tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com

https://www.facebook.com/tutorialspointindia

https://twitter.com/tutorialspoint

About the Tutorial

Wireless security is nothing but protecting computers, smartphones, tablets, laptops and other portable devices along with the networks they are connected to, from threats and vulnerabilities associated with wireless computing.

This is an introductory tutorial that covers the basics of Wireless Security and how to deal with its various modules and sub-modules.

Audience

This tutorial will be extremely useful for professionals who aim to understand the basics of Wireless Security and implement it in practice. It is especially going to help specialists like network engineers, database managers, analysts, programmers and other such professionals who are mainly responsible for applying appropriate countermeasures to secure devices and applications.

Prerequisites

It is a fundamental tutorial and you can easily understand the concepts explained here with a basic knowledge of how to secure your applications of devices from any external threat. However, it will help if you have some prior exposure to various security protocols dealing with computers, applications, and other related devices.

Copyright & Disclaimer

Table of Contents

Wireless Security – Basics

1. Wireless Concepts

In this tutorial, you will be taken on a journey through different methods of wireless communication. You will learn about **Wireless Local Area Network** (WLAN) as most of us know it, and then go deeper into the practical aspects behind wireless security. You will be amazed at how easy it is to collect a lot of sensitive information about wireless network and the data flowing through it, using basic tools that are easily available for anyone who knows how to use it.

Before we go deeper into the **"hacking"** side of the wireless communication, you will need to go through a plethora of theoretical concepts and diagrams of normal wireless system operation. Nevertheless, theoretical content will be kept to absolutely minimum throughout this Tutorial - it is the practical side of the things that is most encouraging and the most enjoyable part for everyone!

When we think about wireless communication, we imagine some systems connected to antennas that speak together over the air using radio waves that are invisible to human eye. Honestly speaking, this is perfectly a true definition, but in order to break things (or rather you prefer the word "hack") you need to learn how all those concepts and architectures work together.

Wireless Terminologies

First, let's go through the bunch of basic terms, related to wireless communication. Progressively, we will get into more advanced stuff going all along this path together.

Wireless Communication

Wireless communication refers to any type of data exchange between the parties that is performed wirelessly (over the air). This definition is extremely wide, since it may correspond to many types of wireless technologies, like:

- Wi-Fi Network Communication
- Bluetooth Communication
- Satellite Communication
- Mobile Communication

All the technologies mentioned above use different communication architecture, however they all share the same "Wireless Medium" capability.

Wi-Fi

Wireless Fidelity (Wi-Fi) refers to wireless local area network, as we all know them. It is based on **IEEE 802.11** standard. Wi-Fi is a type of wireless network you meet almost everywhere, at your home, workplace, in hotels, restaurants and even in taxis, trains or planes. These 802.11 communication standards operate on either **2.4 GHz or 5 GHz ISM radio bands**.

These devices are easily available in the shops that are compatible with Wi-Fi standard, they have following image visible on the device itself. I bet you have seen it hundreds of times in various shops or other public places!

Due to the fact, that 802.11 based wireless network are so heavily used in all types of environments - they are also the biggest subject for various security researches across other 802.11 standards.

Wireless Clients

Wireless clients are considered to be any end-devices with a wireless card or wireless adapter installed. Now, in this 21st century, those devices can be almost anything:

- **Modern Smartphones** – These are one of the most universally used wireless devices you see in the market. They support multiple wireless standards on one box, for example, Bluetooth, Wi-Fi, GSM.
- **Laptops** – These are a type of device which we all use every single day!
- **Smartwatch** – An example of Sony based smartwatch is shown here. It can synchronize with your smartphone via a Bluetooth.

- **Smart-home Equipment** - With the current progress of the technology, smart-home equipment might be for example a freezer that you can control over Wi-Fi or a temperature controller.

The list of possible client devices is growing every single day. It sounds a little scary that all of those devices/utilities we use on a daily basis can be controlled via a wireless network so easily. But at the same time, remember that all the communication flowing through a wireless medium can be intercepted by anyone who is just standing at the right place at the right time.

2. Access Point

Access Point (AP) is the central node in 802.11 wireless implementations. It is the interface between wired and wireless network, that all the wireless clients associate to and exchange data with.

For a home environment, most often you have a router, a switch, and an AP embedded in one box, making it really usable for this purpose.

Base Transceiver Station

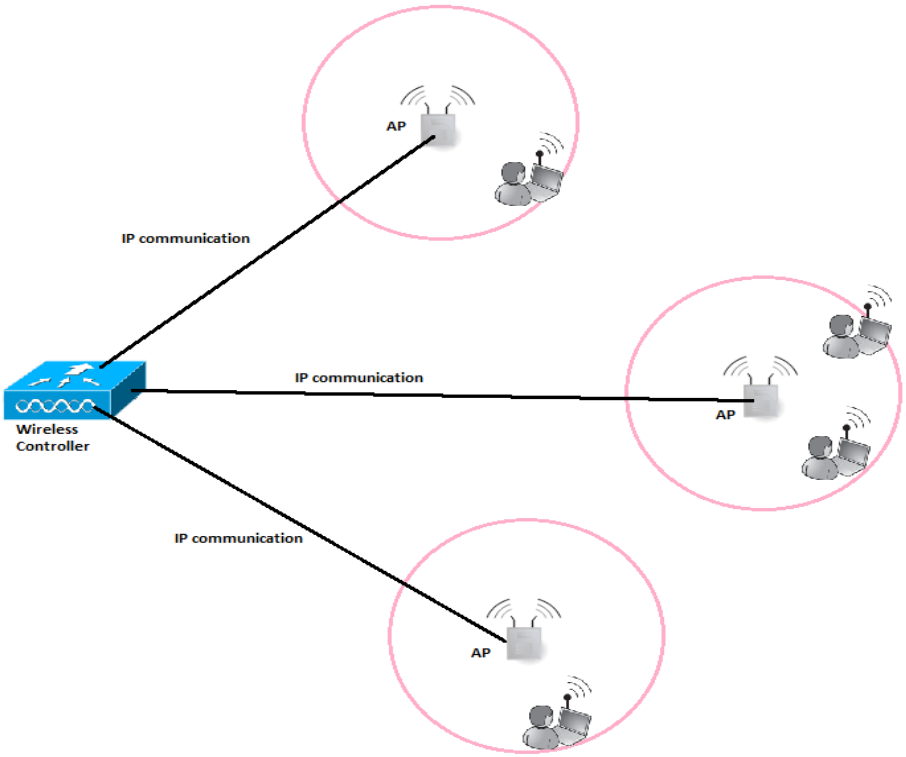
Base Transceiver Station (BTS) is the equivalent of an Access Point from 802.11 world, but used by mobile operators to provide a signal coverage, ex. 3G, GSM etc...

***Note**: The content of this tutorial concentrates on the 802.11 wireless networking, therefore any additional information about BTS, and mobile communication in more detail, would not be included.*

Wireless Controller (WLC)

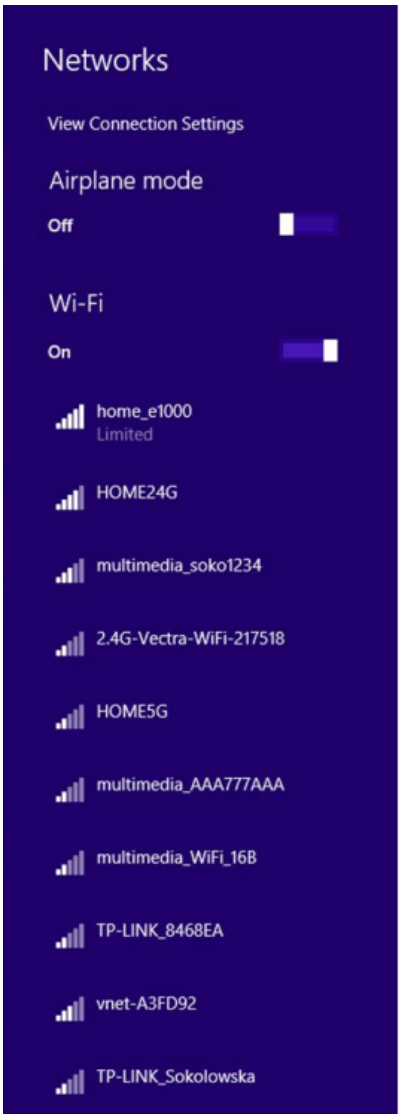
In corporate wireless implementation, the number of Access Points is often counted in hundreds or thousands of units. It would not be administratively possible to manage all the AP's and their configuration (channel assignments, optimal output power, roaming configuration, creation of SSID on each and every AP, etc.) separately.

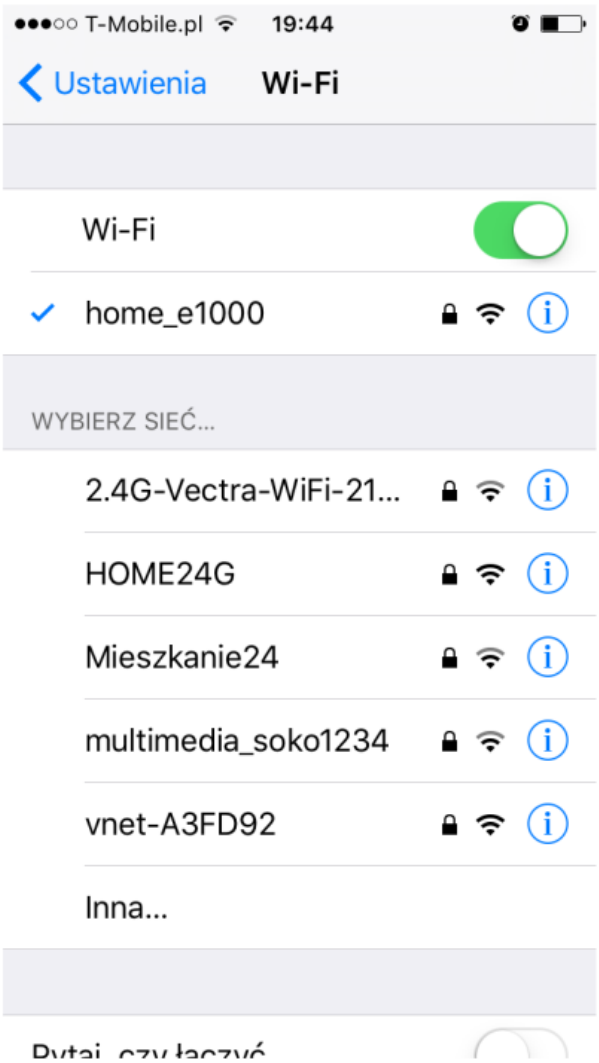
This is the situation, where the concept of wireless controller comes into play. It is the "Mastermind" behind all the wireless network operation. This centralized server which has the IP connectivity to all the AP's on the network making it easy to manage all of them globally from the single management platform, push configuration templates, monitor users from all the AP's in real time and so on.



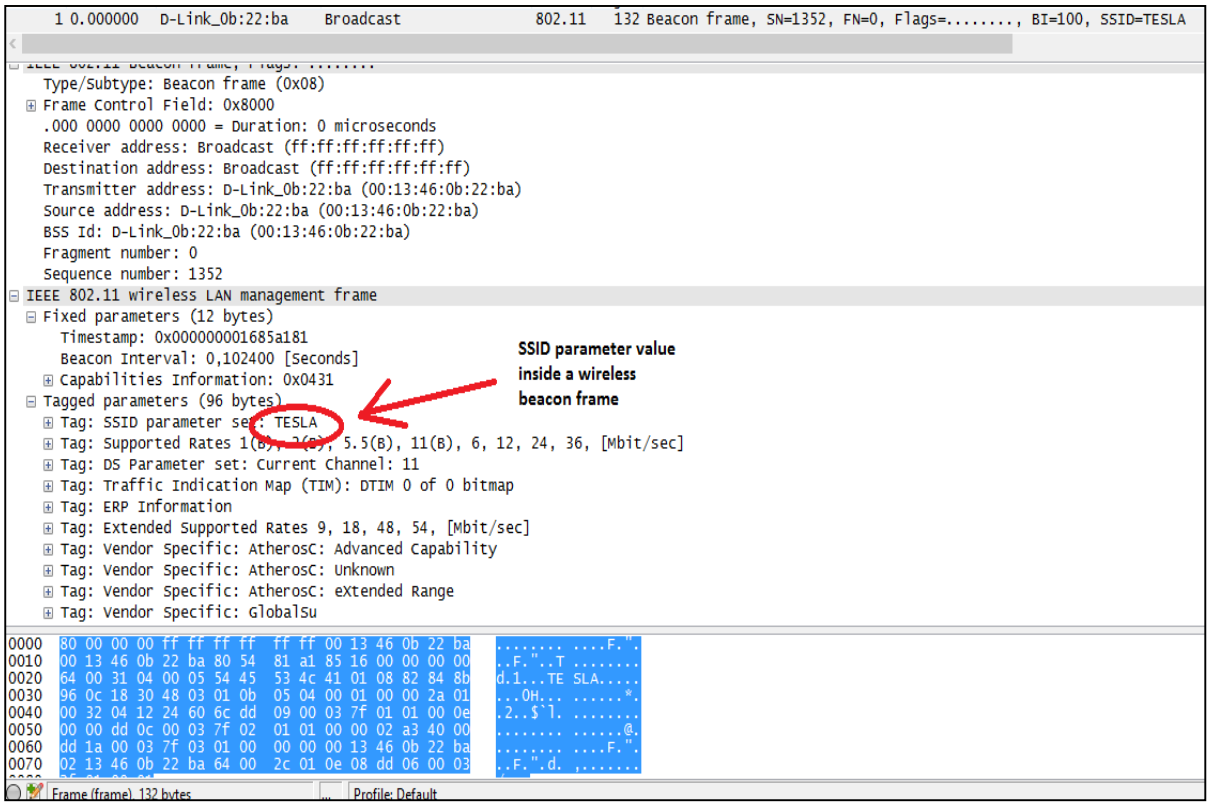
Service Set Identifier (SSID)

SSID directly identifies the wireless WLAN itself. In order to connect to Wireless LAN, the wireless client needs to send the same exact SSID in the association frame as the SSID name, preconfigured on the AP. So the question now arises how to find out which SSIDs are present in your environment? That is easy as all the operating systems come with a built-in wireless client that scans wireless spectrum for the wireless networks to join (as shows below). I am sure you have done this process several times in your daily routine.





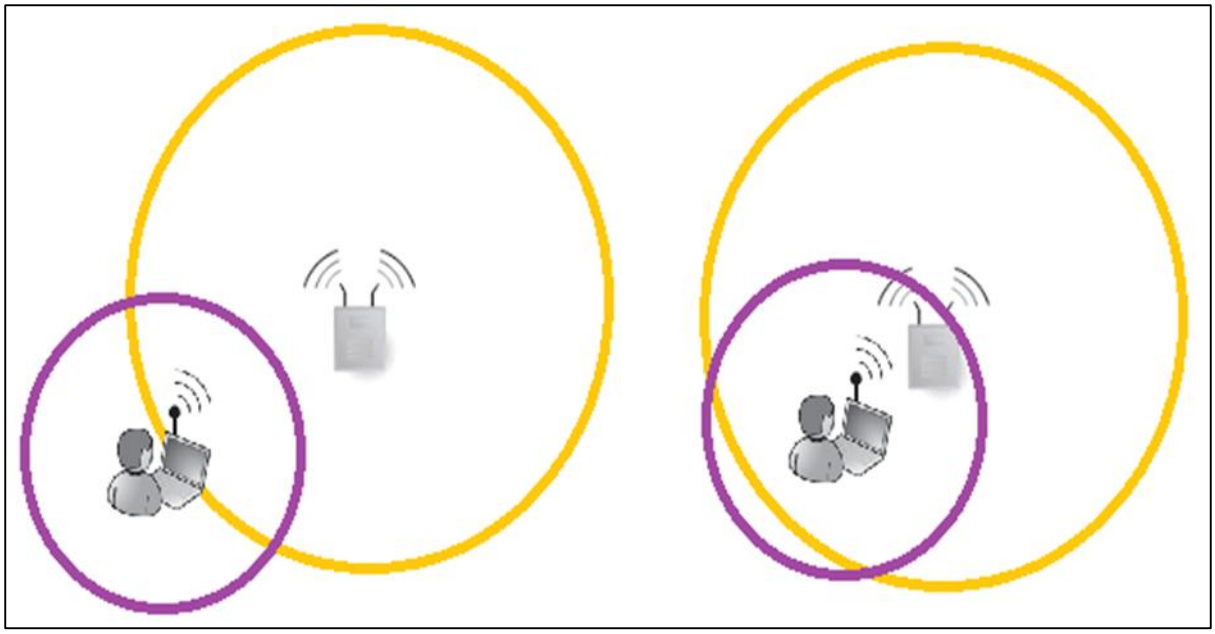
But, how those devices know that specific wireless network is named in that particular way just by listening to radio magnetic waves? It is because one of the fields in a beacon frame (that APs transmit all the time in very short time intervals) contains a name of the SSID always in clear text, which is the whole theory about this.



SSID can have a length of up to 32 alphanumeric characters and uniquely identifies a particular WLAN broadcasted by the AP. In case, when the AP has multiple SSIDs defined, it will then send a separate beacon frame for each SSID.

Cell

A **cell** is basically a geographical region covered by the AP's or BTS's antenna (transmitter). In the following image, a cell is marked with a yellow line.



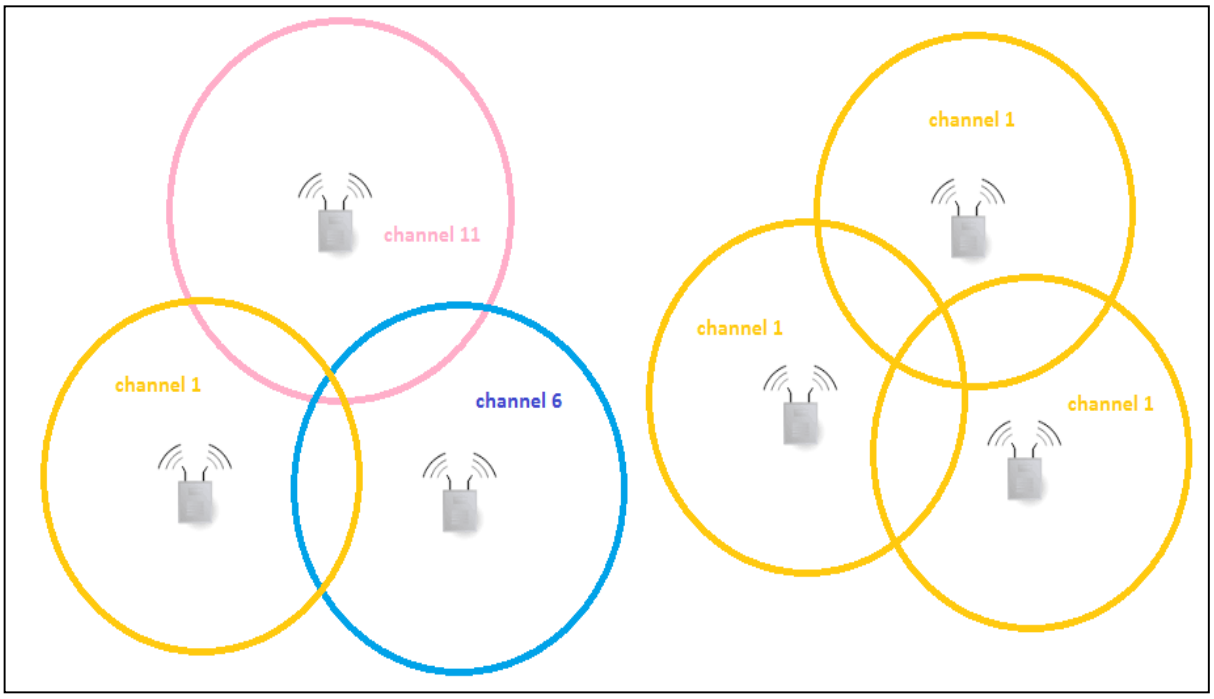
Most often, an AP has much more output power, when compared it with the capabilities of the antenna built-in into the client device. The fact that, the client can receive frames transmitted from the AP, does not mean that a 2-way communication can be established. The above picture perfectly shows that situation. - In both situations, a client can hear AP's frames, but only in the second situation, the 2-way communication can be established.

The outcome from this short example is that, when designing the wireless cell sizes, one has to take into account, what is the average output transmitting power of the antennas that clients will use.

Channel

Wireless Networks may be configured to support multiple 802.11 standards. Some of them operate on the 2.4GHz band (example are: 802.11b/g/n) and other ones on the 5GHz band (example: 802.11a/n/ac).

Depending on the band, there is a predefined set of sub-bands defined for each channel. In environments with multiple APs placed in the same physical area, the smart channel assignment is used in order to avoid collisions (collisions of the frames transmitted on exactly the same frequency from multiple sources at the same time).



Let's have a look at the theoretical design of the 802.11b network with 3 cells, adjacent to each other as shown in the above picture. Design on the left is composed of 3 non-overlapping channels - it means that frames sent by APs and its clients in particular cell, will not interfere with communication in other cells. On the right, we have a completely opposite situation, all the frames flying around on the same channel leads to collisions and degrade the wireless performance significantly.

Antennas

Antennas are used to "translate" information flowing as an electrical signal inside the cable and into the electromagnetic field, which is used to transmit the frame over a wireless medium.

Every wireless device (either AP or any type of wireless client device) has an antenna that includes a transmitter and the receiver module. It can be external and visible to everyone around or built-in, as most of the laptops or smartphones nowadays have.

For wireless security testing or penetration tests of the wireless networks, external antenna is one of the most important tools. You should get one of them, if you want to go into this field! One of the biggest advantages of external antennas (comparing to most of the internal antennas you might meet built-in to the equipment), is that they can be configured in a so-called "monitor mode" - this is definitely something you need! It allows you to sniff the wireless traffic from your PC using **wireshark** or other well-known tools like **Kismet**.

There is a very good article on the internet (https://www.raymond.cc/blog/best-compatible-usb-wireless-adapter-for-backtrack-5-and-aircrack-ng/) that helps with the choice of the external wireless antenna, especially for Kali Linux that has monitor mode capabilities. If you are seriously considering going into this field of technology, I really recommend all of you to purchase one of the recommended ones (I have one of them).

End of ebook preview

If you liked what you saw…

Buy it from our store @ https://store.tutorialspoint.com