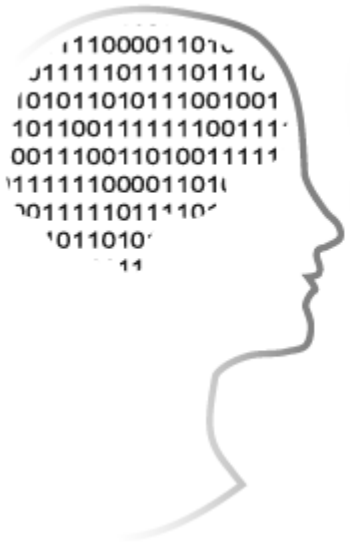
Lección 12: Seguridad en redes Wi-Fi



intypedia

INFORMATION SECURITY ENCYCLOPEDIA

D. Raúl Siles
raul@taddong.com

Fundador y Analista de Seguridad de Taddong

Introducción a la seguridad de las redes Wi-Fi

- Redes inalámbricas o redes Wi-Fi
  - Estándares IEEE 802.11
- Envío de información a través de señales de radiofrecuencia por el aire
- Alcance teórico: 100 m
- Alcance real: varios kilómetros
  - Depende de la existencia de obstáculos, potencia de transmisión, sensibilidad de recepción, utilización de antenas, etc

Clasificación de los ataques en redes Wi-Fi (I)

- Ataques de negación de servicio (DoS)
  - Difícilmente evitable al afectar al funcionamiento de la tecnología
  - Elevado impacto en entornos críticos
  - Afecta a la disponibilidad
- Interceptación de las comunicaciones
  - Acceso a los datos si no están cifrados
  - Indetectable
  - Afecta a la confidencialidad

Clasificación de los ataques en redes Wi-Fi (II)

- Inyección de tráfico en la red Wi-Fi
  - Modificar el comportamiento de la red Wi-Fi sin disponer de acceso a la misma
  - Afecta a la integridad
- Acceso a la red Wi-Fi
  - Conexión no autorizada a la red Wi-Fi
  - Acceso completo
  - Afecta a la integridad

Seguridad de las redes Wi-Fi

- Puntos de acceso y controladores Wi-Fi
- Objetivos
  - Cifrado de las comunicaciones
    - Proteger la confidencialidad de los datos
  - Autentificación y control de acceso
    - Identificar quién puede conectarse a la red Wi-Fi
- Configuración por defecto
  - Abierta o sin mecanismos de seguridad
  - Mecanismos de seguridad débiles (WEP)

Mecanismos de seguridad de las redes Wi-Fi (I)

- WEP (Wired Equivalent Privacy)
  - Mecanismo de autentificación y cifrado antiguo e inseguro
    - Utilización de RC4 de forma incorrecta en su diseño
  - Requiere contraseña
    - Falsa sensación de seguridad
  - Un atacante puede obtener la contraseña en menos de un minuto
  - Se desaconseja su utilización

Mecanismos de seguridad de las redes Wi-Fi (II)

- WPA (Wireless Protected Access)
  - Mecanismo de autentificación y cifrado temporal, empleado durante la migración de WEP a WPA2 en redes Wi-Fi
  - Inicialmente basado en TKIP (Temporary Key Integrity Protocol)
    - Evolución de WEP (RC4) con mejoras
    - Opcionalmente puede ser empleado con AES
  - Se desaconseja su utilización

Mecanismos de seguridad de las redes Wi-Fi (III)

- WPA2 (Wireless Protected Access 2) Personal o PSK
  - Mecanismo de autentificación y cifrado
    - Cifrado: AES (Advanced Encryption Standard)
    - Autentificación: PSK (Pre-Shared Key)
      - Contraseña compartida entre el punto de acceso y los clientes Wi-Fi
      - La contraseña debe ser suficientemente larga (más de 20 caracteres) y difícilmente adivinable
  - Opción recomendada para redes Wi-Fi personales o de pequeñas empresas

Mecanismos de seguridad de las redes Wi-Fi (IV)

- WPA2 (Wireless Protected Access 2) Enterprise
  - Mecanismo de autentificación y cifrado
    - Cifrado: AES (Advanced Encryption Standard)
    - Autentificación: 802.1X/EAP
      - Contraseñas aleatorias (servidor RADIUS)
      - Múltiples tipos de protocolos EAP: Usuario y contraseña, certificados digitales, tarjetas inteligentes (*smartcards*)…
  - Opción recomendada para redes Wi-Fi empresariales o corporativas

Mecanismos de seguridad de las redes Wi-Fi (V)

- Sistema de detección de intrusos inalámbrico (WIDS)
  - Detección y reacción frente a ataques en la red Wi-Fi
- Mecanismos adicionales:
  - Reducir la intensidad y alcance de la señal
  - Filtrado por dirección MAC
  - Ocultación del nombre de la red Wi-Fi
    - Desaconsejado: vulnerabilidad en los clientes

Seguridad de los clientes Wi-Fi (I)

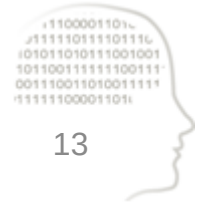
- Ordenadores de escritorio y portátiles, teléfonos móviles o *smartphones*, tabletas, y cualquier otro dispositivo móvil
- Ataques sobre el sistema operativo y el controlador de la tarjeta Wi-Fi
  - Simplemente por tener el interfaz Wi-Fi habilitado
    - Incluso sin estar conectado a ninguna red Wi-Fi
  - Mantener ambos actualizados

Seguridad de los clientes Wi-Fi (II)

- Lista de redes preferidas (PNL)
  - Los clientes Wi-Fi intentan conectarse a estas redes si están disponibles
- Ataque de punto de acceso falso (o *evil twin*)
  - La víctima anuncia sus redes preferidas
  - El atacante suplanta una de las redes Wi-Fi anunciadas y existentes en la PNL
  - La víctima se conecta a la red del atacante

Seguridad de los clientes Wi-Fi (III)

- ¿Cuándo anuncian los clientes Wi-Fi su lista de redes preferidas?
  - No deberían hacerlo si están actualizados
  - Algunos son vulnerables y sí lo hacen
  - Si la red Wi-Fi está configurada como oculta
    - Una red oculta no será visible al preguntar por las redes disponibles en la ubicación actual
    - El cliente debe preguntar específicamente por la red oculta para poder conectarse a ella
      - En el proceso desvela su presencia en la PNL

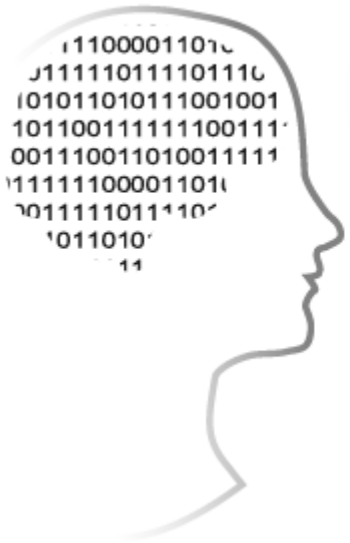


Seguridad de los clientes Wi-Fi (IV)

- Redes Wi-Fi públicas (*hotspots*)
  - Redes abiertas o con mecanismos de seguridad débiles (WEP)
    - Cafetería, biblioteca, hotel, aeropuerto, etc
  - Red Wi-Fi compartida por todos los usuarios
    - Incluido un potencial atacante, permitiendo ataques entre usuarios
    - El tráfico puede ser interceptado por cualquiera
      - Incluso al emplearse cifrado basado en WPA2-AES, ya que la contraseña es común a todos los usuarios

Resumen de recomendaciones de seguridad de redes y clientes Wi-Fi

- Redes Wi-Fi
  - Reducir el alcance de la señal
  - No configurar la red Wi-Fi como oculta
  - Utilizar WPA2-AES Personal (PSK) o Enterprise (802.1x-EAP)
- Clientes Wi-Fi
  - Actualización del sistema operativo y controlador Wi-Fi
  - Deshabilitar el interfaz Wi-Fi cuando no se está utilizando
  - Evitar conectarse a redes Wi-Fi inseguras, como por ejemplo redes públicas abiertas o basadas en WEP
  - Mantener actualizada la lista de redes preferidas (PNL)



intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contacto: info@intypedia.com