IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46ICT/2025/4639525/
Vol. 2025 (35), Article ID 4639525

Design and Experimental Evaluation of a Low-Cost Rogue Access Point Based on SOHO Hardware*

Piotr Augustyniak, Mateusz Boch and Piotr Zwierzykowski

Institute of Computer and Communication Networks,
Faculty of Computing and Telecommunications,
Poznan University of Technology, Poznań, Poland

Correspondence should be addressed to: Piotr Augustyniak, piotr.augustyniak@put.poznan.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

This paper presents the hardware and software possibilities of constructing a Rogue Access Point (RAP) using commonly available SOHO-class devices. The work has an analytical and experimental character and focuses on assessing the practicality of low-cost solutions, selection criteria, and limitations resulting from the use of open-source firmware.

The research replicates audit functionalities inspired by the Wi-Fi Pineapple platform using a TP-Link Archer C7 v2 router with OpenWrt. The results demonstrate both the feasibility and limitations of such an approach, highlighting stability, compatibility, and operational issues. The paper also discusses the implications of RAP attacks and provides recommendations for further security-oriented research.

Keywords: Rogue Access Point, SOHO router, OpenWrt, Wi-Fi Pineapple, network security, captive portal, deauthentication.

Introduction

The objective of this paper is to present the hardware and system-level capabilities for constructing a Rogue Access Point (RAP) using commonly available SOHO devices. The study has an analytical and experimental character and focuses on evaluating low-cost solutions, their selection criteria, and the limitations associated with open-source software.

The paper is structured as follows. Section 2 introduces the concept and characteristics of Rogue Access Points and compares them with other types of unauthorized wireless access. Section 3 presents the objectives of RAP attacks, their potential consequences for the integrity and confidentiality of network infrastructure, methodology of RAP construction. Section 3 describes an implementation using a SOHO router and presents experimental results. Section 4 provides final conclusions and recommendations for future research.

Rogue Access Points: Concept and Objectives

A Rogue Access Point (RAP) is an attack that operates at the intersection of wired and wireless communication domains [**Error! Reference source not found.**]. It involves the unauthorized physical connection of an access point to an organization's internal network without administrator approval. Once installed, the device can provide attackers with wireless access to the internal network, enabling traffic interception, monitoring, or manipulation. Unlike the *Evil Twin* attack, which acts solely in the wireless domain by impersonating a legitimate access point,

Cite this Article as: Piotr Augustyniak, Mateusz Boch and Piotr Zwierzykowski, Vol. 2025 (35) "Design and Experimental Evaluation of a Low-Cost Rogue Access Point Based on SOHO Hardware " Communications of International Proceedings, Vol. 2025 (35), Article ID 4639525, https://doi.org/10.5171/2025.4639525

a RAP exploits physical network access, significantly expanding the attacker's operational scope [**Error! Reference source not found.**,**Error! Reference source not found.**,**Error! Reference source not found.**].

RAP and SoftAP

A *SoftAP* (software-enabled access point) allows an end device to temporarily share its internet connection, often referred to as a "virtual router." Although sometimes used interchangeably with "unauthorized AP," the two terms describe different phenomena. An unauthorized AP may refer to both employee-created SoftAPs violating security policies and privately installed physical devices connected to enterprise networks. In both cases, these actions bypass official protection mechanisms and increase the risk of unauthorized access. Rapid detection and response to such devices should be prioritized in network security policies.

Objectives of a RAP Attack

The main goal of a RAP attack is to gain access to internal resources while bypassing established security measures. A RAP enables an attacker to monitor, capture, and modify network traffic. Depending on intent, the RAP can serve as a simple backdoor or as a man-in-the-middle (MITM) attack vector requiring additional configuration and routing manipulations [**Error! Reference source not found.**].

RAP attacks may succeed even without long-term concealment, especially in environments where detection mechanisms are inactive. Therefore, prevention, monitoring, and physical control of access points are essential [**Error! Reference source not found.**].

Concept and Methodology of RAP Construction

From an attacker's perspective, building a Rogue Access Point requires maintaining anonymity and minimizing residual forensic traces. Reusing previously operated devices increases the risk of identification, as modern forensic tools can recover configuration data and usage artifacts. For this reason, using unlinked, easily replaceable components and artifact-minimizing methods is recommended.

The research goal was to evaluate the feasibility of constructing RAPs with commonly available hardware and open-source software. The pragmatic approach focused on easily reproducible, low-cost, and time-efficient solutions. The selection criteria were:

1. Short preparation time,
2. Availability and low cost of components,
3. Popularity of the hardware model (ensuring repeatability and scalability).

The analysis considered both technical factors (OpenWrt compatibility, radio performance, module availability) and operational aspects (configuration simplicity, stability), as well as market and economic issues (price, availability on the secondary market).

Experimental Implementation on SOHO Router

The experimental work was inspired by the **Wi-Fi Pineapple** auditing platform by Hak5, which is widely used in wireless penetration testing. The platform is available in Nano (2.4 GHz) and Tetra (2.4 GHz and 5 GHz) variants. It offers a web-based graphical interface and a set of open-source tools built on OpenWrt.

Fig. 1. Wi-Fi Pineapple Tetra device in basic version [Error! Reference source not found.**]**

The purpose of this experiment was to determine whether similar functionality could be achieved on low-cost SOHO hardware, maintaining minimal cost and setup time. A **TP-Link Archer C7 v2** router was selected for testing.

Fig. 2. Router TP-Link Archer C7 v2

The main criterion for choosing the **Wi-Fi Pineapple** device was its comprehensiveness. In the commercial solutions market, **Wi-Fi Pineapple**, understood as a device with specific software, is unrivaled.

Price is an important factor when it comes to commercial tools. In the case of a ready-made product, it ranges from PLN 1,343 to PLN 5,239. To provide an economic reference point, the current prices of post-lease laptops (from various manufacturers) with basic specifications: i7-8665u, 16 GB RAM, 500 GB SSD; or AMD Ryzen 3 PRO 5450u, 16 GB RAM, 500 GB SSD can be purchased for around PLN 1,100. These parameters are more than sufficient for comfortable everyday work.

When selecting a device for testing, it was crucial to limit the expenditure to PLN 100 (USD 27) and to meet the following hardware criteria:

- Dual Band 2.4/5GHz support
- (at least one) USB 2.0 port
- the chip must have full support for OpenWrt and be at least as good as the chips used in Wi-Fi Pineapple

The "Tetra" version of Wi-Fi Pineapple is equipped with an Atheros AR9344 [7] SoC chip (interestingly, 802.11n only 2.4 GHz, which is why it is sold with an additional card with an Atheros AR9580 module), so the test equipment must be at least at the same technological level, preferably also from the Atheros family (acquired by Qualcomm) and designed for network devices (wireless routers, Wi-Fi access points, and IoT gateways). The AR9344 chip (launched in 2012-2013) is classified as "mid-range". Together with the AR9331 [8] chip (Wi-Fi Pineapple Nano equipment), it was dedicated to low-budget devices or DIY projects with OpenWRT, where low purchase price and low energy consumption were key.

- amount of Flash memory / amount of RAM (recommended hardware for OpenWRT installation):

16MB Flash will provide for bare minimum installed packages. Devices with more storage is recommended; 128MB RAM will provide for minimal functionality. Devices with more RAM is recommended [9]

Of all the devices in the experimental room, the **TP-Link Archer C7 v2** met all the criteria listed above. The authors were able to proceed with the rest of the study without making any additional purchases (which, economically speaking, wouldn't be a significant expense for someone wanting to test network security – the cost is up to 100 PLN).

The chip used in this device (**TP-Link Archer C7 v2**) is Qualcomm Atheros QCA9558 [10] (launched in 2013-2014). This chip (QCA95xx series) is newer and more advanced than the AR9344 and AR9331 chips (Ar93xx series) mentioned above. The C7v2 version of the device is fully supported by OpenWrt (interestingly, out of the entire range of TP-Link Archer C5/C7 models, two versions, Archer C5 v2 and Archer C7 v1 [11], work with OpenWRT, but there are no drivers for Wi-Fi – to be on the safe side, these two models/versions should be avoided).

Experimental Methodology

The **Wi-Fi Pineapple** platform by Hak5 served as the primary inspiration for this experiment. The design concept of this commercially available device emphasizes ease of use, which is achieved through a **web-based graphical user interface**. The platform is built on **OpenWrt**, a firmware distribution based on the **Linux operating system for embedded devices**. In addition, it integrates a suite of **open-source security tools** equipped with a graphical management layer.
As of 2025, the device is available commercially for approximately **130 USD** in its basic version. To investigate its capabilities and operational principles, an attempt was made to **replicate its functionality** by modifying the firmware of relatively inexpensive, second-hand routers supporting **dual-band operation (2.4 GHz and 5 GHz)**.
The experimental procedure involved a series of controlled steps aimed at minimizing the risk of hardware damage and ensuring reproducibility. The following sequence was adopted:

1. Creating a **backup of the original manufacturer firmware** to enable recovery in the event of an unsuccessful modification.
2. Installing **OpenWrt 19.07.2** on the **TP-Link Archer C7 v2** router, with the goal of reproducing functionalities comparable to those offered by the Wi-Fi Pineapple platform.
3. Performing initial configuration, including setting the time zone, creating administrative accounts, configuring a basic access point, and verifying connectivity.
4. Installing and testing **functional modules** providing features used in security assessments (e.g., *captive portal*, *deauthentication tools*, and *traffic analysis utilities*).

A key feature of the original **Wi-Fi Pineapple** device is the **modular architecture** developed both by the manufacturer and the associated user community. This functionality was also successfully replicated in the **firmware cloned to the TP-Link Archer C7 v2 router**.

Following the completion of the configuration process, systematic **testing of individual modules** was carried out to evaluate their performance and stability.

The results of these tests are summarized in Table 1.

Tab. 1. Summary of Modules in the Modified Firmware Installed on the Router

No.	Module Name	Module Evaluation
1	APITokens	unnecessary
2	autossh	unnecessary
3	base64encdec	unnecessary
4	Cabinet	unnecessary
5	Commander	unnecessary
6	ConnectedClients	unnecessary
7	CursedScreech	*not working*
8	**Deauth**	**working**
9	DNSMasq Spoof	*not working*
10	DNSspoof	*not working*
11	Dump1090	unnecessary
12	DWall	*not working*
13	**EvilPortal**	**working**
14	**get**	**working**
15	HackRF	unnecessary
16	HTTP Proxy	*not working*
17	Internet Speed Test	unnecessary
18	Key Manager	unnecessary
19	LED Controller	unnecessary
20	Locate	unnecessary
21	Log Manager	unnecessary
22	MAC Info	unnecessary
23	Meterpreter	unnecessary

24	Modem Manager	unnecessary
25	Module Maker	unnecessary
26	**ngrep**	**working**
27	nmap	unnecessary
28	Occupineapple	unnecessary
29	Online Hash Crack	unnecessary
30	OpenVPNConnect	unnecessary
31	p0f	*not working*
32	**Papers**	**working**
33	PMKIDAttack	*not working*
34	Portal Auth	unnecessary
35	RandomRoll	unnecessary
36	Responder	*not working*
37	**SignalStrength**	**working**
38	Site Survey	unnecessary
39	SSID Manager	unnecessary
40	SSLsplit	*not working*
41	Status	unnecessary
42	**tcpdump**	**working**
43	Terminal	unnecessary
44	Themes	unnecessary
45	tor	unnecessary
46	urlsnarf	*not working*
47	wps	unnecessary

Results

The testing revealed limited module compatibility. Many components failed to start or crashed due to dependency issues. Functional modules included:

- **Deauth** – effective, but required manual restart of wireless interfaces.

- **EvilPortal** – stable and useful for fake login implementations.
- **ngrep/tcpdump** – suitable for monitoring, but not for HTTPS credential capture.
- **SignalStrength** – effective for reconnaissance and Wi-Fi mapping.
- **Papers** – potentially useful for MITM attacks but limited without DNS spoofing.

The adaptation achieved only partial functionality. Stability issues, outdated code, and resource limitations prevented full operational equivalence with the original Wi-Fi Pineapple platform.

Discussion

The experiment confirmed that porting auditing software to SOHO routers is economically viable but functionally constrained. Key challenges include module incompatibility, dependency conflicts, and insufficient hardware performance.
Despite these limitations, the experiment demonstrated that low-cost platforms can reproduce essential auditing capabilities, making them useful for educational and exploratory security research, provided that ethical and legal boundaries are strictly maintained.

Conclusions and Final Remarks

The study verified the feasibility of constructing Rogue Access Points (RAP) and *Evil Twin* attack frameworks using readily available SOHO hardware.

The main findings are:

- Modifying consumer routers cannot currently achieve full functionality required for advanced RAP/ET scenarios.
- Dedicated auditing platforms or portable computers provide more reliable alternatives.
- Integration with development boards and microcomputers (e.g., Raspberry Pi) may enhance flexibility and performance.
- Continuous module compatibility testing with OpenWrt and clear documentation are essential.
- All empirical research must follow ethical and legal standards within controlled environments.

Overall, this research confirms that a pragmatic, low-cost, and rapid-deployment approach is valuable for exploratory studies, yet additional engineering work is needed to achieve the stability and completeness required in professional penetration testing.

Acknowledgments

This research was funded by the Polish Ministry of Science and Higher Education (No. 0313/SBAD/1311).

References

- P. Augustyniak, O. Rogowicz, P. Zwierzykowski: *Concept and Phases of the Rogue Access Point Attack* [in]: Artificial Intelligence and Machine Learning. 43rd IBIMA Conference, IBIMA-AI 2024, Madrid, Spain, June 26–27, 2024, Revised Selected Papers, Part-I / red. Khalid S. Soliman - Cham, Switzerland : Springer Nature Switzerland AG, 2025 - pp. 290-302
- P. Augustyniak, O. Rogowicz, P. Zwierzykowski: *Theoretical and Practical Aspects of the Evil Twin Attack. The Attacker's Perspective and Defense Methodology* [in]: Artificial intelligence and Machine Learning. 41st IBIMA International Conference, IBIMA-AI 2023, Granada, Spain, June 26–27, 2023, Revised Selected Papers / red. Khalid S. Soliman - Cham, Switzerland : Springer Nature Switzerland AG, 2024 - pp. 224-236
- Juniper Networks: *Understanding Rogue Access Points*, 2018. Available at: [https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/topics/concept/wireless-rogue-ap.html] (accessed on: 27.10.2025).

- S. Harrison: *Rogue Access Point*, Cisco Meraki Blog, 2017. Available at: [https://meraki.cisco.com/blog/2017/09/rogue-access-point/] (accessed on: 27.10.2025).
- SolarWinds Success Center: *What Are Rogue Access Points (AP)*, 2022. Available at: [https://support.solarwinds.com/SuccessCenter/s/article/What-are-rogue-Access-Points-AP?language=en_US] (accessed on: 27.10.2025).
- Hak5: *Wi-Fi Pineapple Product Page*, [https://hak5.org/products/wifi-pineapple] (accessed on: 27.10.2025).
- https://raw.githubusercontent.com/Deoptim/atheros/master/AR9344_May_2012.pdf (accessed on: 02.11.2025)
- https://www.openhacks.com/uploadsproductos/ar9331_datasheet.pdf (accessed on: 02.11.2025)
- https://openwrt.org/toh/views/toh_available_16128 (accessed on: 02.11.2025)
- https://techship.com/download/compex-wpj558-embedded-board-datasheet/ (accessed on: 02.11.2025)
- https://openwrt.org/toh/tp-link/archer_c7 (accessed on: 02.11.2025)