**International Information Technology University**

**Faculty of Computer Technology and Cybersecurity**

**Department of Network Security**

**Mobile security technologies (SEC6205) Project 2**

**Evil Twin Attack: A Threat to Wireless Networks**

Group: SIS-2123

id: 30739

team: only YERKANAT

teacher: Dr. Qais Qassim

Almaty, 2024

**Introduction:**

In the field of Cyber Security, we are struggling with Evil Twin Attack which has enormous opportunities, especially on wireless networks. The goal of MY project is to provide a complete evaluation of the Evil Twin Attack, its mechanics, vulnerabilities, real-world examples, and mitigation techniques.

**Description:**

The main idea is to create a malicious wireless network with the same WIFI name as the original one and see requests.

Evil Twin Attack is a rogue AP that masquerades as a reliable network by adopting an identical SSID name ​​​​and different properties. Once connected, an attacker can intercept and control the facts transmitted between the victim's device and the fake AP.

Technically, the attack can be accomplished by many open source tools such as Wi-Fi Pumpkin, airgeddon.

***What is Evil Twin Attack?:***

So, hacker creates a fake Wi‑Fi network with the same SSID name, similar to an original access point, to steal the victim's information, everything requested using GET/POST/PUT methods.

Evil Twin Attacks are effective because computers and phones only see the main "name" or ESSID of the wireless network, so it makes difficult to determine networks with the same name and the same type of encryption.

The most common kind of Evil Twin Attack is using Captive Portals, a type of network service that is commonly used in public Wi-Fi places: hotels, airports, and cafes to control access to the internet. When a user connects to a network with a captive portal, they are typically redirected to a login page where they must perform certain actions, such as agreeing to terms of service or entering login credentials, before they can access the internet.

When user accesses the internet, actually when it makes GET request, everything will be shown on command line of hacker, so by this way user gives passwords and other personal informations.

After obtaining the victim's credentials, the attacker can use them to log into the legitimate network, effectively hijacking the victim's internet connection. This allows the attacker to monitor unencrypted traffic, inject malicious content, or perform other nefarious activities on the network.

**Exploited Vulnerabilities:**

The Evil Twin Attack thrives (Aaron Boyd, 2020)[[1]](#footnote-1)on exploiting weaknesses found in wireless network setups because of incomplete shown general name and other credentials of potential Wi-Fi network name. For instance, some Wi-Fi networks lack strong encryption methods, making it easier for attackers to sneak in and intercept and keep on data exchanges in real. Additionally, weak authentication protocols allow unauthorized access, while the absence of network monitoring leaves networks vulnerable to unnoticed breaches. In particular, open Wi-Fi networks without encryption create a welcoming environment for attackers to intercept data transmissions without even being detected.

**Real-World Examples:**

(McMillan, 2007), At the Toorcon conference researcher Vivek Ramachandran demonstrated an attack on WEP-encrypted networks, exploiting flaws in WEP to steal data using the Evil Twins Attack. Known as the WEP-enabled clients into connecting to a fake network, facilitating man-in-the-middle attacks to intercept internet activity. Ramachandran's technique underscores the persistent security vulnerabilities associated with WEP.

# I got hacked while using airport WiFi

(Carlton, 2023) At Sydney airport, distracted by deadlines and coffee quests, a traveler fell victim to a Wi-Fi scam. After unknowingly connecting to a fraudulent network, their online banking was compromised, resulting in unauthorized charges. This scam, known as an "Evil Twin" attack, is common in public Wi-Fi areas. To protect against such scams, travelers are advised to be vigilant about Wi-Fi connections and avoid accessing sensitive information on public networks. Utilizing a VPN can also enhance data security. This incident serves as a reminder of the risks associated with public Wi-Fi and the importance of safeguarding personal information online.

My life example…

**Mitigation Strategies:**

Effective countermeasures against the Evil Twin Attack encompass both technical (Lisa Phifer, 2007)and user awareness initiatives. Employing robust encryption protocols such as WPA3 strengthens the security of wireless networks by encrypting data transmissions, thereby thwarting interception attempts. Additionally, implementing strong authentication mechanisms, such as 802.1X authentication, prevents unauthorized access to network resources.

User education and awareness play a pivotal role in mitigating the risk posed by the Evil Twin Attack. Educating users about the dangers of connecting to unsecured Wi-Fi networks and promoting the use of VPNs (Virtual Private Networks) empower them to make informed decisions regarding their online security. Moreover, organizations should regularly monitor their wireless networks for suspicious activity and deploy intrusion detection systems to detect and mitigate potential attacks in real time.

**Conclusion:**

In conclusion, the Evil Twin Attack is a simple and dangerous thing that can be accomplished by anyone, only self-awareness can help you.

# References

Aaron Boyd. (2020, september 16). A team of hackers was able to gain access to Interior networks using publicly available equipment, open source software and a backpack. *NEXTGOV FCW*, 3.

Carlton, A. (2023, april 14). I got hacked while using airport WiFi. p. 3.

hh. (n.d.).

Lisa Phifer, E. S. (2007). *The Caffe Latte Attack: How It Works — and How to Block It.* Toronto: https://wi-fiplanet.com/the-caffe-latte-attack-how-it-works-and-how-to-block-it/.

McMillan, R. (2007, 10 17). *Cafe Latte attack steals data from Wi-Fi users*. Retrieved from https://www.computerworld.com/: https://www.computerworld.com/article/1564878/cafe-latte-attack-steals-data-from-wi-fi-users.html

Shuciran. (2023, 10 01). *Attacking Captive Portals*. Retrieved from Shucirans Pentesting notes: https://shuciran.github.io/posts/Attacking-Captive-Portals/

1. [Interior IG Team Used Evil Twins and $200 Tech to Hack Department Wi-Fi Networks - Nextgov/FCW](https://www.nextgov.com/cybersecurity/2020/09/interior-ig-team-used-evil-twins-and-200-tech-hack-department-wi-fi-networks/168521/) [↑](#footnote-ref-1)