February 28, 2019

Automatic detection of fake Wi-Fi access points

Ning Zhang

Shi Lu

Automatic detection of fake Wi-Fi access points

ABSTRACT

An evil twin access point is an illegitimate access point that masquerades as a legitimate access point and tricks users into connecting to it. Malicious actors use evil twin access points to steal account names, passwords, and other private information of unsuspecting users. This disclosure describes techniques to automatically detect and avoid evil twin access points.

KEYWORDS

- Evil twin attack
- Wi-Fi
- Access point
- Malware
- Phishing
- Hotspot
- Trace route

BACKGROUND

An evil twin access point is an illegitimate access point that masquerades as a legitimate access point, e.g., by using the same SSID as a legitimate access point, and tricks users into connecting to it. Malicious actors use evil twin access points to insert malicious systems into the data flow between victims and the network. Such systems can then eavesdrop on network traffic and attempt to steal account names, passwords, and other private information of unsuspecting users [1], [2].

DESCRIPTION

The techniques of this disclosure leverage certain differences in features between legitimate and evil-twin access points in order to detect an evil twin access point. The differences include, for example:

- An evil twin access point usually adds more hops to the data path.
- An evil twin access point usually serves fewer client devices than a legitimate, commercial access point.
- A legitimate, commercial access point is usually served by a wired back-end connection to a well-known internet service provider (ISP), whereas an evil twin access point often has a wireless back-end.
- A commercial access point is generally a well-known brand of high capacity, whereas an evil twin access point is usually operated out of a laptop or other device.

Each of these differences in features is discussed in greater detail below.

Number of hops in the data path

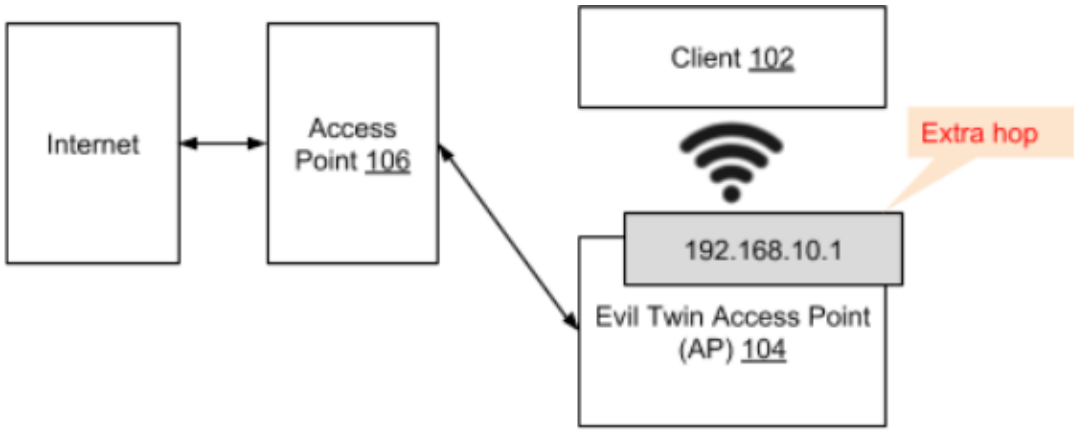

Fig. 1: An evil twin Wi-Fi connection has more hops than a legitimate Wi-Fi connection

As illustrated in Fig. 1, a client (102) that connects via an evil twin access point (104) to a legitimate access point (106) experiences more hops in its data path as compared to a direct connection to the legitimate access point. The greater number of hops in an evil twin connection can be detected using a traceroute tool. For example, a legitimate connection may have, e.g., five nodes in a traceroute call as follows:

```
Client device ↔ access point ↔ ISP ↔ internet ↔ well-known website or internal server.
```

An evil twin connection may have, e.g., six nodes in a traceroute call, as follows:

```
Client device ↔ evil twin hotspot ↔ access point ↔ ISP ↔ internet ↔ well-known website
or internal server.
```

Also, in a genuine connection, there is generally only one private IP address, whereas in a connection established via an evil twin there may be more than one private IP address.

Number of clients served

Host IP Address	Host Name	Host MAC Address	Description
192.168.1.1	Network Router ZZZ	7E-E5-4D-88-	This is Your Router/Modem
192.168.1.5	Smart speaker	84- -69-BC- 90	
192.168.1.6	Lightbulb	88-53- -42- 73	
192.168.1.7	User's smartphone	14- -C5-88- -D5	
192.168.1.8	Laptop	78- -08- 10-37	
192.168.1.9	Home Computer	00- -29-B8- -0D	This is Your Local System

Fig. 2: Number of clients served by an access point

As illustrated in Fig. 2, the number of clients served by an access point can be determined using a Wi-Fi network monitoring tool. A legitimate, commercial access point usually serves more client devices, e.g., smartphones, laptops, PDAs, etc., than an evil twin access point.

Wired vs. wireless backend and analysis of public IP

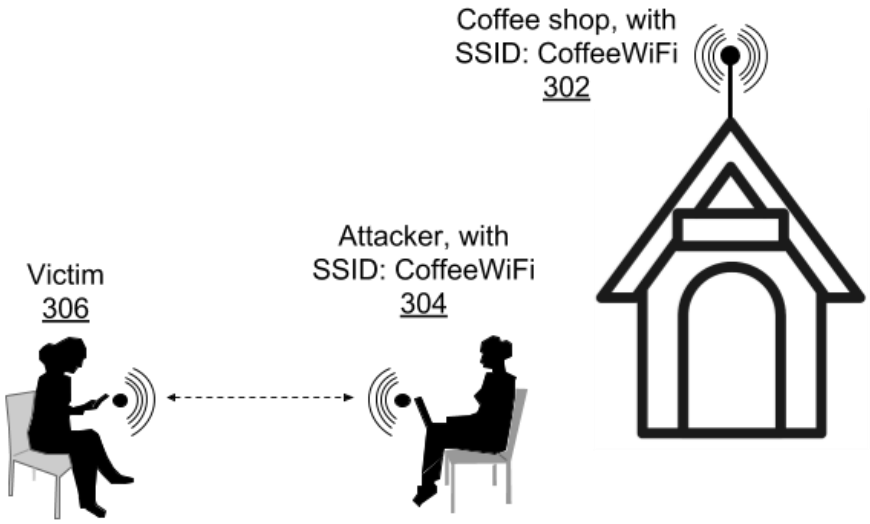

Fig. 3: An evil twin has a wireless backend; a legitimate access point has a wired backend

As shown in Fig. 3, a malicious actor (304) may often set up an evil twin access point near a genuine access point (302) as a Wi-Fi hotspot operating out of a laptop to attempt to have a victim device (306) connect to it. Such an evil twin can be detected by testing if the back-end of the access point is wired or wireless. A legitimate, commercial access point is usually served by a wired back-end connection to a well-known ISP, whereas an evil twin access point often has a wireless back-end. Also, in the case of a legitimate access point, the ISP assigns a public IP address to the client device; a mobile or residential address assigned to the client is likely an indication that the access point is an evil twin.

Type of access point

A commercial hotspot is often served by a business-level WiFi router with identifiable signatures based on ports, brands, OS information, etc. An evil twin hotspot is usually a small or portable router, e.g., a laptop or personal computer with a network card. An evil twin can therefore be detected by analyzing the signature of the access point.

A combination of one or more of the aforementioned techniques can be used to detect an evil twin attack efficiently, often in real time. A database, e.g., comprising access point signatures or other information pertaining to the aforementioned techniques, can be created and stored to facilitate detection of an evil twin.

CONCLUSION

An evil twin access point is an illegitimate access point that masquerades as a legitimate access point and tricks users into connecting to it. Malicious actors use evil twin access points to steal account names, passwords, and other private information of unsuspecting users. This disclosure describes techniques to automatically detect and avoid evil twin access points.

REFERENCES

[1] Andy O'Donnell. "The dangers of evil twin Wi-Fi hotspots." https://www.lifewire.com/dangers-of-evil-twin-wi-fi-hotspots-2487659 accessed on Jan. 28, 2019.

[2] Jeff Ehling, "Hackers set up fake Wi-Fi hotspots to steal your information." https://abc13.com/technology/hackers-set-up-fake-wi-fi-hotspots-to-steal-your-information/835223/ accessed on Jan. 28, 2019.

[3] Song, Yimin, Chao Yang, and Guofei Gu. "Who is peeping at your passwords at Starbucks?—To catch an evil twin access point." *In Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, pp. 323-332. IEEE, 2010.

[4] Matthew Peters. "How would you detect an evil twin attack, especially in a new environment? https://security.stackexchange.com/questions/85138/how-would-you-detect-an-evil-twin-attack-especially-in-a-new-environment/85143#85143 accessed on Jan. 28, 2019.