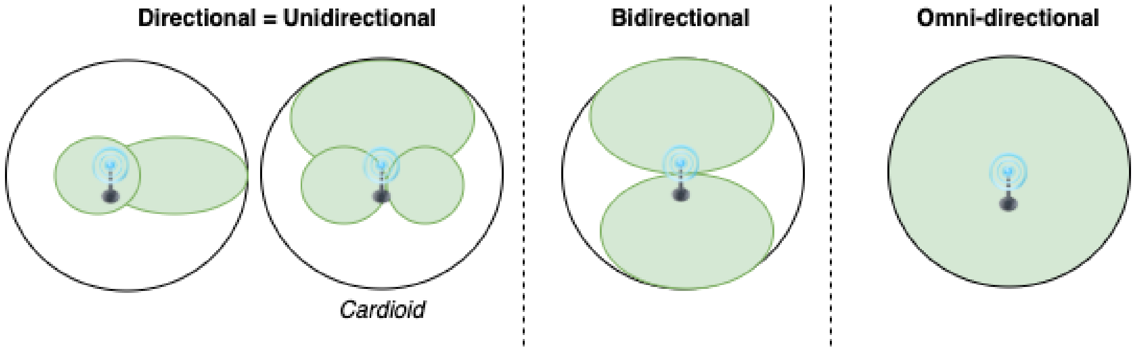
Wireless networks overview

- Wireless network = Wi-Fi
- Type of Wireless Local Area Network (WLAN)
- Standardized by IEEE 802.11
- Allows devices in range of an access point to access the network.

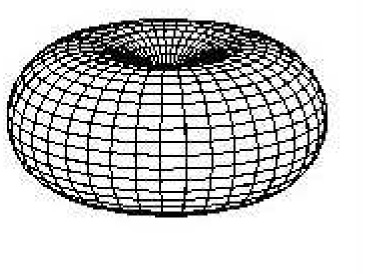
Wireless terms

- **Access Point**
  - Access Point (AP) or Wireless Access Point (WAP)
  - Hardware device that allows wireless connectivity to the end devices.
- **SSID (Service Set Identifier)**
  - Unique name for a wireless Access Point
  - Inserted into the header of every data packet.
- **BSSID (Basic Service Set Identifier)**
  - MAC address of an access point
- **GSM**
  - Global System for Mobile Communication
- **Bandwidth**
  - Amount of information that may be broadcasted over a connection
- **Hotspot**
  - Places where wireless network is available for public use
- **Orthogonal Frequency Division Multiplexing**
  - Encoding method of digital data on multiple carrier frequencies
- **Frequency-hopping spread spectrum (FHSS)**
  - Method of transmitting radio signals rapidly switching a carrier among many frequency channels
- **Phase Shift Keying (PSK)**
  - Modulation technique where phase of carrier signal changed by varying the sine and cosine inputs.
  - Widely used for WLANs, biometric and contactless operations, along with RFID and Bluetooth communications.

Antenna patterns

- 

- 📝 Directional antenna patterns

    - **Directional antenna**
        - Also known as ***unidirectional antenna***
        - Broadcasts and obtains radio waves from a single direction (can be e.g. 30 - 60 degrees)
        - E.g. **Yagi** (also known as ***Yagi–Uda antenna***)
        - Most concentrated, higher range
        - **Parabolic grid antenna**
            - Based on the idea of a satellite dish
            - Can be attacked from farther away as it picks up Wi-Fi signal from 16 km and more
    - **Bi-directional antenna**
    - **Omni-directional antenna**
        - Broadcasts in 360 degrees
        - Most common type of antenna used in wireless communications and networks, especially WiFi
        - Used also in wireless base stations
        - Least concentrated and lower range
        - 
        - **Dipole**: Used for closer proximity e.g. mobile phones, client connections instead of site-to-site

Wireless encryption

Wireless encryption comparisons

WEP

- Wired Equivalent Privacy
- 1997, to provide data confidentiality
- Stream cipher RC4 for confidentiality
- CRC-32 checksum for integrity
- Authentication using WEP-Open and WEP-Shared (using a shared key) modes
- ❗ Weak as it reuses small IVs which allows decoding of its shared key.

WPA

- Wi-Fi Protected Access
- 2003, replace WEPs weak encryption
- Uses **Temporal Key Integrity Protocol (TKIP)**
    - Major improvement over WEP
    - Dynamically changes key as system is used
    - Combined with larger IV, this defeats well known attacks
    - Uses RC4 encryption

- Authentication using WPA-PSK and WPA-Enterprise modes
    - WPA-PSK uses pre-shared (symmetric) key to encrypt the wireless data
- Improved payload integrity vs. WEP
    - Uses more secure message integrity check (MIC) known as Michael
    - Includes a frame counter to prevent replay attacks
- Still subject to attack

WPA2

- Also known as ***Wi-Fi Protected Access 2*** or ***802.11i***
- 2004, replace WPAs weak cipher
- Authentication WPA2-Personal and WPA2-Enterprise modes
- Uses **Advanced Encryption Standard algorithm (AES)**
    - Much harder to decrypt than WPA or WEP
- 📝 Replaces TKIP with **CCMP** (AES-CCMP)
    - Also known as ***Counter Mode Cipher Block Chaining Message Authentication Code Protocol (Counter Mode CBC-MAC Protocol)*** or ***CCM mode Protocol (CCMP)***
    - Uses AES as encryption algorithm instead of RC4 in WPA.

WPA3

- Wi-Fi Protected Access 3
- 2018, introduce Dragonfly handshake, protects against dictionary attacks
- Authentication using WPA3-Personal and WPA3-Enterprise

Wireless cryptographic differences

	WEP	WPA	WPA2	WPA3
Encryption	RC4	RC4 + TKIP	AES-CCMP	AES-CCMP & AES-GCMP
IV Size (Bits)	24	48	48	48
Key Length (Bits)	40/140	128	128	128/256
Integrity Check	CRC-32	Michael/CRC-32	CBC-MAC, CCMP	BIP-GMAC-256

WPA2 and WPA3 Operation Modes

Personal

- Intended for home use, easier setup

Enterprise

- More complex setup, more granular control
- Uses RADIUS authentication with Extensible Authentication Protocol (EAP) extensions for more security

WPA2 vs WPA3 operation modes

	Personal	Enterprise
WPA2	Also called **WPA-PSK** (pre-shared key) as it uses PSK to protect network access	Same encryption
WPA3	Also called **WPA3-SAE** (Simultaneous Authentication of Equals). Uses 128-bit key and Forward Secrecy against dictionary attacks.	Uses 192-bit key

Wireless standards

- **802.15.1 - Bluetooth**
  - Read more on bluetooth
- **802.15.4 - Zigbee**
  - Low-power, low-data-rate, and close-proximity wireless ad hoc networks.
  - Popular IoT connection protocol
- **802.16 - WiMAX**
  - Wireless on "steroids"
  - Written for global development of broadband wireless metropolitan area networks.
  - Big range and fast.
- **Comparing wireless standards**
- **802.11 Specifications**

Standard	Distance	Speed
WiFi	Medium (20-250 m)	Started slow (2 Mbit/s) but fast now (1300 Mbit/s)
ZigBee	Smallest (1-100 m)	Slow (up to 0.25 Mbit/s)
WiMax	Biggest (1.6 - 9.6 km)	Fast (up to 1 Gbit/s)

- 📝 Summary of the standards

Standard	Year	Summary
802.11 (WLAN/**Wi-Fi**)	1997	• 2.4 GHz • DSS, FHSS • Up to 2 Mbit/s • 20 - 100 meters
802.11a (Wi-Fi 2)	1999	• 5 - 3.7 GHz • OFDM • Up to 54 Mbit/s • 35 - 100 meters
802.11b	1999	• 5.4 GHz • DSSS • Up to 11 Mbit/s • 35 - 140 meters
802.11c	2001	Bridge operation procedures; included in the IEEE 802.1D standard
802.11d	2001	International (country-to-country) roaming extensions
802.11e	2005	Enhancements: QoS, including packet bursting
802.11f	2003	Inter-Access Point Protocol, Withdrawn February 2006
802.11g (Wi-Fi 3)	2003	• 2.4 GHz • OFDM • Up to 54 Mbit/s • 38 - 140 meters
802.11i	2004	Defines WPA/WPA2 encryption standards
802.11n (Wi-Fi 4)	2009	• 2.4 - 5 GHz • MIMO-OFDM • Up to 600 Mbit/s • 70 - 250 meters
802.11ac (Wi-Fi 5)	2012	• 5 GHz • MU-MIMO, • Up to 1300 Mbit/s • 70 - 250 meters
802.11ax (Wi-Fi 6)	2019	• 1 - 6 GHz • MU-MIMO, OFDMA • Up to 11 Gbit/s • 70 - 250 meters
802.15.1 (WPAN/**Bluetooth**)	2002	• 2.4 GHz • GFSK, π/4-DPSK, 8DPSK • Up to 50 Mbit/s • 70 - 250 meters
802.15.4 (Low rate WPAN/**ZigBee**)	2003	• 0.868, 0.915, 2.4 GHz • O-QPSK, GFSK, BPSK • Up to 0.25 Mbit/s • 70 - 250 meters
802.16 (**WiMAX**)	2005	• 2-11 GHz • SOFDMA • Up to 1 Gbit/s • 1.6 - 9.6 kilometers

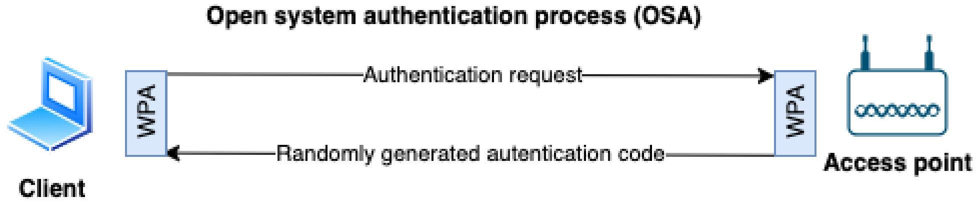
- See also all 802.11 standards and amendments

Wi-Fi authentication

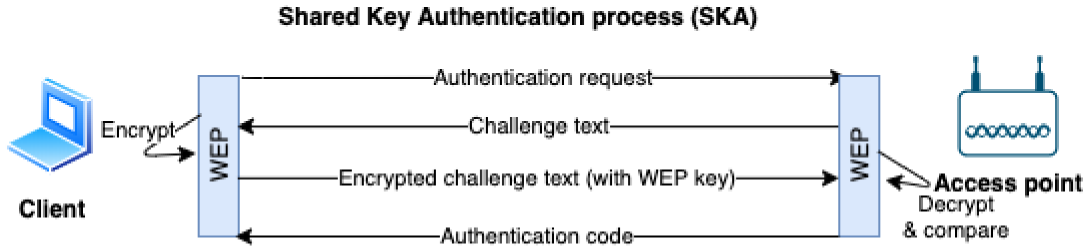
Wireless authentication modes

Open system authentication process (OSA)

- Uses WPA protocol.
- Complete free for all, no auth at all

- 
Open system authentication process (OSA)
Client
WPA
Authentication request
Randomly generated autentication code
WPA
Access point

Shared key authentication process (SKA)

- Uses WEP protocol + a shared secret key
- 

IEEE 802.1x

- 📝 Authentication mechanism for both wireless and physical access to a network
- Authenticate devices to decide to give e.g. corporate or guest access
- Switches uses back-end authentication server, see AAA
- Can authenticate based on MAC address or other requirements (certificate, VLAN etc.)
- Per default all hosts on a wired connection (LAN) can see each other

AAA protocols

- AAA stands for (Authentication, Authorization, Accounting)
- Family of protocols that mediate network access.
- Sometimes these protocols are used in combination with
  - Point-to-Point Protocol (PPP)
  - Extensible Authentication Protocol (EAP)
  - Protected Extensible Authentication Protocol (PEAP)
  - Lightweight Directory Access Protocol (LDAP)
- Most commonly used protocol is RADIUS and then Diameter, meanwhile older systems use TACACS and TACACS+

RADIUS

- Stands for **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice
- 📝 Commonly used by ISPs (Internet Service Providers) and corporations for access control
- Primarily used to manage access to the internet or other networks
  - Networks can employ a variety of networking technologies, including analog modems, DSL, wireless local area networks (WLANs), and VPNs.
- Based on UDP (User Datagram Protocol)
- Flexible and extensible offering a variety of ways to authenticate the user
- Requires setting-up a RADIUS back-end server.
  - Usually integrated with AD (active directory)

Extensible Authentication Protocol (EAP)

- Authentication framework used by Enterprise WPA operation mode.
- Strong when used with TLS (EAP-TLS)
  - Higher security when client-side certificates are hosted in smart cards.
- Extends and replaces Point-to-Point Protocol (PPP).

EAP Transport Layer Security (EAP-TLS)

- Secure standard using TLS protocol
- Requires mutual authentication
  - Where the client-side certificate can be stored in e.g. smart cards.

Diameter

- Successor to RADIUS
- Not directly backwards compatible
- Security is provided by IPsec or TLS and privacy protocols.

TACACS

- Terminal Access Controller Access-Control System
- Remote authentication protocol

- Commonly used in networks of UNIX systems

TACACS+ (TACACS plus)

- Terminal Access Controller Access-Control System Plus
- Provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers.
- Based on TACACS but an entirely new protocol (incompatible with TACACS)
- Runs on older systems but generally replaced by RADIUS

Wireless threats and attacks

Wireless threats

- **Access control attacks**
  - Evading access control measures such as Access Point MAC filters, port access control
- **Integrity attacks**
  - Sending forged frames
  - E.g. data frame injection, bit-flipping.
- **Confidentiality attacks**
  - Intercepting confidential information transmitted over the network
  - E.g. traffic analysis, session hijacking, MITM, etc...
- **Availability attacks**
  - Attempting to prevent users from accessing WLAN resources.
  - E.g. flooding, ARP poisoning, De-Authentication attacks
- **Authentication attacks**
  - Steal identity information or impersonating clients
  - E.g. password cracking, identity theft, password guessing
  - See also Authentication attacks | Hacking Web Applications
- **Misconfigured access point attack**
  - Accidents for configurations that you can exploit
- **AD Hoc connection attack**
  - Connecting directly to another device via ad-hoc network.
  - Not very successful as the other user has to accept connection
- **Honeyspot access point attack**
  - Using multiple WLANs in area and use same SID.
- **AP MAC spoofing**
  - MAC spoofing to mask an authorized client
- **Jamming signal attack**
  - Jamming or blocking the wireless communication, causing a denial of service

De-authentication attack

- Also known as **deauthentication attack**
- Used to capture the handshake traffic.
- Can also be used to DoS the client by continuously de-authenticating the device.

Evil twin attack

- Also known as **client mis-association**
- 📝 A rogue access point outside the place with the legitimate one
- E.g. can lure the employees of the organization to connect with it
- Can be done using Airsnarf

Honeyspot attack

- Faking a well-known hotspot on a rogue AP
- E.g. as McDonald's or Starbucks free Wi-Fi spot

Rogue Access Point Attack

- Fake AP with same SSID as legitimate one.
- Allows hijacking connections and acting as a middle man sniffing
- Differs from evil twin attack as it focuses on MITM instead of WiFi passwords.

Sinkhole attack

- Compromised node tries to attract network traffic by advertise its fake routing update.
- Allows traffic to be directed away from its target.
- Can be used to launch other attacks like dropping or altering routing information.

DNS sinkhole

- Also known as a ***sinkhole server***, ***Internet sinkhole***, or ***Blackhole DNS***
- DNS server that gives out a false result for a domain name.
- Used to attack on sensor/IoT device networks
- Can be prevented by owning own DNS server or hardcoding IP addresses.
- E.g. WannaCry malware was stopped spreading as a worm by Marcus Hutchins who discovered kill switch in the malware and Registering a domain name for a DNS sinkhole.

Wireless hacking methodology

1. **Wi-Fi Discovery**
    - find wireless networks
2. **GPS mapping**
    - List of discovered Wi-Fi networks
3. **Wireless Traffic Analysis**
    - Capture the packets to reveal any information (SSID, authentication method, ...)
4. **Launch Attacks**
    - E.g. ARP poisoning, MAC spoofing, De-Authentication, Rogue access point, MITM.

Wireless discovery

- Also known as Wi-Fi discovery
- **Wardriving**: Using a mobile vehicle to detect WiFi networks
    - 📝 E.g. T.J. Maxx Data Theft where 45 million credit/debit card data was stolen because of weak WEP encryption.
    - Also used: warbiking, warcycling, warwalking.
    - **Warchalking**: drawing of symbols in public places to advertise an open Wi-Fi network.
- Tools such as WiFiExplorer, WiFiFoFum, OpenSignalMaps, WiFinder
    - WIGLE: map for wireless networks
    - NetStumbler: Windows tool to find networks
    - Kismet
        - Wireless network detector, sniffer, and intrusion detection system.
        - Works without sending any packets (passively)

    - NetSurveyor: Windows tool similar to NetStumbler and Kismet
    - Silica: Discovers and shows vulnerabilities

Wireless encryption attacks

WEP cracking

- Weak IV (Initialization Vectors)
    - Small
    - Get reused frequently
    - Are sent in clear text during transmission
- Can take a few seconds to discover the shared secret key.
- The goal is to collect as many IVs as possible
    - 💡 Inject packets to speed it up
- 📝 Can be cracked using Aircrack-ng:
    1. Listen to the traffic
        - Start a compatible adapter with injection and sniffing capabilities
        - `airmon-ng start <interface-name>`
    2. Start a sniffer to capture packets
        - `airodump-ng --bssid <AP-MAC-address> -c 11 -w <output-file> <interface-name>`
    3. Create more packets to escalate the process to collect more IV
        - Inject ARP traffic: `aireplay-ng -3 -b 00::09:58:6F:64:1E -h 44:60:57:c8:58:A0 mon0`
    4. Run a cracking tool to extract encryption keys from the collected IVs
        - `aircrack-ng <output-file>.cap`
        - Default method is PTW (Pyshkin, Tews, Weinmann), other (older) supported methods include:
            - FMS (Fluhrer, Mantin, Shamir) attacks: statistical techniques
            - Korek attacks: statistical techniques
            - Brute force
- Using separate tools for sniffing and cracking:
    1. Gathering packets through e.g. Wireshark or Prismdump
    2. Crack using e.g. WEPCrack, AirSnort, Aircrack-ng, and WEPLab

WPA/WPA2 cracking

- Much more difficult than WEP
- Uses a constantly changing temporal key and user-defined password
- **Key Reinstallation Attack (KRACK)**
    - Replay attack that uses third handshake of another device's session
- Most other attacks are simply brute-forcing the password that take a lof time.

Sniffing 4-way handshake

- 4-way handshake is the ceremony between AP and the device
- Vulnerability in WPA and WPA-Personal (WPA-PSK, pre-shared key)
- During WPA handshake, password is shared in encrypted form (called **PMK (pairwise master key)**)
- Flow:
  1. Client tries to connect to an AP (access point)
     - If the client is already connected then [deauthentication attack]() can be used to disconnect the client and sniff when client is reconnecting.
  2. Grab packets while client goes through a 4-step process of authentication
  3. Crack WPA keys from recorded packets
     - Can be an offline attack e.g. utilizing a cloud virtual machine.
     - E.g. using `hashcat`
- Steps
  1. Recording and deauthenticating using [`aircrack-ng`]()
     - 🤗 Used often in movies as it looks cool
     - `airmon-ng start <interface-name>` to create a new interface and enable monitor mode
     - `airmon-ng <interface-name>` to list access points with BSSID, encryption (WPA2 etc.) and more.
     - `airmon-ng -c2 -w capture -d <BSSID> <interface-name>` to listen
       - Shows each client MAC and logs their traffics notifying handshakes.
     - `airplay-ng -deauth 100 -a <BSSID> -c <client-MAC> <interface-name>` to inject packets to de-authenticate the client
  2. Crack the password using `hashcat`
     - Convert log files from `airmon-ng` from `.cap` to `.hccapx` using e.g. an [online tool]()
     - Run `hashcat.bin -a 3 -m 2500 converted-file.hccapx ?d?d?d?d?d`
       - `-m 2500`: hash mode for `WPA-EAPOL-PBKDF2`
       - `-a 3 ?d?d?d?d?d`: attack mode: bruteforce with mask telling 5 any characters.

WPA3

- More secure against sniffing, brute force and WPS attacks.
- However has implementation bugs that can be exploited using:
  - [potential side channel attacks]()
  - [DoS attacks]()

Tools for wireless encryption attacks

Aircrack-ng

- 📝 Sniffer, detector, traffic analysis tool and a password cracker
- Official webpage | Source code
- Uses dictionary attacks for WPA and WPA2.
  - Other attacks are for WEP only

Cain and Abel

- Also known as **Cain & Abel** or **Cain**
- 📝 Windows tool to sniff packets and crack passwords
- Relies on statistical measures and the PTW technique to break WEP
- See also • Cain and Abel | Web server threats and attacks • Cain and Abel | Sniffing tools

Wireless security tools

Wireless Intrusion Prevention Systems (WIPS)

- Also known as **Wireless IPS**
- Network device
- 📝 Intrusion detection by monitoring the radio spectrum for the presence of unauthorized access points (e.g. evil twins)
- Intrusion prevention by taking steps to mitigate the threat (e.g. deattaching it).
- E.g. • Cisco Adaptive Wireless IPS • WatchGuard WIPS

Wireless Intrusion Detection Systems (WIDS)

- Also known as **Wireless IDS**
- Monitors radio spectrum used by wireless LANs and alerts whenever a rogue access point is detected.
- Alerts a systems administrator whenever a rogue access point is detected

Wi-Fi security auditing tools

- AirMagnet® WiFi Analyzer PRO
  - Real-time analysis of 802.11a/b/g/n/ac wireless networks
- RFProtect Wireless Intrusion Protection
  - Prevents denial-of-service and man-in-the-middle attacks and mitigates over-the-air security threats.
- FruityWiFi
  - Open source tool to audit wireless networks
  - Allows the user to deploy advanced attacks by directly using the web interface or by sending messages to it.
- Fern Wifi Cracker
  - Security auditing and attack software program
  - Can run attacks such as cracking WEP/WPA/WPS keys
- OSWA-Assistant
  - Organizational System Wirelss Auditor

Wi-Fi predictive planning tools

- Allows to plan and design Wi-Fi 6 networks
- E.g.
  - AirMagnet® Planner
    - Plan networks, estimate budgets, optimize, plan mitigation strategies
  - Cisco Prime Infrastructure
    - Solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices
  - Ekahau Pro
    - Tool for designing, analyzing, optimizing, and troubleshooting Wi-Fi networks.
  - TamoGraph Site Survey

        - Wireless site survey software tool for collecting, visualizing, and analyzing 802.11 a/b/g/n/ac/ax Wi-Fi data.
    - NetSpot
        - Wi-Fi analysis, and troubleshooting on Mac OS X and Windows.
        - Visualize, manage, troubleshoot, audit, plan, and deploy your wireless networks.

Wi-Fi vulnerability scanning tools

- Zenmap
    - Official Nmap GUI.
- Nessus
    - Read more on vulnerability analysis
- Network Security Toolkit
    - Bootable Fedora with network security tools
- SecPoint® Penetrator™ Vulnerability Scanner & Assessment
    - Comes with WiFi pen-testing tools
- SILICA
    - Automated, WiFi specific, vulnerability assessment and penetration tool.
- WebSploit
    - MITM framework with WiFi attacks
- Airbase-ng
    - Multi-purpose tool aimed at attacking clients as opposed to the Access Point (AP) itself

Wi-Fi security tools for mobile

- Wifi Protector
    - Android WiFi firewall
- WiFiGuard
    - iOS/Android app to scan and detect devices on WiFi network
- Wifi Inspector
    - Android app to scan and detect devices on WiFi network
- ARP Guard
    - Android app for protection against network attacks including ARP posioning.

Bluetooth

- Range is typically less than 10m
- Operates on the 2.4 GHz
- Discovery feature can control the visibility of the device
- **Bluetooth Low Energy (BLE)**: Bluetooth >= 4.0
- **Bluetooth Classic (BC)**: Bluetooth < 4.0
- Uses WPAN (wireless personal area network)
- Utilize the Gaussian Frequency Shift Keying (FSK) to exchange information in the basic rate (BR) of usually 1 mbps.

Bluetooth security

- Standard provides three basic security services:
  - **Authentication**
    - To verify the identity of communicating devices
  - **Confidentiality**
    - To prevent the compromise of information and ensure that only authorized devices can access and view data.
  - **Authorization**
    - To allow the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.
- ❗ Standard does not address address other security services such as audit and non-repudiation.
- Four security modes (levels):
  1. **Mode 1**: No authentication/encryption.
  2. **Mode 2**: Authorization with access control policies.
  3. **Mode 3**: Mandate authentication and encryption using secret key with paired devices
  4. **Mode 4**: Secure Simple Pairing using Elliptic-Curve Diffie-Hellman (ECDH) for key exchange and link key generation

Bluetooth device discovery

- BlueScanner: Finds devices around and displays information
- BT Browser: Find and enumerate nearby devices

Bluetooth attacks

BlueSmacking

- 📝 DoS attack using echo.

BlueJacking

- 📝 Sending unsolicited data to bluetooth devices
- Allows spamming for bluetooth also known as **BlueSpamming**
- ❗ Not related to hijacking

BluePrinting

- 📝 Extracting information about the device

BlueSnarfing

- 📝 Stealing data from target device
- E.g. calendars, contact lists, emails and text messages

BlackJacking

- 📝 Exploits a blackberry device to attack corporate LAN directly
- Compromises blackberry then proxies between corporate servers and attacker.

BBProxy

- 📝 Bluejacking tool
- Included in BlackBerry Attack Toolkit
- Announced by DefCon

BlueBugging

- Also known as **bluebug-attack**
- Create a backdoor attack before returning control of the phone to its owner
- Extends BlueJacking and BlueSnarfing (allows attacker to access data)
- E.g. by pretending to be a headset to receive phone calls
- Not so common as vulnerabilities are generally patched

Bloover

- A proof-of-concept tool
- 📝 Exploits bluebugging targeting J2ME (Java micro edition) enabled phones such as Nokia
- Bloover II: Exploits bluebug and also helomoto, bluesnarf and OBEX object push attacks

Bluetooth attacks countermeasures

- Check paired devices
- Turn off visibility / turn off Bluetooth if not used
- Use strong PIN
- Use encryption
- Use the strongest security mode available
- Don't accept unknown requests
- Use bluetooth security tools

Bluetooth security tools

- Bluetooth firewall
  - Mobile app for logging and monitoring Bluetooth connections
  - Radar feature allows you to scan nearby bluetooth devices
  - Scan feature lists apps that can perform bluetooth actions
- Bluediving
  - Bluetooth penetration suite
  - Exploits BlueBug, BlueSnarf, BlueSnarf++ and BlueSmack
- Bluelog

  - Linux Bluetooth scanner
- btscanner
  - Debian tool to extract information from a Bluetooth device without the requirement to pair.
- BlueRanger
  - Simple Bash script which uses Link Quality to locate Bluetooth device radios