activity-label-stu-ngr-med 1.7 Network attacks

Network attacks

Each layer and protocol exposes information and functionality. Seemingly secure functionality at layer 2 could enable attacks at layer 3. Sophisticated attacks often exploit multiple layers. Let’s look at some examples of attacks.

Jamming

A **jamming attack** is an attack in which malicious nodes block legitimate communication by causing intentional interference in networks. The link layer is typically broadcast-based and only one user can talk at a time. The jamming attack works by hogging the broadcast medium so no one can talk. It’s done most easily on ethernet or Wi-Fi.

You can see, in the picture, what a portable jammer looks like. It works for Wi-Fi and 3G/4G networks. It has a range of about 5–20 meters, and costs between £100 and £200.

Sniffing

A **sniffing attack,** or a sniffer attack, is a theft or interception of data. It works by capturing the network traffic using a sniffer which is an application aimed at capturing network packets. When data are transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer. Using a sniffer application, an attacker can analyse the network and gain information to eventually cause the network to crash or to become corrupted, or read the communications happening across the network.

You might remember that in some movies law agencies and criminals used to bug the telephone lines to hear the calls that a person receives in order to get some information. This is a perfect example of sniffing attacks. This technology can be used to test the telephone lines and determine the quality of the call but criminals used it for their own illegitimate purpose.

View transcript

Hi, in this video we are going to take a look at a network attack called ‘sniffing’, which is a theft or interception of data.

We are going to have a look at an example from *Mr Robot*.
This clip from *Mr Robot*, season 1, episode 6, shows us a sniffing attack.
Let's give a look at it.

[From the clip, Elliot speaking:] 'I need 30 to 40 seconds from the patrol car’s Bluetooth connection to run the exploit on the PLC'.

Elliot, the hacker that is talking, aims to get into the police network infrastructure through the laptop in the patrol car in order to upload a malicious code. In order to get access to the police infrastructure, he is performing a sniffing attack on the Bluetooth network that the patrol's laptop has.

Here it is possible to see three terminal windows. Let's focus for a moment on the window on the right.
Here, Elliot activates the Bluetooth device and checks to see if it is actually working, as well as its properties.

Let's now focus on the windows on the bottom left. Here, you can see that he is using ‘hcitool’, a built-in Bluetooth configuration tool in Kali Linux used to scan for Bluetooth connections.

Now, let's check the window on the top left of the screen. Although the ‘bluesniff’ tool is real, it actually just discovers Bluetooth devices, which Elliot already did with ‘hcitool’.
If you look closely at the commands used here, it’s apparent that Elliot is actually using a real tool called ‘csr_sniffer’. Csr_sniffer isn’t used to spoof keyboards. Rather it is used to ‘sniff’ Bluetooth communications, with the hope that you can catch the pairing process, and later crack the PIN used to secure devices. Catching this pairing process is very unlikely, as it usually only happens once. In short, the tools shown in the background during this

Bluetooth hack would not allow Elliot to ‘force’ his virtual keyboard to connect to the police car computer. In fact, to be more realistic, Kali Linux has a tool designed to spoof Bluetooth devices called ‘spooftooph’.

But, let’s assume Elliot could do this. The FTP portion of this attack is legit. Often, when attackers first spawn a PC, they’ll use FTP to quickly download their favourite tools and scripts to load onto the victim’s computers and start lateral attacks. Seeing Elliot download his ‘PLCpackage.exe’ makes sense.

However, at this point, the attack becomes very abstract since it would require a much more complicated procedure to really execute what Elliot wants to do, but for us, the interesting part was the Bluetooth sniffing procedure.

However, at this point, the attack becomes very abstract since it would require a much more complicated procedure to really execute what Elliot wants to do, but for us, the interesting part was the Bluetooth sniffing procedure.

This is just a glimpse of a practical way to perform a sniffing attack, so if you are more curious about this type of attack in practice, I encourage you to investigate more about it, especially in wifi and wired networks.

[From the clip, Elliot speaking:] ‘About the exploit, drive. Darlene is no longer part of the plan.'

In the world of the Internet, sniffing can be performed using an application or hardware devices at both the network and host level. Any network packet having information in plain text can be intercepted and read by the attackers. This information can be usernames, passwords, secret codes, banking details or any information which is of value to the attacker. This attack is just the technical equivalent of a physical spy. Sniffing can also have a benign purpose as it is very useful for network debugging and diagnostics.

Spoofing

A **spoofing attack** is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. It is necessary to understand what our identity is inside the network. If we consider the Internet, we are an IP address. If we consider a LAN, a smaller and local network, we are a MAC address.

What is an IP Address?

View answer

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network, eg 208.80.154.224.

An IP address serves two principal functions. It identifies the host, or more specifically its network interface, and it provides the location of the host in the network, and thus the capability of establishing a path to that host. Its role has been characterised as follows: ‘A name indicates what we seek. An address indicates where it is. A route indicates how to get there.’

What is a MAC Address?

View answer

A Media Access Control address (MAC address) is a unique identifier physically embedded inside a network interface card (eg, the network card, the Wi-Fi card, the Bluetooth card) for use as a network address in communications, eg 00:0a:95:9d:68:16.

There are several different types of spoofing attacks that malicious parties can use to accomplish this. Some of the most common methods include IP address spoofing attacks, ARP spoofing attacks and DNS server spoofing attacks. Spoofing forms the basis of a lot of attacks because it is very easy to change your address.

Hijacking

Hijacking is a type of network security attack in which the attacker takes control of a communication between two entities, similarly to an aeroplane hijacker taking control of a flight. For instance, a session hijacking attack involves an attacker intercepting packets between two components and taking control of the session between them by inserting their own packet.

Poisoning

We refer to **poisoning** as a way to contaminate some source of information that we usually believe is good. Later on in the module, we are going to see ARP poisoning and DNS cache poisoning.

Each type of attack can be linked to one of the security principles.

Sniffing attacks the confidentiality of the communication, since it corresponds to theft or interception of data by capturing the network traffic. A potential solution for sniffing is using cryptography to encrypt the communication.

Spoofing and poisoning attack the integrity. The goal of a poisoning attack is to change something. A spoofing attack also attacks integrity, since it pretends to be someone else. In order to protect the integrity, we can leverage using keys to sign what we want to protect. In case of alteration, we would be able to discover that our data were tampered with.

A jamming attack compromises the availability of the communication channel, creating noise to make the communication impossible. Policies are a measure to help protect against jamming attacks, restricting what the users can do in the communication channels.

Of course, the above solutions are not always feasible and often we need to balance the practicality, cost and importance of the data we want to protect.

Off-path vs on-path attackers

Finally, here is a useful distinction between two different types of attack: on-path and off-path. On-path means the attacker is operating within the same network. Off-path means they are attacking from outside the network. On-path attacks are much more powerful as it is very difficult to insert false data off-path.

There was a lot of terminology introduced in these opening sections. Take your time to review the definitions as they are used throughout the module.