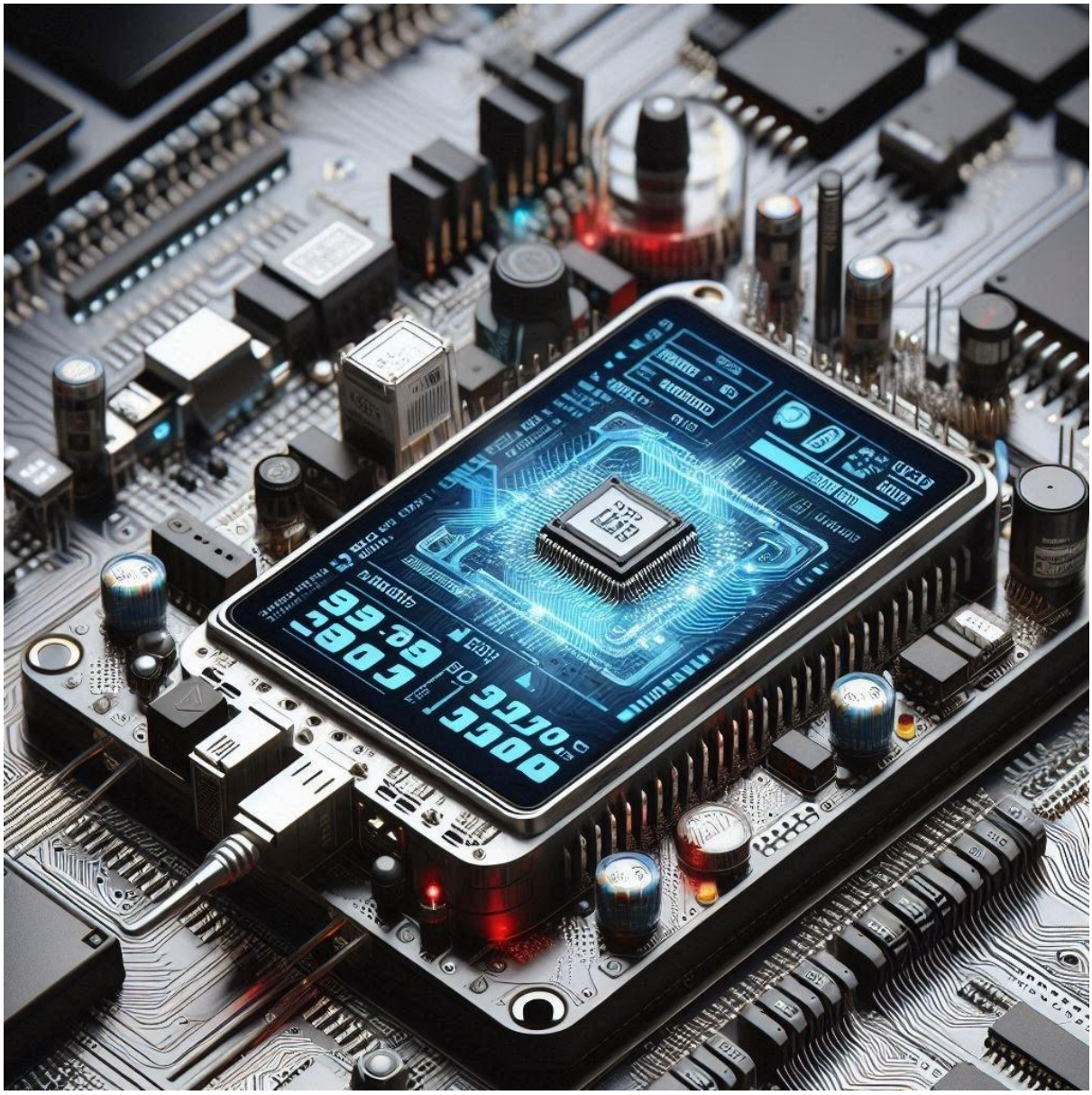


Evil-M5Project

Cheap Yellow Display (CYD)

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€.

11,19€ ~~13,81€~~ -18% dto.

Al por mayor +10 unidades, -1% dto. extra

El precio incluye IVA

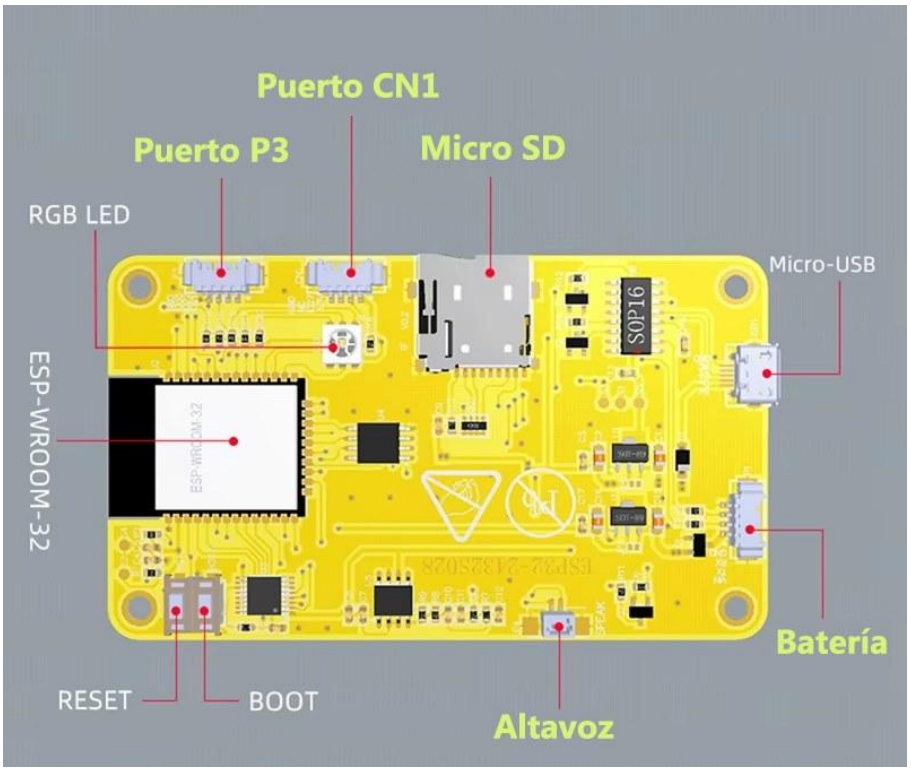
-2,00€ dto. en pedidos +19,00€ ›

Placa de desarrollo ESP32 Arduino LVGL WIFI y Bluetooth 2,8 "240*320 pantalla inteligente módulo TFT LCD de 2,8 pulgadas con tacto

★★★★★ **5.0** 5 valoraciones | 75 vendido

punto de venta

- Diseño IoT Versátil : Perfecto para IoT, desde dispositivos inteligentes hasta sistemas de monitorización y reconocimiento de QR.
- Modos de Dormir Eficientes:Incluye modos de dormir para reducir el consumo de energía, desde 6 mA hasta 310 mA.
- Pantalla LCD TFT 2.8":Pantalla LCD TFT de 2.8" con resolución de 320*240, ideal para interfaces de usuario.



Proyecto Evil-M5Project

Evil-M5Project es una herramienta innovadora desarrollada para pruebas éticas y exploración de redes WiFi. Aprovecha la potencia del dispositivo M5Core2 para escanear, monitorear e interactuar con redes WiFi en un entorno controlado. Este proyecto está diseñado con fines educativos, ayudando a comprender la seguridad y vulnerabilidades de la red.

Puedes encontrar toda la documentación en este enlace:

https://github.com/7h30th3r0n3/Evil-M5Project

Todas las características del proyecto malvado-M5

- **Escaneo de redes WiFi** : Identificar y mostrar redes WiFi cercanas.
- **Clonación de red** : Compruebe la información y reproduzca las redes para un análisis en profundidad.
- **Gestión de Portales en** Cautivo : Cree y expa un portal cautivo para incitar a los usuarios con una página sobre conexión.
- **Manejo Credential:** Capturar y administrar credenciales del portal.
- **Remote Web Server:** Monitoree el dispositivo de forma remota a través de una interfaz web sencilla que pueda proporcionar credenciales y cargar portales que almacenan archivos en una tarjeta SD.
- **Sondas de olfateo:** Oiff y almacenar sondas cercanas en una tarjeta SD.

- **Karma Ataque:** Pruebe un simple ataque de Karma en una sonda capturada.
- **Ataque automático de Karma:** Pruebe el ataque de Karma en las sondas cercanas automáticamente.
- **Bluetooth Serial Control** : Puedes controlarlo con Bluetooth.
- **Wardriving:** Llegada con salida de formato Wigle en SD.
- **Beacon Spam:** Genera múltiples SSID a tu alrededor.
- **Deauther:** Envía marcos de de autautenticación y olfatea 4-libros y PMKID.
- **Cliente Sniff y Deauth:** Clientes de Sniff conectados a AP y auto deauth mientras olfateaban EAPOL.
- **EAPOL/Deauth detection.**: Detecta paquetes de denantticación, apretones de manos de 4 vías, PMKID y pwnagotchi cerca de ti.
- **Wall Of Flipper:** Detectar y guardar Flipper Zero con Bluetooth habilitado cerca de usted y detectar BLE SPAM.
- **Enviar código Tesla con RFunit** : Utilice RFunit para enviar códigos Tesla, imitando las capacidades de Flipper Zero.
- **Red de** escaneo **y puerto:** Realizar escaneos de red y puertos para descubrir dispositivos y servicios, comprobando el estado de los hosts.
- **SSH Shell** : Conéctese a los servidores SSH directamente desde el dispositivo, permitiendo la ejecución del comando a través de una shell en el dispositivo.
- **Web Crawler** : Sitios web de arrastre para extraer información, asegurando la autorización para arrastrar antes de su uso.
- **PwnGrid** : Cara de sopa y mensaje en dispositivos pwnagotchi cerca, causando una negación de pantalla PWND.
- **Skimmer Detector:** Detectar posibles skimmers Bluetooth usando módulos HC-03, HC-05 y HC-06.
- **BadUSB** : Ataques de BadUSB emulando entradas de teclado/ratón para ejecutar scripts predefinidos o comandos con script proporcionado.
- **Wardriving Master:** Realizar unidades de guerra con esclavo de la familia para carfetar redes de mapas en un área definida, analizando señales e identificando puntos de acceso.
- **WebUi BadUSB** : Inicia los ataques de BadUSB a través de una interfaz web.
- **Wi-Fi Canal Visualizer** : Visualice el número de Wi-Fi cercano en cada canal.

- **Cliente Sniff** : Capture tráfico de clientes conectados para analizar comunicaciones y detectar posibles vulnerabilidades e informaciones filtradas.
- **Raw Sniffing** : Realizar capturas de paquetes crudos para un análisis en profundidad de los datos de red WiFi intercambiados.
- **Handshake Master**: Capturar y analizar apretones de manos WPA/WPA2 con Esclavo Sniffer en canal estático.
- **Customing Theming:** Personalice la interfaz de la herramienta y los temas para adaptar la apariencia para preferencias o necesidades específicas de la misión.
- **Escaneo de red completa:** Realice un escaneo completo de red para identificar dispositivos conectados, 70 puertos abiertos y servicios de ejecución.
- **Reverse TCP Tunnel**: Utilice remodetamente desde cualquier lugar de la WebUI.

¿Qué es un ataque de WiFi Karma?

Introducción al ataque de Karma

El Karma Attack representa una sofisticada explotación técnica cibertécnica. Mezcla el comportamiento común y a menudo pasa por alto el comportamiento de dispositivos inalámbricos como teléfonos inteligentes, computadoras portátiles y tabletas, que se programan para una conveniencia inusual, pero crean una laguna de seguridad.

La funcionalidad básica de los dispositivos inalámbricos

Para entender la mecánica del Karma Attack, es esencial entender cómo la mayoría de los dispositivos inalámbricos operan con respecto a las redes Wi-Fi. Estos dispositivos están diseñados para recordar redes Wi-Fi a las que se han conectado previamente.

Esta característica, conocida como reconexión automática, significa que es proporcionar acceso a Internet sin fisuras al conectarse automáticamente a redes familiares sin requerir la intervención del usuario cada vez. Cuando entras en tu casa u oficina, por ejemplo, tu dispositivo se reconecta automáticamente a la red Wi-Fi que reconoce porque se conecta con ella antes.

Aquí radica el defecto fundamental que el Karma Attack explota:

Cuando fuera de las redes conocidas, estos dispositivos emiten 'solicitudes de sonda'. Estas peticiones son esencialmente el dispositivo de vocación para cualquier red familiar. Dicen: "Está 'MyHomeNetwork' disponible? O "Puedo conectarme con 'CoffeeShopWifi'? Esta consulta automática es un proceso estándar, destinado a conectarte a redes conocidas más tarde.

La Mecánica del ataque al Karma

Un atacante, equipado con las herramientas adecuadas, escucha estas peticiones de sonda en lugares públicos. El equipo del atacante está diseñado para detectar los nombres de las redes que están buscando los dispositivos. Al capturar una solicitud de sonda, el equipo de atacante se hace pasar por la red solicitada creando un punto de acceso Wi-Fi pícaro con el mismo nombre. Para el dispositivo desprevenido, esta red pícara aparece como la red familiar y de confianza que se buscó.

En la práctica, para la mayoría de los equipos, sólo el nombre del SSID debe corresponder si la red original está abierta, si está protegida por WPA2 es necesario crear una red wifi que tenga la misma contraseña.

Cuando el dispositivo se conecta automáticamente a esta red pícara, creyendo que es la legítima, el atacante gana un fútbol significativo. El dispositivo está ahora en una red completamente controlada por el atacante, que luego puede iniciar una variedad de actividades maliciosas.

Riesgos y Explotaciones potenciales

Los riesgos aquí son múltiples:

- El atacante puede monitorear todos los datos que pasan por la red, potencialmente capturando información sensible como contraseñas, números de tarjetas de crédito y mensajes personales.
- El atacante podría manipular su experiencia en Internet, redirigirlo a sitios web fraudulentos o mal inyectar material en su dispositivo.
- En escenarios más avanzados, esto podría incluso conducir a un compromiso más profundo de la seguridad del dispositivo.

Vista de una víctima

1. **Bob está en el Park** pero no tenga conexión en la red.
2. **Bob se conecta a la verdadera red pública Wi-Fi** llamada "KarmaPark". Bob tiene un teléfono que recuerda redes Wi-Fi a las que se ha conectado previamente por defecto.
3. **Bob utiliza la** conexión **a Internet** normalmente.
4. **Cuando Bob abandona el parque**, su teléfono comienza automáticamente a buscar sondas "creamming" para que se conecte redes Wi-Fi conocidas. En particular, busca la red conectada anterior de KarmaPark sin que Bob se dé cuenta.
5. **Un hacker malicioso cerca** utiliza un dispositivo especial para olfatear sondas que están cerca de él. Este dispositivo es capaz de detectar que el teléfono de Bob está

activo buscando la red "KarmaPark" y crea un punto de acceso Wi-Fi falso con el mismo nombre.

6. **El dispositivo del hacker responde al teléfono de Bob**, haciéndose pasar por "KarmaPark. El teléfono de Bob, pensando que está conectado a la red anterior que necesita conectarse si se ve, se conecta automáticamente a ella.
7. **Ahora que Bob está conectado a la red falsa**, el hacker puede hacer modificaciones en la red. Esto incluye espiar sus comunicaciones, insertar malware, robar contraseñas y crear un portal cautivo.

¿Por qué el ataque del Karma es tan efectivo?

La eficacia del Karma Attack radica en su explotación de una función estándar y fácil de usar, la reconexión automática a las redes Wi-Fi conocidas. Este ataque no atrae a habilidades sofisticadas de hackeo o profundos defectos técnicos en el protocolo Wi-Fi. En cambio, aprovecha los comportamientos predecibles y automatizados de la mayoría de los dispositivos inalámbricos modernos.

En resumen, el Karma Attack es un duro recordatorio de los compromisos entre conveniencia y seguridad en la era digital. Subraya la importancia de conocer las posibles vulnerabilidades que vienen con las tecnologías cotidianas y la necesidad de prácticas diligentes de ciberhigiene.

Instalación

M5burner

1. Conecte su M5Core2 a su computadora.
2. Descargar M5burner en la sección de UIFLOW FIRMWARE BURNING TOOL en : M5Stack Centro de descargas
3. Coloque el contenido de archivo SD necesario en la raíz de la tarjeta SD. (Esto es necesario para acceder a todos los archivos del proyecto).
4. https://downgit.github.io/#/home

1. Escriba "evil-" en la barra de búsqueda y compruebe el dispositivo que tiene.
2. Haga clic en descargar y flash.