

ENITSDA

Cybercamp

Málaga 29/11/2018

ENITSDA

Nace originariamente de la idea de usar técnicas clásicas de MAC-Catching para triangular dispositivos en una zona mediante dispositivos de bajo coste y consumo.

Se plantea como un sistema de monitorización pasiva de dispositivos wireless que poseen Wifi o Bluetooth y son detectables.

La idea de porqué hacerlo con dispositivos ESP32 es por su bajo coste y porque no hay apenas competencia en el mercado.

ENITSDA

El sistema se enfoca como una red de seguridad perimetral, capturando el envío libre de paquetes. La transmisión de la información se hace vía wifi.

La elección en su conjunto va enfocada a que cualquiera, aunque su presupuesto sea bastante limitado pueda implementar su propia red.

Este sistema no es una malla de mithril, es pasivo, y aporta un plus a seguridad perimetral, siendo complementario a otras herramientas.

La recolección de los datos también puede ser tratada para futura inteligencia.

ENITSDA

Hay proyectos de auditoría wifi que serían capaces de hacer algo similar pero se desconoce de ningún proyecto relacionado en concreto con los ESP32 y las funcionalidades descritas, si es cierto que existen WIDS que capturan información similar pero el hardware es totalmente distinto y más caro.

Basándonos en la idea de intentar triangular la posición de un terminal con wifi activado, nos dimos cuenta de la información que podíamos usar y simplemente decidimos usar esa información como objeto de revelación de presencia o de identificación de un dispositivo en tiempo y lugar.

ENITSDA

El chip se ha elegido por su coste, gran documentación y versatilidad pese a las vicisitudes mencionadas.



El software de la parte de recepción y alerta se ha elegido por ser de el que se tenía algo de conocimiento, sopesando que fuese posible adaptarlo en tiempo y forma para el hackaton.



ENITSDA

Previamente hemos hecho pruebas básicas de que el dispositivo ESP32 era apto para usarlo con el proyecto (rendimiento, cambio de tecnologías, tls 1.2, etc).

Se aporta como material previo al hackaton una Raspberry Pi con raspbian instalado y un AP con wifi configurado con WPA2 para usarlo como conexión de los ESP32 e instalar el entorno de desarrollo en ella si lo soporta con fluidez.

Se trabajará sobre el software de captura en el ESP32, el de envío, y el de detección en el aspecto wifi/bluetooth. De la parte servidor se trabajará en el desarrollo de toda la estructura donde el sistema enviará y la gestión de macs y alertas, además de un módulo paralelo sobre deauths y su alerta.

ENITSDA

Factores a tener en cuenta:

ESP32 ni ESP8266 soportan MFP, son vulnerables a Deauths. Para ello se activará un sensor pasivo de desautenticaciones a dispositivos específicos en el AP receptor de información.

El acceso simultáneo al chip wifi y bluetooth no es posible, así como, la carga de las librerías para HTTPS no caben en el dispositivo junto a las de los dos anteriores haciendo uso de la API de Arduino, porque se valorará por la solución más factible en tiempo para el proyecto.





open source



ESPRESSIF

Espressif SDK

Usamos las API's de Espressif, bajo la licencia Apache License 2.0, para realizar la programación del ESP32.



ENITSDA GPL

Generación de un sistema de bajo coste implementado bajo licencia GPL para que pueda ser usado por cualquiera.

La ciberseguridad al alcance de todos

"Demuestra tu potencial"






**29 Noviembre - 2 Diciembre
2018**

contacto@cybercamp.es
cybercamp.es



**Recinto del Antiguo
Edificio de Tabacalera
(Málaga)**

 @CyberCampEs
 @CyberCampEs
 INCIBE

David Santos

Málaga

@dsecuma



Jorge Peñalba

Madrid

@jpsminix

