Seguridad en redes wireless

5º Ing de Telecomunicaciones
R.O
R.B.A
G.S.R.O

Peng Yan Song
Joaquín Pezonaga Montes-Jovellar

INDICE

Introducción

- IEEE 802.11
- Formato de tramas
- Seguridad 802.11
- Algoritmo de cifrado WEP
- Ataques Estadísticos al cifrado WEP
- Ataques Inductivos al cifrado WEP
- Realización práctica de los ataques
- Conclusiones

Introducción

- En el año 1997 el IEEE aprobó el estándar 802.11 redes inalámbricas de área local (Wireless LAN). El primer estándar fue complementado al poco tiempo por otro llamado IEEE 802.11b (1999), Para garantizar la compatibilidad entre diferentes implementaciones del estándar IEEE 802.11
- Se creó una nueva organización llamada WECA (Wireless Ethernet Compability Aliance, ahora conocida como WiFi Alliance). El objetivo de esta asociación fue crear una marca que permitiese fomentar más fácilmente la tecnología y asegurase la compatibilidad de equipos, popularizo el emblema Wi-Fi (Wireless Fidelity).

Introducción

- Los sistemas inalámbricos en la actualidad están en auge por la versatilidad que nos proporcionan de movilidad y el ahorro en costosos cableados.
- Todas las empresas y particulares están optando por esta tecnología. Lo que desconocen son las debilidades que tiene la encriptación de las redes wireless.
- Vamos a ver la desde un punto de vista técnico. El protocolo 802.11, la debilidad de la encriptación WEP, los principales ataques a las redes wireless (desde un punto de vista teórico) y su realización práctica.

Introducción

- AP (Acces Point) punto de acceso: La función más importante es la de puente entre la tecnología wireless y la tecnología ethernet, también hacen llegar las tramas a los usuarios.
- DS (Distribution System) sistema de distribución: Es un componente lógico que se usa para repartir y enviar las tramas a su punto de acceso correspondiente.
- Estaciones (Station): los PC con acceso wireless.

IEEE 802.11

- Servicios redes Wireless:
  - Distribución: Este servicio es el que distribuye la información entre los AP o el router. Las tramas que utiliza este servicio son las de datos, también es el servicio que nos permite transmitir datos entre dos PC de la misma red pasando a través del AP.
  - Privacidad: La encriptación de la trama para evitar que otros usuarios lean mis tramas.
  - MSDU delivery: Servicio que hace llegar los datos a destino.
  - Asociación: Servicio que permite a una estación unirse a un AP para que a través de este le lleguen las tramas de información y control.
  - Reasociación: Servicio que permite ir moviéndose de AP a AP, esta transición se realiza cuando la estación detecta que recibe más potencia de otro AP de la misma red. Este servicio lo inicia siempre la estación.

IEEE 802.11

- Cuando se reasocia, el sistema de distribución se actualiza para modificar el flujo de tramas a esa estación, y que se realice a través del nuevo AP.
- Disociación: Servicio por el cual avisamos del fin de asociación al AP. Este protocolo permite a una estación irse de la red sin utilizar este servicio.
- Autentificación: Cada cierto tiempo el AP realiza unas autentificaciones rutinarias para asegurarse de que las estaciones asociadas están autorizadas.
- Desautentificación: Servicio para avisar del fin de las autentificaciones.
- Integración: Servicio que permite comunicarse entre AP con protocolos que no pertenecen al IEEE 802.

IEEE 802.11

- ***DCF:*** función básica del estándar CSMA/CA del mecanismo de acceso.
  - Se mira que el canal esté limpio para evitar colisiones.
  - Controla los tiempos de pausa después de cada trama.
  - Si el medio no se vacía de tráfico el DCF puede utilizar las funciones RTS/CTS para limpiar de tráfico.
- ***PCF:*** (Point coordination function)
  - Provee de servicios libre de discusión, algunos tipos de servicios de control o de gestión de la red, no requieren un envío constante de tramas, por ello se reserva un tiempo para que se intercambien las tramas sin petición de medio, NAV y otros requisitos del protocolo.
  - Algunas estaciones se encargarán de que el medio se usa sin problemas, principalmente serán los AP.
  - Para mayor prioridad permite a algunas estaciones transmitir tramas después de intervalos más pequeños.

IEEE 802.11

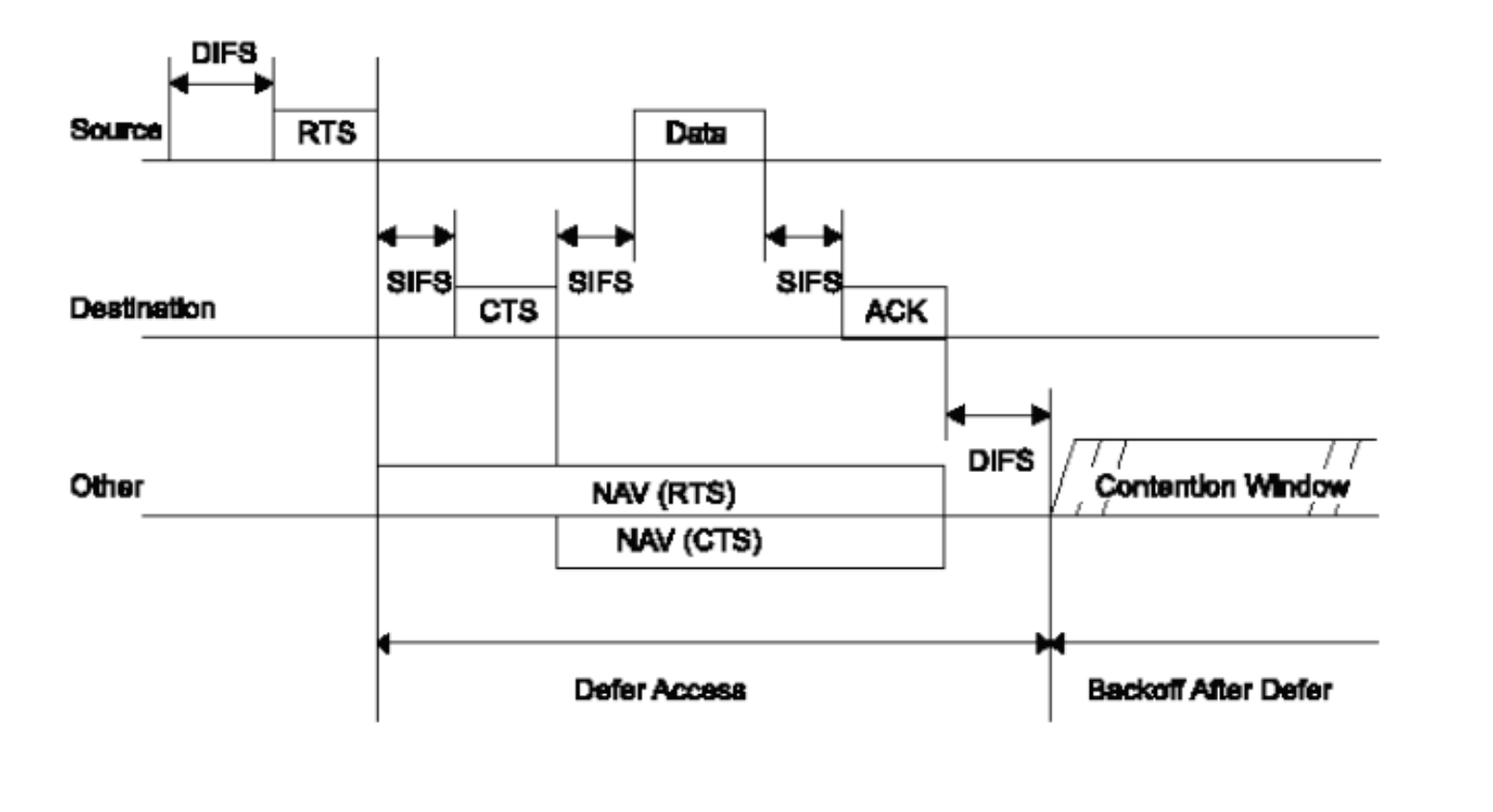
- CSMA/CA y Espacios entre tramas
  - no se pueden detectar las colisiones, no CSMA/CD. por lo que se implementa CSMA/CA que es un esquema de control de acceso al medio de transmisión.
  - Además el CSMA/CA prove el Network Allocation Vector (NAV) que indica el tiempo aproximado que va a estar el medio usado. Otras estaciones ponen el contador al valor del NAV y van contando hacia atrás, mientras el NAV sea distinta de cero la estación no emite .
  - DIFS: Tiempo de espera entre tramas (menor prioridad). Es el tiempo de espera cuando una estación no esta en una transmisión y quiere acceder al medio, o el que esperan todas las estaciones cuando 2 estaciones acaban de transmitir.
  - PIFS: Tiempo intermedio (prioridad media). Sirve para que ciertas tramas con prioridad adquieran el medio antes que intercambios normales, siempre y cuando el medio esté libre.
  - SIFS: Tiempo menor de espera entre tramas (máxima prioridad). Este es el tiempo de espera mínimo para asegurar que el medio está libre, este tiempo es el mínimo de espera y el que esperan las estaciones dentro de una transmisión.

IEEE 802.11

- BackOff
  - Cuando una estación acaba todas las estaciones esperan un tiempo DIFS y se preparan para realizar el Algoritmo de Backoff. Después de este tiempo DIFS viene una ventana dividida en slots. Cada estación que quiera acceder al medio selecciona un slot de forma aleatoria y espera a que este slot llegue.
  - Cuando llega el slot la estación transmite. Si tenemos varias estaciones, la estación que transmitirá será la que menor slot haya seleccionado. El tamaño de la ventana backoff es de 2^x-1 con x=5, 6, 7, 8, 9, 10 primero se empieza por 5 y cada vez que una trama falla se incrementa en uno, si falla 5 veces o más la ventana se quedara estable en x=10. Si el envió es correcto se vuelve al valor mínimo x=5. el número mínimo de slots 35 y el número máximo de slots 1023.
  - Al final lo que hacemos es que cada estación espere un tiempo DIFS más un tiempo aleatorio, el que menor tiempo aleatorio espere ganara el medio (callando a las demás estaciones con el NAV). Si se produce un error esas estaciones vuelven a esperar un tiempo aleatorio.

IEEE 802.11

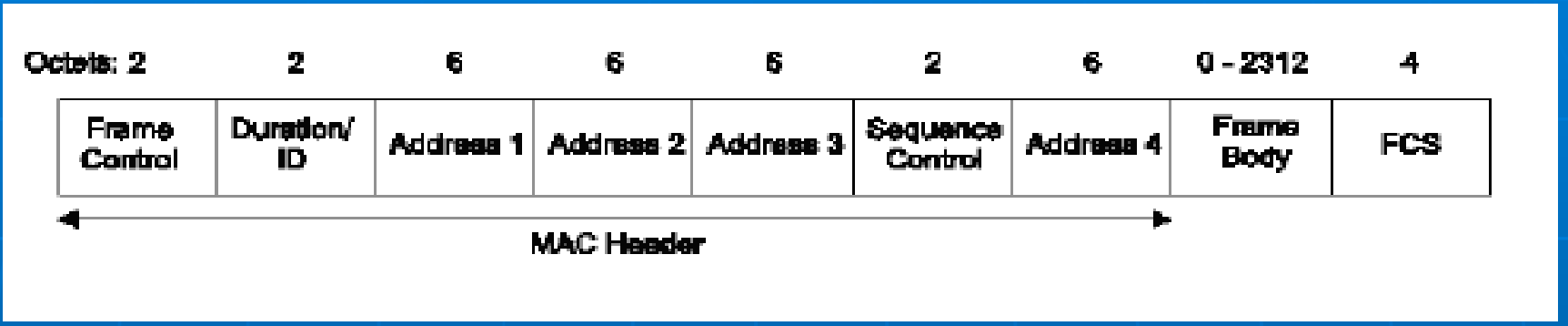
- Funcionamiento



IEEE 802.11

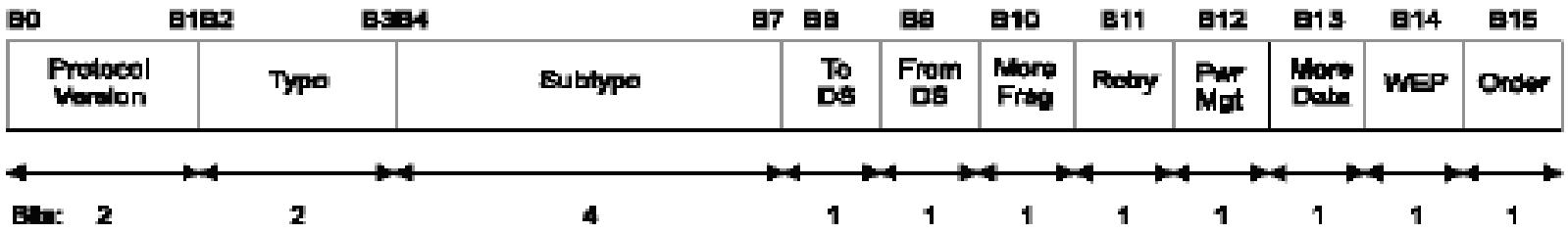
- ***Errores:***
  - En las tramas tenemos un retry counter, en los AP tenemos 2. A cada trama se le ponen un tiempo de vida máximo si este tiempo de vida se pasa (el número de reenvíos pasa a su tiempo de vida) esta trama queda descartada y si es de una multitrama quedaran descartadas todas las siguientes.
- ***Fragmentación:***
  - El 802.11 tiende a fragmentar los paquetes grandes, por el ruido que tenemos en el medio. El microondas (principal enemigo de las redes inalámbricas) tiene una de ruido específica. En el protocolo se tiene en cuenta esta forma de emitir del microondas, y por ello las tramas grandes se fragmentan, para que solo pequeñas partes estén afectadas y no afecte a todo la trama.
  - El tamaño máximo de las tramas con cabeceras es 2346 bytes, sin cabeceras 2312 bytes. Cada fragmento tiene la misma secuencia pero un campo que indica el orden de los fragmentos. También tenemos la fragmentación burst que incluye el RTS/CTS.

Formato de tramas



- Campo de control de trama.
- Duration/ID. En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para el NAV.
- Campos address1-4. Contiene direcciones de 48 bits donde se incluirán las direcciones MAC de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.
- Campo de control de secuencia. Contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.
- Cuerpo de la trama. Varía según el tipo de trama que se quiere enviar.
- FCS. Contiene el checksum.

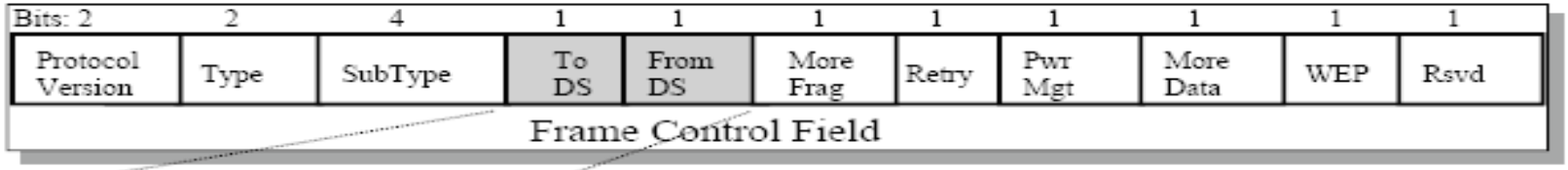
Subcampo control de trama.



- Versión.
- Type/Subtype
- ToDS/FromDS: Identifica si la trama si envía o se recibe al/del sistema de distribución.
- Más fragmentos: Se activa si se usa fragmentación.
- Retry: Se activa si la trama es una retransmisión.
- Power Management: Se activa si la estación utiliza el modo de economía de potencia.
- More Data: Se activa si la estación tiene tramas pendientes en un punto de acceso.
- WEP: Se activa si se usa el mecanismo de autenticación y encriptado.
- Order: Se utiliza con el servicio de ordenamiento estricto, en el cual no nos detendremos.

Formato de tramas

- ToDs 0 y FromDs 0: Se usa en las redes ad-hoc.
- ToDs 0 y FromDs 1: Cuando la trama va del AP a la estación.
- ToDs 1 y FromDs 0: Cuando la trama va de la estación al AP.
- ToDs 1 y FromDs 1: Cuando usamos como sistema de distribución un enlace wireless, al intercambiarse tramas entre AP´s.

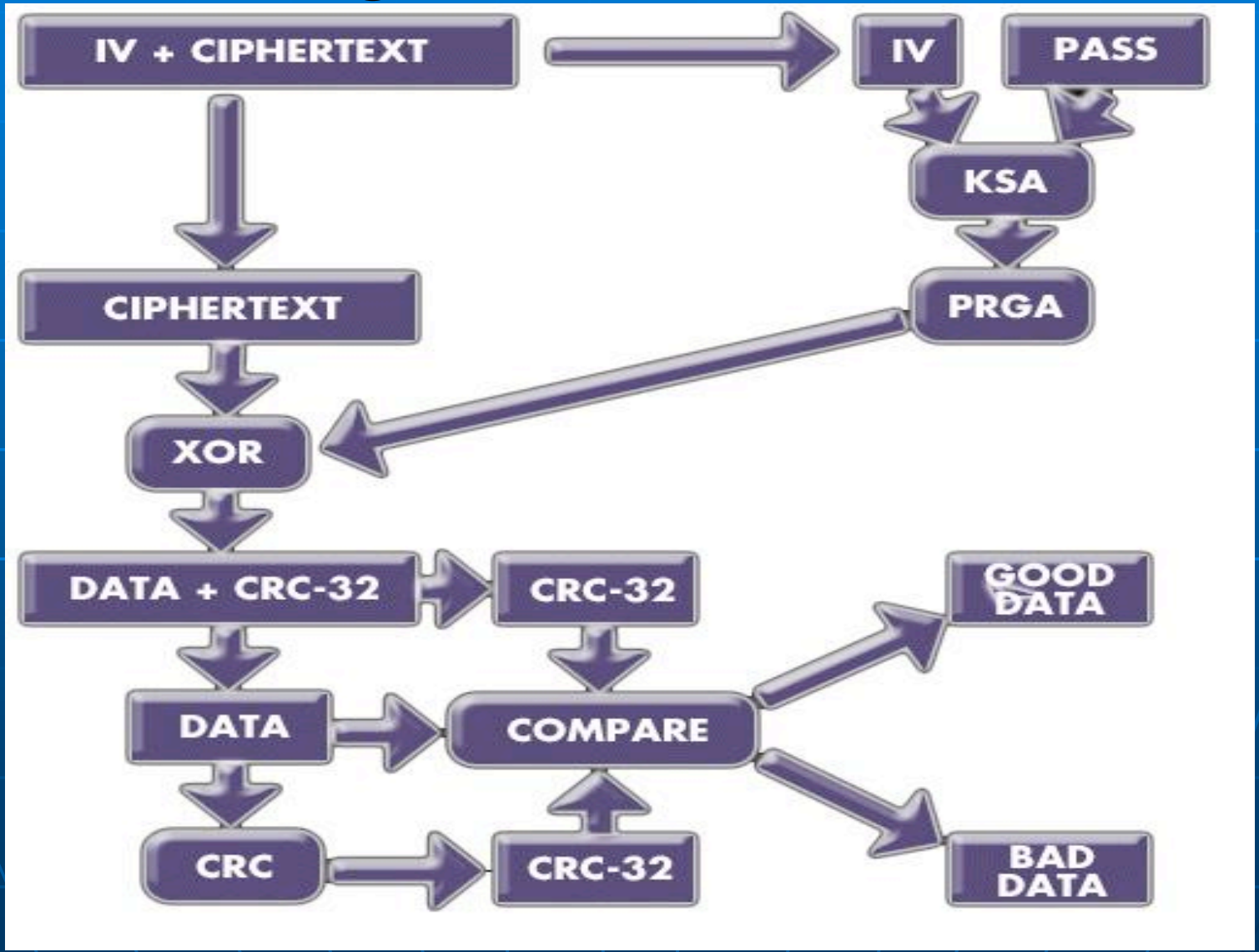


To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Seguridad 802.11

- **WEP (*Wired Equivalent Privacy*, Privacidad Equivalente al Cable)** es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, sistema de encriptación estándar implementado en la capa MAC.
- Proceso con la clave de 64 bits, están formados por 24 bits correspondientes al vector de inicialización, siempre tiene el mismo tamaño, más 40 bits de la clave secreta, estos son los bits que varían si ponemos claves de mayor tamaño, esta clave secreta sirve tanto para cifrar como para descifrar por ello se dice que es una clave simétrica.
- El vector de inicialización (IV), es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir ataques. Ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.
- A la contraseña común se concatena el IV del paquete y se introduce como semilla en el algoritmo RC4, a la salida obtenemos una secuencia del tamaño del cuerpo'+ICV llamada keystream.
- El ICV (Integrity Check Value) es un CRC-32 que se añade a los datos, sirve para comprobar que el descifrado ha sido correcto, un valor de comprobación. Este valor también se cifra.

Seguridad 802.11



Seguridad 802.11

- ***PRINCIPALES DEBILIDADES DEL ENCRIPTADO WEP.***
- Debilidades que afectan cifrado WEP, son las relacionadas con las claves, su conformación y distribución.
- El protocolo 802.11 da la opción de utilizar el cifrado WEP pero no comenta nada de la gestión de las claves, la forma en la que se ha implementado es que cada usuario introduzca la clave manualmente. Un gran problema de que cada usuario introduzca la clave manualmente, es que si la red crece mucho, la clave es conocida por más gente.
- Otro problema es que si tenemos mucha gente con la misma clave, facilitamos el trabajo a los atacantes ya que tienes muchos paquetes con la misma clave.
- Este problema se puede corregir cambiando cada cierto tiempo de clave, pero si la cantidad de usuarios es muy elevada es difícil de reconfigurar todos los equipos rápidamente, esto implica un mantenimiento exhaustivo de la red, que no se suele dar.
- También podemos configurar las estaciones y los AP parar que varíen las claves de forma automática entre unas cuantas claves predefinidas, aun así todos los usuarios tienen que seguir conociendo todas las claves.

Seguridad 802.11

- ***SEMILLA RC4***

- Otro problema es como WEP genera la semilla del algoritmo RC4. Tenemos varios tamaños de semilla 64bits, 128bits. Por definición el vector IV tendrá un tamaño de 24 bits, y la clave secreta aportará el resto de bits, 40 o 104 bits. Como sabemos el vector IV se envía en el paquete sin cifrar, lo que hace que en cada paquete ya conozcamos 24 de los bits de la semilla. Como el algoritmo RC4 también es conocido, solo tenemos que descubrir los 40 o 104 bits de la clave secreta para tener la clave WEP descifrada.

- Este problema hace que disminuya la efectividad de la clave, como la clave manual es de tamaño fijo solo vamos a tener $2^{24}=16777216$ secuencias de salida del algoritmo RC4 (keystream), uno por cada IV. Si tuviéramos 64 bits de clave efectiva, tendríamos $2^{64}=1.84467440737*10^{19}$ claves diferentes. Y con 128, tendríamos $2^{128}=3.40282366921*10^{38}$ claves diferentes, tamaños suficientemente grandes para eliminar algunos ataques o para evitar repeticiones.

Seguridad 802.11

- ***REUTILIZACIÓN DE LOS KEYSTREAM.***

  - Los IV son demasiado cortos y se permite la reutilización de IV, a este problema se le suma que una debilidad bien conocida de los algoritmos de cifrado de flujo es que cifrando dos mensajes (P1, P2) con la misma clave (k) y vector IV se puede revelar información sobre ambos mensajes

    Si C1 = P1 (+) RC4(iv, k)
    y C2 = P2 (+) RC4(iv, k)

    C1 (+) C2 = (P1 (+) RC4(iv, k)) (+) (P2 (+) RC4(iv, k)) = P1 (+) P2

    En otras palabras, aplicando XOR a los dos textos cifrados (C1 y C2) el keystream se cancela, y el resultado que obtenemos es el XOR de ambos textos planos (P1 (+) P2).

    Esto nos brinda las siguientes posibilidades:

  - Conocido el texto plano de uno de los mensajes, dispondremos del otro texto plano.
  - Podremos recuperar P1 y P2 teniendo sólo P1 (+) P2, debido a la redundancia que habitualmente tienen los textos planos. Podemos buscar dos textos sobre los que, aplicados un XOR, resulten en el valor dado P1 (+) P2.

Seguridad 802.11

- Ya que los IVs son públicos, el duplicado de IVs puede ser fácilmente detectado.
- El estándar WEP recomienda (pero no requiere) que IV cambie en cada paquete, pero no dice nada acerca de los mecanismos aconsejables para seleccionar IVs y, por esta razón, algunas implementaciones del sistema lo hacen precariamente. Hay un gran número de las tarjetas que reestablecen IV a 0 cada vez que son reiniciadas, e incrementan IV en uno en cada paquete posterior.
- Los keystream correspondientes a IVs de valor bajo son susceptibles de ser reutilizados muchas veces durante el tiempo de vida de la clave privada. Peor aún, como IV tiene tan sólo 24 bits, está prácticamente garantizando que se usará un mismo IV en múltiples mensajes.
- Un cálculo rápido de un punto de acceso ocupado que transmita paquetes de 1500 bytes a una media de 5Mbps de ancho de banda (la velocidad máxima correspondería a 11Mbs) agotará todos los valores posibles de IV en menos de doce horas. Teniendo en cuenta que en la actualidad hay redes a mayora velocidad los IV se reutilizarán en menos tiempo, también influye el número de usuarios que tiene la red, cuantos más usuarios más paquetes de gestión de protocolo IP se envían. Esto hace que tengamos mayor número de paquetes con texto plano.

Seguridad 802.11

- Una implementación que utilizase un IV aleatorio para cada paquete hará que se repita un IV cada 5000 paquetes aproximadamente, que se resumen en tan sólo varios minutos de transmisión.
- Pero lo peor de todo es que el estándar 802.11 no exige que IV cambie en cada paquete, lo que podría permitir el uso de un IV idéntico en todos los paquetes sin que ello suponga una disconformidad con la norma estándar.

- ***LINEALIDAD DEL CRC.***

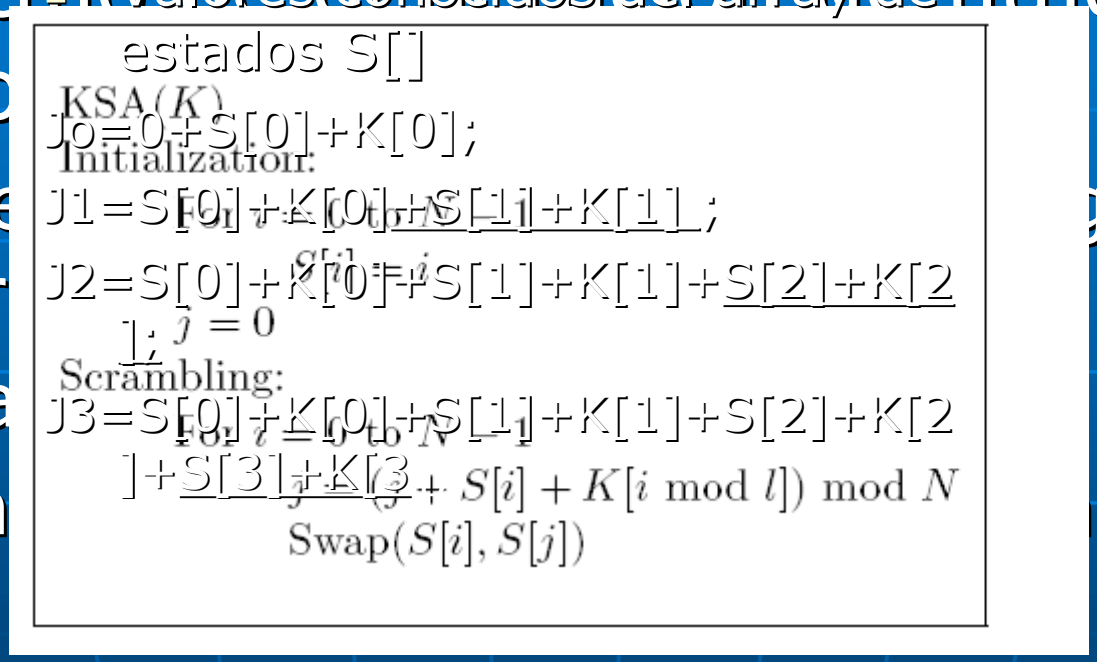
  - No existe una comprobación de integridad apropiada, se utiliza CRC-32 para la detección de errores y no es criptográficamen-te seguro por su linealidad, esto nos permite descifrar partes del keystream, como conocemos los tamaños de los campos que son cifrados, el CRC es un punto débil. Ello es debido a que CRC-32 es un mecanismo de control del mensaje y en su momento no se pensó como elemento para garantizar su seguridad.

Algoritmo de cifrado WEP

- Basado en el algoritmo de cifrado RC4.
- Ideado por Ron Rivest de la RSA Security (Rivest,Shammir,Adleman) en 1987.
- Dominio público desde 1994 (Cypherpunks)

Algoritmo Cifrado WEP

- Algoritmo de generación de flujo de cifrado
  - Valores conocidos del array de estados S[]
  - Prime… algor…
  - Tabla…
  - Perm… de la …ción
  - Obtención array de estados S[]

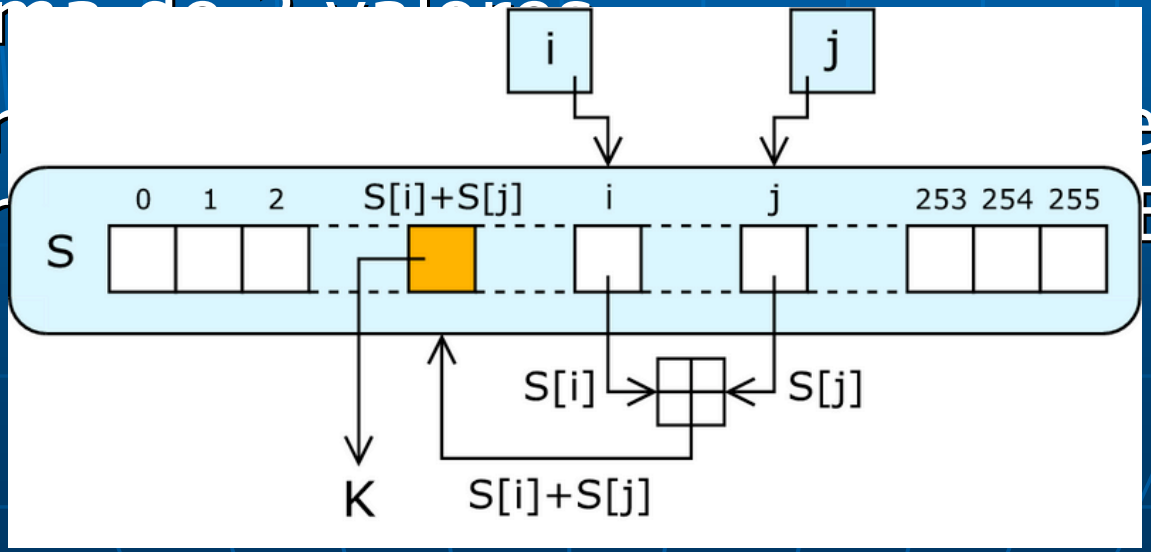


Algoritmo de cifrado WEP

- Algoritmo

  PRGA(K)
  Initialization:
  $i = 0$
  $j = 0$
  Generation loop:
  $i = i + 1$
  $j = j + S[i]$
  Swap$(S[i], S[j])$
  Output $z = S[S[i] + S[j]]$

  - Pseudo- algorithm.
  - Se gene y de estados S[].
  - Sum
  - El r eta ger EAM.



Ataques Estadísticos al cifrado WEP

- ATAQUE FMS (Fluhrer, Martins, Shamir)
  - Deriva la clave secreta K[]
  - Busca IV's "débiles" [X+3,255,Y]
  - Ataca a la primera palabra del mensaje cifrado.
  - Requiere analizar 1-4 millones de IV's
  - Probabilidad éxito= e^-x

Ataques Estadísticos al cifrado WEP

- ATAQUE FMS
  - Ejemplo: IV=3,255,Y

3	0	5+Y	6+Y+K[3]

PRGA(K)
Initialization:
$i = 0$
$j = 0$
Generation loop:
$i = i + 1$
$j = j + S[i]$
Swap$(S[i], S[j])$
Output $z = S[S[i] + S[j]]$

  - Output=S[S[i]+S[j]]=S[3]=6+Y+K[3]

Ataques Estadísticos al cifrado WEP

- Ataque FMS
  - Problemas:
    - Siempre hay que conocer el texto claro de la primera palabra del mensaje cifrado.
    - Hay pocos IV's débiles. Solo define 256 IV's débiles por cada posición de la clave secreta.
    - Habrá muchos Secret Keys incorrectos.

Ataques Estadísticos al cifrado WEP

- ATAQUE FMS avanzado
  - Publicado 22-02-2002 por H1kari.
  - No reconocido oficialmente.
  - Mejoras:
    - Ataque a la segunda palabra del mensaje cifrado.
    - Casos especiales: Probabilidad éxito = 13%
    - Nuevos IV's débiles
    - Número de paquetes necesarios reducidos a la mitad.

Ataques Estadísticos al cifrado WEP

- ATAQUE FMS avanzado
  - Ejemplo IV= 4, 252, 252
    - 4 1 255 3+255+K[3]

1 Iteración,
i=1; j=S[1];
swap (S[1], S[S[1]]);
o1=S[S[1]+S[S[1]]];
2 Iteración,
i=2; j= S[1]+S[2];
swap (S[2], S[S[1]+S[2]]);
o2= S[S[2]+S[S[1]+S[2]]];

Ataques Estadísticos al cifrado WEP

- ATAQUE FMS avanzado
  - Ejemplo: caso especial P.éxito=13%
    - _ 3 _ 0
    - Output=S[S[i]+S[j]]
    - S[1] , S[S[1]], S[S[1]+S[S[1]]]

Ataques Estadísticos al cifrado WEP

- Ataque FMS y FMS avanzado
  - Problemática
    - Captura de muchos paquetes.
    - No aplicable a todos los generadores de IV's.
    - Actualmente los IV's débiles de FMS son bloqueados por los fabricantes.
    - Dejan lugar a más IV's débiles posibles.

      $0 <= S[1] <= B+3 \; ; \; S[1]+S[S[1]] = B+3$

Ataques Estadísticos al cifrado WEP

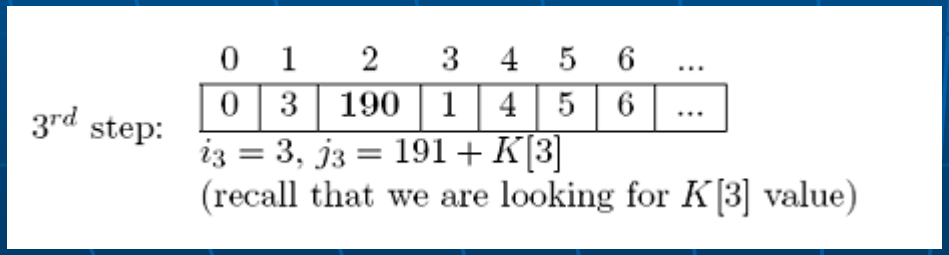
- ATAQUES KOREK
  - Publicado 8-08-2004
  - Compuesto por 17 ataques divididos en 3 grupos.
  - No define IV's de manera estática.
  - Realiza el ataque FMS a la inversa.
  - Implementado actualmente por Aircrack.

Ataques Estadísticos al cifrado WEP

- ATAQUES KOREK
  - Ejemplo: 3º Ataque KoreK A u13 1
  - Ataque a la primera palabra texto cifrado.
  - Péxito=13%
  - Condiciones para aplicarlo
    - S[1]=P siendo P la posición de la clave que estemos buscando.
    - Output1= ((1-P) mod 256);

Ataques Estadísticos al cifrado WEP

- ATAQUES KOREK
  - Ejemplo: IV= 0, 2, 185
  - 0 X 190 3
  - O1= S[X+3]=….254
  - K[3]=254-1-190=63
  - K[p]=(1-p) mod 256 – S[3] – Jp-1



Ataques Estadísticos al cifrado WEP

- ATAQUES KOREK
  - Reducción de número de paquetes a capturar.
  - Difícil de bloquear por software
  - Aplicable a todos los generadores de IV’s

Ataques Inductivos al cifrado WEP

- No tratan de derivar la clave secreta.
- Explotan otras debilidades de WEP
  - Reutilización de IV
  - MIC independiente de la clave
  - Características lineales del CRC

Ataques Inductivos al cifrado WEP

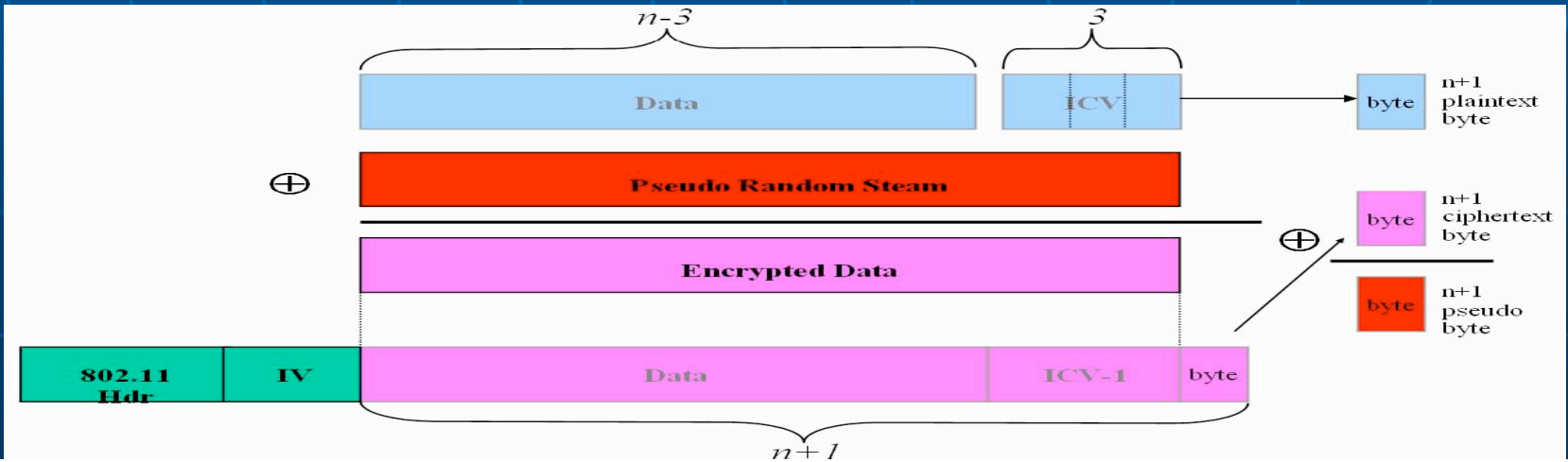
Ataque Arbaugh

- Publicado por William Arbaugh mayo 2001.
- Es un ataque con texto claro conocido.
- Explota la debilidad de que WEP tiene un mecanismo de control de mensajes independientes de la clave.
- mvalido=(musuario,crc(musuario))+K

Ataques Inductivos al cifrado WEP

Ataque Arbaugh

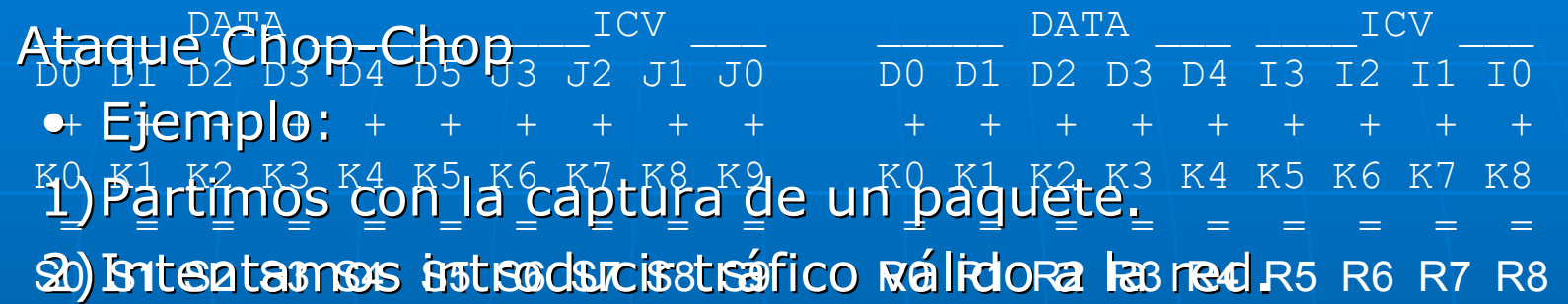
- Partimos de una frase secreta capturada de tamaño n.
- Construir tramas válidas de tamaño n-3
  - Averiguar por prueba y error el ultimo byte de la trama. (256 posibilidades)
  - Cuando demos con el valor correcto, el AP aceptará nuestra trama y ésta será reenviada.
  - Al disponer del texto claro y el texto cifrado del último byte obtenemos también un byte más del keystream.
  - El proceso se repite hasta conseguir un keystream de tamaño 1500 bytes.
  - Obtener los restantes Ivs hasta obtener todos los keystreams.



Ataques Inductivos al cifrado WEP

- Ataque KOREK chop-chop
  - Publicado el 14-9-2004
  - Permite descifrar cualquier trama
  - No evitable incluso con Dinamic Keyring
  - Explota la debilidad de la linealidad CRC

Ataques Inductivos al cifrado WEP



- Ataque Chop-Chop
  - Ejemplo:

1) Partimos con la captura de un paquete.
2) Intentamos introducir tráfico válido a la red.
3) Para hacerlos nos basamos en las siguientes fórmulas:

$R5=S5+X;$

$CRC(m \oplus k) = CRC(m) \oplus CRC(k);$

$ICV'=CRC(m')=CRC(m) \oplus CRC(X)=ICV \oplus CRC(\Delta);$

$k \oplus m' = k \oplus (m \oplus \Delta) = (k \oplus m) \oplus \Delta$

$k \oplus ICV' = k \oplus (ICV \oplus CRC(\Delta)\ ) = (k \oplus ICV) \oplus CRC(\Delta)$

Ataques Inductivos al cifrado WEP

- Otros ataques menos utilizados
  - Ataque fuerza bruta.
  - Ataque diccionario.
  - Ataque por fragmentación.

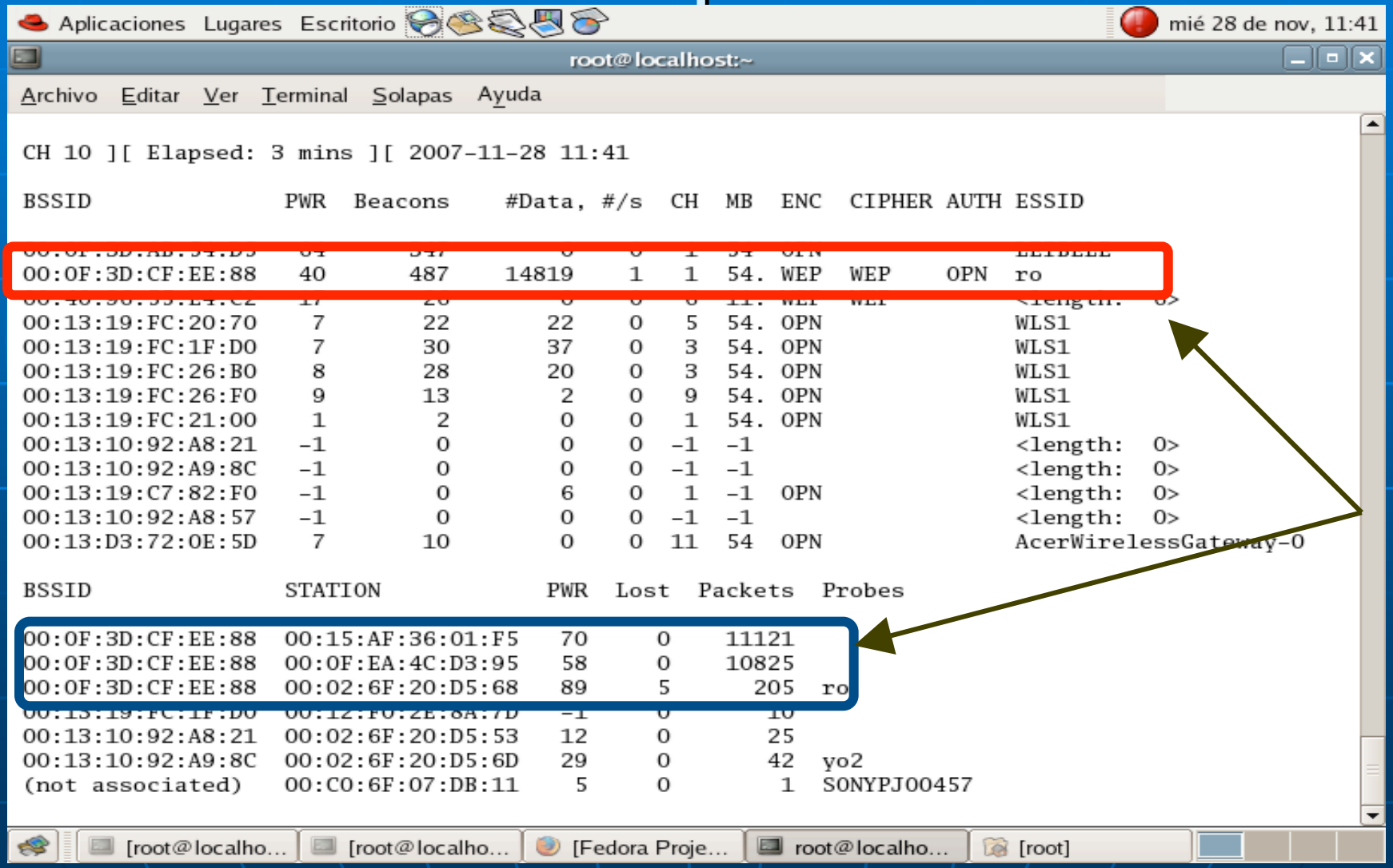
Realización práctica de los ataques

- Maqueta en el laboratorio de telemática:
  - punto de acceso D-Link DWL-2100AP
  - ordenador con Linux Red-hat y dos tarjetas de red con capacidad de trabajar en modo monitor (promiscuo)
  - 3 ordenadores portátiles.
- Lo primero que hicimos fue instalar todas las herramientas.
  - Aircrack, Airodump, Aireplay y Airdecap.
- Configuramos la red, el nombre es “ro”, activamos el DHCP para los ordenadores portátiles y le pusimos diferentes claves WEP.
- Forzamos el tráfico para no perder mucho tiempo en capturar los paquetes necesarios, con las diversas contraseñas. instalamos un servidor FTP en uno de los ordenadores portátiles generando una cantidad suficiente de paquetes cifrados.

Realización práctica de los ataques

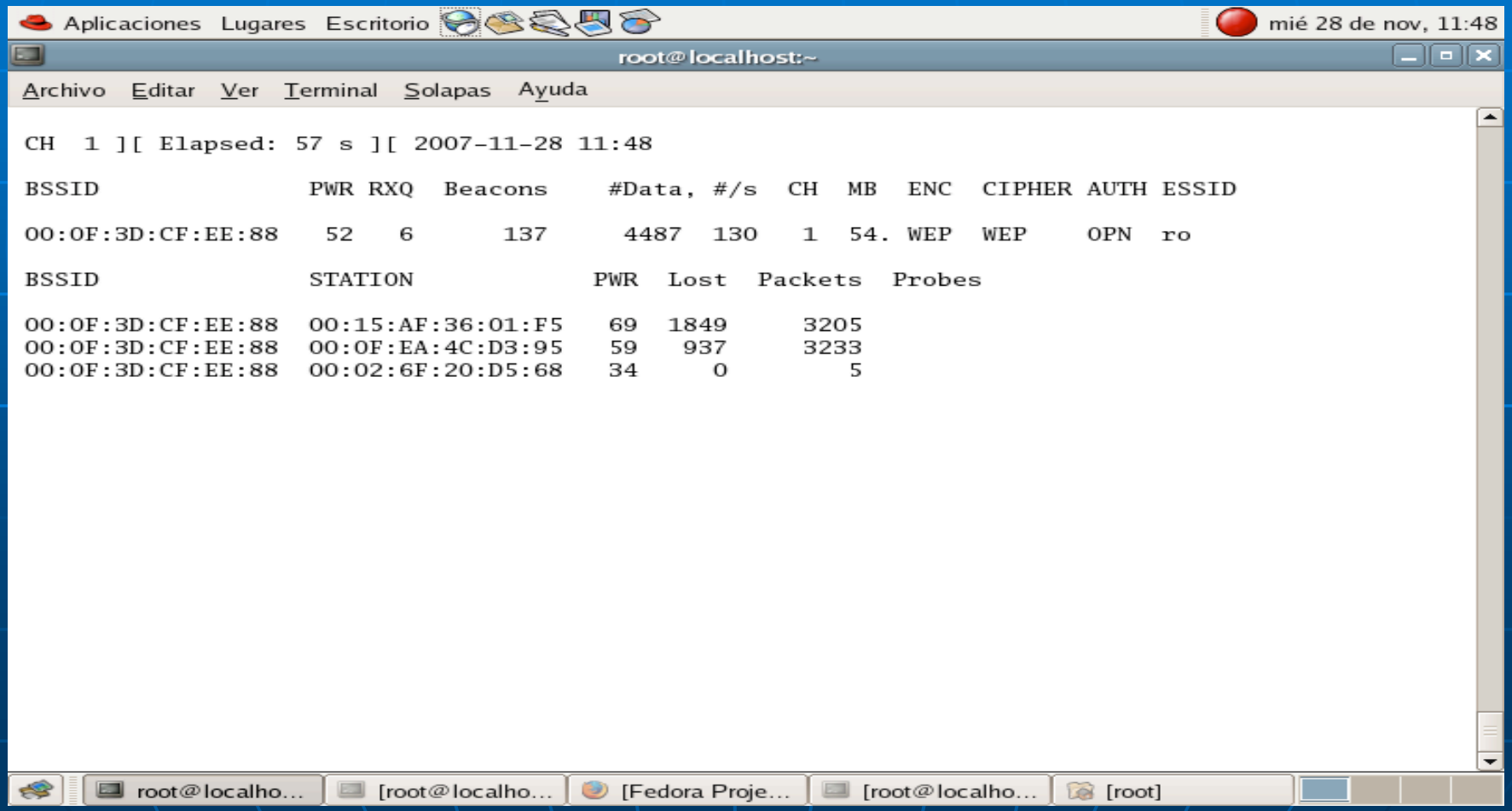
- Capturar, y las tarjetas del PC las ponemos en modo monitor (promiscuo):
  - iwconfig ath0 mode monitor
  - iwconfig ath1 mode monitor
- Así tenemos preparada la maqueta, el PC para capturar tráfico, los ordenadores portátiles para generarlos y el AP como enlace de los portátiles. Como explicamos en el protocolo todas las tramas pasarán a través del AP.

Realización práctica de los ataques

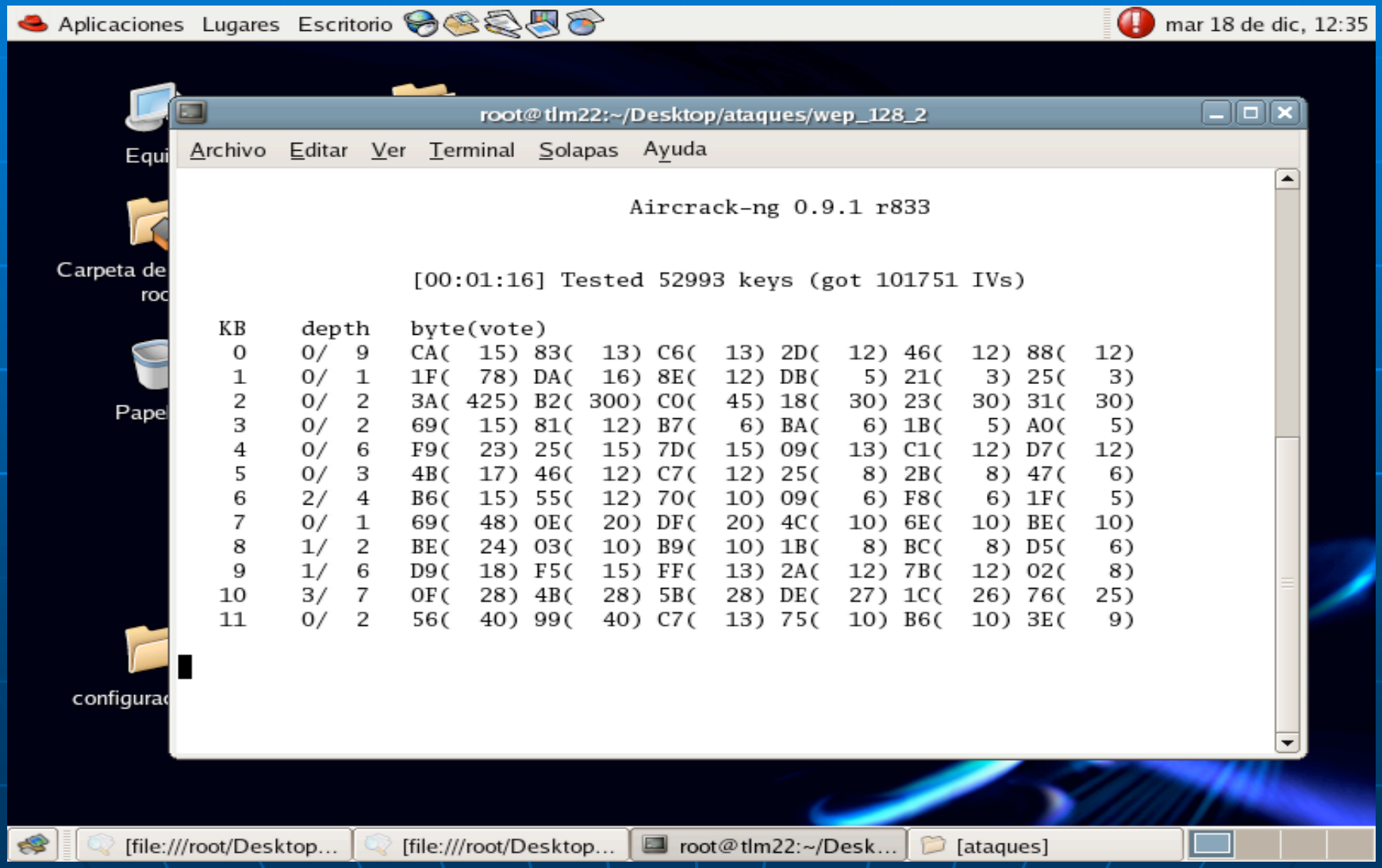


Realización práctica de los ataques

Airodump-ng --ivs –c 1 –BSSID 00:0F:3D:CF:EE:88 –w captura ath1



Realización práctica de los ataques



Realización práctica de los ataques

- Cada byte de la clave es tratado de forma individual.
- Con cada captura crece un 15% la probabilidad de encontrar un byte determinado si para ese IV es correcto.
- Se van acumulando posibilidades o votos (votes) para cada byte de la clave WEP. Cada ataque tiene un número diferente de votos asociado con él, la probabilidad de cada ataque varía matemáticamente.
- Cuantos más votos tengamos de un byte o valor particular, mayor probabilidad hay de que sea el correcto. La clave que tenga el mayor número de votos es la que más probabilidades tiene de ser la correcta, pero no está garantizado. Aircrack probará continuamente de la más probable a la menos probable para encontrar la clave.

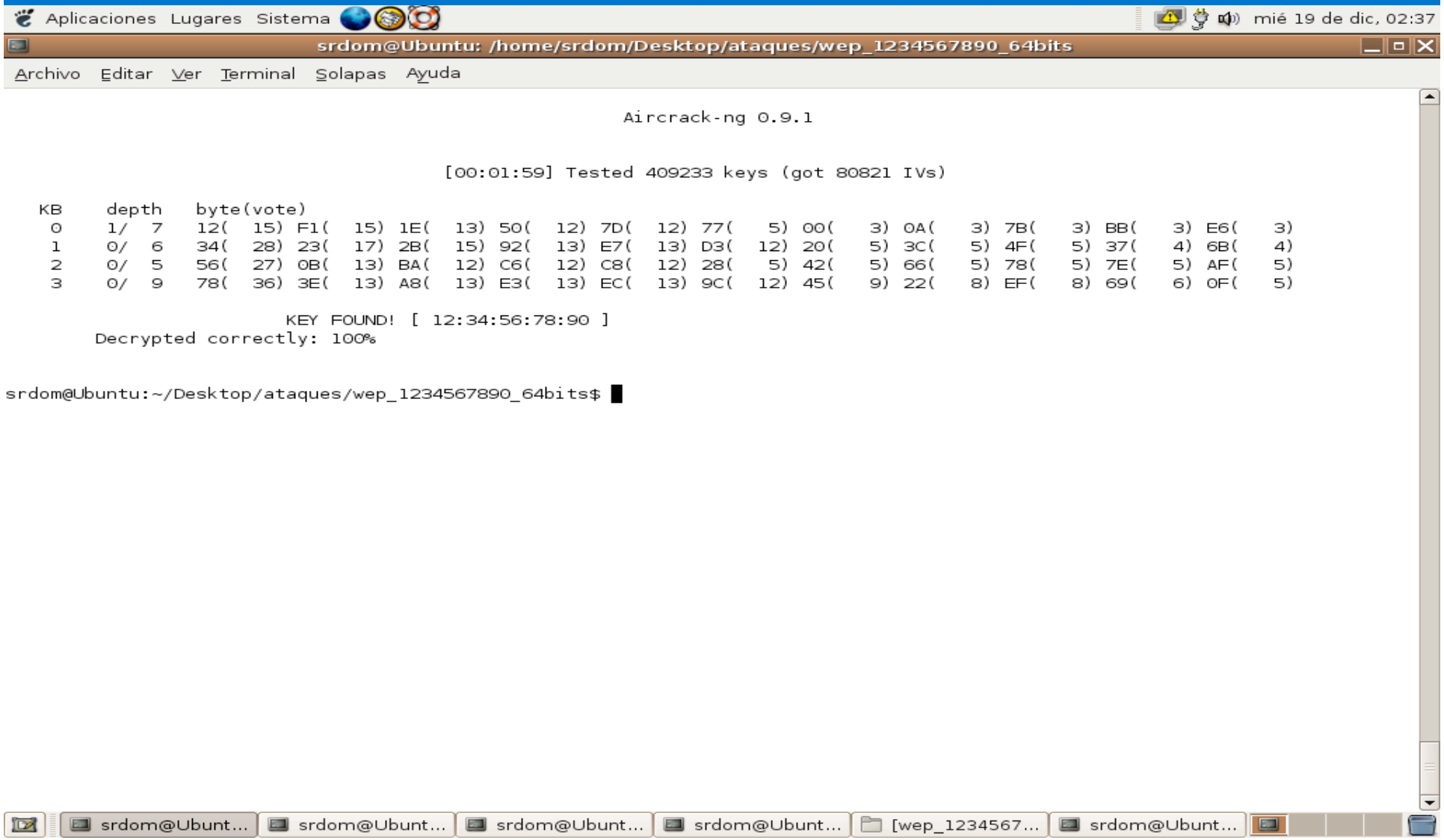
Realización práctica de los ataques

- a: Fuerza el tipo de ataque (1=WEP estática, 2=WPA/WPA2-PSK).
- e: Si se especifica, se usarán todos los IVs de las redes con el mismo ESSID.
- n: Especifica la longitud de la clave, 64 bits para WEP de 40 y 128 bits para WEP de 104, la opción por defecto es 128.
- f: Fudge factor o Factor de elusión Por defecto, esta opción está fijada en 2 para WEP de 104-bit y en 5 para WEP de 40-bit. Especifica un valor más alto para elevar el nivel de fuerza bruta: la obtención de la clave llevará más tiempo, pero la probabilidad de éxito será mayor.
- k: Hay 17 ataques korek de tipo estadístico. Algunas veces un ataque crea un falso positivo que evita que encontremos la clave, incluso con grandes cantidades de IVs. Prueba -k 1, -k 2, … -k 17 para ir desactivando cada uno de los ataques.

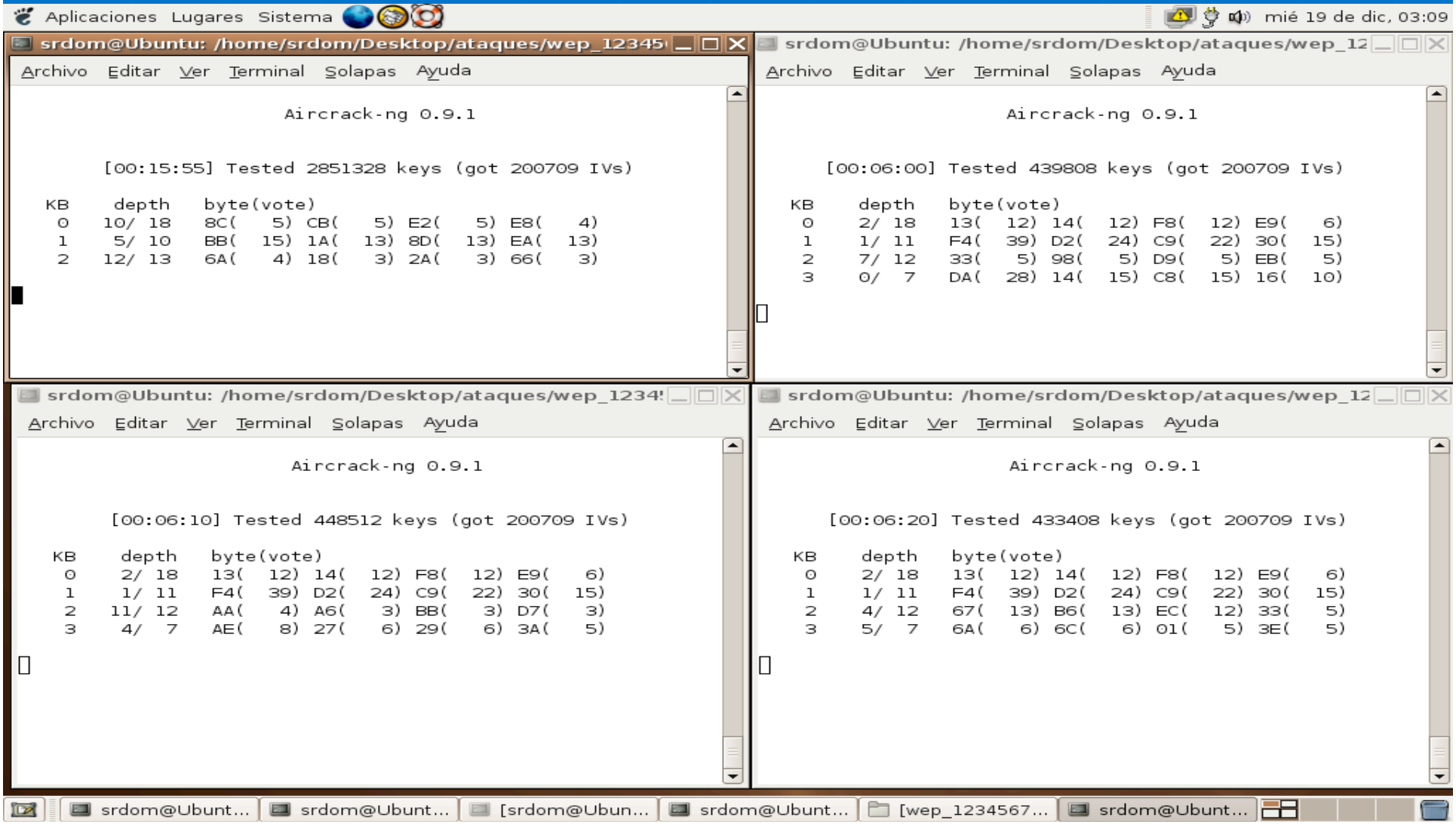
Realización práctica de los ataques

- 64bits
  - *1234567890*
  - *92a2e8df30*
- 128bits
  - *df65889baaa1b2c3d4e5f601a2*
  - *67823adf83ae3c8098ffcade32*
- Captura de tráfico para cada clave
  - Hemos capturado archivos de diferentes tamaños, y no se repiten los Ivs en los archivos.
  - Para cada clave hemos capturado diferentes cantidades.

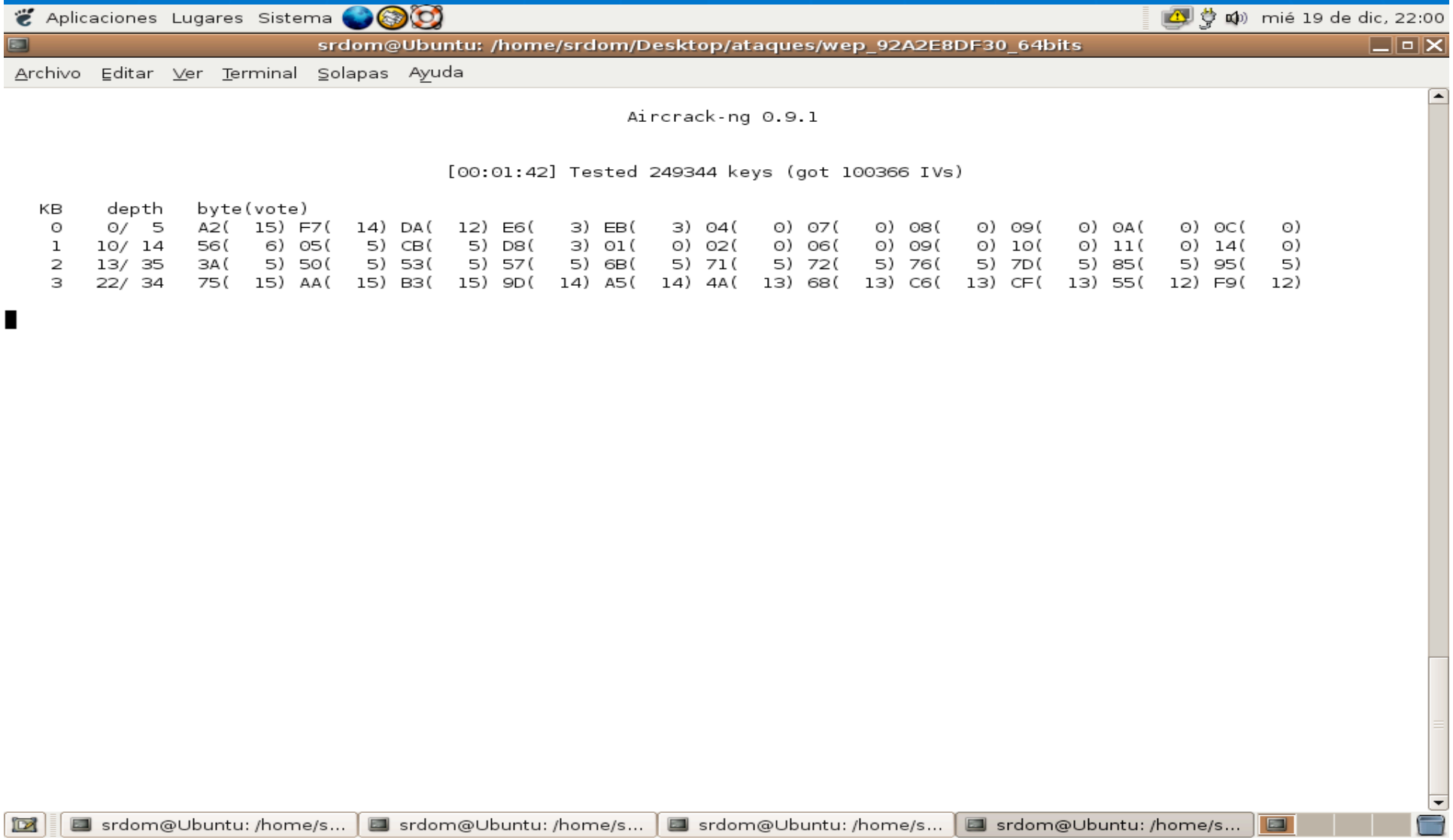
Realización práctica de los ataques



Realización práctica de los ataques



Realización práctica de los ataques



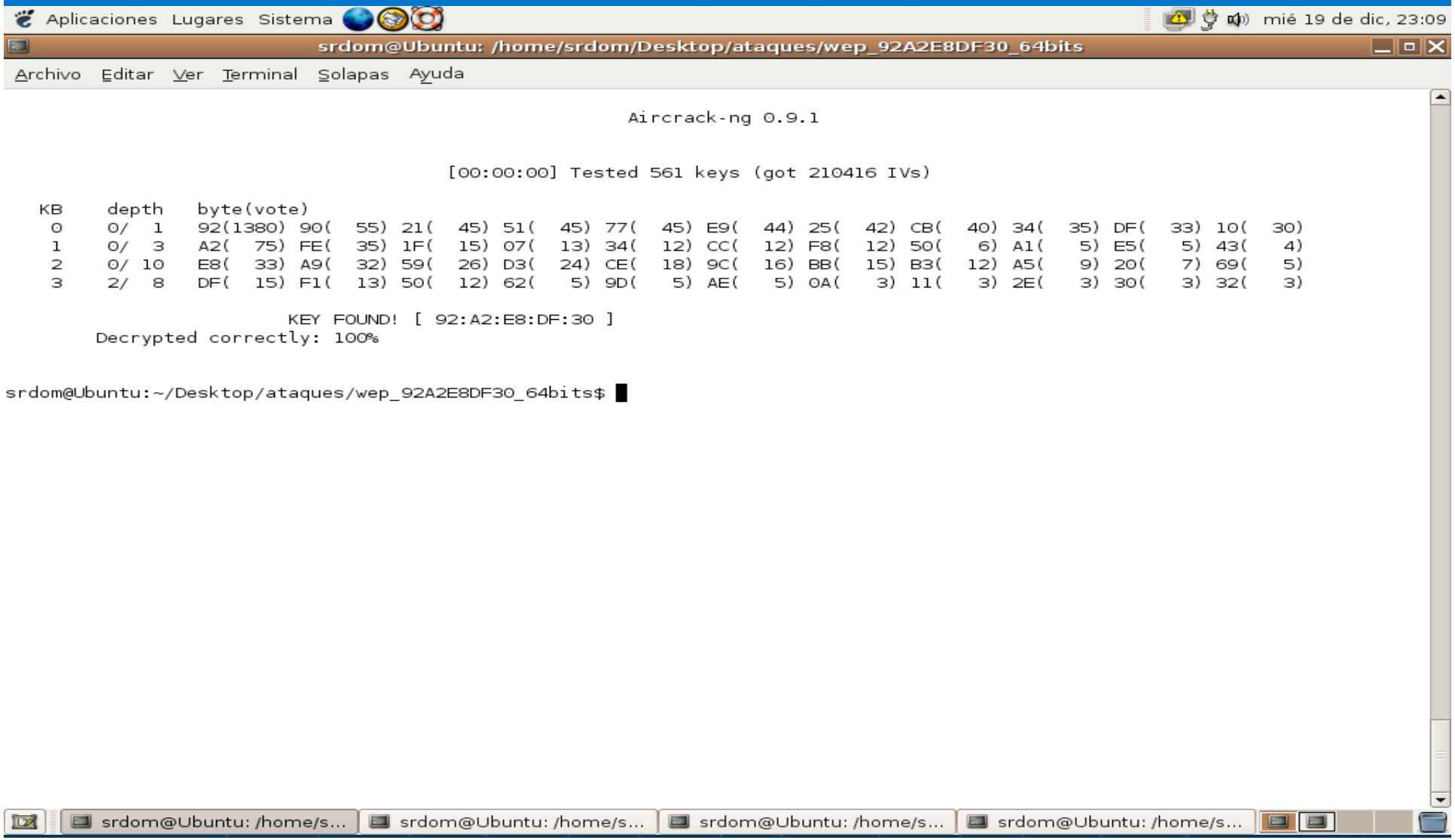
Realización práctica de los ataques

- No parece ser un falso positivo.
- Por si acaso probamos 17 veces eliminando cada vez un ataque Korek distinto.
- Después de los 17 intentos fallidos, probamos variando el factor de elusión (-f), pero no lo encontramos.
- 60000-01.ivs si, 100000-01.ivs no, 150000-01.ivs si, 200000-01.ivs no y 200000-02.ivs si.

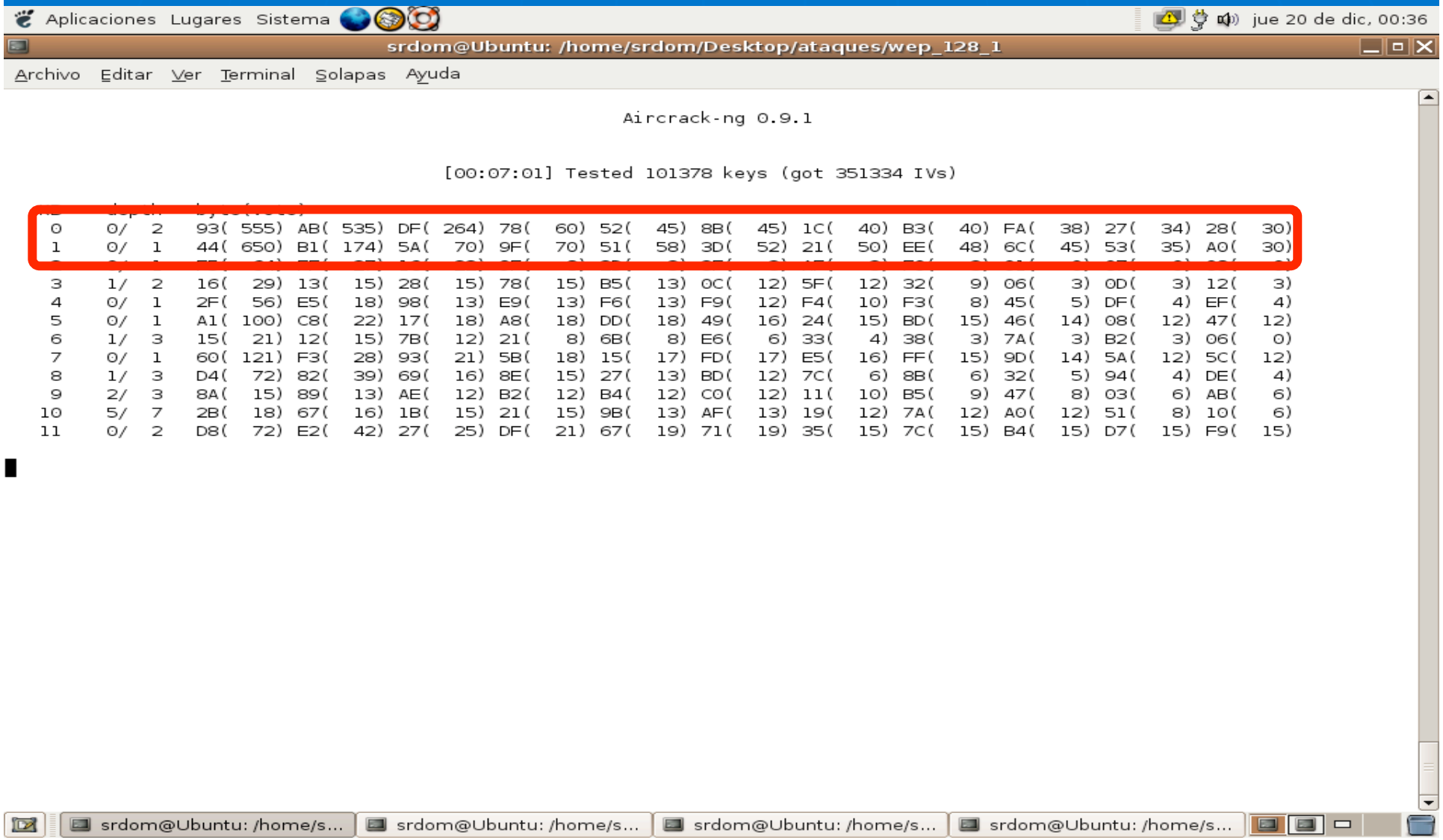
Realización práctica de los ataques

- Creemos que el número correcto de IVs a partir del cual Aircrack descifra la clave para este caso particular es 200000 Ivs
- Los casos anómalos no son 100000_01.ivs y 200000_01.ivs sino 60000_01.ivs y 150000_01.ivs que tendrán alguna weak key facilitando la labor de encontrar la clave con una menor cantidad de IVs.
- No es seguro y no lo podemos corroborar, son suposiciones que hacemos después de ver el comportamiento del programa, y repetirlo una y otra vez para ver si siguen o no el mismo patrón cada vez que lo ejecutamos.

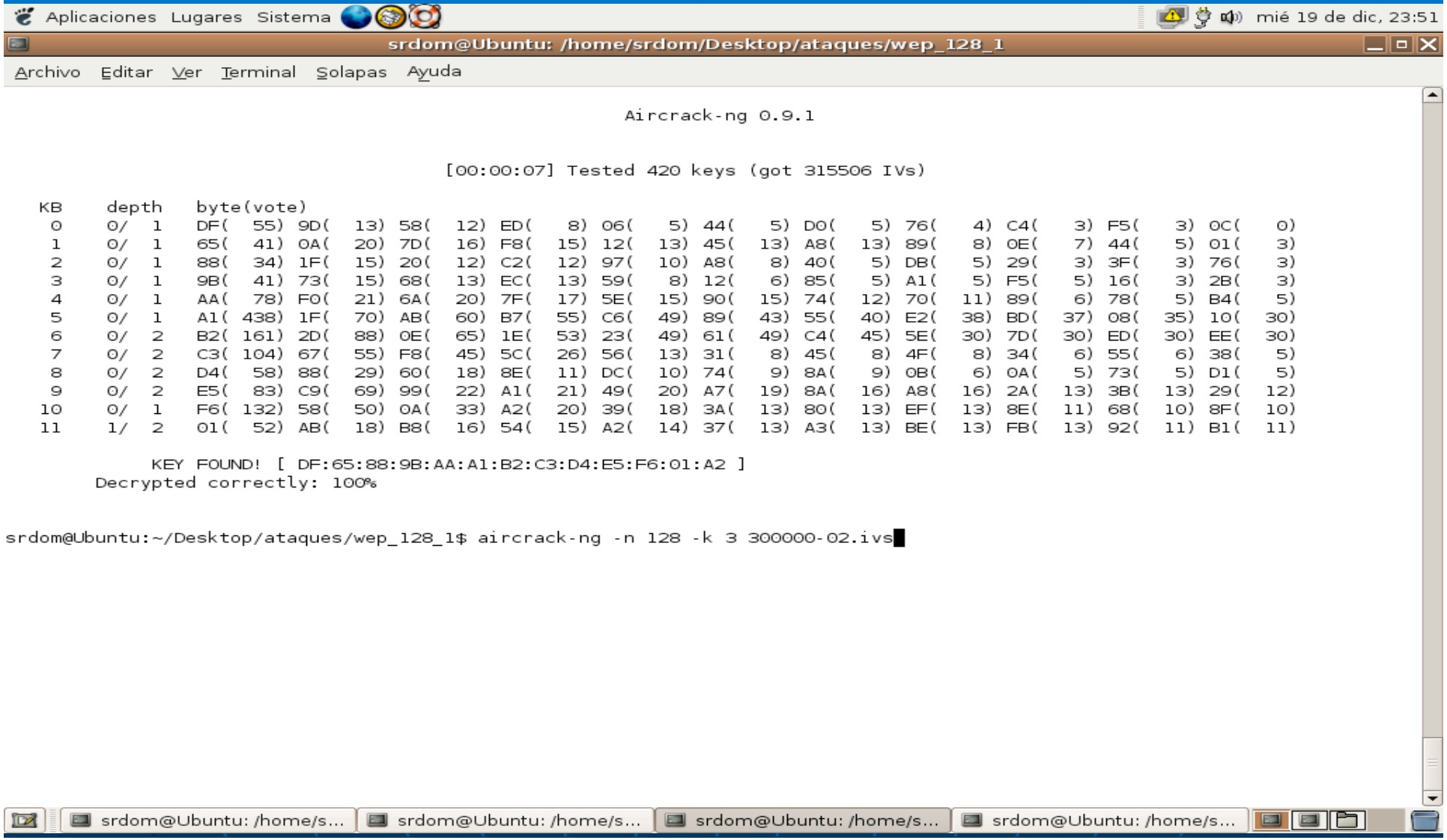
Realización práctica de los ataques



Realización práctica de los ataques



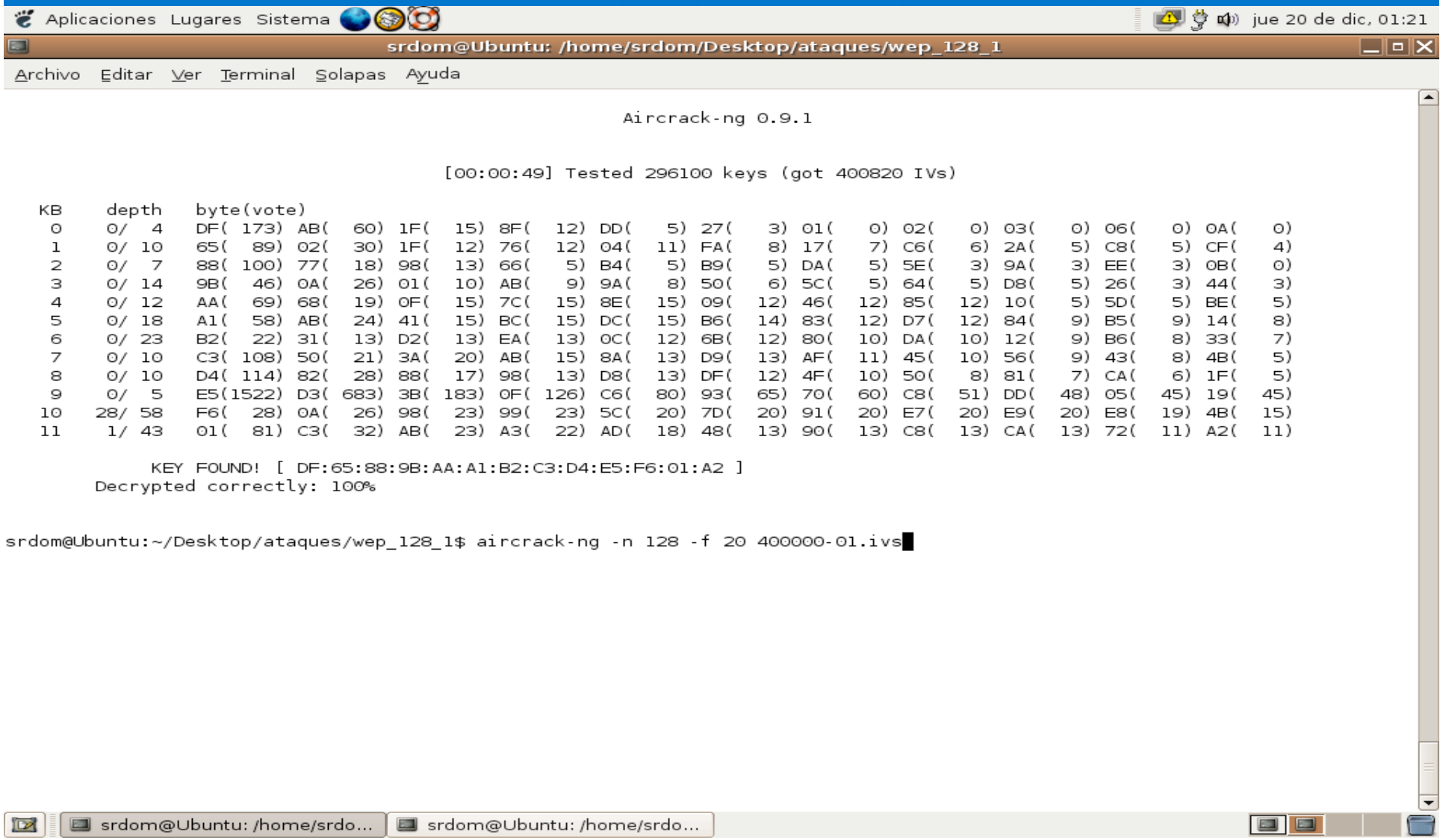
Realización práctica de los ataques



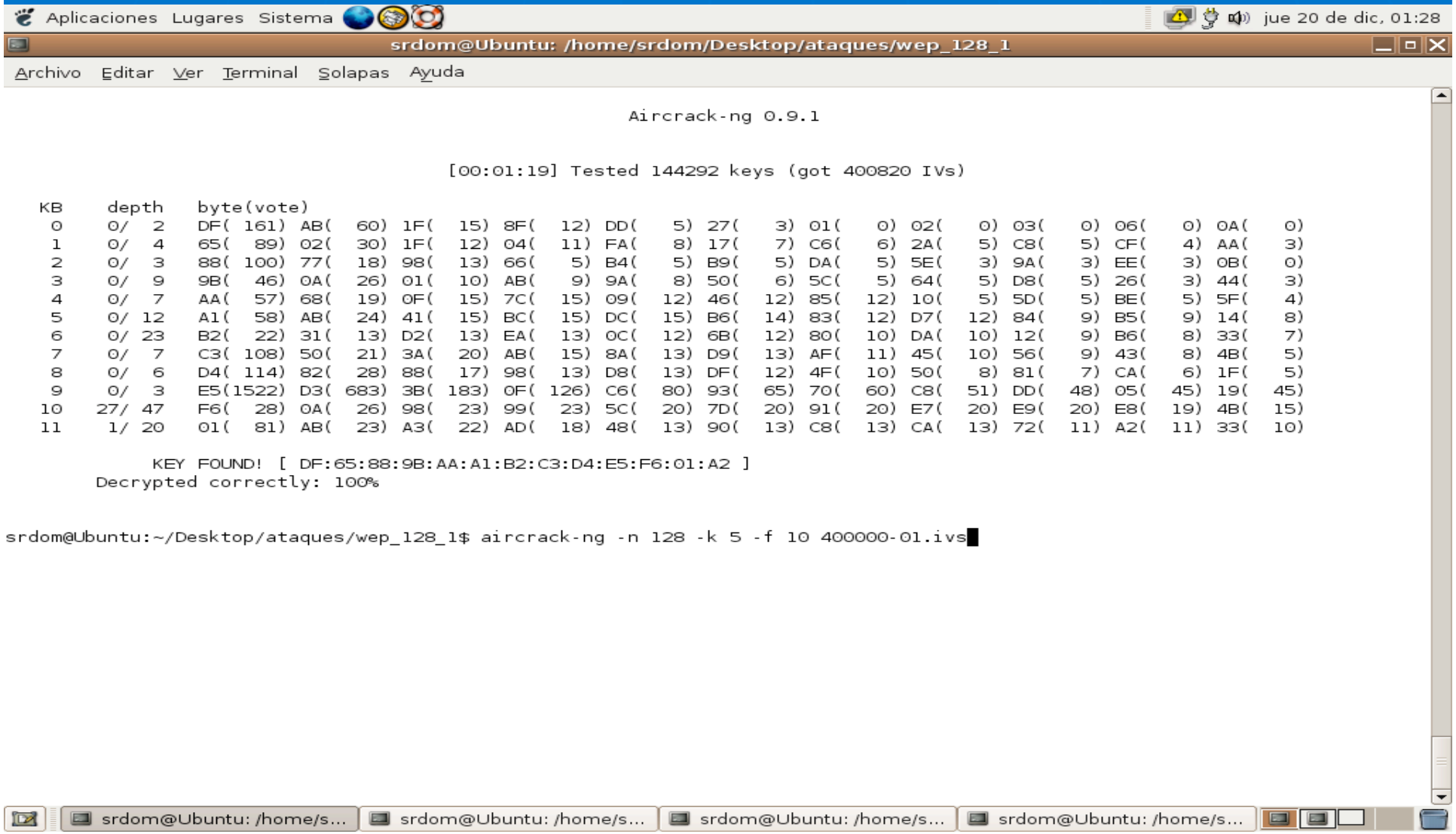
Realización práctica de los ataques

- ***Falsos positivos:***
  - Cuando un ataque Korek da una probabilidad muy alta a ciertos valores (incorrectos) haciendo que Aircrack los priorice sobre los valores reales dándonos error en la obtención de la clave.
  - No se sabe cual es la causa exacta de los falsos positivos ni que ataque lo puede producir en cada momento, pero tenemos que saber que la estadística no es una ciencia exacta y que puede suceder.
  - Creemos que una forma de detectar los falsos positivos es controlando los votos de los valores, si vemos que se desmadran podemos empezar a intuirlo.

Realización práctica de los ataques



Realización práctica de los ataques



Realización práctica de los ataques

- ***67823adf83ae3c8098ffcade32***

  - Por último hemos seguido los mismos pasos que con las otras tres contraseñas, y no nos ha sucedido nada que reseñar, encontramos la contraseña con los archivos que tenían 300000 IVs o más, de forma rápida, sin falsos positivos y sin ni aumentar del factor de elusión.

  - Trabajamos de forma más exhaustiva con el archivo de 250000 IVs para ver si podíamos encontrar la clave, probamos eliminando los ataques Korek y parecía que eliminando el primero podría encontrarlo pero no fue así, no lo encontró en ningún caso ni subiendo el factor de elusión.

Conclusiones

- No podemos decir que hay ninguna técnica exacta que nos encuentre la contraseña, es diferente para cada clave, hay que fijarse mucho en los datos que nos ofrece el programa durante la ejecución para detectar los casos anómalos.
- Una recomendación es capturar muchos IVs, esto siempre nos proporcionará una mayor probabilidad de encontrar la clave. Una buena recomendación es entorno a los 300000 IVs.
- Cada caso es diferente, puede que una clave de 128 bits la obtengas de 5000 IVs y una de 64 bits la obtengas de 600000 IVs el número que damos es una recomendación, habrá casos que se consigan con esa cantidad de IVs y casos que no.

Conclusiones

- Respecto a la seguridad queda claramente demostrado que la encriptación WEP no es fiable, y que ha sido superada con creces, recomiendo a todo el mundo encarnecidamente que migre a otros sistemas de encriptación más fiables.
- La vulnerabilidad de la encriptación WEP es muy grande.

Conclusiones

FIN