DEVELOPMENT OF A WI-FI SECURITY APPLICATION FOR DETECTING AND MITIGATING EVIL TWIN ATTACKS

Undergraduate Thesis
Submitted to the Faculty of the
Department of Computer Studies
Cavite State University - Imus Campus
City of Imus, Cavite

In partial fulfillment
of the requirements for the degree
Bachelor of Science in Computer Science

CZAR JOHN VILLAREAL
LOUISE MARK BANDOJA
VON PHILIPPE ACERO
January 2025

CAVITE STATE UNIVERSITY
Imus Campus
Cavite Civic Center Palico IV, Imus, Cavite
(046) 471-66-07 / (046) 471-67-70/ (046) 686-2349
www.cvsu.edu.ph

BAGONG PILIPINAS

Department of Computer Studies

PROPOSAL APPROVAL SHEET

Author(s): **CZAR JOHN VILLAREAL**
LOUISE MARK BANDOJA
VON PHILIPPE ACERO

Title of the Study: **DEVELOPMENT OF A WI-FI SECURITY APPLICATION FOR DETECTING AND MITIGATING EVIL TWIN ATTACKS**

Degree or Course: **BACHELOR OF SCIENCE IN COMPUTER SCIENCE**

APPROVED:

ROSALINA D. LACUESTA, MIT ______
Adviser Date

RAMIL V. HUELE ________
Technical Critic Date

GRACE S. IBAÑEZ, MSCS _______
Department Chairperson Date

LIANE VINA G. OCAMPO, PhD ______
Campus Research Coordinator Date

JENNY BEB F. ESPINELI, PhD ______
Campus Administrator Date

INTRODUCTION

Background Of The Study

Wireless networks have revolutionized modern communication, providing convenience and connectivity across diverse environments. Their widespread adoption has enabled seamless interaction for personal, professional, and industrial purposes. However, this ubiquity has also exposed them to numerous security threats, one of the most prominent being the Evil Twin Wi-Fi attack. This type of attack is particularly insidious as it exploits users' trust in familiar wireless networks, creating a fraudulent access point that deceives users into connecting to it.

Evil Twin Wi-Fi attacks pose a significant risk to both individuals and organizations, often leading to unauthorized access to sensitive data, such as login credentials, financial information, and personal communications. The simplicity and effectiveness of these attacks make them a popular choice for cybercriminals, especially in public spaces like airports, cafes, and educational institutions. Despite advancements in cybersecurity technologies, these attacks continue to thrive due to the interplay of human factors and technical vulnerabilities.

Understanding the mechanisms behind Evil Twin Wi-Fi attacks is crucial for developing robust countermeasures. These attacks exploit weaknesses in wireless protocols, network configurations, and user behavior. By analyzing the strategies employed by attackers, researchers and cybersecurity professionals can identify critical vulnerabilities and develop targeted solutions to protect wireless networks and their users from exploitation.

This study aims to provide an in-depth analysis of Evil Twin Wi-Fi attacks, examining both the technical and behavioral aspects. Through case studies, simulations, and a review of existing mitigation methods, the research seeks to bridge gaps in current practices and propose innovative strategies for detection and prevention. The insights gained will contribute to the broader goal of enhancing wireless security and protecting user data.

Statement Of The Problem

The effectiveness of existing mitigation methods for Evil Twin attacks in wireless networks has yet to be fully assessed. While numerous countermeasures have been proposed, such as encryption improvements, monitoring systems, and user authentication enhancements, their ability to consistently prevent such attacks in diverse network environments remains unclear. The evolving nature of these attacks, alongside the continuous adaptation of attacker techniques, further complicates the evaluation of current solutions. This research seeks to conduct an in-depth analysis of the existing mitigation methods for Evil Twin attacks, examining their strengths, limitations, and practical applicability. By identifying gaps and inefficiencies, this study aims to contribute to the development of more robust, scalable, and effective strategies to enhance the security of wireless networks against evolving threats. *How can an analysis of existing mitigation methods for Evil Twin attacks contribute to enhancing the security of wireless networks?*

Evil Twin attacks, a form of Wi-Fi spoofing, pose significant security threats to wireless networks by impersonating legitimate access points to deceive users into connecting to malicious networks. These attacks can lead to unauthorized access, data breaches, and the exposure of sensitive information. Despite the increasing awareness of such attacks, current mitigation methods remain insufficient in addressing the evolving tactics employed by attackers, particularly in dynamic and large-scale environments. This thesis aims to analyze and evaluate various methods of mitigating Evil Twin attacks, assessing their effectiveness in preventing unauthorized access, securing user data, and improving the overall safety of wireless networks. The research will provide insights into the strengths and limitations of existing solutions for securing wireless communications against this growing threat. *How effective are the current mitigation methods in preventing Evil Twin attacks?*

Wireless networks are susceptible to various security threats, including Evil Twin attacks, which can compromise the integrity and confidentiality of data. While several countermeasures exist to address these attacks, their effectiveness remains uncertain in different network environments. This research aims to assess the effectiveness of the proposed countermeasure in preventing Evil Twin attacks, considering its potential advantages over existing solutions and evaluating its ability to provide a more secure wireless network environment. *How effective is the proposed countermeasure in preventing Evil Twin attacks on wireless networks?*

Objectives Of The Study

Generally, this thesis aims to analyze existing mitigation methods for Evil Twin attacks, evaluate their effectiveness in enhancing the security of wireless networks, and propose a countermeasure for more robust defense mechanisms.

Specifically, the study aims to:

1. Perform an analysis on existing mitigation methods for Evil Twin attacks to contribute to enhancing the security of wireless networks.

2. Analyze the effectiveness of the current mitigation methods in preventing Evil Twin attacks.

3. Analyze the effectiveness of the proposed countermeasure in preventing Evil Twin attacks on wireless networks.

Time And Place Of The Study

The study "DESIGN AND DEVELOPMENT OF A WI-FI SECURITY APPLICATION FOR DETECTING AND MITIGATING EVIL TWIN ATTACKS" was conducted at Cavite State University - Imus Campus over a whole academic year, from September 2024 to June 2025, During this period, the development, assessment and testing phases of the project was meticulously carried out. This time frame allows for the thorough refinement and validation of the project's analysis to effectively meet the required outcomes.

Scopes And Limitations

This study focuses on the mechanisms of Evil Twin Wi-Fi attacks, exploring their setup, execution, and potential impact on users and systems. It aims to analyze detection and mitigation techniques, including hardware-based solutions, software algorithms, and user-awareness campaigns. Public wireless networks, such as those found in cafes, airports, and educational institutions, are emphasized, given their susceptibility to such attacks. The study also incorporates case studies and simulations to demonstrate the practical implications of these attacks and the effectiveness of proposed countermeasures.

The research is constrained by ethical considerations, which preclude the deployment of real-world Evil Twin attacks for analysis. Instead, the study relies on theoretical frameworks and simulated environments to understand the attack mechanisms. Additionally, the scope does not extend to other types of wireless security threats or physical-layer attacks unrelated to Evil Twin scenarios. Proprietary or specialized security measures that are inaccessible for analysis are excluded from this study

Definition Of Terms

Evil Twin Attack: A cyberattack where a malicious actor sets up a fraudulent wireless access point that mimics a legitimate one to intercept sensitive user data.

Wireless Network: A network that allows devices to connect and communicate using radio waves instead of physical cables.

Mitigation Methods: Strategies and technologies employed to reduce or prevent the impact of cyberattacks.

Access Point (AP): A hardware device or software that allows wireless devices to connect to a network.

SSID (Service Set Identifier): The unique name assigned to a Wi-Fi network, which is broadcast by access points.

Man-in-the-Middle (MITM) Attack: A type of cyberattack where an attacker secretly intercepts and relays communication between two parties.

Encryption: The process of converting data into a coded format to prevent unauthorized access.

Simulation: The use of a virtual environment to model and study the behavior of systems under specific conditions.

Cybersecurity: The practice of protecting systems, networks, and programs from digital attacks.

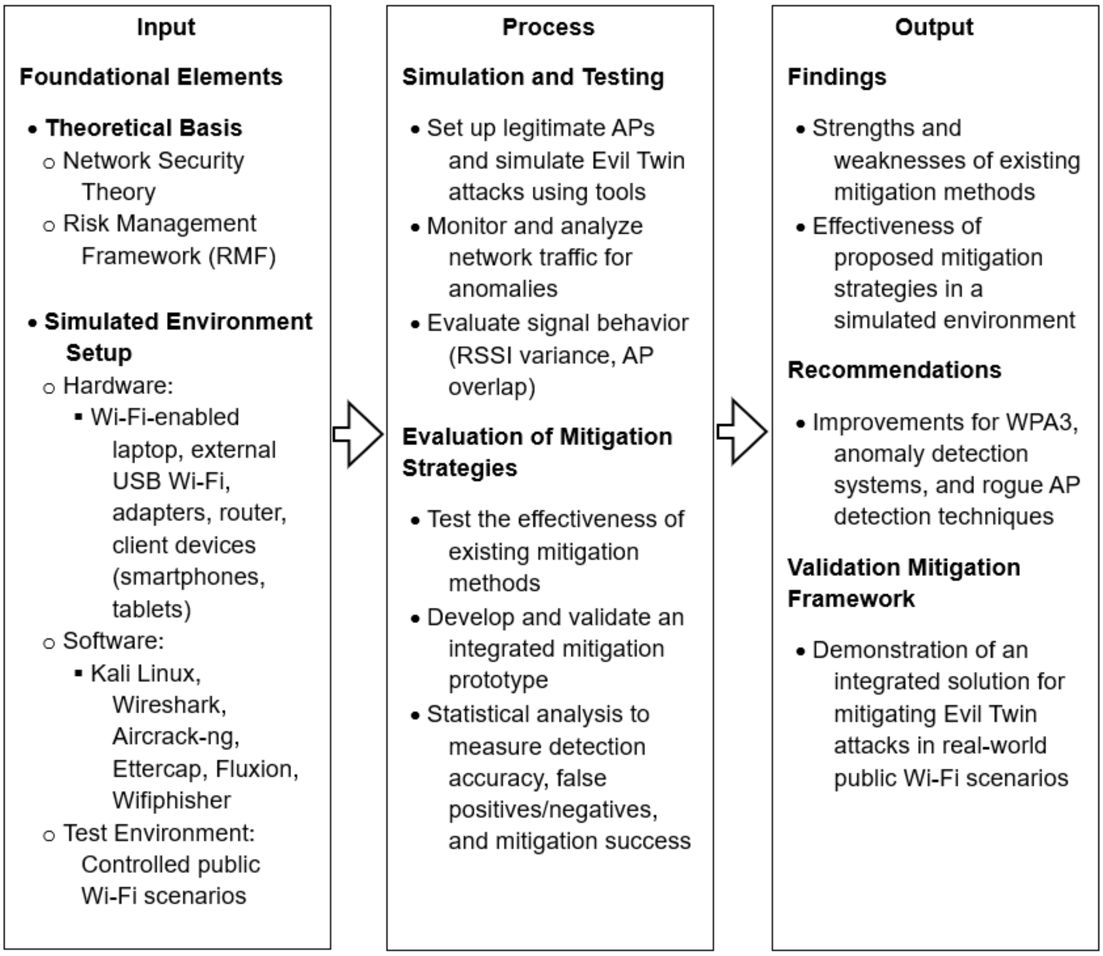
User Awareness: Education and training programs designed to help individuals recognize and avoid potential cybersecurity threats.

Theoretical Framework

In this study, Network Security Theory and the Risk Management Framework (RMF) will serve as the primary theoretical foundations for analyzing existing mitigation methods for Evil Twin attacks. Network Security Theory focuses on the principles, protocols, and technologies designed to protect networks from malicious threats. Specifically, encryption protocols like WPA2 and WPA3, along with authentication mechanisms such as mutual authentication, are crucial in safeguarding networks against attacks like Evil Twin. By examining these protocols through the lens of Network Security Theory (Stallings, 2016), this study will assess how effectively these security measures prevent attackers from impersonating legitimate access points and gaining unauthorized access to user data. The theory will guide the evaluation of technical mechanisms employed in securing wireless networks, such as the encryption of communication, detection of rogue access points, and intrusion detection systems, to determine their real-world effectiveness.

Furthermore, the Risk Management Framework (RMF), as outlined by the National Institute of Standards and Technology (2018), will provide a structured approach to identifying, assessing, and mitigating security risks, including those posed by Evil Twin attacks. The RMF emphasizes a comprehensive, multi-level approach to managing security and privacy risks in information systems. By applying the RMF to existing security measures, this study will evaluate how well current mitigation strategies address the risks associated with spoofed access points and rogue networks. The framework's process of categorizing information systems, selecting and tailoring security controls, assessing their effectiveness, and continuously monitoring for changes will help in understanding the strengths and weaknesses of existing methods. This will also enable the identification of gaps in current defenses and contribute to recommendations for improving the security of wireless networks against such attacks.

Conceptual Framework



Input

Foundational Elements

- **Theoretical Basis**
  - Network Security Theory
  - Risk Management Framework (RMF)
- **Simulated Environment Setup**
  - Hardware:
    - Wi-Fi-enabled laptop, external USB Wi-Fi, adapters, router, client devices (smartphones, tablets)
  - Software:
    - Kali Linux, Wireshark, Aircrack-ng, Ettercap, Fluxion, Wifiphisher
  - Test Environment: Controlled public Wi-Fi scenarios

Process

Simulation and Testing

- Set up legitimate APs and simulate Evil Twin attacks using tools
- Monitor and analyze network traffic for anomalies
- Evaluate signal behavior (RSSI variance, AP overlap)

Evaluation of Mitigation Strategies

- Test the effectiveness of existing mitigation methods
- Develop and validate an integrated mitigation prototype
- Statistical analysis to measure detection accuracy, false positives/negatives, and mitigation success

Output

Findings

- Strengths and weaknesses of existing mitigation methods
- Effectiveness of proposed mitigation strategies in a simulated environment

Recommendations

- Improvements for WPA3, anomaly detection systems, and rogue AP detection techniques

Validation Mitigation Framework

- Demonstration of an integrated solution for mitigating Evil Twin attacks in real-world public Wi-Fi scenarios

Figure 1. Conceptual Framework in a Input-Process-Output Format

REVIEW OF RELATED LITERATURE AND STUDY

This section of the study reviews the existing body of literature on Evil Twin attacks, focusing on their detection and mitigation methods. It highlights diverse approaches, including the use of whitelist mechanisms, advancements in certificate management, innovative IoT security frameworks, and multi-hop detection systems. Each study is analyzed in terms of methodology, findings, and the gaps that remain unaddressed. By synthesizing insights from these works, this review aims to establish a comprehensive understanding of current challenges and potential avenues for further exploration in mitigating Evil Twin Wi-Fi attacks.

Evil Twin Attack Mitigation Techniques in 802.11 Networks

A study in the International Journal of Advanced Computer Science and Applications (2021) investigates Evil Twin attacks within the IEEE 802.11 standard. The researchers developed an algorithm that uses a whitelist approach to detect rogue APs by analyzing network traffic. This method showed effectiveness in identifying fake APs by comparing the detected APs against a pre-approved list. The algorithm achieved high accuracy in controlled environments and demonstrated the potential for practical implementation in small-scale networks.

However, the reliance on a static whitelist emerged as a significant limitation, as it required manual updates to accommodate legitimate AP changes. This lack of adaptability made the approach less effective in dynamic environments, such as public Wi-Fi hotspots or enterprise networks, where legitimate APs frequently change.

The Devil is in the Details: Hidden Problems of Client-Side Enterprise Wi-Fi Configurators

A 2023 study examined the effectiveness of Wi-Fi configurators designed to protect users from Evil Twin attacks in enterprise environments. Researchers analyzed multiple configurators, including the trust-on-first-use (TOFU) configurator on Android, two open-source Android Wi-Fi configurators, and a commercial configurator. Their findings revealed that all these tools suffered from weaknesses caused by design flaws, implementation errors, or poor deployment practices. Notably, the TOFU configurator contained design flaws that allowed attackers to execute stealthy Evil Twin attacks.

Additionally, open-source configurators failed to enforce proper server authentication under specific conditions, often due to complexities in certificate name matching and Android API limitations. The commercial configurator, while widely used, permitted insecure Wi-Fi configurations and allowed the covert injection of certificates, potentially intercepting other TLS traffic. The study concluded that developing a user-friendly yet secure Wi-Fi configuration system remains a challenge, highlighting the ongoing relevance of the Evil Twin threat.

A Robust Certificate Management System to Prevent Evil Twin Attacks

In 2023, researchers proposed a robust certificate management system (RCMS) to address vulnerabilities in 802.1X authentication. The system focused on enhancing the verification of network certificates, reducing the chances of users being tricked into connecting to rogue APs. The RCMS system incorporated automatic certificate validation and user notification mechanisms, significantly reducing the likelihood of user error and increasing overall network security.

While promising, RCMS exhibited gaps, particularly in its lack of real-world testing. The study primarily validated its approach through simulations, leaving uncertainties about its effectiveness in diverse network conditions. Furthermore, the system heavily depended on user compliance with certificate checks, an area that requires further exploration to ensure consistent security practices.

WiFiHop - Mitigating the Evil Twin Attack through Multi-hop Detection

WiFiHop, proposed in a recent study, introduced a multi-hop detection method to mitigate Evil Twin attacks. The system identified anomalous multi-hop network paths, using deviations in network routing patterns to pinpoint rogue APs. Simulations revealed that WiFiHop effectively detected Evil Twin attacks with minimal false positives, offering a novel proactive defense mechanism.

Nonetheless, the study primarily focused on simulated environments, raising questions about the approach’s scalability and performance in real-world scenarios. Moreover, WiFiHop did not address potential evasion techniques, such as attackers modifying network paths to mimic legitimate traffic patterns, limiting its robustness against more advanced adversaries.

EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi Networks

This study explores the use of Software-Defined Networking (SDN) to detect and mitigate Evil Twin attacks. By leveraging SDN’s centralized control, the method monitors network traffic patterns to identify anomalies indicative of an Evil Twin presence. The approach demonstrated high accuracy in detecting malicious access points with minimal processing overhead.

However, the study's reliance on SDN infrastructure limits its applicability to networks that have adopted SDN. Furthermore, the real-world deployment of this method in legacy Wi-Fi systems remains a challenge, necessitating additional research to address these constraints.

Public Wi-Fi Security Threat: Evil Twin Attack Detection Based on Signal Characteristics

This research focuses on detecting Evil Twin attacks by analyzing signal characteristics, such as strength and variance, to distinguish legitimate APs from rogue ones. The approach does not require additional hardware or protocol modifications, making it a practical solution for public Wi-Fi security.

Nevertheless, the study was conducted in controlled settings and did not account for dynamic interference or other real-world challenges. Its reliance on signal-based detection may also face limitations in environments with overlapping network signals or high noise levels.

ETGuard: Detecting D2D Attacks Using Wireless Evil Twins

ETGuard introduces an incremental fingerprinting-based mechanism to identify Evil Twin access points. By analyzing beacon frames, ETGuard constructs unique fingerprints for each AP to detect anomalies. The system operates passively in real-time and demonstrated high accuracy with minimal false positives in controlled tests.

However, ETGuard focuses solely on detection, leaving gaps in prevention and mitigation strategies. Its performance in highly dynamic or high-density network environments has yet to be validated.

Table 1. Table of Comparison

	ETAMT	TDINTD	RCMS	WiFiHop	EvilScout	PWST	ETGuard	DDWSADMETA
Year	2021	2023	2023	2021	2020	2022	2021	2025
Features:								
Fake AP Detection	✔	✔	✔	✔	✔	✔	✔	✔
IEEE 802.11	✔	✖	✔	✔	✔	✔	✔	✔
Encryption & Authentication	✖	✔	✔	✔	✔	✖	✔	✔
Signal-based Detection	✖	✖	✔	✖	✖	✔	✔	✔
Client-based	✔	✔	✖	✖	✔	✔	✔	✔
Packet Analysis	✖	✖	✖	✔	✔	✔	✔	✔
Security Control	✔	✔	✔	✖	✔	✔	✖	✔

LEGEND:

ETAMT - Evil Twin Attack Mitigation Techniques in 802.11 Networks

TDINTD - The Devil is in the Details: Hidden Problems of Client-Side Enterprise Wi-Fi Configurators

RCMS - A Robust Certificate Management System to Prevent Evil Twin Attacks in IEEE 802.11 Networks

WiFiHop - WiFiHop: Mitigating the Evil Twin Attack through Multi-hop Detection

EvilScout - EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi

PWST - Public Wi-Fi Security Threat: Evil Twin Attack Detection Based on Signal Characteristics

ETGuard - ETGuard: Detecting D2D Attacks Using Wireless Evil Twins

DDWSADMETA - DESIGN AND DEVELOPMENT OF A WI-FI SECURITY APPLICATION FOR DETECTING AND MITIGATING EVIL TWIN ATTACKS

METHODOLOGY

This chapter outlines the methodology that will be followed in the development of technical mitigation methods for Evil Twin Wi-Fi attacks in public networks. It provides an overview of the steps and processes to be employed, including the materials, simulation setup, and testing methods that will be used to design and evaluate the proposed solution. Additionally, the chapter will describe the experimental units which will be implemented and tested throughout the project. The methodology aims to provide a structured approach to ensure the solutions effectively address the research objectives and enhance public Wi-Fi security.

Materials Used

The primary hardware requirement is a Wi-Fi-enabled laptop or desktop configured with a Linux distribution such as Kali Linux. This device serves as the core platform for running penetration testing tools and monitoring the testing environment. External USB Wi-Fi adapters are also necessary, as they provide support for monitor mode and packet injection, critical capabilities for simulating and analyzing Evil Twin attacks. Signal jammers will be included to test interference scenarios and evaluate the robustness of mitigation methods. These devices generate radio frequency signals that can disrupt communication between devices and access points, allowing researchers to simulate and address overlapping network signals or attempts to block legitimate APs.

A router is used to establish legitimate access points within the testing environment. This ensures a controlled setup where the interaction between legitimate and rogue APs can be closely monitored. Furthermore, client devices such as smartphones and tablets are included to simulate victim behavior, testing the compatibility and reliability of proposed mitigation strategies across diverse operating systems.

On the software side, Kali Linux offers a comprehensive suite of pre-installed penetration testing tools. Aircrack-ng is utilized for creating and monitoring rogue access points, while Wireshark is employed for detailed network traffic analysis. Ettercap is used to simulate man-in-the-middle (MITM) attacks, a common tactic in Evil Twin scenarios. Finally, specialized Evil Twin attack frameworks like Wifiphisher and Fluxion allow for the simulation of advanced attack techniques, providing a realistic environment to validate mitigation methods.

Additionally, Python, with its extensive libraries like Scapy, enables custom scripting and automation for penetration testing tasks, while Visual Studio Code (VSCode) provides an efficient development environment with features like debugging, syntax highlighting, and version control integration to streamline code management.

Experimental Units

The experimental units of this research represent the components and entities being tested and analyzed in the context of Evil Twin attack mitigation in public Wi-Fi networks. Each unit is crucial to simulate real-world scenarios and validate the proposed methods.

The Legitimate Access Point (AP) serves as the baseline for testing. It is a genuine Wi-Fi hotspot configured to adhere to standard wireless network protocols. This experimental unit simulates typical public Wi-Fi networks, helping to evaluate how effectively rogue APs mimic legitimate ones.

The Rogue Access Point (Evil Twin) is the malicious AP set up to impersonate the legitimate AP. Tools like WiFiPhisher or Fluxion will be used to configure this AP with similar characteristics to simulate an Evil Twin attack. This unit is essential to create controlled attack scenarios for testing detection and mitigation strategies.

Client Devices (Victim Devices) include smartphones, laptops, and tablets configured to mimic users connecting to public Wi-Fi. These devices test user vulnerability and behavior under various attack and mitigation conditions, simulating real-world interactions.

Network Monitoring Tools, such as Wireshark, Ettercap, and Aircrack-ng, capture and analyze network traffic to identify anomalies indicative of an Evil Twin attack. These tools validate the effectiveness of detection methods.

The Signal and Behavior Analysis Framework analyzes signal strength, variance, and other characteristics to differentiate between legitimate and rogue APs. This unit is integral for refining detection methods using real-time network data and simulating interference or overlapping network signals.

The Public Wi-Fi Environment consists of simulated setups like cafes or libraries with multiple APs and overlapping signals. This environment mimics real-world conditions to evaluate the performance of mitigation methods in dynamic and high-density network scenarios.

Finally, the Mitigation Framework or Prototype is the software or system developed as a result of this research. It integrates techniques such as automated AP verification and signal-based anomaly detection. This framework serves as the primary output, demonstrating the proposed methods' effectiveness in combating Evil Twin attacks.

Experimental Design

This research focuses on evaluating the mitigation strategies for Evil Twin attacks in public Wi-Fi networks through experimental units that simulate real-world scenarios. The Legitimate Access Point (AP) serves as the baseline, configured as a genuine public Wi-Fi hotspot. In contrast, the Rogue Access Point (Evil Twin) is a malicious AP designed to impersonate the legitimate one using tools like WiFiPhisher or Fluxion. Client Devices, including smartphones and laptops, simulate users connecting to Wi-Fi, testing user behavior and vulnerability. Network Monitoring Tools, such as Wireshark and Aircrack-ng, analyze network traffic to detect anomalies caused by Evil Twin attacks. Additionally, a Signal and Behavior Analysis Framework evaluates signal strength and characteristics to differentiate legitimate APs from rogue ones.

The experiments are conducted in simulated public Wi-Fi environments to mirror real-world conditions with multiple overlapping signals. A Mitigation Framework or Prototype, developed as the research outcome, integrates methods like automated AP verification and signal-based anomaly detection. This framework demonstrates the effectiveness of the proposed solutions. The research emphasizes the integration of various components to validate detection and mitigation strategies for combating Evil Twin attacks in dynamic and high-density network scenarios.

This research will use statistical methods to measure and analyze the listed mitigation strategies' effectiveness. Evaluation of mitigation strategies will be done by assessing detection accuracy, false positive and negative rates, and user device vulnerability, and response to attack. Statistical methods will analyze the framework's effectiveness across different environmental and network setups to ensure reliability and validity in real-world applications.

REFERENCES

Agrawal, A., & Maiti, R. R. (2023). *iTieProbe: Is your IoT setup secure against (modern) evil twin?* arXiv. https://doi.org/10.48550/arXiv.2304.12041

Banakh, R., Piskozub, A., & Opirskyy, I. (2023). Devising a method for detecting “evil twin” attacks on IEEE 802.11 networks (Wi-Fi) with KNN classification model. Eastern-European Journal of Enterprise Technologies, 3(9 (123)), 20–32. https://doi.org/10.15587/1729-4061.2023.282131

Daldoul, Y. (2023). *A robust certificate management system to prevent evil twin attacks in IEEE 802.11 networks*. arXiv. https://doi.org/10.48550/arXiv.2302.00338

Hsu, F. H., Lee, C. H., & Wang, C. S. (2023). An active user-side detector for evil twins. In G. A. Tsihrintzis, S. J. Wang, & I. C. Lin (Eds.), *2021 International Conference on Security and Information Technologies with AI, Internet Computing and Big-data Applications* (Vol. 314, pp. 199–210). Springer. https://doi.org/10.1007/978-3-031-05491-4_16

Louca, C., Peratikou, A., & Stavrou, S. (2023). A novel Evil Twin MiTM attack through 802.11v protocol exploitation. *Computers & Security, 130,* 103261. https://doi.org/10.1016/j.cose.2023.103261

Muthalagu, R., & Sanjay, S. (2021). Evil twin attack mitigation techniques in 802.11 networks. *International Journal of Advanced Computer Science and Applications, 12*(6). https://doi.org/10.14569/IJACSA.2021.0120605

Rofoo, F. F. H., Galety, M. G., Arulkumar, N., & Maaroof, R. (2022). DPETAS: Detection and Prevention of Evil twin Attacks on Wi-Fi Networks. In Lecture notes in electrical engineering (pp. 559–568). https://doi.org/10.1007/978-981-16-9012-9_45

Seo, J., Cho, C., & Won, Y. (2020). Enhancing the reliability of Wi-Fi network using Evil Twin AP detection method based on machine learning. jips-k.org. https://doi.org/10.3745/JIPS.03.0137

Shrivastava, P., Jamal, M. S., & Kataoka, K. (2020). EvilScout: Detection and mitigation of evil twin attack in SDN-enabled WiFi. *IEEE Transactions on Network and Service Management, 17*(1), 89–102. https://doi.org/10.1109/TNSM.2020.2972774

Wang, Z., Feng, X., Li, Q., Sun, K., Yang, Y., Li, M., Du, G., Xu, K., & Wu, J. (2024). *Off-path TCP hijacking in Wi-Fi networks: A packet-size side channel attack*. arXiv. https://doi.org/10.48550/arXiv.2402.12716

What is an Evil Twin Attack? Evil Twin Wi-Fi Explained. (2017, October 13). /. https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks

Wu, K. L., Hue, M. H., Tang, K. F., & Chau, S. Y. (2023). The devil is in the details: Hidden problems of client-side enterprise Wi-Fi configurators. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23)* (pp. 251–261). Association for Computing Machinery. https://doi.org/10.1145/3558482.3590199

Yang, Y., Feng, X., Li, Q., Sun, K., Wang, Z., & Xu, K. (2024). *Exploiting sequence number leakage: TCP hijacking in NAT-enabled Wi-Fi networks*. arXiv. https://doi.org/10.48550/arXiv.2404.04601