**Wireless Network Attacks**

***Table of Contents Pages***

*Introduction………………………………………….(1-3)*

*Wireless Network Attacks…………………………...(3-4)*

*Rogue Access Point…………………………(3-4)*

*Wireless Evil Twins…………………………(4)*

*Wardriving……………………………………(4)*

*Citations*

Daniel Rao

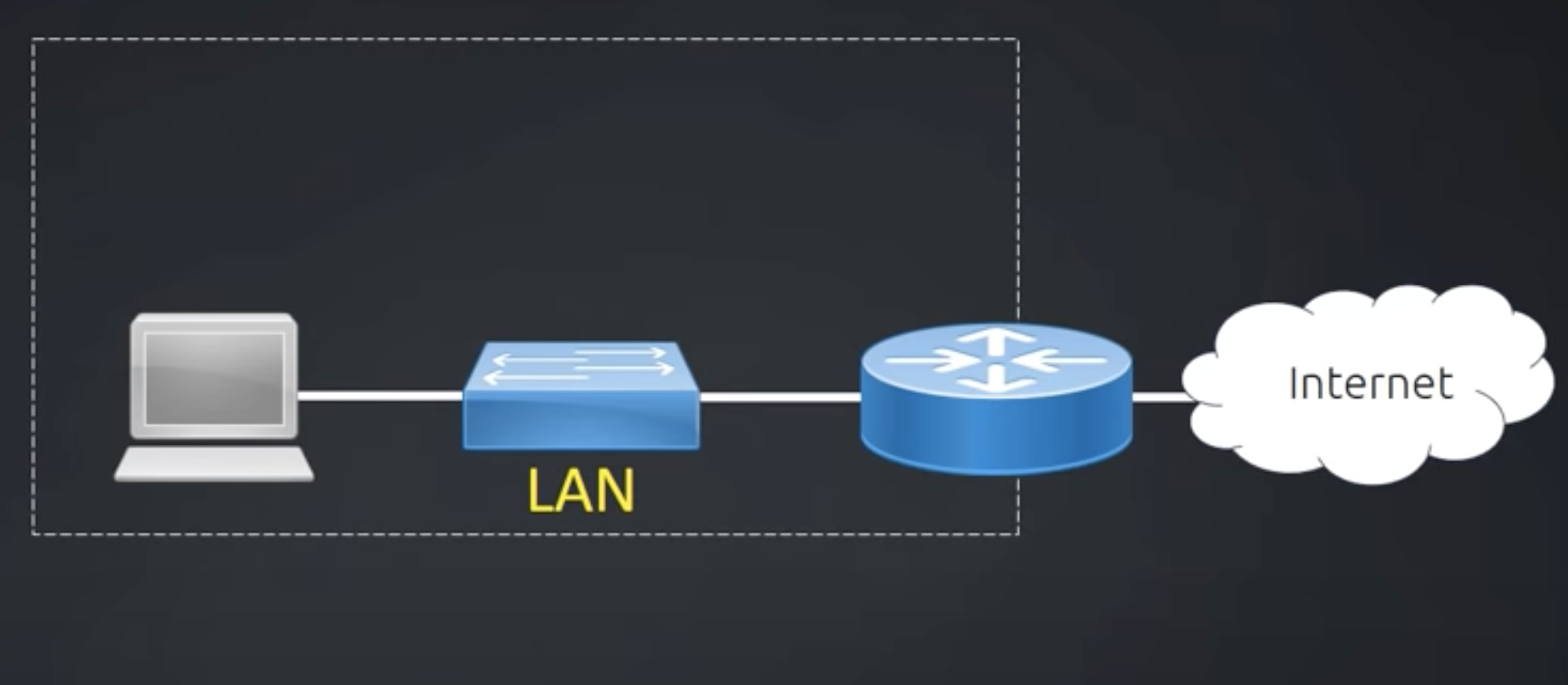
April 4th, 2021

Vince Skinner

**Introduction**

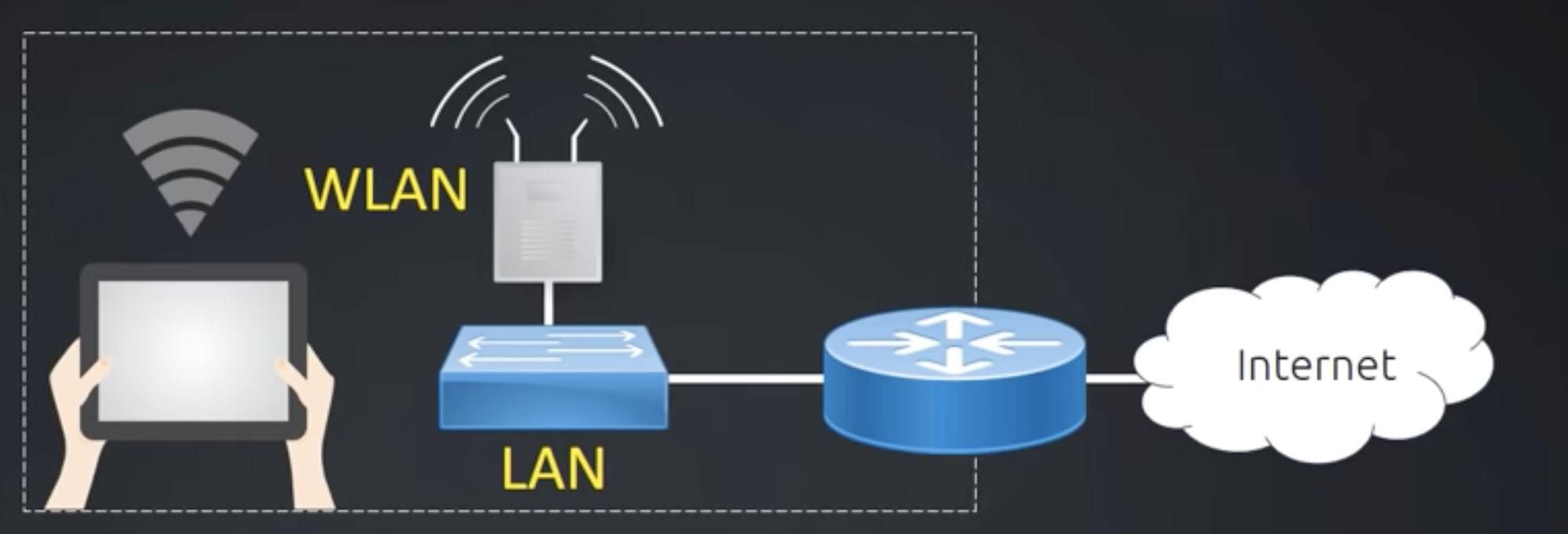
The term wireless is generally used to describe equipment and Technologies operating in the radio frequency spectrum between 3 hertz and 300 gigahertz. Some of the most common examples of Wireless Technologies are AM/FM radio, Wireless networking devices such as cell phones, and radar systems. With the Boost in technology, these devices continue to grow and become more popular which as a result it has become much more important to secure these wireless devices from attacks.

As regular computer users, we have most likely used Wireless Access Point before. Before understanding wireless access point we must first understand what traditional wired networks are and that's where are wireless access points go so for that I have a diagram that has been provided below:



In the above diagram we have a host computer that's wired into a hardwired switch, which itself is wired to the router which provides access to the internet. In simple words this describes a wired connection, which is also called LAN ( local area network).

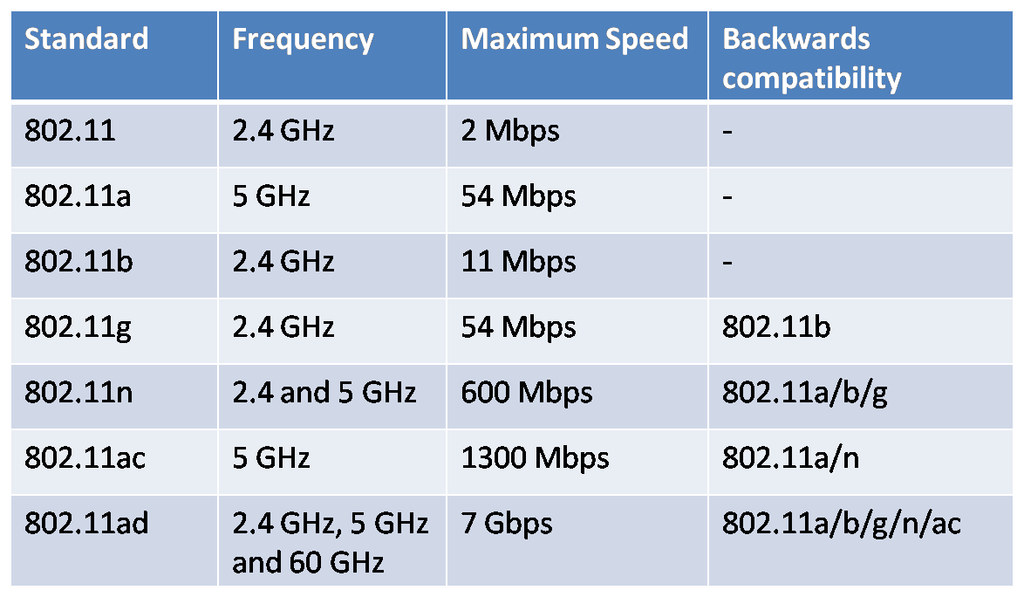
Now the question is what if we had a house that needed to access the network wirelessly? well then we need a specific type of device which is called an access point or a wireless AP, also known as WAP (wireless Access Point).



Most of the common small office/ home office routers come with a built-in Wireless connectivity. So the device we have in our house is usually a combo device with a router and a switch and a wireless access point. whenever we install a wireless AP, without realizing we have created W WLAN also known as wireless local area network.

not most Wireless LANs fall under the standard 802.11. There are several flavors of 802. 11 that represents different speed, different bandwidth and things like different data rates.

These are given as follows:



**Wireless Network Attacks**

In this paper I am going to discuss a few ways through which a wireless network can be attacked and exploited, with some of the real life scenario:

**Rogue Access Point**

These are significant Potential backdoors with a huge security concern. These are very easy to plug in anywhere in the building without really having to configure anything extra. The attackers will have access to the internal network thereby bypassing any security controls on the inside or outside of the network. This is why we would probably want to do regular walk around building/campus or floors. One must consider using 802.1X also known as Network Access Control where the user must authenticate, regardless of any connection type and since rouge access point will not be able to authenticate. The rogue access point strategy becomes useless.

**Wireless evil Twins**

This is another dangerous attack to look out for. This attack doesn't really require a lot of resources. Here an attacker needs to buy a wireless access point oftentimes which costs less than $100 US and is configured the exact same way as an existing network which implies that same SSID and same security settings. The device must over power the existing access points which in turns the following devices will try to connect to the attackers access point which may not even require the same physical location. One way to defend against this type of attack would be to use HTTPS and VPN which is using private tunnels to protect the data going across the internet via the attackers access point. This will lead to no one being able to understand the traffic being generated by the victim.

**Wardriving**

Wardriving is as simple as it sounds which combines with Wifif monitoring and a GPS .The attacker must simply hop in the car and drive around to collect huge amount of intel in a short period of time and with surprising results such as what Access Point are open, or which ones are close, or what their SSID might be or even what type of encryption is being used on the network. There are several tools that can be used to conduct this kind of research such as: Kismet, inSSIDer, Wireless Geographic Logging Engine.

**Citations**<https://www.computerworld.com/article/2577244/top-10-vulnerabilities-in-today-s-wi-fi-networks.html>

<https://www.pandasecurity.com/en/mediacenter/security/wardriving/>