Tecnologías NFC, Bluetooth, WiFi y WiMAX.

Seguridad en Redes Inalámbricas.

Vulnerabilidades Conocidas y Capas de Protección

Christian Hernández Mares

Redes de Computadoras II
Ing. en Computación
7mo Semestre
Grupo 704

Noviembre 27, 2025

Tecnologías inalámbricas

NFC (Near Field Communication)

NFC es una tecnología de comunicación **inalámbrica de muy corto alcance** (unos pocos centímetros) que permite el intercambio rápido de datos al acercar dos dispositivos. Aparece en teléfonos móviles, tarjetas de transporte o pasaportes electrónicos. Su uso más común es el **pago sin contacto** con el móvil o identificación (por ejemplo, al pasar el teléfono junto a un datáfono o lector). Al operar a muy corta distancia, NFC obliga a acercar deliberadamente los equipos, lo que dificulta el espionaje remoto.

Bluetooth

Bluetooth es una **especificación para redes inalámbricas de área personal (WPAN)** creada por el Bluetooth SIG. Trabaja en la banda de 2,4 GHz y está diseñado para conectar dispositivos cercanos sin cables. Permite transmitir voz y datos entre teléfonos, auriculares, parlantes, teclados, ratones, etc. en un rango típico de unos pocos metros. Es decir, Bluetooth es ideal para enlazar equipos personales de corto alcance (por ejemplo, un manos libres con un móvil) sin necesidad de configuración compleja.

Wi-Fi

Wi-Fi es la familia de protocolos inalámbricos basados en el estándar **IEEE 802.11** para redes locales (LAN). En la práctica, Wi-Fi permite que dispositivos como computadoras, teléfonos y tabletas se conecten a Internet o entre sí sin cables. Opera en frecuencias típicas de 2,4 o 5 GHz, ofreciendo altas velocidades dentro del área de cobertura de un punto de acceso (p. ej. un router). Por ejemplo, en el hogar o en la escuela se usa Wi-Fi para navegar en Internet desde una habitación sin cables, compartiendo el enlace de banda ancha entre varios usuarios.

WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) es una norma de **banda ancha inalámbrica de largo alcance** basada en IEEE 802.16. Opera en frecuencias de microondas (aprox. 2,5–5,8 GHz) y puede cubrir distancias de decenas de kilómetros. Se concibió como “última milla” inalámbrica para llevar Internet a zonas rurales o como alternativa al cable. Una ventaja de WiMAX es dar **acceso de banda ancha en zonas extensas** donde el tendido de fibra o cable es costoso.

En resumen, NFC y Bluetooth sirven para conexiones muy cercanas (metros o centímetros), Wi-Fi para conexiones locales de unos cientos de metros, y WiMAX para cobertura mucho más amplia (hasta decenas de km)

Seguridad en redes inalámbricas

La **seguridad en redes inalámbricas** son las medidas y tecnologías que protegen la red sin cables de accesos o alteraciones no autorizadas. Esto es fundamental, pues sin la protección adecuada cualquier atacante podría interceptar comunicaciones o infiltrarse en la red, robando datos o afectando servicios. Los principales objetivos de la seguridad se basan en la tríada conocida como **CIA**:

Confidencialidad

proteger que solo usuarios autorizados accedan a los datos (los datos deben mantenerse privados)

Integridad

asegurar que la información no sea modificada maliciosamente durante su transmisión (los datos deben permanecer completos y sin alteraciones)

Disponibilidad

garantizar que la red y los servicios estén siempre accesibles para usuarios legítimos cuando los necesiten

---

Para cumplir estos objetivos se implementan **medidas básicas de seguridad** en la red inalámbrica. Entre ellas destacan:

Contraseñas fuertes y ocultar SSID

Cambiar el nombre (SSID) y la clave por defecto del router impide accesos obvios. Evitar contraseñas débiles o comunes.

Cifrado de la señal

Usar protocolos actuales de cifrado (WPA2 o WPA3 con AES) garantiza que los datos viajen codificados por el aire. No se recomienda WEP u otros métodos obsoletos, pues son vulnerables.

Autenticación robusta

Usar WPA2-PSK (con contraseña segura) o, en entornos avanzados, 802.1X/EAP (autenticación centralizada) refuerza el acceso autorizado.

Firewall (cortafuegos)

Activar el firewall integrado en el router o en dispositivos de la red bloquea conexiones no deseadas.

Actualizaciones

Mantener el firmware del router y el software de los equipos actualizados corrige vulnerabilidades conocidas.

Otros controles básicos

Desactivar funciones inseguras (por ejemplo WPS o UPnP en el router) y usar redes VPN para cifrar el tráfico cuando se accede a la red desde ubicaciones remotas

---

Con estas acciones se refuerzan la **confidencialidad, integridad y disponibilidad** de la red inalámbrica, dificultando que un intruso lea datos sensibles o interrumpa los servicios

Vulnerabilidades y ataques comunes

Las redes inalámbricas son más vulnerables que las cableadas, pues la señal viaja por el aire y puede ser captada por cualquiera en el área. Entre las **vulnerabilidades conocidas** se incluyen la falta de cifrado en redes abiertas, contraseñas predeterminadas débiles y protocolos obsoletos. Esto facilita varios **ataques comunes**, por ejemplo:

Sniffing (captura de paquetes)

El atacante utiliza un software “sniffer” para **espiar el tráfico inalámbrico**. Así puede leer datos enviados por otros (credenciales, mensajes, etc.). La contramedida básica es el cifrado fuerte (por ejemplo WPA2 o WPA3).

Suplantación de identidad (spoofing/Evil Twin)

Se crea un punto de acceso falso con el mismo nombre (SSID) de una red legítima. Los usuarios se conectan sin saberlo a esta “red trampa” y el atacante intercepta sus datos. Prevenirlo exige validar siempre el nombre del AP y, de ser posible, usar certificados o VPN; además, redes cifradas impiden la suplantación sencilla.

Ataques de denegación de servicio (DoS/DDoS)

Se interfiere la señal (por ejemplo con ruido intencionado en la misma frecuencia) o se saturan los recursos del router con tráfico, provocando que la red deje de responder. Las contramedidas incluyen configuraciones que limitan la tolerancia a tráfico anómalo y el uso de calidad de servicio (QoS), además de mantener equipos actualizados.

Man-in-the-Middle (MITM)

El atacante se coloca entre el emisor y el receptor (por ejemplo abriendo un AP rogue) y modifica o redirige la comunicación. El uso de cifrado de extremo a extremo (HTTPS/TLS sobre Wi-Fi) y autenticación mutua previene en gran parte estos engaños.

Otros ataques

Incluyen intentos de adivinar contraseñas (fuerza bruta o diccionario) si la clave es sencilla, el secuestro de sesión abierta, o exploits de fallos en protocolos como WPS. Cada uno se evita con contraseñas robustas, desactivando funciones vulnerables (p. ej. WPS) y usando siempre la versión más segura del protocolo Wi-Fi disponible.

En resumen, la **defensa en redes inalámbricas** debe ser “por capas”: en la capa de enlace de datos usar cifrado y autenticación fuertes; en la capa de red activar firewalls y sistemas de prevención/detección de intrusos (WIDS/WIPS); y en capas superiores aplicar VPN o cifrado de aplicaciones. Un buen diseño de varias capas dificulta que un atacante logre acceso no autorizado, altere datos o deje fuera de servicio la red