The advent of Wireless devices has caused a huge increase of the size of any given network. The ease of use, and less dependence on wire are few of the many advantages, that the Wireless technology bring in. However, this technology must be used carefully.

Many organizations are using Wireless Access Points to provide more flexibility, and so to speak “roaming” facility, to the users within the organization. The users, which may be an ordinary programmer, or the CEO, are enjoying the flexibility of sitting anywhere within the building, and yet remain connected to the network. The same is more useful, when there is a meeting or a training session, and all of a sudden there is a need of 20+ network connections. When wireless is being used, you don't worry about 2 or 20 or 200, as there is no wired connection needed. (The only worry is availability of enough bandwidth, of-course).

This flexibility and availability can easily become a security hazard when not used correctly. In a wired network, you normally have only enough connections available to satisfy the needs of the total number of PCs in your network. In case some cracker wants to connect to your network and want to sniff, or steal your data, then he has to be physically connected to the network. Physical connection has it's dangers, as the cracker has to be very close, normally inside the building, and may need to unplug the network cable from a PC to connect his laptop, etc. Crackers normally refrain from attempting any crimes in such networks. Or, the type and approach of attacks on these networks are different.

In case a wireless access point (WAP) exists in the network, then the attacker does not have to be anywhere close to building. He can perform his attacks from anywhere close enough to the building, where he can get good signal strength to launch his attack. This place can be the office of some other company on the other side of the hardboard wall, separating your office and the other office. (Common scenario in rented office areas, such as technology parks). It can be the waiting area for the visitors and guests coming into your physical premises during the working hours. Or, it can be a home, or cafeteria, or an office building on the other side of the road. And, with the help of wireless signal boosters and home made “cantennas”, you can expect your attacker to be anywhere, even a mile away!

Here is the point I am trying to highlight. When a Wireless Access Point is connected “directly” to your wired network segment, then it is as bad as sitting in an open field, with no protection at all. Even if you have a firewall device placed between your internet connection(s) and your LAN, that firewall is not protecting you from the crackers trying to break into your network, and steal your data coming in from the unprotected wireless access point. When you connect your

wireless access point directly into your LAN switch, then the cracker sitting a mile away does not have to go through a firewall to get to what he needs. He simply connects to your wireless access point, and lands straight into your LAN. In this case, there is no internet involved, and no records are maintained at any ISP or router along the way. The cracker successfully avoided all that, thanking your system administrator (or you, if you are the system admin of this network). Don't be surprised if he even leaves you a thank you note for the same!

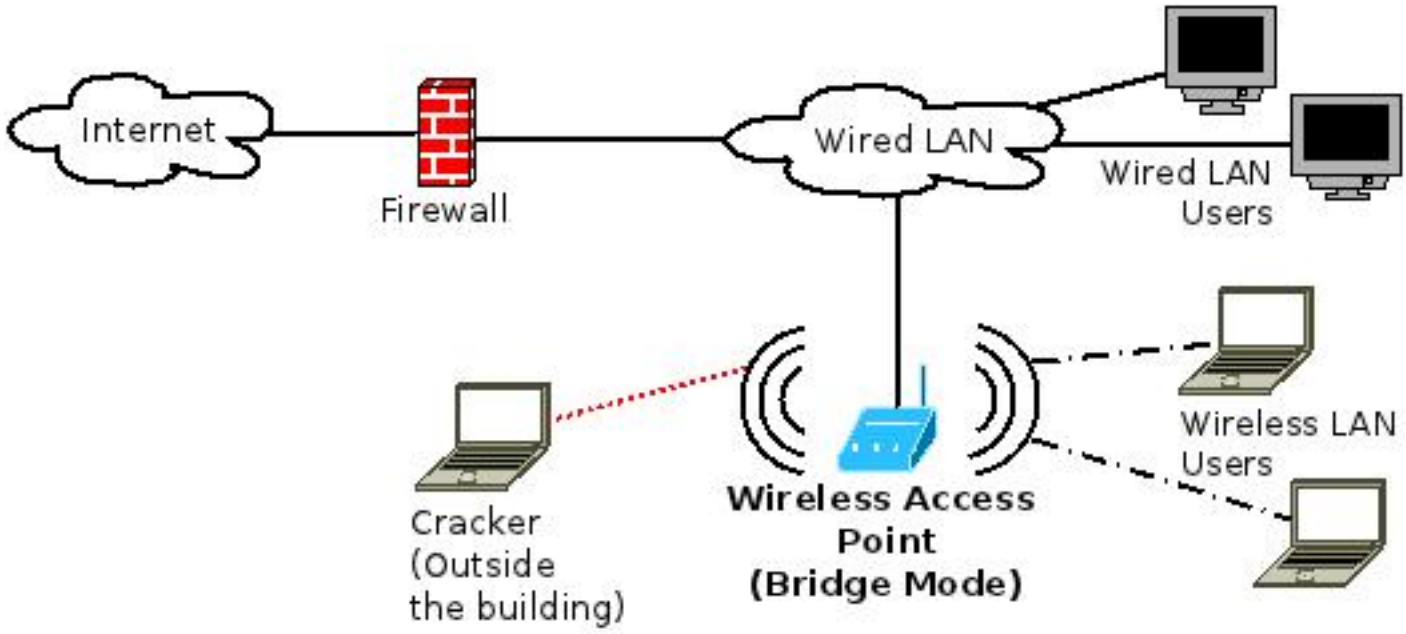

Figure 1: WAP connected directly to Wired LAN

If you are just a plastic trash-bin manufacturing company, then may be your data is not much value to you, or a cracker. But when you are a company with does research, or service integration, or deal with government departments and military organizations, then your data “is” important for you. And it is important to ensure it's Confidentiality, Integrity and Availability.

As explained above, your data may nor be of any value to you or a cracker. However, that should not let you be easy on your network security. There may be no data, “but”, your network (and it's resources, such as PCs, IPs, etc), can be used as a launch pad, to launch attacks on other “more juicy” targets, normally located outside of your network. This means, you still need to make sure that your IT infrastructure is secure, even if there is no valuable data.

Some system admins make a list of MAC addresses of the wireless network cards of all the wireless clients in an organization and add that to the wireless device, restricting allowed traffic only to/fro these MAC addresses. This is **not** a good solution for reasons:

1.

It is not practical to keep track of all the MAC addresses of everyone in the organization. Especially, if the count of wireless devices is more than five.

2.

Some cheap/in-expensive wireless access points have a restriction, that only allows a MAC list of about 20 addresses. In case you have more devices then it is again a problem.

3.

Wireless devices (clients) come and go, all the time. It is not possible (not practical) to edit the MAC list every time some new device joins in, or leaves.

4.

It is not difficult to spoof a MAC address. And if in case the cracker sees that a MAC address is in use during some time of the day, he will wait for the time when the device stops communicating with the wireless access point. Normally this happens at the day end, when the workers/employees go home. The employees of-course go home, and their laptops, etc, are turned off, or are disconnected; the MAC list still allows traffic from those MAC addresses. When a cracker sees this (who has been sniffing the network traffic, all day long, and noting MAC addresses), simply assigns (spoofs) one of the many “allowed” MAC addresses to the his laptop, and starts using your network.

To avoid all the problems described above, the best practice is to connect your wireless access point directly to a firewall, which in-turn should be connected to your wired LAN. This way, you can allow required (but limited) traffic flow between wired and wireless clients within the organization. Also, your wireless devices can be provided with (limited / controlled) internet access, through this firewall. One example can be, that you only allow/open windows files sharing ports on the firewall, between the wireless clients and the wired clients. You can, for example, allow only web and FTP traffic from your wireless clients towards the internet, and block the rest of traffic. In addition, you can restrict outgoing SSH traffic only from the wired

network. Or, whatever suits you. This way, it would be difficult for a wireless client connected to your network, to launch an attack against your own LAN resources, or against some other network somewhere else in the world.

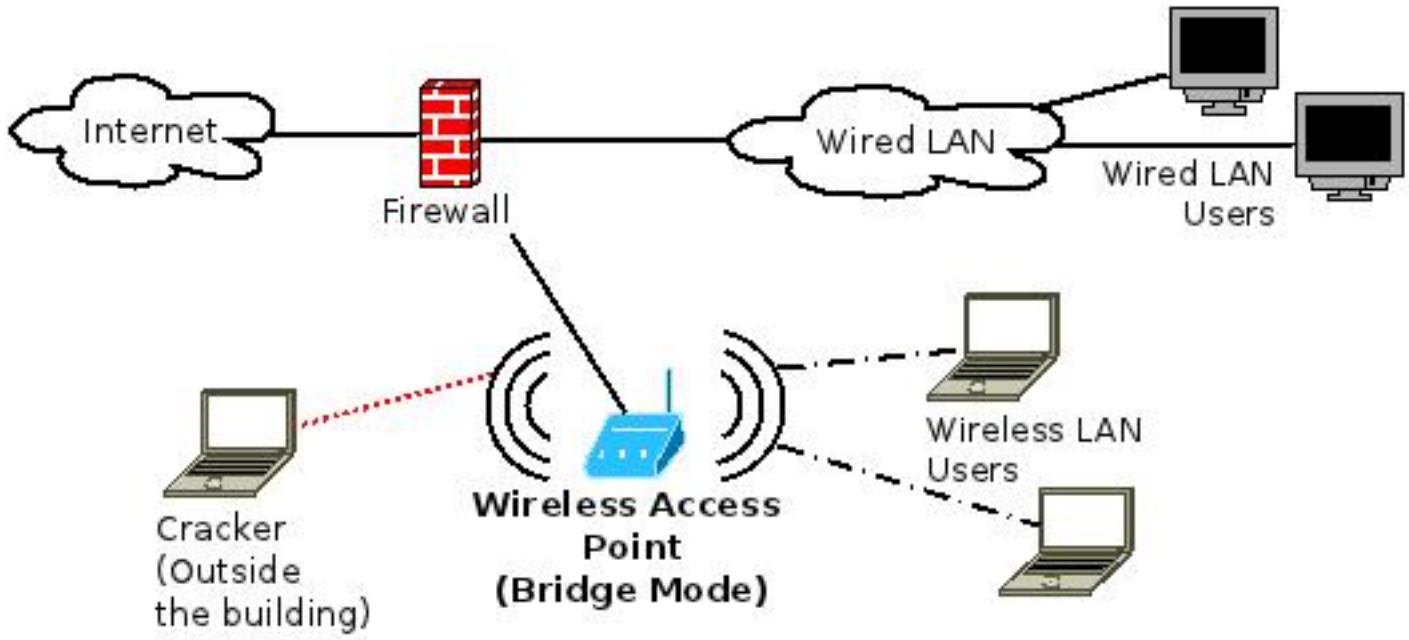

Figure 2: WAP connected to Wired LAN "through the Firewall"

Be warned though, that connecting your wireless access point to a firewall, instead of plugging it in directly to your network switch, is **not** the only protection you should consider for your network. It should be your first logical step towards securing your network. In addition to this, you should beef-up your security profile by:

1.

Connecting your wireless access point to a firewall, instead of plugging it in your LAN switch. (as mentioned above). You need to have an additional physical interface on the firewall for this to work.

2.

Using WPA2 security mechanism in your wireless access point.

3.

Encrypting the traffic flowing through your wireless access point using strong encryption, such as AES.

4.

Restricting the type of traffic flowing between your wireless devices, your LAN devices and the internet, using the firewall.

5.

Educate your users on how to use the system, and how to prevent security incidents from happening.

On the closing note, I would like to remind you, that data security is a responsibility of everyone in the organization, ranging from a normal user to the CEO. Be diligent.