My WiFi in Paranoid Mode

Pablo González
@pablogonzalezpe

$whoami

HoneyCON By HoneySec

Pablo González (MVP Microsoft 2017-2018-2019)

- Ingeniero Informático
- Fundador de hackersClub
- Co-fundador de Flu Project
- 2009 – 2013 Informática 64
- 2013 - ?? Telefónica Digital España
- Algunos libros (OxWord):
  - Metasploit para pentesters
  - Pentesting con Kali
  - Ethical Hacking
  - Got Root: El poder de la mente

@pablogonzalezpe

¿De dónde vengo?

HoneyCON
By HoneySec

- Departamento de Ideas Locas CDO
- ¿Qué hacemos?
- ¿Qué aportamos?
- ¿Estamos locos?

@pablogonzalezpe

WiFi y la PSK

HoneyCON
By HoneySec

	Open	WEP	WPA-PSK	WPA2-PSK
Traffic sniffing/ analysis	X	X[1]	X[2]	X[2]
Session hijacking	X	X[3]	X[3]	X[3]
Access point spoofing	X	X[4]	X[4]	X[4]
Man-in-the-middle	X	X[1]	X[2]	X[2]
Information manipulation[5]	X	X		
Denial of service	X	X	X	X

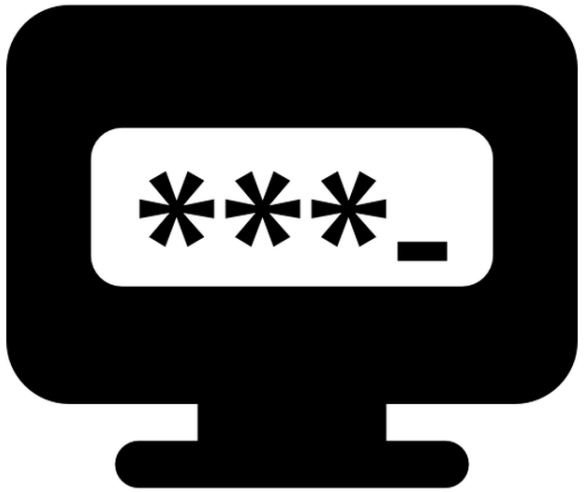
https://www.slideshare.net/chemai64/viviendo-en-la-jungla-27121575

@pablogonzalezpe

WiFi y las claves infinitas

HoneyCON
By HoneySec

¿Cuántos cambiáis la clave de vuestra WiFi en casa?



@pablogonzalezpe

La temporalidad

HoneyCON
By HoneySec

Concepto interesante

Acompañado de otros factores suma seguridad

Rebaja la exposición

Rebaja la probabilidad

```ruby
#!/usr/bin/ruby

require 'rotp'
require 'base64'
require 'open3'

unless ARGV.length == 2
  puts "Dude. Usage: ruby totp.rb <interface> <SSID>"
  exit
end

totp = ROTP::TOTP.new("Y64VEVMBTSXCYIWRSHRNDZW62MPGVU2G")
puts totp.now

enc = Base64.encode64(totp.now)
puts enc

connected = true
begin
    begin
        puts "Trying connection to... #{ARGV[1]}"
        Open3.popen3("networksetup -setairportnetwork #{ARGV[0]} #{ARGV[1]} #{enc}") do |stdin, stdout, stderr, thread|
        message = stdout.read.chomp
        puts "Message: #{message}"
        if message == ""
            connected = true
        end
    end
    rescue
        puts "Problem with connection to #{ARGV[1]}..."
    end
end while !connected
```

...24/Desktop — pgonzalez@pg-usrv01: ~ — -bash | ~/data/TOTP Wifi — ruby totp.rb en1 TOTP | ~/data/TOTP Wifi — ping 8.8.8.8 | ...Wifi — pi@raspberrypi: ~ — ssh pi@192.168.0.29

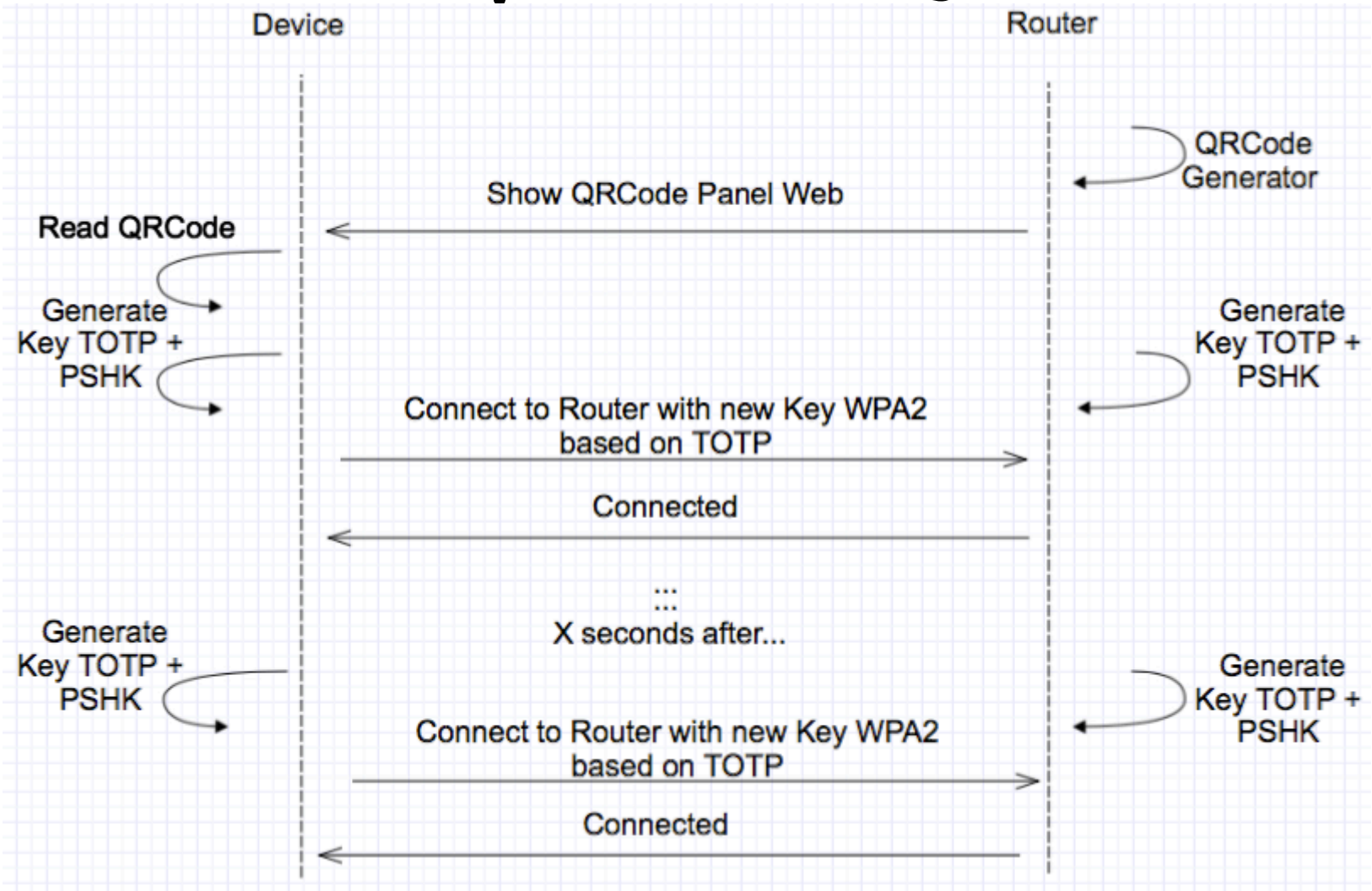
```
Message:
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
Toca cambiar clave
new key: MzczNjE5
Trying connection to... TOTP
Message:
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
Toca cambiar clave
new key: MDAzMDYy
Trying connection to... TOTP
Message:
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
```

@pablogonzalezpe

```
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
Toca cambiar clave
new key: ODg3Njgx
Trying connection to... TOTP
Message:
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
Toca cambiar clave
new key: Mzg3ODEz
Trying connection to... TOTP
Message:
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
No toca cambiar
```

@pablogonzalezpe

Idea 2: De script a Proyecto



De script a Proyecto

HoneyCON By HoneySec

1. La App dispone de un lector de QRCode.
2. En el QRCode, el router inserta toda la información necesaria: semilla para la generación del TOTP, la clave Pre-Shared Half Key, el nombre del SSID y el intervalo en segundos de la generación del nuevo TOTP.
3. En el instante que la app obtiene esta información puede hacer el cálculo de la clave derivada, basándonse en el TOTP que se genera cada 'x' segundos y la clave Pre-Shared Half Key.

Idea 3: de Rasp al Router

HoneyCON
By HoneySec

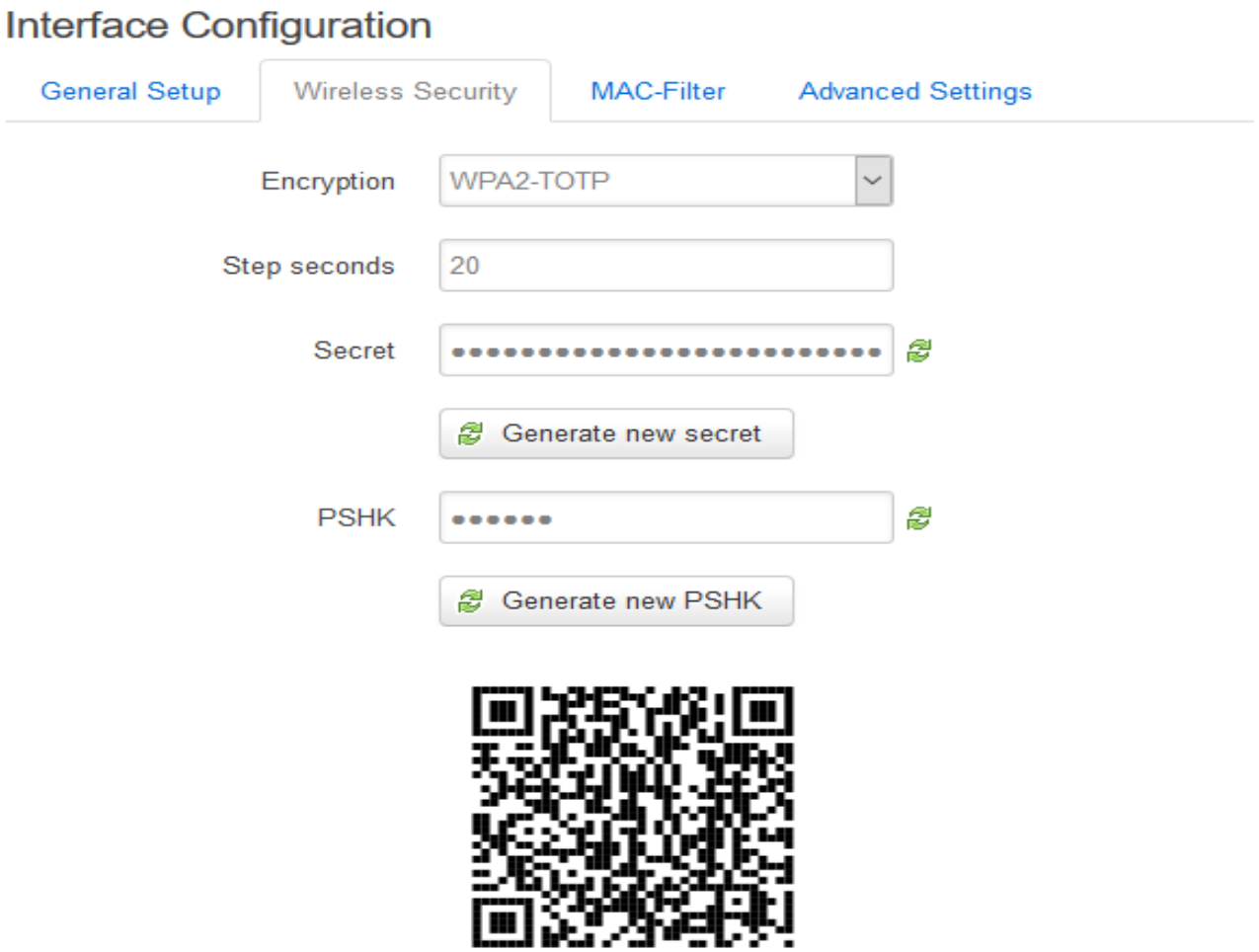
Router Amper 26555

LEDE

+LUCI Custom

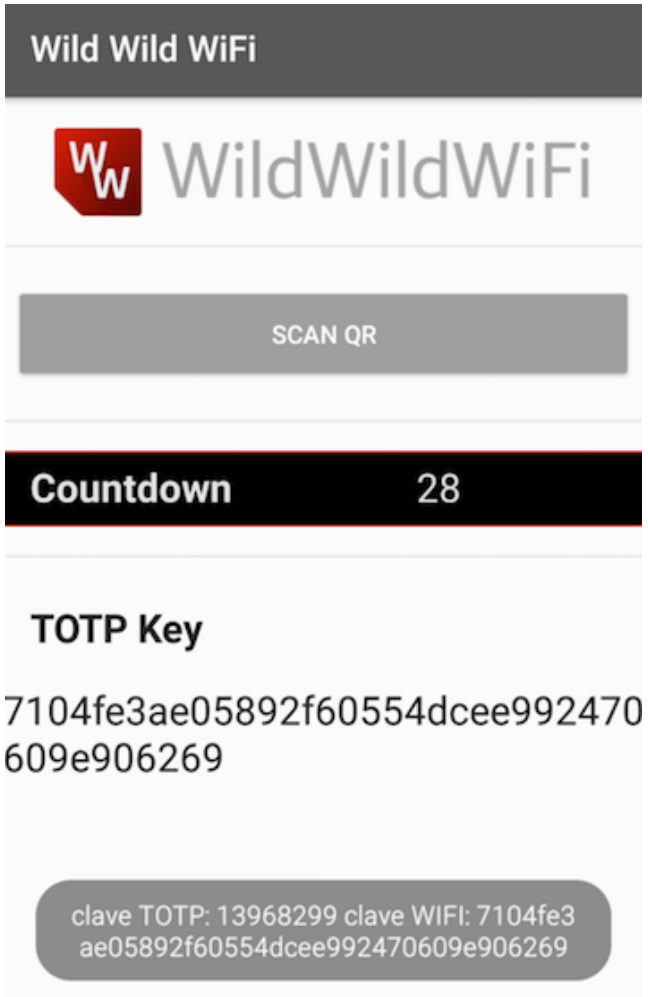
@pablogonzalezpe

Configuración del Router



@pablogonzalezpe

Apps creadas



@pablogonzalezpe

@pablogonzalezpe

Patente (All-in-one)

HoneyCON
By HoneySec

Autenticación temporal (TOTP)

Generación aleatoria semilla

Rasgo biométrico

Autenticación periódica

Entorno físico para lectura de QRCode

Demo time

HoneyCON
By HoneySec

@pablogonzalezpe

The end

HoneyCON
By HoneySec

Pablo González

My WiFi in
Paranoid Mode

@pablogonzalezpe