Evil Twin Attack and Its Detection

[1]Jatin Nagpal, [2]Rajesh Patil, [3]Vikas Jain, [4]Rajesh Pokhriyal, [5]Rajveer Rajawat
[1]Dy Manager, [2]Manager, [3] Sr Manager, [4]Manager, [5]Dy Manager
[1]Data Center
[1]RailTel Corporation, Gurugram, India

Abstract: One of the most common and damaging type of attack is the Evil Twin Attack also referred to as ETA. This type of attack is opportunistic in nature where a hotel, cafe, mall, airport or a railway station public Wi-Fi user easily falls prey to bogus SSID set up by illegitimate users with the intent to eavesdrop their connection to steal user credentials like bank login, email account login etc. It is a highly effective attack since user unknowingly connects to the rogue access point under the pretext that they are connecting to genuine access point without verifying the Service Set IDentifier (SSID).

Index Terms- Wi-Fi networks, Rogue Access Point, Evil Twin Attack, SSID, Authentication request, Authentication Response.

I. INTRODUCTION

Wi-Fi has seen tremendous growth in the recent years. Various wireless technologies include Wi-Fi, Bluetooth, Infrared, broadcast radio, Microwave radio, satellite communication, ZigBee, wireless sensor networks etc. Users enjoy un-interrupted communication at their homes, offices, libraries, coffee-shops while on the move without the hassles of the wired connection.

However all these benefits have their evil side. The communication between the user and access point happens over the air. This communication can be eavesdrop by anybody sitting meters away from the user. Wi-Fi networks are prone to attacks like MAC spoofing, authentication flood, de-authentication flood, jamming, man in the middle attack, war driving etc. The primary reason for Wi-Fi to be prone to numerous type of attacks is due to inherent weakness of 802.11 protocol. By setting up a RAP, an attacker can re-direct clients to fake login portal(s), steal passwords, access credit card information by eavesdropping on communication medium, launch man-in-the-middle attacks etc.

Most of the modern operating systems (OS) are configured to connect to the AP providing higher signal strength in-case there are multiple APs associated with the same SSID. In presence of an evil twin AP, if the signal strength of the evil twin exceeds the signal strength of the genuine AP, the client(s) get associated with the evil twin AP. Higher signal strength leads to higher throughput and less frame loss. Hence a client always prefers to opt for APs offering higher signal strength. All modern operating systems display the list of available APs in order of their signal strengths offered.

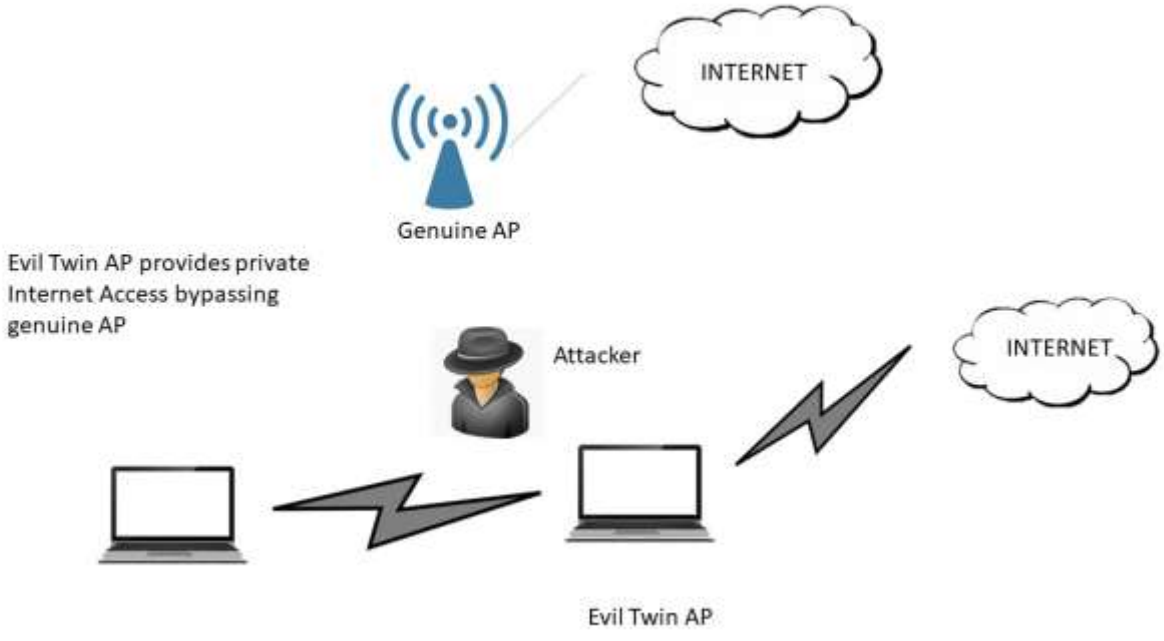
INTERNET
Genuine AP
Evil Twin AP provides private Internet Access bypassing genuine AP
Attacker
INTERNET
Evil Twin AP

Fig.1 Evil Twin Setup

Ma et al. [3] have given a comprehensive taxonomy of different classes of RAP as shown in Table 1.

TABLE-1 Type of rogue access point

SN	Type of rogue access point	How it is exploited
1	Improperly configured AP	Administrators setting default/weak passwords or unknowingly installing faulty/buggy device driver making AP vulnerable
2	Unauthorized AP	Setup without the prior permission of the network administrator
3	Compromised AP	Attacker cracks the encryption key using key cracking tools to evade security
4	Evil twin (Phishing) AP	Clone (mimic) a legitimate Wi-Fi AP

II. Detection of Evil Twin Attack

1) Maintaining white-list of MAC addresses of A.P.s in the network and monitoring the traffic continuously. Any new A.P. not marked in the authorized list of A.P.s is marked as rogue access point.

2) Timing based scheme for rogue A.P. detection - Evil twin AP forms a bridge between the genuine AP and a client to provide Internet services. Due to bridging an additional hop is introduced. Timing based solutions work upon the extra delay occurring due to the additional hop. This extra delay provides evidence for detection of evil twin AP. Han et al. [1] have proposed a method in which they measure the Round Trip Time (RTT) for a DNS query.

3) Pradip et al. [2] propose the use of a special probing unit that sends a pre-detection message to all associated client(s) informing them not to respond to probe request. It then sends a probe request. All APs responding to it are marked as evil twin APs.

4) Using IDS for detecting evil twin attack- In this method, IDS sniffs the authentication request and response frame. The activity is marked suspicious if more than 1 authentication response frame is received. The retry bits, sequence number and association ID (AID) of multiple responses are analyzed for concluding if evil twin AP is present. This technique can be used to detect multiple evil A.P.s. [4].

References

[1] H. Han, B. Sheng, C. Tan, Q. Li and S. Lu, A timing-based scheme for rogue AP detection, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, No. 11, pp. 1912–1925, 2011.

[2] P. K. Dubey, and J. N. Verma, *Method And Apparatus For Detecting A Rogue Access Point In A Communication Network*. URL http:// www.googl e.com/paten ts/US201 20124 665 2012.

[3] L. Ma, A. Y. Teymorian, X. Cheng, and M. Song, RAP: protecting commodity Wi-Fi networks from rogue access points. In: *The Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness Workshops, QSHINE '07*, pp. 21:1–21:7. ACM, New York, NY, USA 2007.

[4] *Article in International Journal of Wireless Information Networks · March 2018*
DOI: 10.1007/s10776-018-0396-1
https://www.researchgate.net/publication/324215846