# WIRELESS EVIL TWIN ATTACK

**Prof. Pragati Goel**
Associate Professor,
NCRD's Sterling Institute of Management Studies, Navi Mumbai

**Mr. Chetan Singh**
NCRD's Sterling Institute Of Management Studie, Navi Mumbai

## ABSTRACT

*In Today's world multiple Wireless Local Area Networks (WLANs) can coexist in a airspace. Every wireless mobility devices tries to find the access point through probe request using a unique name that is the Service Set Identifier (SSID) of the network to make automatic authentication. As a wireless user you are concerned only with the broadcast SSIDs that let you connect to a WLAN. This paper discusses about the Wireless Mobility devices communication security issues using Basic Service Set Identifier BSSID or Extended Service Set Identifier ESSID which a network administrator need to keep track of. Also it discusses about the available flaws in it and how by modifying the probe request header we can make the connectivity more secure for the new generation of devices.*

***Keywords:*** *Wireless, Evil Twin, Wi-Fi Security, Security, Exploitation.*

## INTRODUCTION

Every wireless mobility devices tries to find the access point through probe request using a unique name that is the Service Set Identifier (SSID) of the network to make automatic authentication. The users are usually unaware of which basic service set (BSS) they belong to. When the user physically moves the laptop from one room to another, the BSS used could change because of moving from the area covered by one access point to the area covered by another access point, but this does not affect the connectivity of the laptop. In this paper we are going to study how a mobility device automatically connect to a Access point, the normal mechanism how a mobility device connects to an know Access point is very unsecure, also how an attacker take advantage of this connectivity mechanism for his/her benefit to hack AP's clients. The paper is organized as follows. In section 2, we will see that how a client and access point connects with each other by taking an Open Authentication method. All the handshakes and which packet header parameters are benefiting for that attacker malicious activities. In section 3, we will get to know that how a Wi-Fi Attacker will exploit the Client-Access Point (AP) Connection for malicious benefits in an open authentication environment. In section 4 we will discuss it in different scenarios e.g. In WEP, WPA or WAP2 environment. In section 5 we present how a client can defend these malicious attacks by the attacker. In section 6 we provide some concluding remarks.

## WORKING OF CLIENT – AP CONNECTION PACKETS

In general every mobile device which wants to connect to a specific Access Point sends a Probe Request. The request either can be one to many (Broadcast) or one to one depending on the scenario whether it is a fresh connectivity or already connected connectivity. How exactly a client and Access points connect with each other is depicted in Figure 1.

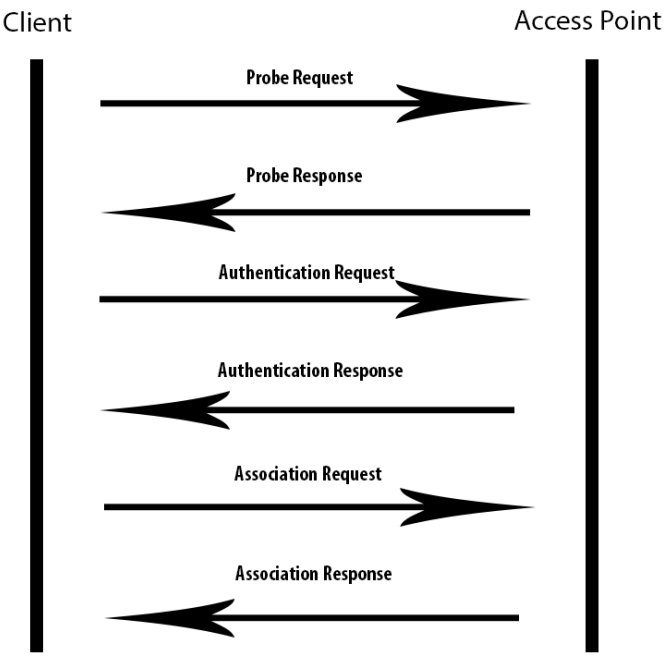


**Fig. 1 Client AP-Connection Packet**

At first when a client wants to connect to an Access Point it sends a Probe Request either by broadcasting telling to all AP's to identify themselves or a single Access Point to identify them by the ESSID (Access Point Name), then the AP's response the client their ESSID via a Probe Response. Once the client receives all the probe responses it will send an Authentication request to the Access Point which it wants to connect and then the Access Point sends an Authentication Response. In this Authentication Request-Response phase the client and AP authorize each other. Once the authentication is done the client sends an Association Request to the AP and the AP responses with the Association Response packet.

In this way a client and the Access point connect with each other which is shown below through the Wireshark Dump shown in Figure 2.

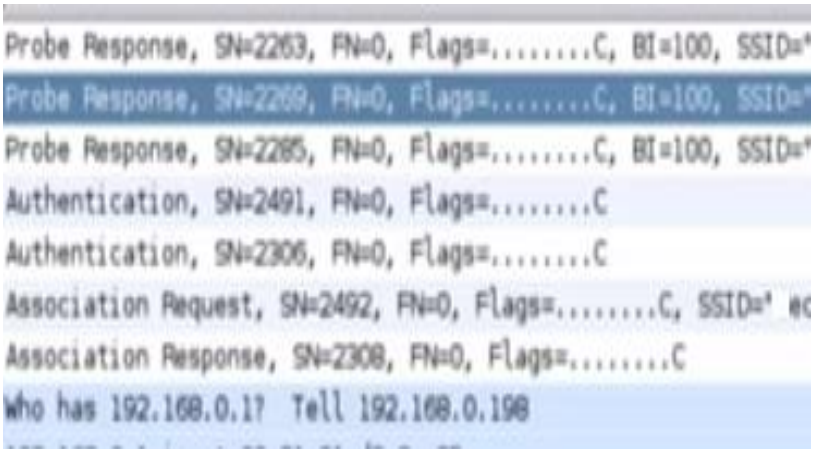


**Fig. 2 Client AP-Connection Packet Wireshark Dump**

The Probe response packet shown in Figure 3 disclose its Name through the SSID

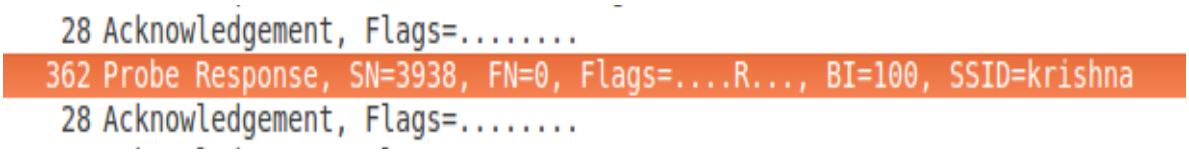


**Fig. 3 Probe Response Packet**

This packet comes in handy when an attacker wants to target an AP client.

**Problem in Client-Access Point Connection**

When a client tries to connect to an AP it first sends a Probe Request and then the Access Point's reply with their ESSID, here the client only checks for the ESSID rather than the Access Point BSSI. This means any fake Access Point having the same name (SSID) as the legitimate client AP will get connected with the client without any verification.
This kind of attack is known as **"Evil Twin Attack".** In Figure 4 there are two Access Points with the same name (ESSID) "TrickOrTreat". The first AP is fake and the second one is real.

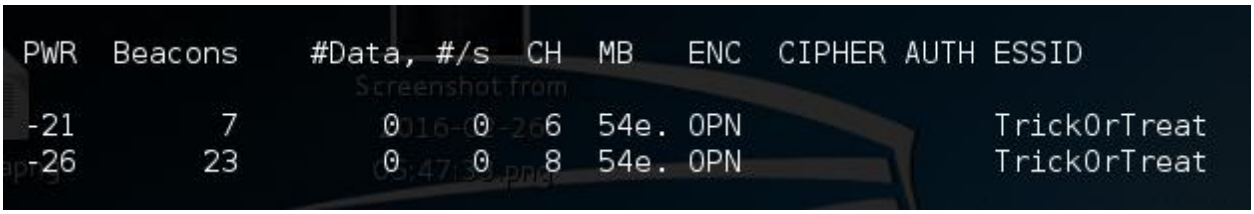


**Fig. 4 Same ESSID – TrickOrTreat for both the AP's**

Figure 5 shows that the client is connected to the fake access point without any verification.

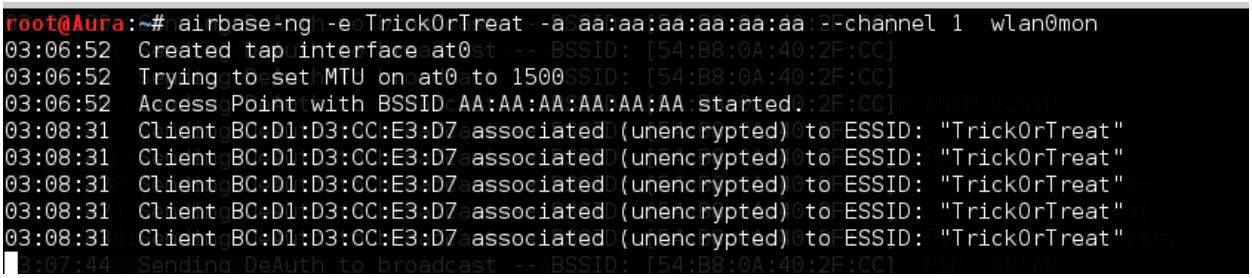


**Fig. 5 Client connected to fake Access AP**

This shows that how easy it is to fool any mobility client by making a Fake Access Point name same as that of the original AP.

**EXPLOITING CLIENT-AP CONNECTION**

As we have seen that any Wi-Fi Attacker can create a Fake AP and fool any mobility devices to make them connect to the Wi-Fi attacker can also use the same method to launch a Man in the Middle Attack (MITM). MITM attack can be launched in two ways.

**Case 1. By Creating a Fake AP and waiting for the victim to automatically connect.**
Here the attacker sniffs the air to find out for which ESSID the client is probing for. Once it receives the clients AP it will create a Fake AP as the same name as the Original AP and will wait for the victim to automatically connect to the Fake Access Point.

**Case 2. Explicitly disconnecting the victim from the original AP and making it connect to the fake AP.**
In this case the client is connected to the legitimate Access Point and the attacker will explicitly launch a de-authentication attack on the legitimate AP (Figure 6). The legitimate AP goes in disconnect mode after receiving a de-authentication request. In the mean time the attacker will create a Fake AP as the same name as the original AP and the client will connect to the Fake AP as the original AP is in sleep mode.
Once the victim connects to the Fake AP, the attacker will just setup a bridge between the Client and Internet and whatever the victim will browse on the internet the packets will go from the attacker machine. The attacker can now sniff every data which is going through his/her machine.

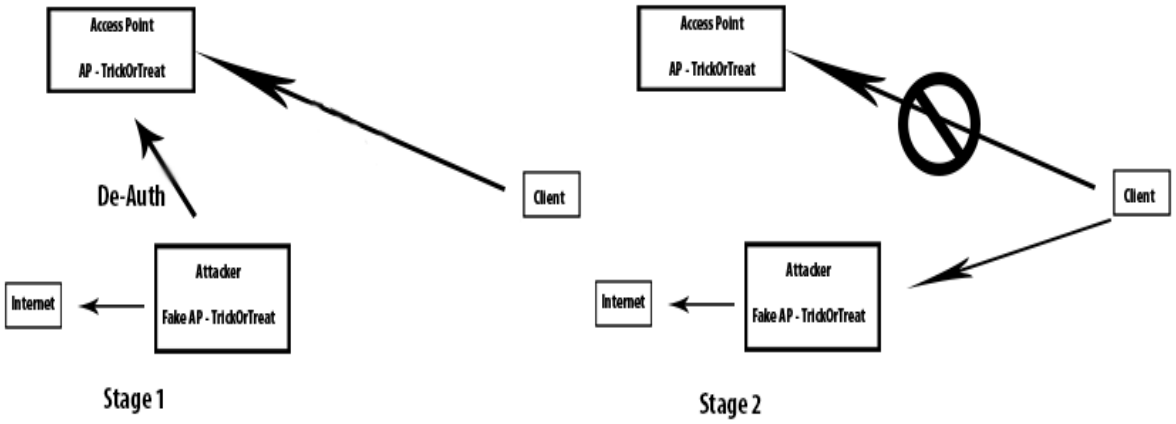


**Fig. 6 De-authenticate the AP and launch MITM attack.**

## VARIATION IN EVIL TWIN ATTACK

Till now we have discussed all the examples in the Open Authentication Scenario, but what if the client wants to connect to an AP which is secured by a Security protocol (WEP or WPA/WPA2). Well the Wi-Fi hacking is a big Scope where attacker can use their creativity to launch any attack

- **Cracking the password.**

To crack any Wi-Fi password it is required to know the encrypted or unencrypted data packet. We discuss both the case of WEP protocol and Handshake packets in case of WPA/WPA2.

**WEP (Wired Equivalent Privacy) –**
In case of WEP the attacker could gather ARP Encrypted Data packet by Evil twin attack and crack the password from the Weak Initialization Vector (IV). In WEP it is possible to crack the key in just couple of seconds. The attacks in WEP vary like Korek Chop Chop, Caffe Latte, and

Fragmentation Attacks. These attacks take advantage of the Weak Encryption algorithm of the WEP Security Protocol [1].

**WPA/WPA2 (Wi-Fi Protected Access)–**

In WPA/WPA2 [1] we could capture the handshake and by launching a Brute force or Dictionary based attack on the packets the attacker could get the key. But WPA/WPA2 is better than WEP protocol as it is the strongest Wi-Fi Protocol. It is available in two forms i.e. Standard and Enterprise 802.1x Radius Server. The usage rate of WAP/WAP2 is more as shown in Figure 7.

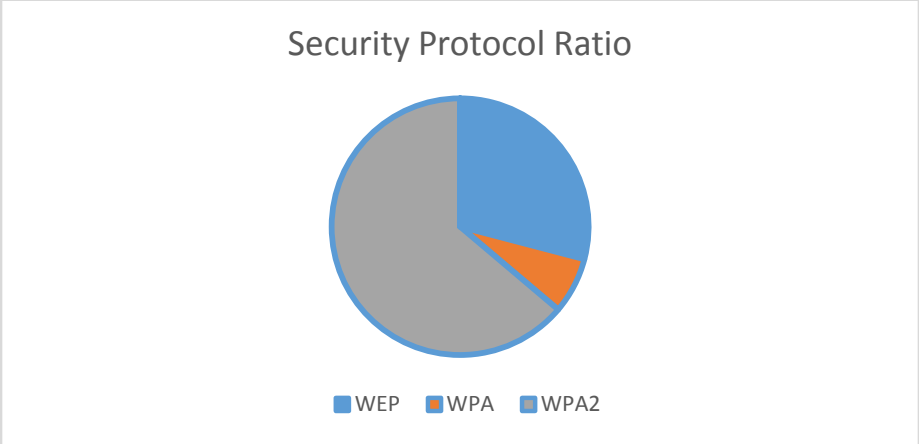


**Fig. 7 Usage of Security protocols**

## DEFENDING FROM EVIL TWIN ATTACK

So far we have discussed how an attacker can launch Evil twin attack to fool any client. The problem arises when then client tries to associate with the AP's without checking the BSSID of the Access Point. Now we discuss the cases which may be able to defend these attacks.

**Case 1.**

If the client checks the BSSID before making a communication there are 70% chances that Evil Twin might fail. For an attacker it's a very easy task to launch an Evil Twin attack with the same BSSID as well as ESSID as that of the legitimate AP if they share the same airspace. So if the client is far away from the legitimate AP and the attacker doesn't know the BSSID it will be hard for him/her to hack the client.

**Case 2.**

The other solution could be adding a key check mechanism while the client and AP connect with each other so that the Client-AP Connection mechanism becomes more secure. The idea is the WEP Key authentication mechanism and also using a Hashing Mechanism.

Here we are going to take help from WEP authentication in which when client wants to connect to the Access Point then the AP first sends a challenge to the client and then the client encrypts that challenge [1] and sends it back to the Access point. Now the Access Point checks that encrypted challenge is valid or not and if its valid the Access Point allows the client to connect to it otherwise it does not allow the client to make a communication.

Also we will use a hash function [3] with salting mechanism to make the challenge more complex.

## CONCLUSION

From the last few years various security mechanisms has been created and they had been bypassed by security researchers. The Evil Twin attack is successful in the case where a Wi-Fi Attacker exploits the Client-Access Point (AP) Connection for malicious benefits in an open authentication environment. Also there are many variations of using of Evil twin in different scenarios where a WEP or WPA/WPA2 is used. By the above mentioned techniques we can make the fake authentication phase to fail. If the attacker's Client-AP connection fails then the attacker will not be able to get the actual packets which are required for the cracking or for any malicious activity. By implementing a key check mechanism or a Hashing key check mechanism we can make the communication more secure.

## REFERENCES

[1] Comparative Study of Wireless Security Algorithm and Usage (Chetan Singh)
[2] IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability http://www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf
[3] BackTrack 5 Wireless Penetration Testing Beginner's Guide (Book)
[4] SecurityTube (Vivek Ramachandran) http://www.securitytube.net
[5] The Shellcoder's Handbook Discovering and Exploiting Security Holes (Book)
[6] Mobile commerce: Promises, challenges, and research agenda, Siau, Keng; Ee-Peng, Lim; Shen, Zixing. Journal of Database Management 12.3 (Jul-Sep 2001): 4-13.