Encryption Overview

William H. Wolfe II **(4 mins)**

We'll talk about the evolution of encryption and remember, this is the encryption of the data and the wireless frames that are propagating the radio frequency transmissions between the client and the access point.

So we obviously started off with WEP, we moved to TKIP, and finally ended up with AES, which I mentioned earlier, is a NIST and FIPS standard with the FIPS 197 document.

Temporal Key Integrity Protocol is generally only used today for legacy clients that don't have AES support, and to be honest that is very far and few between today. It was a software update, however, for WEP only clients, and they're still in use.

Some devices that are WEP only, very old inventory scanning guns and older technologies such as, surprisingly enough, the Nintendo DS that actually supported 802.11b, and only had WEP encryption. Not that anyone uses Nintendo DS anymore, but if you happen to have an old one sitting around, you could actually connect it to your environment. You could protect it with WEP although not very protective.

TKIP can also be run in conjunction with AES, but generally you won't find that being done unless you're supporting WPA with TKIP, and WPA2 with AES.

Again, most devices today, will have WPA2 and AES support. TKIP and WPA really has been discontinued by the WiFi Alliance and is no longer considered certified.

Now, the AES Advanced Encryption Standard-that one required hardware, could not be done with just a software upgrade. Anything post 2005 has AES encryption, and generally will also mean that it has WPA2. Eleven years since that was developed, will pretty much indicate that it's standard in the industry today. The other thing that AES offers is it has line-rate speed capability and it is the only encryption standard supported for the data rates in the 802.11n protocol.

Just review on why TKIP was considered vulnerable? That is that the MIC key that's used for the Message Integrity Code facilitated potential packet forgeries, and the encryption key is not recoverable. Therefore, the data traffic cannot be read via this attack, so this is a little bit different than the WEP crack from years back. But, what's the risk? There is a risk that traffic can be replayed for a limited duration of time and TKIP encryption tied with WPA can be made vulnerable and be attacked.