Linux Chapter 8: Wireless Networks

Joseph Livesay • Julian Richen

Introduction

- Wireless networks have become prevalent in almost every aspect of our everyday lives
- However as the amount of wireless communication increases, the amount of security needed to fortify and protect users will also increase
- This chapter focuses on auditing wireless networks in the Linux environment

Wireless Setup - Linux Wireless Chipsets

- Atheros
  - Supports the MADWifi (Multiband Atheros Driver for Wireless Fidelity) for native compatibility with Linux
  - Has the ability to audit both the access point and the wireless clients connected to it

Wireless Setup - Linux Wireless Chipsets

- Conexant PrismGT
  - Allowed Linux users to gain full access of chipsets from Prism54
  - Uses built in Wireless-Tools (ex. **iwconfig**, **iwpriv**, etc..)
    - As opposed to previous chipsets like the Atheros
  - Uses a mix of FullMAC and SoftMAC Cards
    - FullMAC requires firmware to be loaded WNIC
    - SoftMAC offload work done on firmware to host machine

Wireless Setup - Linux Wireless Chipsets

- Ralink and Serialmonkey
  - Only supports the ability to monitor traffic, cannot be used as an access point for security auditing
- Intel Centrino and IPW2200
  - One of the most common wireless chipsets in computing
  - Only natively supports monitoring mode
    - Limited usage in its native form as it does not support frame-injection
  - There is a master mode driver that is currently in development, however it requires additional installing onto the Linux machine

Wireless Setup - Linux Wireless Chipsets

- Other Wireless Chipsets
  - Many other chipsets exist for WNIC
    - Ex: from Broadcom and Texas Instruments
  - Linux support may be patchy
  - Avoid them if possible, if you can't:
- NDISwrapper/Driverloader
  - A wrapper for the Windows WNIC driver
    - Nearly every WNIC ships with a Windows driver built in
  - Acts as an abstraction layer and allows Linux machines to use functionality found in the Windows driver
  - Not full-proof
    - Does not allow monitor or master mode, which allows using full power of chipset

Combating attacks from Linux wireless chipsets

- The appropriate measures of defense against an attacker utilizing Linux wireless chipsets and tools are:
    - Drying up the supply of Linux-native-supported wireless chipsets
    - Stopping the development of the Linux-native wireless drivers that enable the use of the hardware
    - Running RF- or protocol-based denial-of-service (DoS) attacks against the attacker's hardware
- The first two options are practically impossible, while launching an RF attack is usually impossible because typically the attacker is only passively listening on wireless traffic
- The only plausible defense is a protocol-based DoS attack, however this can be an illegal activity if attacking the wrong target

Wireless Hacking Physics

Radio Frequency

- The transmission medium which 802.11x operates on
    - Other protocols also work on radio frequency [802.15 (Bluetooth) and 802.16 (WiMax)]
- It is important to understand RF signals as we can use them to exploit WNIC
- RF exists as a waveform and can experience noise and other forms of signal loss

Radio Frequency

- Frequency of an RF signal is how often the signal repeats or “cycles” in a given time period (normally 1s)
  - Ex: 2.4 Ghz cycles 2,412,000,000 times a second
- We need the wavelength to determine the range which a signal can travel
  - You can find a wavelength by using:
    - *Wavelength = Speed of Light * (1/Frequency)*
  - Normally APs limit the “effective” range to a 100-meter bubble
  - Using a Cantenna we can pick-up signals far away from the bubble

Impact of Frequency and Wavelength on Offense and Defense

- Utilizing the frequency of the access point, the wavelength it is producing can be derived
- Using this information, a cantenna can be made that utilizes this calculated wavelength
    - A cantenna has the ability to far extend the normal operating range of an access point, allowing a hacker to access the network far outside any physical barriers that might exist and to retain their anonymity
- Physically reducing the effective range of the access point is a defense against this form of attack

Amplitude

- The amplitude of a wave determines the amount of electrical energy it possesses
  - The stronger the amplitude, the stronger the signal from the access point is
- The more amplitude that an attacker can get, the easier it will be to decode signal because they will have more data to utilize
- This can be defended against by lowering the amplitude from the access point to a level appropriate for its range

Non-Protocol-Based DoS

- Noise is undesirable interference of RF
  - Can distort signal properties
- Noise can be man-made or natural
  - Ex. Military sending noise to interfere with enemy signals (ECM)
  - Ex. Natural barriers and signal preventing material
- Signal encoding & decoding can help reduce noise or parse signals with a lot of noise, but not always
  - Ex. Direct Sequence Spread Spectrum (DSSS)
  - Ex. Orthogonal Frequency Division Multiplexing (OFDM)
- In the end noise based DoS attacks will override attempts to parse noise interfered signals

Attenuation

- Attenuation is the reduction of amplitude
  - Caused by physical obstruction or atmospheric interference on the RF waves
- Attenuation can occur in three different ways:
  - Reflection
  - Refraction
  - Absorption
- The sum of all effects of attenuation form a quantity called path loss
  - Measured in decibels (dB)
- In order to achieve the best amplitude from the signal, an attacker must take into account all aspects of attenuation

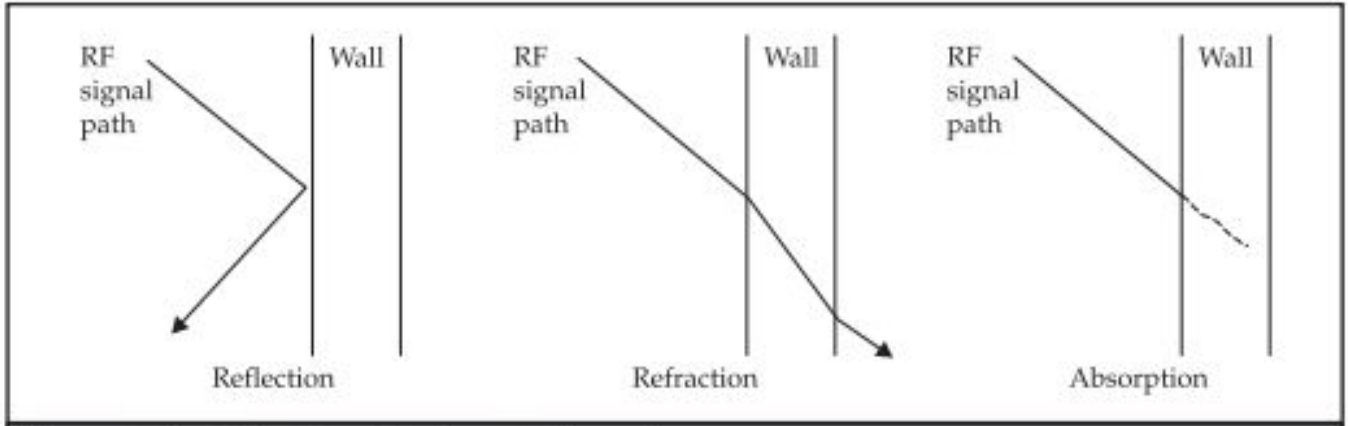


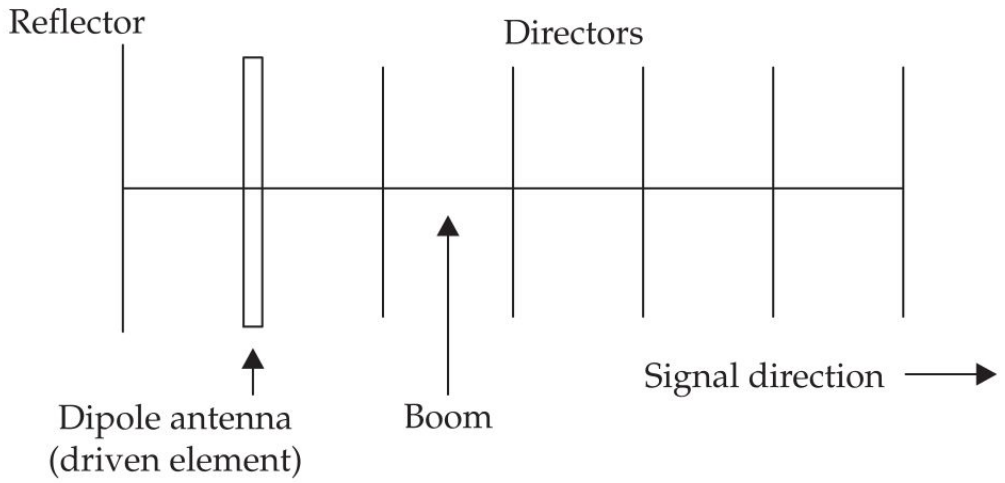
Figure 8-2 Reflection, refraction, and absorption

RF Hacker Improvement Kit: Antennas and Gain

- Signals are often not strong enough to “hack” from range
- Use the knowledge of RF to create devices to enhance signal reception and transmission
- Antennas come in multiple forms
  - Omnidirectional
    - Sends signals in multiple directions
    - What most store-bought consumer APs are
  - Direct Antenna
    - Sends signals in one direction, but much stronger than Omnidirectional
    - Mostly seen on TVs

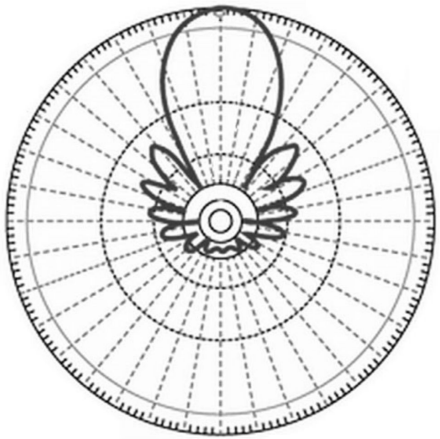
RF Hacker Improvement Kit: Antennas and Gain

Yagi-Uda antenna design



RF Hacker Improvement Kit: Antennas and Gain

Yagi-Uda antenna RF footprint



RF Hacker Improvement Kit: Antennas and Gain

- Using the antenna designs found on the previous slides we can create an antenna that can pick-up and transmit RF signals from a much greater range than a normal AP.
- The Yagi-Uda antenna can transmit a signal 1.5km if both APs are setup correctly and have the power
- Using one of these antennas directed at a normal household AP we can pick-up signals far away
    - All that is left is to break the APs wireless security
- This is the main concept of a Cantenna and “hacking” RF signals

Defense against RF exploitation

- Defending against the exploitation of an access point's wave transmission centers around limiting the range of its transmission.
  - Primarily using attenuation.
- Placing obstacles such as high-density cubicles, wire-mesh barriers, and aluminum-based paint can distort the RF signal to a point it can't be utilized unless it is within these obstacles
- Also utilizing RF equipment with shorter wavelengths can increase the effect of attenuation

RF SPECTRUM ANALYSIS

Identifying Frequency Usage and Patterns

- The investigating and identifying of patterns in RF activity in a given range of frequencies is the core of RF spectrum analysis
- Use a RF spectrum analyzers to receive, record, and plot RF energy in a given frequency band
- You can use spectrum analyzers for good by analyzing frequency range for other APs operating in the same RF
    - Helps to determine a better range to broadcast in (ie. 5Ghz if a lot of noise already exists on 2.4Ghz)

Defending Against RF Spectrum Analysis

- Very difficult to defend against since it is a passive attack
- You can attempt to identify an attacker by looking around for anyone with a hand-held device or WiFi dongle
  - A device is required to pick-up the signal
  - However, not all devices are used for attacks
    - Someone might have a WiFi dongle for legitimate reasons

EXPLOITING 802.11

802.11

- 802.11 is the most commonly used wireless technology for IP-based data
- Frame analysis is a common exploit of the 802.11 communication technology

Frame Analysis

- Frame transmission can be a large target for manipulation because they do not have any form of encryption
- In order to avoid collisions with data transmissions, the access point and client send frames of data back and forth to each other to confirm when they’re able to receive and transmit data
- If an attacker is able to bombard the receiving channel of the access point, they can control the flow of frames requesting transmission

Frame Analysis

- By analyzing the frames being passed in the network, an attacker can determine if the frame is being sent to the access point or from the access point.
- Once a frame has been sent, the attacker can spoof a frame to cause dissociation from the network, starting a DoS attack which can spread throughout the network
- This can also be used to sniff out data in the frame

Defending Against 802.11 Frame Analysis

- Like RF Spectrum Analysis, Frame Analysis is difficult to counter as it is a passive attack
- One possible counter is to send out crafted frames that exploit a DoS vulnerability in the attackers WNIC chipset
  - This assumes you know the attackers chipset (not likely)
  - Any other legit user with the same chipset would be affected
- In order to really counter attack the 802.11 spec would need to be re-written to protect frame headers and/or introduce mutation based authentication on packets
  - Up to IEEE, not likely for the time being

WIRELESS AUDITING ACTIVITIES AND PROCEDURES

Keep in mind

- When you or a business have a wireless network auditing is needed to verify integrity and wireless exposure of the network
  - Compatible with OSSTMM-based security test
- Attackers don’t need to keep in mind wireless policies
  - Auditors and white-hat hackers do

Auditing Wireless Policies

- A security policy is critical for managing a companies security
  - Often the most neglected area of an organizations
- Some companies believe they don't need one if they don't have a wireless network, wrong
- Users that plug rogue AP device can create wireless networks that act as the companies network
  - Can fool users and cause damage

Auditing Wireless Policies

- Other non-AP devices may be introduced that would require an wireless security policy, ex.
  - wireless-enabled laptops
  - PDAs
  - handphones
- Some users may bring their own devices creating hotspots and cause security holes in a network with no security policy
- Auditing is required to enforce rules

Auditing Wireless Policies

- Auditing policy should expand into:
  - Access policy
  - Authentication policy
  - Accountability policy
  - Availability
  - System and network maintenance policy
  - Acquisition guidelines
  - Violations reporting
  - Audit policy

Assembling a Linux-based Auditing/Hacking Platform

- Common software and hardware:
  - Wireless Sniffers
  - Wireless Frame Injectors
  - WEP/WPA-PSK Crackers
  - Wireless MITM
  - Wireless Client Auditing
  - Wireless Fuzzers
  - Wireless Fingerprinting
  - Specialized Wireless Auditing LiveCD Toolkit

Wireless Sniffers

- Come under two categories
  - Passive Sniffer
    - Does not send any kind of data to WNIC
    - Picks-up wireless frames when WNIC is broadcasting in RFMON mode
  - Probing Sniffer
    - Sends our data to WNIC in probe request
    - Used when trying to find out APs in area
    - Needed when you need to find out information about AP
- Common wireless sniffers on Linux include
  - **Kismet**, **Airodump-ng**, and **Prismstumbler**

Wireless Frame Injectors

- Allows an attacker to customize frames to cause dissociation from the network
- Creates frames that can be used in any situation with 802.11
- Can fool users into thinking they are accessing a legitimate access point
- Used in with frame analysis

WEP/WPA-PSK Crackers

- Tools used to crack WEP and WPA-PSK encryption
- WEP Attack
  - Attack happens by capturing enough WEP encrypted data frames so tools can find a pattern
- WPA-PSK Attack
  - Uses Password-Based Key Derivation Function v2.0 (PBKDF2) math formula to break encryption
- Tools include
  - **WEPCrack**, **Airsnort**, **Aircrack-ptw**, and **Aircrack-ng**
  - **Cowpatty**, **Aircrack-ng v0.7** (For WPA-PSK)

Wireless MITM

- A tool that establishes a man-in-the-middle attack
- Sets up the wireless chipset to master mode
- Forms a DHCP server, an HTTP server, and a DNS server on the attackers computer so that the clients think they are accessing a legitimate AP
- Directs traffic through to a legitimate network, but the attacker simultaneously sniffs all of their data

Wireless Client Auditing

- Many devices that have WNIC (laptops, phones, etc..) have wireless chipsets that are left on
  - Attackers can use tools to trick client device into connecting to them
  - Assuming the client is connected to the wired network as well the Attacker now uses the established wireless network to the client device to bridge them to the connected wired network
- Tools:
  - **Probemapper**, **Karma**, and **Hotspotter**

Wireless Fuzzers

- Tools that generate a series of wireless frames and throw them at wireless devices at a configurable speed and quantity
- Used to test wireless drivers found in Linux Kernel
- Tools:
  - **Fuzz-e**, part of the Airbase package

Wireless Fingerprinting

- Tool used to remotely find make and model of WNIC
- Traditionally auditors attempt to guess make and model of wireless device by using the device's MAC address
  - Unreliable since MAC can be spoofed
- Tools:
  - **Jc-duration-printer**
- Note:
  - New technology, still not proven

Specialized Wireless Auditing LiveCD Toolkit

- Compresses the entirety of the Linux operating system and environment into a single disc media
- Allows for a “live” instance of linux that can be loaded onto a Windows machine and run wireless auditing tools
- This can be used with versions of Linux that are specifically designed for frame-injection and wireless auditing

Defending Against Auditing & Hacking Platform Assembly

- It's impossible to completely defend against hacking and auditing tools
- Anyone is free to create auditing and hacking tools
  - Nothing inherently wrong with those
- Creating laws to make it illegal to create auditing and hacking tools won't do much and would hurt white hat hackers
  - Countries have tried (ie. Germany)

Wireless Infrastructure Auditing

There are various technical activities for auditing wireless infrastructure:

- RF spectrum analysis
- Wireless infrastructure device identification
- Cracking encryption
- Layer 3 connectivity testing
- RF propagation boundaries
- DoS/hijacking

RF Spectrum Analysis

- You can use RF Spectrum Analysis to identify RF signals outside of your normal operating range
- Ex. If a company operates APs on Channels 1, 6, & 11 and during an audit notice RF signals that operate on Channel 13 & 14 an attacker might be running a rogue AP on the network that most WNIC would not see due to operating out of range
    - Also running on channel 13 & 14 violates FCC rules

Wireless Infrastructure Device Identification

- Identify devices by analyzing layer 2 information
  - Ex. Use a tool like **Kismet** & **Airodump-ng**
- **Kismet** can
  - Detect wireless networks (802.11/a/b/g)
  - Sniff traffic
  - Offers limited intrusion detection capabilities
  - Works with an WNIC supporting raw RF monitoring (RFMON)

Wireless Infrastructure Device Identification (cont.)

- Using tools like **Kismet** you can find information like:
  - SSID (ESSID)
  - BSSID (MAC-48 convention ID)
  - RF Channel
  - Supported Rates
  - Wireless clients connected

Cracking Encryption

- Multiple methods and tools exists to crack WEP/WPA/WPA2
- **Airsnort** & **Dwepcrack**
  - First generation WEP crackers work by capturing millions of packets to find patterns
- **Aircrack-ng**
  - Second generation WEP crackers that only require capturing a few hundred packets to find patterns
- **Aireply-ng**
  - Used to inject packets into connection to crack encryption

Cracking Encryption (cont.)

- **Airdecap-ng**
  - Decrypts WEP/WPA capture files (.cap)
- **Packetforge-ng**
  - Used to forge wireless frames

Cracking Encryption (cont.)

- WPA made cracking wireless encryption slightly harder but was more of a patch for really weak WEP
  - Improved WEP by using Temporal Key Integrity Protocol (TKIP)
  - Added 802.1x access control mechanism
  - Extensible Authentication Protocol (EAP)
- WPA2 was much stronger
  - Implemented 802.11i spec
  - Introduced AES-based algorithm
  - Counter-mode
  - CBC-MAC Protocol (CCMP)

Cracking Encryption (cont.)

- WPA-Enterprise offers more protection by using authentication server
- WPA-PSK offer more protection by using pre-shared key

Not in the book:

- WPA2 was recently exploited (Oct. 2017) using KRACK , WPA3 in the works

Layer 3 Connectivity Testing

- A number of tools and methods exists to get your device on a network and find other clients to attack
- Auditors can bypass MAC filtering on APs by using existing “allowed” wireless clients connected to AP
  - Tools: **Airodump-ng** and **Probemapper** scan for currently “allowed” clients connected to AP that you as an auditor can use
- Auditors can obtain a “legit” IP addresses by capturing data frames using tools like **Wireshark** and/or **Tcpdump** to determine a range of IP addresses the network uses
  - Note: Assuming network is unencrypted or cracked

Layer 3 Connectivity Testing (cont.)

- Once on the network uses tools like **Nmap** to scan for open ports to potential services which can be compromised

RF Propagation Boundaries

- Audit used to determine the range RF signals reach from an AP
- Might seem simple and pointless, however, limiting the range an AP broadcast can help secure network
  - If attacker needs to be close enough to network then those operating the network might visually see threat
  - Can also be helpful when trying to create a timeline of a suspected wireless intrusion and determining time & place of attack

Denial of Service/Hijacking

- Can occur on several layers of the wireless protocol
- RF jamming
  - Type of DoS by sending more powerful RF signal that drowns out other wireless signals
- Protocol DoS / Layer 2 DoS
  - Edit management and control frames sent to client, causing client to loss connection
    - Most clients don't validate management and control frames and sending packets that seems to come from a legit AP with request to disconnect can trick the client into disconnecting from the AP (Use **WLAN-Jack** & **Aireplay-ng** to do this)

Denial of Service/Hijacking (cont.)

- Flooding
  - Flood AP with fake clients, making it impossible for real clients to connect; Tools: **File2air**, **Void11**, **MDK2**, and **MDK3**
- Evil Twin (ph00ling)
  - Client connects to fake AP thinking it's the real AP, Tools: **Airsnarf**
  - Or manually by
    - Setting WNIC in master mode
    - Configuring a HTTPD server to serve pages matching the captive portal of the spoofed service
    - Establishing a DHCPD and DNS server so the victim receives the IP address attack chooses for them

Practical Wireless Deployment Methodology (PWDM)

1. Deployment analysis
2. Contractual negotiation
3. Deployment tactical planning
4. Deployment procedural rollout
5. Supporting infrastructure rollout
6. AP security issues
7. Layer 3 mitigation strategies
8. Gateway management
9. Management overlay issues
10. UAT and commissioning

PWDN is designed to help any size organization deploying a WLAN to consistently and effectively by following a series of steps that cover many aspects of WLAN and WLAN security.

More at http://pwdm.net

Using Linux to Deliver Secure Wireless Infrastructure Devices

Wireless Access Point

- You can DIY your own AP
  - Offers more customization and control
- 3 Solutions
  - **Hostapd**
    - Software only solution
  - **OpenWRT/DD-WRT**
    - Extends existing hardware like the Linksys WRT Router
  - Combined Stack
    - Mix software solutions like **Soekris**, **PC Engine WRAP Board, Pyramid Linux** and a variety of other Linux based router software to enable existing or new chipsets

Authentication Server

- Linux offers software solutions like **FreeRADIUS** to add backend authentication server to WPA/WPA2

Captive Portal

- Captive Portals offer business, or anyone running an AP to regulate access with their AP either by requiring authentication or accepting terms and usage rules.
- Linux offers Free Software solutions like **wifidog** and **NoCatAuth** to implement on Linux based APs.

Wireless Intrusion Detection System (WIDS)

- Wireless IDS work like regular IDS but, well… for wireless
- WIDS requires more tools that can cover
  - Attacks using deauthentication packet floods
  - Detecting fake APs & captive portals
- Free Software solutions for IDS/WIDS are:
  - **Snort**
  - **Snort-Wireless**
    - Simply setup a Linux machine with a wireless card in RFMON mode and start using Snort
  - **Kismet Wireless**
  - **WIDZ**

Incident Response Kit

- Use Linux laptops with various tools during a incident response to find rogue AP
  - **wavemon**
    - Terminal (ncurses-based) wireless network monitor
  - **probemapper**
    - Map network based on strength of AP and physical barriers
- Other tools
  - OSWA-Assistant
    - Wireless auditing toolkit
  - Iperf
    - Wireless network performance monitoring tool

Wireless Client Auditing (Steps)

- Wireless client fingerprinting
  - Determine the wireless chipset & driver
  - Use information to harden known vulnerabilities
- Wireless client profiling
  - Identify the various wireless clients that are sending data
  - Helps to find gaps in network policies for connecting clients
- Wireless client connect
  - Verify all connecting clients are following network policies set in place

Ending Notes

1. Everything can be hacked
2. Everything should be secured
3. Everything should be audited