

Tricky question...

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-10/3150.html>

From: Gabriel (en_hemlig_person@hotmail.com)

Date: 09/29/02

From: en_hemlig_person@hotmail.com (Gabriel)

Date: 29 Sep 2002 12:58:50 -0700

The setup is as follows: Three access points (AP1, AP2 and AP3) are connected to a switch and to each of the access points one laptop is associated (Lap1, Lap2 and Lap3). Each of the three laptops uses a different WEP key (WEP1, WEP2 and WEP3) when they associate to their access point.

Question: Is it possible for Lap1 (in this case the attacker and associated to AP1 using WEP1) to perform a Man-in-the-Middle attack using ARP cache poisoning (with e.g. Ettercap) against Lap2 and Lap3 (i.e. sniffing the communication between Lap2 and Lap3)? Assuming that Lap2 is associated to AP2 using WEP2 and Lap3 is associated to AP3 using WEP3???

I am thinking that WEP only encrypts the data that travels through the air between a laptop and the AP, which would mean that it travels in clear text between the AP and the switch?? If this is the case Lap1 should be successful in carrying out a MITM attack against Lap2 and Lap3 since it "intercepts" the data through the switch. Am I right or am I wrong?

If I am right this scenario would be possible: AP1 is NOT using WEP, which (basically) means that anyone can associate with it, but AP2 and AP3 are using WEP. Now Lap1 (the attacker) can perform a MITM attack against Lap2 (associated to AP2 using WEP2) and Lap3 (associated to AP3 using WEP3) without any problems whatsoever since it didn't have to crack a WEP key...

A big Thank you in advance.

/ Gabriel- A Norwegian WLAN expert wannabe :)

- **Next message:** chris@nospam.com: "Re: Tricky question..."
- **Previous message:** Bryan: "CISSP San Diego Dec. 7th"
- **Next in thread:** chris@nospam.com: "Re: Tricky question..."
- **Reply:** chris@nospam.com: "Re: Tricky question..."
- **Reply:** [Alan Schwartz](mailto:Alan_Schwartz): "Re: Tricky question..."

comp.security.misc: Tricky question...

- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]