Cisco Networking Academy® Mind Wide Open™

Overview of Wireless LAN Security

William H. Wolfe II **(7 mins)**

Wireless LAN security is extremely important because with a wireless environment, we are not tied directly to physical switch connectivity. So, physical switch connectivity is going to give us a little bit tighter security profile than wireless since anyone might be able to see her wireless environment.

Authentication is one piece of wireless security, and as we proceed through this material today, we'll see that we'll have some in-depth review and discussion on some specific topics.

One of those topics is 'Authentication'. With authentication, it's about proving your identity and that is something that you know- a password or something you do, something that you have - a physical object, or a device that a value can be read from, or something that you are, biometric access methods such as thumbprint, retina scan, etc. So one of the things that has to occur in wireless first, as we'll see later, is authentication to the SSID must occur first before we can get access to our wireless environment. We can authenticate devices, or we can authenticate users. We'll see how different methods are used again as we proceed through this program.

Device authentication ensures that the device that we'll using, is in fact the device that it says it is, and gains access to the wireless environment. Authenticating a user is really about tying your user ID, its credentials, and its authorization to use services to the wireless environment. We will cover that in a more in-depth discussion around Extensible Authentication Protocol (EAP) later on.

Encryption is another component of wireless. We generally don't see this in a wired environment, so, at least from a layer 2 switching LAN environment, but, in wireless, we want to make sure that the traffic, the messages, the data, moving from the actual wireless client to the wireless access point are not able to be intercepted. We don't want people to be able to do packet captures, and see our data. So in wireless, all the RF transmission goes through an encryption process where all the data is encrypted between the client and the access point. We're going to cover details of encryption algorithms a little bit later as they are used in wireless, and best practices from the industry.

From a high-level introductory point of view, encryption is basically taking a non-encrypted or plain text message, placing it through a encryption algorithm, or cipher process, generating a ciphered text message, and then reversing that process or de-encrypting when it gets to the receiving end.

There are two types of encryption, there is symmetric encryption and asymmetric encryption. Symmetric encryption uses the same encryption key both for encryption and decryption. Asymmetric encryption uses different keys. Generally this is referred to as the Public Key Infrastructure (PKI), so you would have a public key and a private key that are in pairs that match each other, therefore, becoming in asymmetric encryption algorithm. We won't spend a lot of time on the details of these two different encryption methodologies, but as an introduction. You should now understand the difference between them.

Wireless threats is certainly an area that we're going to spend some time in. We're going to look at some very specific types of threats, some mitigation techniques and some tools actually that are available from Cisco to help us in this regard.

In general, we're going to be looking at rogue access points, ad hoc networks, mis-associations from the client perspective where they actually could be forced to associate to an AP that has an open SSID, and allow people to gain access to the client.

And then of course, some very specific types of wireless attacks, active attacks, passive attacks, and one that Cisco actually has a specific process to help mitigate called 'Management Frames Snoofing' and we'll discuss that a little bit later.

One of the things that can be done in the wireless environment is to include Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) at the wireless RF level. We'll cover some of this a little bit more in detail as we get into the attack portion.

Management Frame Protection as I mentioned earlier, is a specific Cisco activity, and we'll cover that more in detail.

In summary, for this section as an introduction, in wireless networks, authentication allows us to determine who gets access to the network, and the encryption protects that wireless traffic flow at the RF level going from the client to the access point over the air. We need to add encryption so that we can add privacy. We can add intrusion detection, intrusion prevention and some other specific management protection with some of our Cisco technologies.