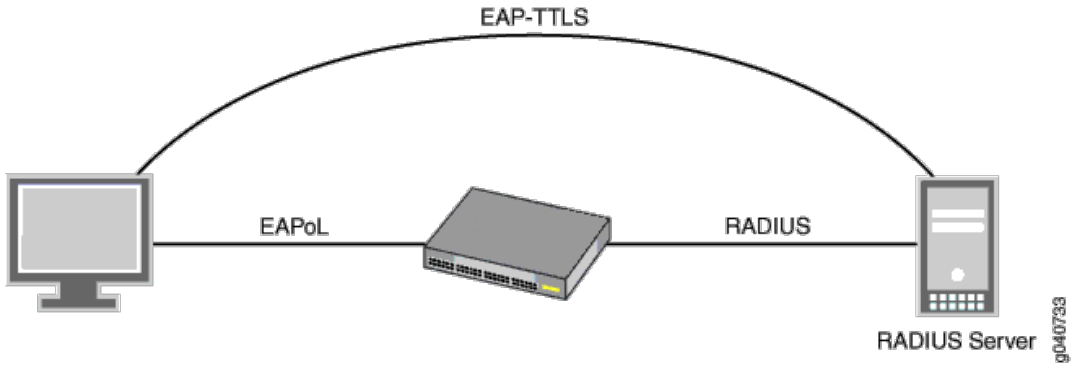
Edurogue
Viejos Riesgos
Duras Realidades

Víctor Barahona (UAM)

XVIII Jornadas Técnicas REDIMadrid

Robo de credenciales. Ese puñetero temita...

El problema explicado en pim pam pum



- 802.1X (EAPOL)
- Roles:
  + Suplicante/Cliente
  + Autenticador (Red wireless o wired)
  + Serv. de Autenticación (Radius)
- La comunicación se cifra en un tunel TTLS
- Si el cliente no valida el certificado del radius... le da la contraseña a cualquiera que se la pida
- **ES UN PROBLEMA DE CONFIGURACIÓN DEL CLIENTE NO ES UN PROBLEMA DE LA INFRAESTRUCTURA WIFI NI DE EDUROAM**

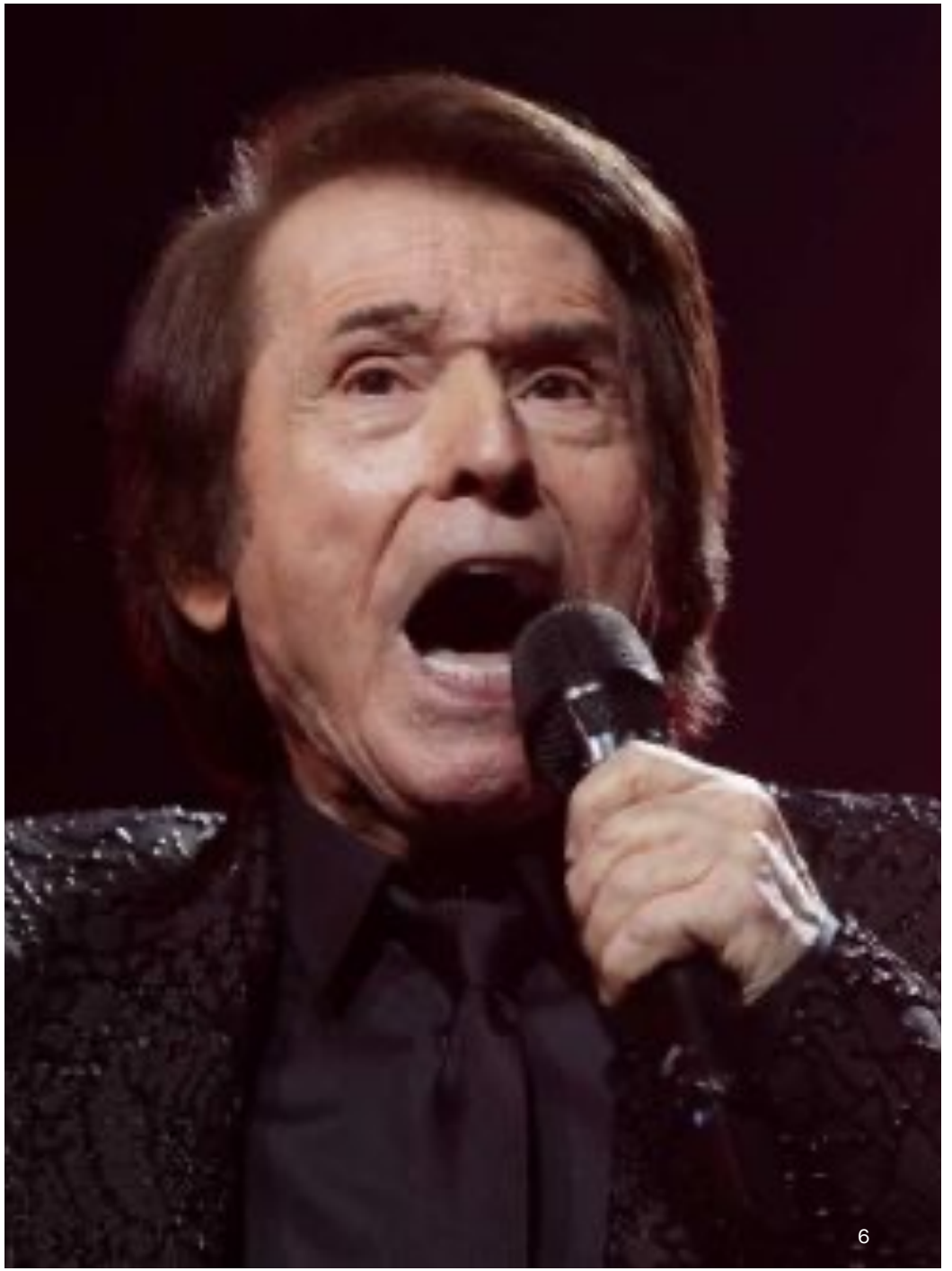
Timeline

- Madrid GT2007 - Nicolas Velázquez (UAM): Configuración de SecureW2
- Shmoocon 2008 - PEAP Pwned Extensible Authentication Protocol - Josh Wright and Brad Antoniewicz
- Eduroam CAT 2013 - Configuration Assistant Tool
- Santander GT2017 - Alberto Martínez (Deusto): Edurogue

PoC Hostapd-wpe GT2017

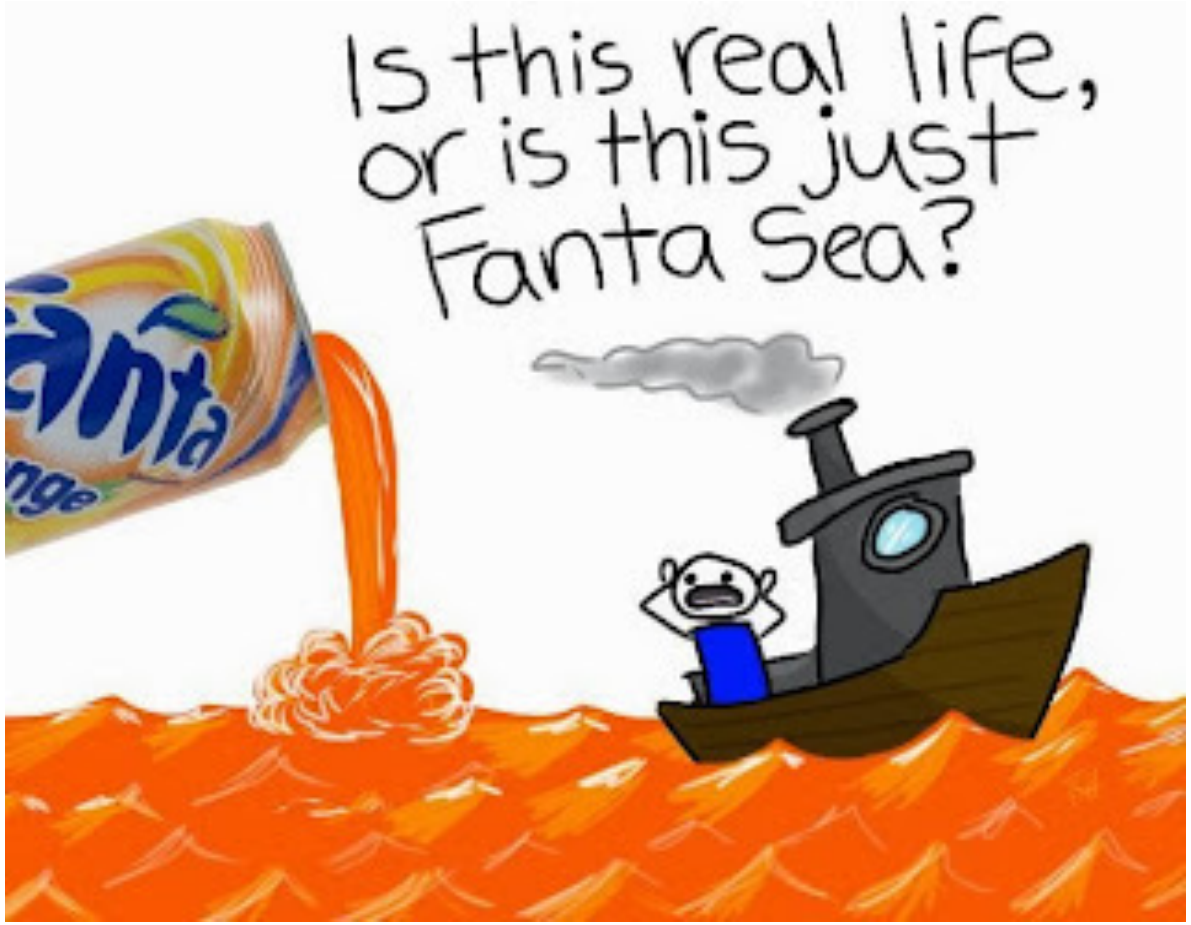
Escándalo

- Shock inicial
- 1ª Fase del duelo: negación
- 2ª Fase del duelo: ira



Fase 3
Negociación

- Y frases como estas resuenan por tu cabeza:
  + Quizás no haya muchos afectados
  + CAT Eduroam lleva tiempo disponible
  + Seguramente el problema es ya residual
  + Los SO han mejorado en su configuración
  + Ahora están las apps de geteduroam
- ¿Seguro? Necesitamos datos



Proyecto edurogue: objetivos

- Ayudarnos a entender que está pasando
- Permitirnos estimar el alcance del problema
- Identificar dispositivos vulnerables (y a sus usuarios)
- No debe suponer intervención del usuario
- No causar degradación o corte en la experiencia del usuario
- Ser muy barato (o gratis)

Edurogue: implementación

- Maquina corriendo kali linux 2020.4 (no posterior)
- Hostapd-wpe 2.7
- MariaDB
- Programado en Python3
- Drivers wifi apropiados para poner el interfaz wifi en modo monitor
- Telegram-bot (como interfaz de logs)

edurogue

Prototipo móvil (<80€)

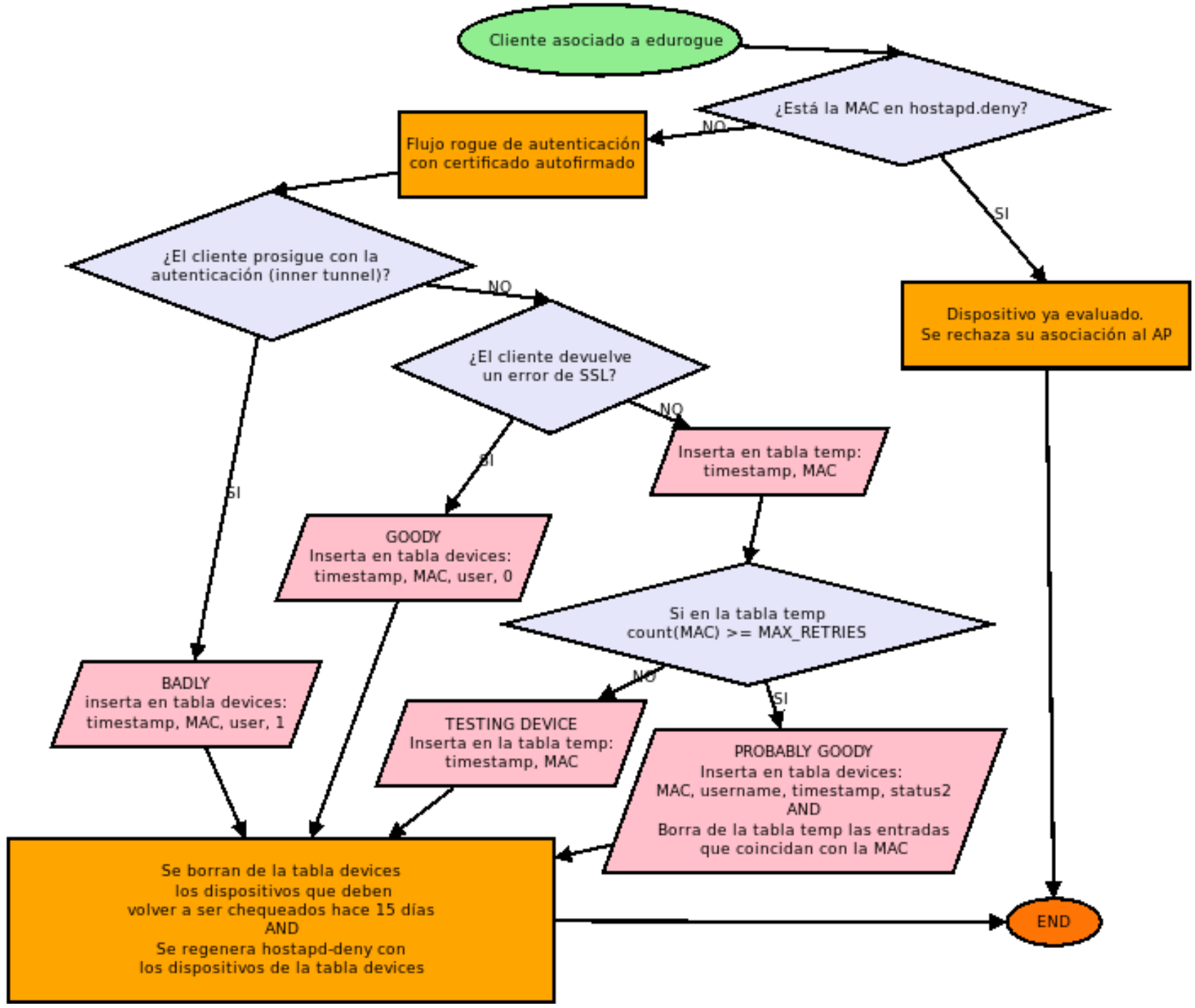
Raspberry Pi 3b - 50€

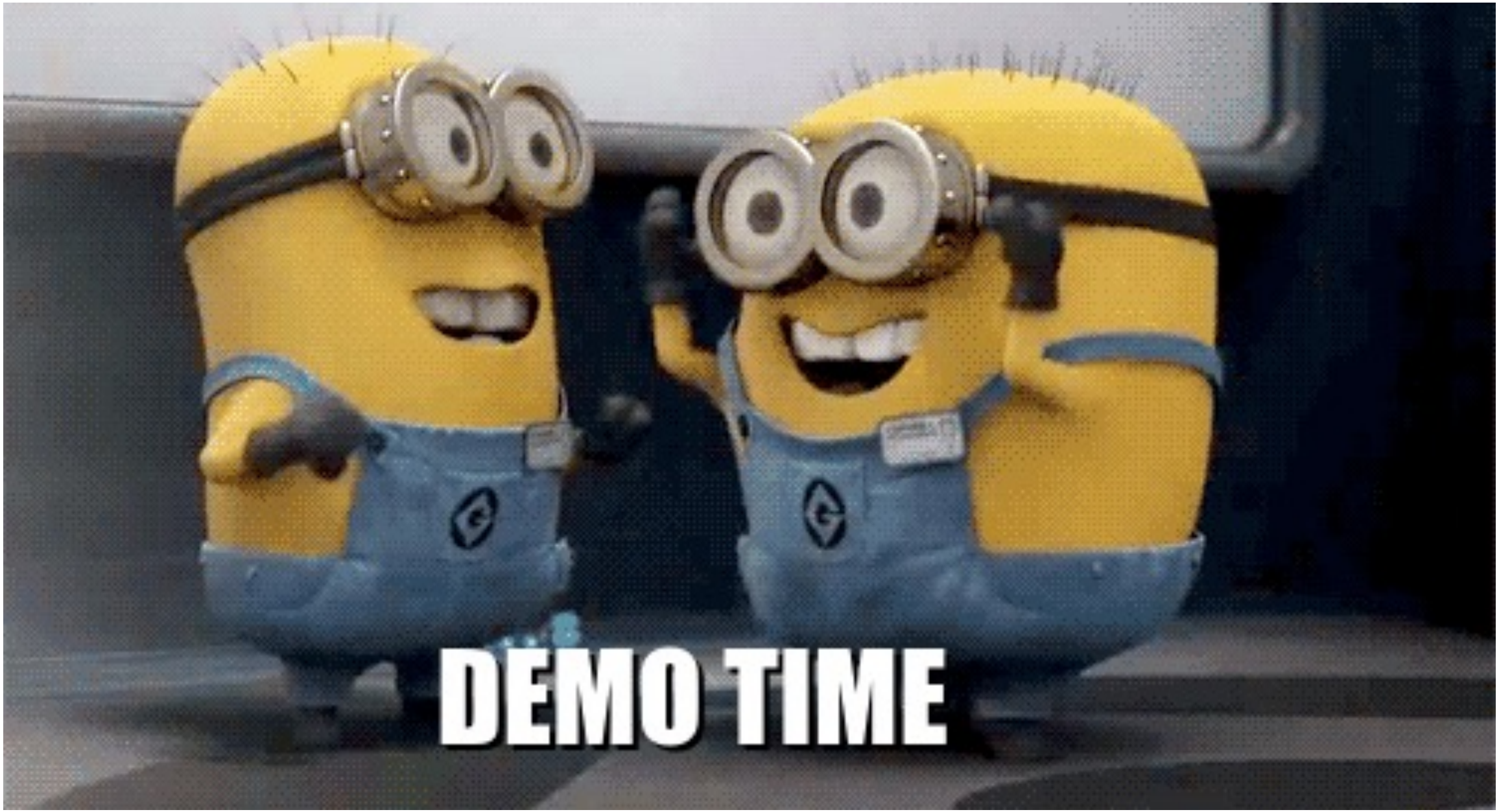
+

Adaptador de red
Tp-link WN722N v1/v3 10€

+

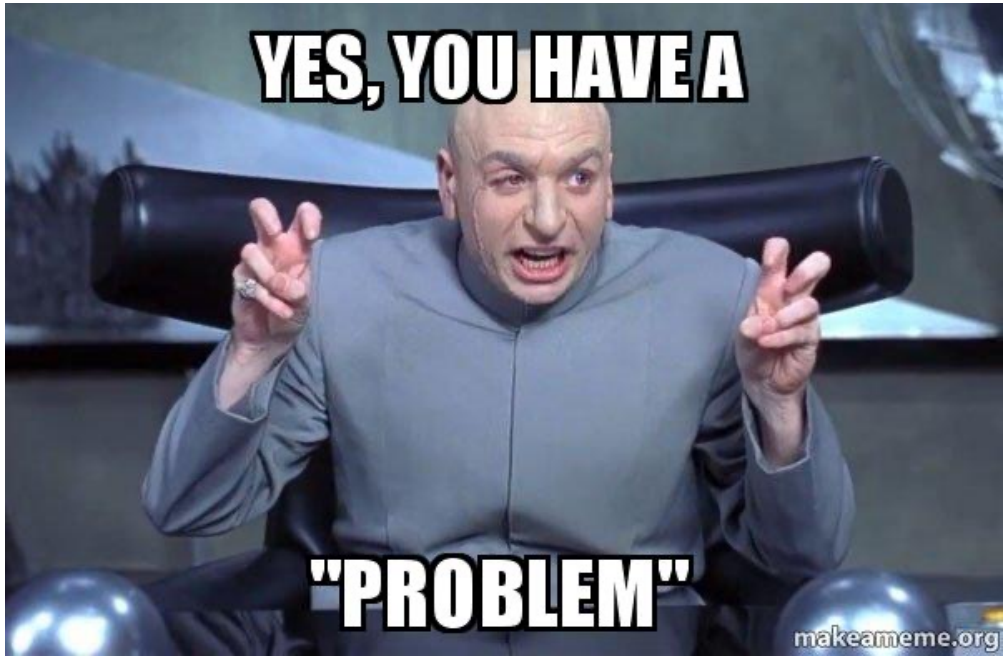
Bateria externa 20€


Cliente asociado a edurogue
¿Está la MAC en hostapd.deny?
NO
SI
Flujo rogue de autenticación con certificado autofirmado
¿El cliente prosigue con la autenticación (inner tunnel)?
NO
SI
Dispositivo ya evaluado.
Se rechaza su asociación al AP
¿El cliente devuelve un error de SSL?
NO
SI
Inserta en tabla temp:
timestamp, MAC
GOODY
Inserta en tabla devices:
timestamp, MAC, user, 0
Si en la tabla temp
count(MAC) >= MAX_RETRIES
NO
SI
BADLY
inserta en tabla devices:
timestamp, MAC, user, 1
TESTING DEVICE
Inserta en la tabla temp:
timestamp, MAC
PROBABLY GOODY
Inserta en tabla devices:
MAC, username, timestamp, status2
AND
Borra de la tabla temp las entradas
que coincidan con la MAC
Se borran de la tabla devices
los dispositivos que deben
volver a ser chequeados hace 15 días
AND
Se regenera hostapd-deny con
los dispositivos de la tabla devices
END
hostapd.deny
blacklisted devs
Variables de configuración:
MAX_RETRIES = 5 #reintentos
TTL_TO_RETEST = 15 #dias
devices
timestamp
device
user
status
temp
timestamp
device
log
timestamp
device
user


DEMO TIME

Fase 4 del duelo: depresión

- Según los datos recogidos el 31% de dispositivos son vulnerables
- ¡Son miles de usuarios!
- Afectan a todos los colectivos, pero no por igual:
  + Estudiantes 33%
  + Personal 25%
- Y si, también al personal TIC



Fase 5 del duelo: aceptación y aprendizaje

- **Tenemos un problema que no puede ser ignorado**
- Necesitamos revertir la situación actual
- No puede ser una sonda aislada
- Nuestra aproximación: Integrar edurogue en nuestra infraestructura
- Cada dispositivo será testeado al entrar en la red
- Presentación JJTT 2023 Zaragoza - Carlos Maqueda (UAM)
- Solución basada en producto comercial (ClearPass)
- Pero podría hacerse con un freeradius

Recapitulando

- Eduroam es seguro
- Un dispositivo mal configurado convierte en vulnerable al dispositivo
- El ataque es contra el dispositivo
- El objetivo del atacante son las credenciales del usuario
- El problema es muy real
- Usad edurogue para valorar el problema en vuestras instituciones
- Desplegad MFA en el resto de servicios

Referencias

- **Configuración de SecureW2 en una organización eduroam -** *Nicolas Velazquez (UAM)* - https://eduroam.es/presentaciones/SecureW2.pdf
- **PEAP Pwned Extensible Authentication Protocol** - Josh Wright and Brad Antoniewicz
  + Video https://www.youtube.com/watch?v=EUcEcqJj24s
  + Presentación https://www.willhackforsushi.com/presentations/PEAP_Shmoocon2008_Wright_Antoniewicz.pdf
- **edurogue: Captura de credenciales institucionales desde terminales Android** - Alberto Martinez (DEUSTO)
  + Video: https://tv.rediris.es/video/592edc10a7bc283f008b456f
  + Presentación: https://www.rediris.es/jt/jt2017/programa/jt/ponencias/?id=jt2017-jt-exp_comu_a5-a8b3c1.pdf
- **Implementación de Edurogue en la red inalámbrica de la UAM** - Carlos Maqueda (UAM)
  + Video https://tv.rediris.es/es/jjtt2023/video/64817b75d2fafa003532c044
  + Presentación: https://www.rediris.es/jt/jt2023/programa/ponencias/?id=jt2023-jt--a6b1c1.Presentacion-Edurogue-UAM.pdf
- **Hostapd-wpe:** https://github.com/OpenSecurityResearch/hostapd-wpe
- **Old Kali Linux Stuff:** http://old.kali.org

¿Preguntas?