

The Need for WLAN Security

William H. Wolfe II (9 mins)

Wireless Vulnerabilities and Threats. Why are wireless LANs prone to attack? Well, there are various reasons.

First of all, the open-air nature of radio frequency technology. Propagation of that RF signal is very hard to control. Typically physical barriers don't block the RF signal. Even though certain characteristics of certain materials will attenuate the signal greater than others, the signal can still get beyond the confines of what you consider to be your physical security perimeter.


The 802.11 protocol and all of its specific protocol variants - 802.11 'a', 'b', 'g', 'n' and even 'ac' as the newest protocol today. They're all very well documented, very well understood. That way, we provide for interoperability between different vendors' products. We obviously are using the unlicensed frequency bands of 2.4GHz and 5GHz.

So why do we need LAN security? Well, we need to protect ourselves against that open, pervasive nature of RF. We need to protect ourselves from the business impact of stolen data. We need to make sure that we design our 802.11 wireless network with basic security in mind. We want to make sure that we understand the vulnerabilities that are out there. We want to be able to understand how to mitigate different types of attack vectors such as denial-of-service attacks, jamming, flooding, man-in-the-middle, and of course, the big one is there's no protection in the general RFC and the IEEE standard for 802.11 for management and control frames. Most of that protection is only on the data frames. We spoke about that during the overview where we're going to actually encrypt our data frames as they propagate the RF space.

There are some advanced technologies that we'll speak about later in this session that will help us control management and control frames. And of course we need to protect and authorized access to all network services and resources because wireless is actually an extension of our wired local area network.

The security risk assessment that we have to go through for wireless is really no different than it is for wired. We have to consider what sensitive data, and whether or not people should have access to that sensitive data, whether they're on the wired or the wireless network.

Same thing with network services. Network services are those services that allow users to perform their job functions, to perform in their everyday lives. So we need to have basic services available, whether it's on the wired network or the wireless directory services, Internet connectivity.




We also need to be able to get access to our virus and intrusion detection services. So, for our wired desktops, we're going to have a virus protection software on there. It might need updates. Well, same thing is going to hold true with a wireless device. A wireless device, if owned by the company is going to have the same standard antivirus protection software and might need to get updated. If it's a guest device meaning it's not owned by the company, or it's a Bring-Your-Own-Device model, we might want to make sure that those systems have in fact, the latest antivirus software on them, the latest critical updates, system and those need to be delivered wirelessly.

So we're kind of in a catch 22 where we need to be able to give access to network services over the wireless network but maybe that device isn't secure enough or does not adhere to our policies, or doesn't meet a posture assessment, but yet, we need to remediate it, and it has to be done over wireless connections. So, there is a little bit of a catch 22 there.

We obviously as a company need to define security policies for not only access to information and data but also for network services and we have to understand the capabilities of our clients. Many organizations will actually develop a security policy that is very specific for wireless connectivity vs. wired connectivity. Lots of companies will also have policies for their guest users by setting up a guest wireless network that only allows access to again certain network services or resources only supports certain client capabilities, or client wireless interface card drivers or software. Those things are all part of a new company's security policy.

We talk a lot about wired, wireless LANs security importance. It's because we always will have vulnerabilities. We will always have hackers and criminals trying to get to information that helps us run our company and make our company differentiated from its competitors. We're going to have employees who go beyond the confines of the rules and regulations of the company or even break those security policies that we've defined by putting in their own wireless router, their own wireless access point or possibly even putting in a peer-to-peer wireless network device that can act as a bridge, and allow for exploits and vulnerabilities. And of course we have the war drivers who are constantly looking for open wireless connectivity that's leaking out of the physical perimeter of your building. Hence, that concern about the open air concept of RF.

Wireless LAN security has a lot of visibility. Public wireless LAN and WiFi hotspots—they're all over and many of them, as some of you have probably noticed, will give you an alert message that indicates that this is a public WiFi, none of the data is encrypted. So, it's your responsibility if you are going to do secure transmission of information, banking, financial information, connecting to your company via VPN, that it's your responsibility as the user to make sure that you are secured because the wireless environment being public using what we call open authentication which we'll be discussing a little bit further later, leaves us vulnerable. We can have identity theft. We can have phishing. We could even have people utilizing open-source publicly.



available tools. They can actually sniff the air while you're sitting inside a Starbucks using their WiFi hotspot