TFT
135x240
ST7789V2
SCL : G22
SDA : G21
6-Axis IMU MPU6886
RTC BM8563
MIC
SPM1423
DATA: G34
CLK: G0
SLEEP WAKE G35
HOLD G4
BATTERY:200mAh
PWR 2s=ON 6s=OFF
M5 STACK
GROVE
BUTTON C G35
G
5V OUT
G 32
G 33


Ant
SI4713 FM RDS Radio
adafruit!
CS
SDA
GP2
GND
LIN
GP1
3vo
RIN

Pins

Pins

Si4713	M5StickC	Cardputador
RST	ATENCION	ATENCION
SCL	Grove G33	Grove G1
SDA	Grove G32	Grove G2
GND	Arrastrar G	Arrastrar G
VIN	Arrastrar 5V	Arrastrar 5V

Si4713

M5StickC

Cardputador

RST

ATENCION

ATENCION

SCL

Grove G33

Grove G1

SDA

Grove G32

Grove G2

GND

Arrastrar G

Arrastrar G

VIN

Arrastrar 5V

Arrastrar 5V

ATENCION: Es necesario encender el dispositivo (StickC/Cardputer), colocar 1 alambre en el pin RST del Transmisor FM y tocar rápidamente el extremo del alambre a GND para activar el

RST, de esta manera no es necesario utilizar el Sniffer de la tarjeta SD o el pin G0 de StickC. También es posible colocar un botón o resistencia para esta operación, si lo prefiere.

Ejemplo de vídeo

Características

- Estándar de transmisión

Corriente de transmisión desde el Si4713 a la frecuencia seleccionada.

Para ser más fácil de elegir, es necesario seleccionar primero las decenas: 80, 90o o 100 MHz.

Entonces elegirá la unidad: 81, 82, 83, 84 MHzetc. y, por último, la frecuencia de radio: 81.1, 81.2, 81.3 MHzetc.

Cuando se inicia la transmisión, puede dejar el menú de radio FM y ejecutar otra cosa. La transmisión de FM se ejecutará en el fondo.

Modo automático disponible.

Transmisión reservada

Advertencia: esto podría ser ilegal dependiendo de su país. Sólo un propósito educativo.

Trabajar de la misma manera que la norma de transmisión pero en las frecuencias reservadas, que son de 76 a 87,5 MHz.

Modo automático disponible.

- Parada de transmisión

Deja de emitir.

Espectro FM

Trabajo en curso.

Mostrar el espectro de ruido en una frecuencia dada.

Modo automático disponible.

Hijack TA

Advertencia: esto podría ser ilegal dependiendo de su país. Sólo un propósito educativo.

Trabajo en curso.

Secuestra una estación de radio de anuncios de tráfico para iniciar y establecer automáticamente la frecuencia de los coches alrededor del transmisor. La transmisión está

funcionando y la bandera de TA está en marcha, pero el arranque automático y el cambio de las radios del coche no funciona por ahora.

La radiofrecuencia se establece para la estación de tráfico de información que es 107.7 MHz.

- Config

Trabajo en curso.

- Modo de autos

En este modo, el Si4713 escuchará toda la frecuencia y seleccionará la que tenga un nivel mínimo de ruido, que representa una estación de radio gratuita.

Atención

Actualmente, el audio se transmite a través del cable P3, es decir, es necesario que un dispositivo externo conectado al cable P3 envíe el audio al Transmisor FM, un ejemplo estaría utilizando el smartphone con un cable P3 - P3, conectado al transmisor y colocando algo de música para reproducir en su smartphone.

Archivos

SD

Crear carpetas o Renombrar, Copia (a LittleFS también) y Borrar archivos.

Pequeños

Eliminar, Copia, Renombra o Leer archivos de LittleFS.

WebUI

Hazte dispositivo como un AP o conectarte a una red para usar el WebUI, con esto puedes administrar tus archivos en la tarjeta SD y también LittleFS Antes de configurarse, es necesario acceder a http://bruce.local con las credenciales en pantalla para tener acceso al gerente.

Almacenamiento de masas

Ahora puede emular un dispositivo de almacenamiento USB y acceder a los archivos de SD Card o LittleFS a través de USB.

Otros

SD Card Mngr

Crear carpetas o Renombrar, Copia (a LittleFS también) y Borrar archivos.

LittleFS Mngr

Eliminar, Copia, Renombra o Leer archivos de LittleFS.

WebUI

Hazte dispositivo como un AP o conectarte a una red para usar el WebUI, con esto puedes administrar tus archivos en la tarjeta SD y también LittleFS Antes de configurarse, es necesario acceder a http://bruce.local con las credenciales en pantalla para tener acceso al gerente.

Rastreador GPS

Utilice un módulo GPS para rastrear el dispositivo. Crea un archivo .gpx que se puede cargar a espectadores de gpx en línea como GPX Studio y GPS Visualizer o a cualquier aplicación de visor gpx para ver la ruta en un mapa.

BadUSB

Sólo DuckyScript se admiten cargas útiles. para más información sobre la creación de su propio DuckScripts leer aquí

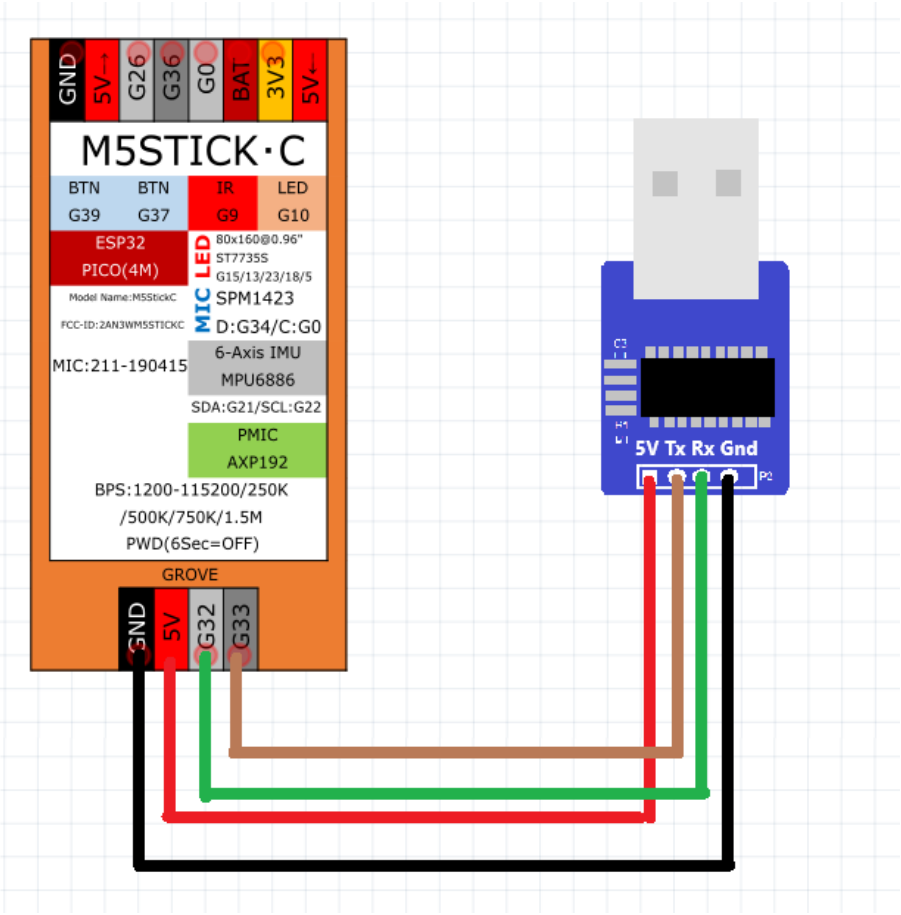
Para elegir una carga útil para el BadUSB en Cardputer en lugar de conseguir rickrolled, usted necesita crear un archivo en el directorio raíz de la tarjeta SD que termina con ".txt". A continuación, puede seleccionar qué carga útil se enviará cuando el Cardputer se conecta a través de cable USB.

Otros métodos para ejecutar los guiones de badusb:

1. a través del gestor de archivos SDCard/LittleFS en el menú "Otros" (seleccione un .txtarchivo)
2. remotomente a través de la WebUI, haga clic en el botón similar a la antena junto al archivo
3. a través de un serial cmd como badusb run_from_file HelloWorld.txt

Utilizando dispositivos malos USB en StickCs y Core/Core2

Tendrás que usar un módulo CH9329 como este o esto para ejecutar el Bad USB en tu dispositivo, cableándolo en el conector Grove de la misma manera:



Control de Led

Control ESP32 S3 Stamp RGB LED, con las opciones de color púrpura, blanco, rojo, verde y azul a más, también led parpadear parpadeos el LED.

Openhaystack

Esto es un poco más complejo de configurar, pero básicamente se puede utilizar este repositorio para generar una llave pública de AirTag codificada en base64. Entonces, para trabajar para Bruce, deberías decodificar tu llave pública con base64 y guardarla en un archivo en la raíz SD llamada "pub.key". Para crear archivo pub.key usted debe ejecutar esto en bash:

base64 -d <<< "your_base64_public_key"|tee pub.key**iButton**

Hacedor de clicker

Llamador USB Mouse que puede controlar el retraso entre los clics, esto se utiliza generalmente para hacer trampa en algunos juegos de clicker.