Computers and Electrical Engineering 000 (2015) 1–10

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

A client-side detection mechanism for evil twins☆

Fu-Hau Hsu, Chuan-Sheng Wang*, Yu-Liang Hsu, Yung-Pin Cheng, Yu-Hsiang Hsneh

Department of Computer Science and Information Engineering, National Central University, Taiwan

ARTICLE INFO

Article history:
Received 1 September 2014
Revised 25 October 2015
Accepted 26 October 2015
Available online xxx

Keywords:
Wireless
Evil twin
Rogue AP
Wi-Fi

ABSTRACT

In this paper, we propose a client-based solution to detect "evil twin" attacks in wireless local area networks (WLANs). An evil twin is a kind of rogue Wi-Fi access point (AP) which has the same SSID name as a legitimate one and is set up by an attacker. After a victim associates his device with an evil twin, an attacker can eavesdrop sensitive data forwarded through the evil twin. Most existing detection solutions are administrator-based, which are used by wireless network administrators to verify whether a given AP is in an authorized list or not. Such administrator-based solutions are limited, hardly maintained, and difficult to protect users 24–7. Hence, we propose a client-based detection mechanism, called evil twin detector, to detect this type of attacks. An evil twin detector changes its wireless network interface card (WNIC) to monitor mode to capture wireless TCP/IP packets. Through analyzing captured packets, our detector allows client users to easily and precisely detect an evil twin, thus avoids threats created by evil twins. Our method does not need to know any authorized AP list, and does not rely on data training or machine learning technique. Finally, we implement a detecting system on Windows 7.

1. Introduction

Nowadays, wireless local area networks (WLANs) are widely used in many public places, such as airports, schools, hotels, or cafés. Using the Wi-Fi access points (APs) installed at these places, users can use their mobile devices or laptop computers to connect to the Internet. Although wireless networking is more convenient than wired networking, it faces much more security threats. According to many Wi-Fi security reports, such as [1,2], rogue (phishing) AP is always among the top three wireless threats. "Evil twin" is a kind of rogue APs. According to the definition of [3], a rogue access point is a wireless access point that is installed on a network without explicit authorization from the administrator of the network. When a user connects to the Internet through a rogue AP, the creator of the rogue AP can sniff the data sent by the user. If the data are not encrypted, the attacker can obtain sensitive information contained in the data. Because a rogue AP is easy to setup, it raises serious menace to wireless users.

A rogue AP itself could connect to the Internet either through a wired network or a wireless network. A wired rogue AP is also called as a "wired rogue" and an "evil twin" is a wireless rogue AP. Usually an evil twin is set up with the same AP name (SSID) as a legitimate AP, called good twin, to attract normal users to connect to it, because normal users cannot distinguish an evil twin from the related good twin. Most modern operating systems connect to the AP with the best Received Signal Strength Indication

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. W-H Hsieh.

* Corresponding author. Tel.: +886-3-4227151.
E-mail address: 995402007@cc.ncu.edu.tw, luckyqqmaster@yahoo.com.tw (C.-S. Wang).

http://dx.doi.org/10.1016/j.compeleceng.2015.10.010
0045-7906/© 2015 Elsevier Ltd. All rights reserved.

(RSSI) [4] when they find multiple APs with the same SSID. Hence, an evil twin usually tries various approaches to generate strong RSSI to its target machines. However, in order to expand the signal coverage range of a WLAN, many organizations also assign the same SSID to multiple APs, which makes it more difficult to detect an evil twin.

To launch an evil twin attack, an attacker can configure a laptop to be an evil twin first. To enhance an evil twin's RSSI to its targets, the attacker either could deploy his evil twin at a location that is close to its targets or use a directional antenna. Then the attacker uses the SSID of related good twin to set the SSID of the evil twin. As a result, if a user tries to connect the Internet through the good twin, he may be cheated to use the evil twin, instead of the good twin. Besides, the attacker can launch a de-authentication attack [5] to force a victim to connect to the evil twin. After the above steps, the attacker can sniffer data forwarded through the evil twin.

An attacker typically launches an evil twin attack at public places, such as airports, schools, hotels, or cafés. Through setting up an evil twin, an attacker is able to obtain sensitive data of various users, such as passwords, web sessions, or credit card information, if these data are transmitted in plain text form in wireless packets. Besides, an attacker can also use an evil twin to launch a man-in-the-middle attack. Due to the serious threats created by evil twins, it becomes a critical issue to develop an evil twin detection mechanism.

This paper proposes a client side solution, ET detector, which can securely and reliably detect evil twins without any data training. It is difficult for an adversary to evade the detection of ET detector, even though the attacker knows the detail of ET detector. ET detector changes the wireless network interface controller (WNIC) of a laptop to monitor mode so that the laptop can capture all packets that are transmitted through the channel monitored by the WNIC and are transmitted through IEEE 802.11 protocols[1]. Via analyzing sniffed packets, ET detector can determine whether an AP forwards wireless packets to another AP. Because packet forwarding is a key property of evil twins, ET detector uses this property to accurately detect evil twins. ET detector has the following advantages. (i) ET detector does not require any authorized list. (ii) By switching a WNIC to monitor mode, a user does not need to associate his laptop with any AP while making detection. Thus, background processes, such as auto-login processes, that send sensitive data automatically to remote servers when connecting to the Internet will not unwittingly leak the information to the owners of evil twins. (iii) When making detection, ET detector does not need to pass web authentication, because it is a passive solution. However, many former solutions need to associate their machines with an AP first to connect to the Internet and make their detection. Hence, if the related AP uses web authentication to make access control and a tester does not have a related account, the tester cannot use the solutions to detect an evil twin. (iv) ET detector does not require any parameter training and is more reliable than others in a complicated condition. (v) An attacker is hardly to evade the detection of ET detector, because he cannot remove the packet forwarding feature of evil twins.

The rest of the paper is organized as follows. Section 2 discusses related work. Section 3 describes the principle and the detection algorithm of our solution. Section 4 discusses various experimental results to evaluate the effectiveness and efficiency of our solution. Section 5 gives the conclusion.

2. Related work

There are two categories of solutions to detect evil twin attacks. The first one is administrator-based solutions. This kind of solutions usually perform RF signal monitoring. It may be implemented on the core network, such as switches or routers or special devices. Besides, these solutions usually verify specific "fingerprints" of an AP based on a pre-defined authorized list. [6–14] belong to this kind of solutions. An administrator-based solution is usually used by network administrators. However, when an attacker launches an evil twin attack, it is difficult for these solutions to provide a real-time protection. [15–21] monitor traffic at a traffic aggregation point of the wired side, such as gateway, to determine whether a machine uses wired or wireless connections. These solutions also compare collected information with an authorization list to determine whether the associated AP is a rogue one or not.

The other type of solutions is client-based solutions, which is usually deployed on users devices to detect evil twins. The advantage of this solution is that when users are not sure if a wireless network is secure, they can make the detection themselves. Therefore, they can protect their information more timely. Song et al. [22] proposed a client-side system to detect evil twin attacks. They proposed two detection algorithms to detect evil twins, which are called Train Mean Matching (TMM) and Hop Differentiating Technique (HDT). The TMM requires training of one-hop and two-hop wireless connection features. The HDT does not need training of wireless connection features. Panch and Singh [23] proposed a key exchange method after handshaking to detect evil twins. Nikbakhsh et al. [24] detects evil twins by checking IP addresses from APs.

To detect evil twin attacks on client side, the above solutions need to associate a computer with an AP first, then either connects to the Internet or not. Due to this property, some of them needs to specify the AP to associate with. It is impossible to detect an evil twin when having a low RSSI or be attacked by a de-authentication attack. Moreover, some of them do not work, if the AP under tests requires a user to provide account information to log in and the user does not provide it before the tests.

3. Principle and detection algorithm

This section describes the monitor mode of a Wireless Network Interface Controller (WNIC), fundamental phenomenon of evil twin attacks, and the detection algorithm of ET Detector.

[1] WLAN frequency band standards described in IEEE 802.11, for instance, 802.11g.

Please cite this article as: F.-H. Hsu et al., A Client-side detection mechanism for evil twins, Computers and Electrical Engineering (2015), http://dx.doi.org/10.1016/j.compeleceng.2015.10.010