Seguridad en *wireless*

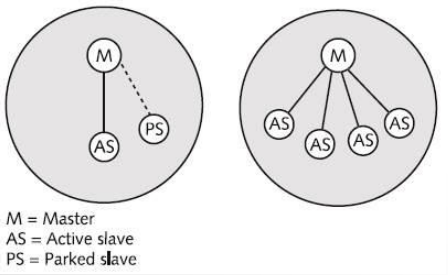
Ataque Wireless

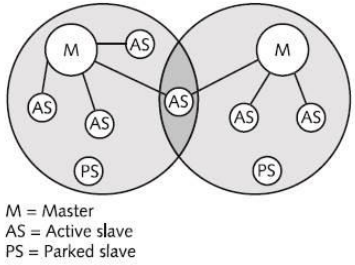
Introducción: Car Hacking

- Car Hacking
  - Irrumpir en el sistema electrónico del coche
- Se puede
  - Cambiar ajustes y settings
  - Desactivar sistemas de seguridad
  - Borrar información
  - Acceso remoto (wireless)
- Vías de ataque
  - Red bluetooth
  - 3G a bordo
  - Troyano en mp3
    - Apagar motor
    - Bloquear puertas
    - Desactivar frenos
    - Cambiar el velocímetro
- Escenario
  - Hacer que el coche transmita marca/modelo y posición GPS
  - Ladrones comprueban qué coches están en su área
  - Pagan y el hacker abre las puertas y desactiva el sistema de seguridad del coche
- Detalles
  - No es necesario estar conectado, ubicuidad
  - En el siglo XX comunicación de voz, en el siglo XXI comunicación de datos
  - Permite mejorar la productividad y la economía
  - Tienen vulnerabilidades y son el objetivo de ataques
  - La seguridad ha mejorado de forma significativa

Bluetooth

- Es una tecnología PAN (Ericsson 1994)
  - 10 metros, 1Mbps
- Dispositivos
  - Manos libres, auriculares, cámaras, ratón y teclado, mando para juegos, monitor de pulsaciones, sensor de presión sanguínea, etc.
- 2 topologías: Piconet y Scatternet





- Bluejacking
  - Envío de mensajes no solicitados a dispositivos activos
  - Consiste en texto, imágenes o sonido
  - Es más molesto que dañino (spam)
  - Ha sido utilizado por anunciantes
- Bluesnarfing
  - Acceder información no autorizada a través de conexiones bluetooth
  - El atacante puede copiar e-mails, calendario, contactos, fotografías, vídeos…
  - Se ha usado contra celebridades
  - El bluetooth debe estar desactivado cuando no se utilice

Ataque WiFi

- Estándares
  - 1990 IEEE 802.11 (2Mbps)
  - 1999 IEEE 802.11b (11Mbps)
  - 2003 IEEE 802.11g (54Mbps)
  - 2009 IEEE 802.11n (600Mbps)
  - 2013 IEEE 802.11ac (1000Mbps)
- Dispositivos
  - Adaptador Wireless
  - Punto de acceso
    - PA autónomos
    - Routers wireless

- Las transmisiones wireless no están sujetas a los mismos límites que las cableadas
- Un atacante puede interceptar, fácilmente, transmisiones no cifradas recuperando contraseñas, información privada e incluso modificar el mensaje.
- También se puede producir un ataque de interferencia remoto mediante un inhibidor de frecuencias (DoS)

Descubrimiento

- Beaconing
  - Transmisión cada 100µS para anunciar la presencia de una red WiFi
  - Los atacantes usan esta información para encontrar y catalogar redes WiFi
- War Driving
  - Consiste en buscar redes en coche o a pie usando un dispositivo móvil
- Herramientas
  - Dispositivo móvil
  - Adaptador externo
  - Antenas
  - Software específico
  - Receptor GPS

Ataques mediante espectro RF

- Análisis de protocolo
  - Se puede analizar el tráfico capturado de igual forma que se hace en conexiones cableadas
  - El interfaz puede estar en
    - master (punto de acceso)
    - managed (normal)
    - repeater
    - mesh
    - ad-hoc (punto a punto)
    - ***monitor***
  - Es necesario el modo monitor para que pueda capturar paquetes sin estar asociado a un punto de acceso
- Interferencia
  - Como dispositivos operan en RF, existe la posibilidad de interferencias
    - Por parte del propio dispositivo
    - Señales de otros dispositivos
  - Dispositivos que pueden provocar interferencias
    - Microondas, ascensores, fotocopiadoras, teléfonos inalámbricos, bluetooth, etc.
  - Un atacante puede provocar interferencias para evitar que un dispositivo se comunique con el punto de acceso

Ataques con Puntos de Acceso

- Punto de acceso no autorizado
  - Instalación no autorizada de un punto de acceso por un empleado
  - Generalmente mal configurado o sin seguridad
  - Permite el acceso a la red interna desde el exterior de las instalaciones sin control del firewall
- Gemelo maligno
  - Punto de acceso instalado por un atacante
  - Emula un punto de acceso legítimo por lo que los dispositivos se conectan al mismo
  - El atacante puede capturar el tráfico que proviene de los usuarios conectados

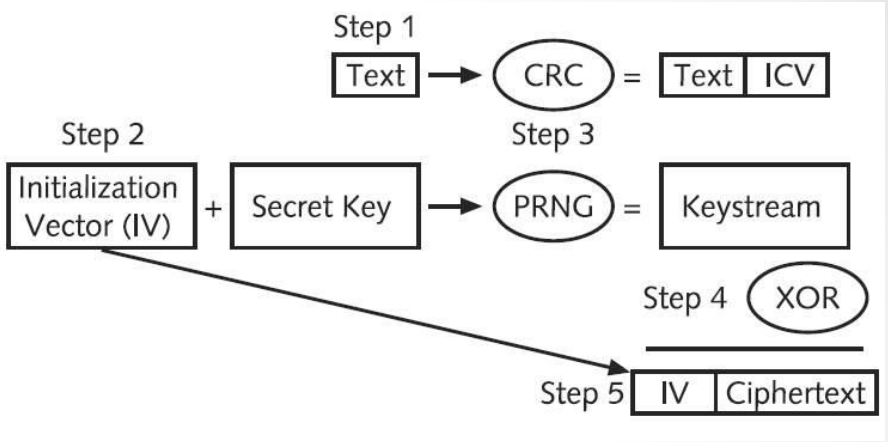
Vulnerabilidades de IEEE 802.11

- Filtrado de MAC
  - Es un esquema de seguridad que limita el acceso a ciertas MAC legítimas
  - Permite bloquear o autorizar direcciones
  - Es susceptible de ataque puesto que se intercambian en abierto
  - Resulta muy difícil gestionar grandes cantidades de usuarios de esta forma
- Retransmisión SSID
  - Autentificación abierta
    - Sólo es necesario el SSID correcto
    - El atacante puede obtener el SSID de diversas formas
  - Ocultar SSID
    - El SSID se transmite también en otros paquetes de gestión
    - Puede evitar el roaming
    - No siempre se puede ocultar
    - En Windows XP siempre se conecta al dispositivo con retransmisión de SSID

WEP

- Proporciona un cierto nivel de confidencialidad
- Se basa en una clave precompartida entre el punto de acceso y los dispositivos
- La clave puede ser de 64 o 128 bits

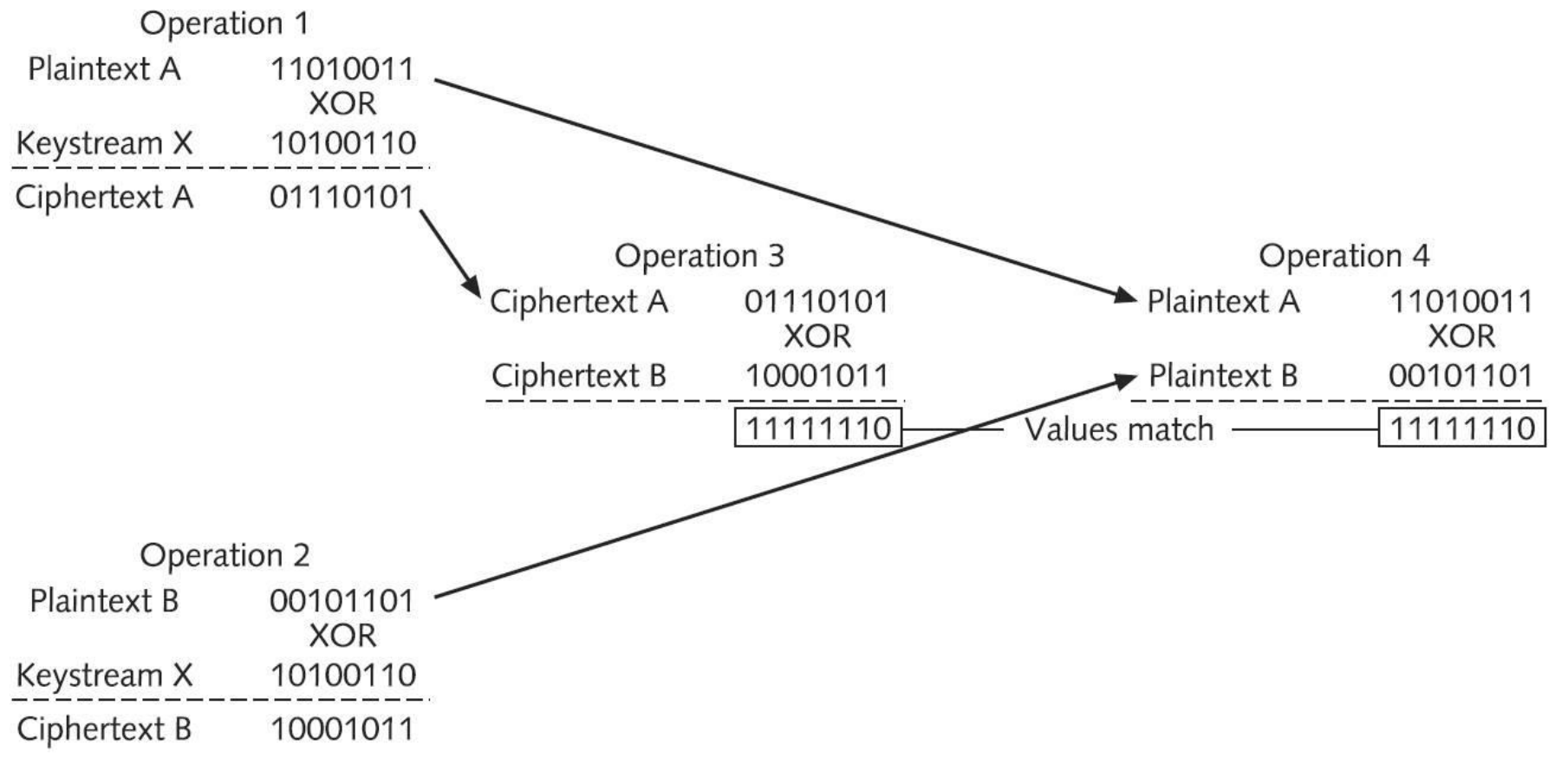
1. Se añade un CRC a los datos a transmitir (ICV)
2. Se combina la clave precompartida con un vector de inicialización (IV) de 24 bit, éste cambia por cada paquete
3. La clave y el IV se utilizan como semilla en PRNG basado en RC4
4. Se cifra utilizando esta secuencia cifrante
5. Se añade el IV al principio del paquete sin cifrar



- Vulnerabilidades
  - IV de 24 bit
  - El sistema de IV presenta un patrón explotable (fallo de diseño)
  - Un punto de acceso a 11Mbps puede recibir y enviar 700 paquetes por segundo. Los IV se empiezan a repetir antes de 7 horas
  - Un atacante puede usar esto para romper WEP
  - Las técnicas recientes permiten romper WEP en minutos

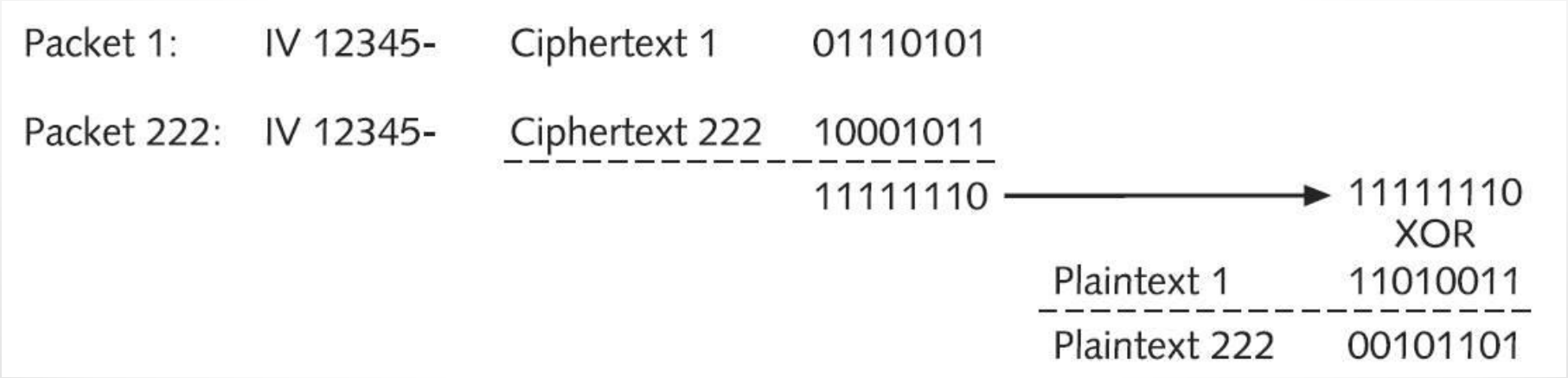
WEP

- Un XOR entre dos textos cifrados equivale a un XOR entre dos textos en claro



WEP

- Si el atacante captura los paquetes 1 y 222 con el mismo IV
- Al atacante le basta con descubrir el texto en claro de uno de los paquetes (o parte) para descubrir el texto en claro de todos los paquetes que usen el mismo IV



WEP

¿Cómo puede el atacante encontrar suficiente texto en claro del paquete 1 para obtener el paquete 222?

- Conoce ciertos campos de los paquetes
  - Valores de la cabecera
  - Otros valores tienen posibilidades limitadas (direcciones IP)
- El cuerpo del paquete suele contener ASCII
  - El atacante obtiene suficientes paquetes con el mismo IV y adivinar partes sustanciales de la secuencia cifrante (descifrado iterativo)
- Un atacante puede capturar un paquete de 28 bytes sabiendo que es una petición ARP
  - Puede inundar la red con la misma petición ARP, lo que produce una cantidad de datos enorme con la que trabajar
- Se puede enviar datos desde fuera de la red (Internet) al dispositivo
  - El atacante conoce el mensaje por lo que recuperar la secuencia cifrante resulta trivial

Soluciones de Seguridad Wireless

WPA (802.11i)

- WPA-TKIP
  - Sustituye WEP por Temporal Key Integrity Protocol
  - Utiliza claves de 128 bits y cambian en cada paquete, evitando las colisiones
  - También se sustituye el CRC por un Message Integrity Check (MIC) ~ Hash
  - Existe una medida opcional de desautorizar a todos los clientes y evitar asociaciones por un minuto si ocurre un error MIC
- WPA-PSK
  - La autentificación WPA se logra usando 802.1x o PreShared Key
  - La clave debe estar precompartida en el punto de acceso y todos los dispositivos
  - Al contrario que en WEP la PSK no se utiliza para el cifrado, se utiliza como punto de inicio para la función generadora de claves de cifrado

WPA· vulnerabilidades

- WPA fue diseñado para evitar las vulnerabilidades de WEP de forma cómoda
- En muchos casos, basta con actualizar el software y firmware de los dispositivos y puntos de acceso para soportar WPA
- No obstante, existen vulnerabilidades en WPA centradas en dos áreas
  - Gestión de claves
  - Contraseñas

WPA: vulnerabilidades

- Gestión incorrecta de claves PSK
  - La distribución de claves PSK se realiza de forma manual y sin seguridad añadida: cualquier usuario que obtenga la clave es considerado auténtico
  - Las buenas políticas de seguridad exigen el cambio de claves de forma frecuente; esto requiere reconfigurar la clave en cada punto de acceso y dispositivo
  - Cuando se autoriza a un invitado el acceso, recibe la PSK y esta debe ser cambiada cuando el invitado departe para garantizar la seguridad de la WLAN
- Las contraseñas PSK
  - Otra área de vulnerabilidad es el uso de contraseñas débiles
  - Una clave PSK es un número de 64bit que se genera, frecuentemente, mediante una contraseña de 8 a 63 caracteres de longitud
  - Las contraseñas menores de 20 caracteres son susceptibles de ataques, al igual que aquellas creadas en base a una palabra de diccionario
  - Algunos fabricantes intentan evitar este problema proporcionando un método automático de creación y transmisión de contraseñas PSK fuertes

WPA2

- En septiembre de 2004, la WiFi Alliance introdujo WPA2
- El objetivo es evitar las vulnerabilidades basadas en autentificación y el sistema de cifrado en WLANs
- WPA2 utiliza AES para el cifrado de datos y soporta tanto PSK como IEEE 802.1x para la autentificación

WPA2

- AES-CCMP
  - WPA2 utiliza AES en modo contador (CTR) para la privacidad y en CBC-MAC para la integridad de datos
  - AES se utiliza con bloque de 128 bits y clave de 128, 192 o 256 bits. Sólo la clave de 128 bits es obligatoria en WPA2
  - Es necesario realizar las operaciones de AES en hardware para poder atender la demanda de múltiples dispositivos
  - Los dispositivos antiguos no pueden soportar AES por falta de capacidad de cómputo
- IEEE 802.1x
  - Este estándar, diseñado para redes cableadas, implementa seguridad por puerto
  - Bloquea el tráfico puerto a puerto hasta que el cliente se ha autentificado mediante las credenciales almacenadas en un servidor de autentificación
  - De esta forma se evita que un dispositivo sin autorización reciba ningún tráfico hasta que su identidad pueda ser verificada
  - Utiliza el framework EAP

EAP

Es un framework que define los mensajes a utilizar por los protocolos de autentificación definidos sobre el mismo.

Usa 4 tipos de paquetes:

- Request
- Response
- Success
- Failure

- Lightweight EAP (LEAP)
  - Creado por CISCO (propietario)
  - No soportado en Windows
  - Vulnerable
- Protected EAP (PEAP)
  - Diseñado para utilizar logins y passwords de Windows
  - Crea un canal cifrado entre el cliente y el servidor de autentificación: más flexible
- Existen 5 EAPs para WPA y WPA2.

Resumen de soluciones de seguridad

Nombre	Cifrado	Autentificación	Seguridad
WEP	WEP	Clave compartida	Bajo
WPA	TKIP	PSK o 802.1x	Medio
WPA2	AES	PSK o 802.1x	Alto

Otros factores

- Disposición de antenas
  - Los puntos de acceso deben ser colocados en el centro del área a cubrir
  - Idealmente se colocarán en el techo para evitar interferencias y robo del dispositivo
  - Se debe minimizar la cantidad de señal que alcanza fuera del edificio o campus
- Control de potencia
  - Algunos puntos de acceso permiten ajustar la potencia para restringir la señal a la zona requerida
- Descubrimiento de puntos de acceso no autorizados
  - Es un problema delicado para las organizaciones de cierto tamaño
  - Existen varios métodos para detectar estos puntos de acceso
    - Manual, recorriendo el perímetro descubriendo las redes no autorizadas
    - Automatizado, empleando sensores y monitorización continua
  - Hay 4 tipos de sensores wireless
    - Dispositivo wireless convencional
    - PC sobremesa con interfaz USB
    - Puntos de acceso con sensor incluido
    - Sensor dedicado, similar en apariencia a un punto de acceso

Otros factores

LANs Virtuales Wireless

(WVLANs)

- Consiste en segmentar las redes wireless para aumentar la seguridad
- Muchas organizaciones establecen 2 redes virtuales:
  - Una para acceso de empleados que tiene acceso a la base de datos y ficheros
  - Una para invitados con acceso limitado a Internet o archivos públicos
- Existen 2 enfoques:
  - División en switch con varios puntos de acceso
  - Puntos de acceso con soporte para VLAN