Wi-Fied

An Educational Platform for Hands-on Wi-Fi Security

Graduate

Alice Glaus

Mario Burger

Introduction: Wi-Fi networks are an essential part of modern life, used daily in homes, schools, and businesses. Security awareness is critical for operating these networks responsibly and securely. As wireless communication becomes more widespread, the importance of understanding its vulnerabilities increases. The lack of suitable tools for exploring Wi-Fi threats in education highlighted the need for a tailored, extensible platform.

Objective: The Wi-Fied Platform is designed to support hands-on experimentation with Wi-Fi security in a safe, isolated lab environment. It is inspired by the team's preliminary academic research on the classification and impact of wireless threats and focuses on real-world learning. Three stakeholder groups guided its design: educators, students, and developers or maintainers. Educators can integrate Wi-Fied into teaching plans; students benefit from interactive exploration; and developers can extend the platform over time. Rather than replace existing tools, Wi-Fied complements them by bridging the gap between theory and applied understanding of Wi-Fi attacks and defenses. A stakeholder diagram (see Figure 2) illustrates shared and unique interests across these groups.

Result: Wi-Fied enables practical demonstrations of common vulnerabilities in IEEE 802.11 networks, such as deauthentication attacks or WPA2 handshake exploits. It emphasizes reproducibility, controlled testing, and accessibility through affordable hardware like Raspberry Pi devices (see Figure 3). Its modular architecture allows further development and the easy addition of new attack scenarios or learning tools. The platform lays a flexible foundation for expanding educational use and supporting security experimentation in academic contexts. Future

directions may include more advanced scenarios, interactive visualizations, and a graphical user interface to improve accessibility. Wi-Fied is well-suited for integration into cybersecurity lab courses or workshops, promoting hands-on, inquiry-based learning. Next steps involve testing the tool in lab-sessions with students.
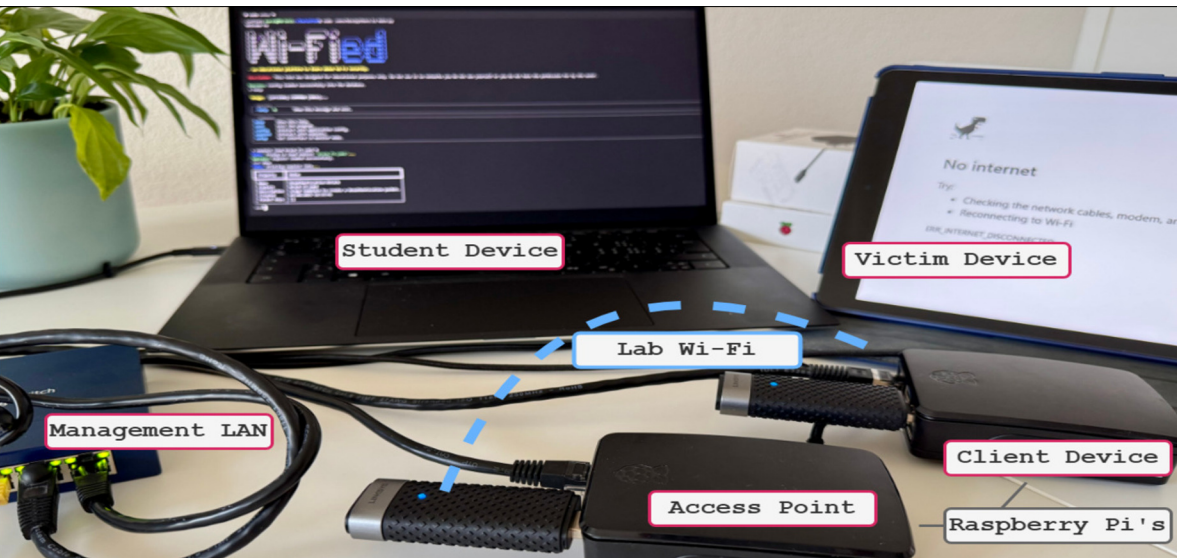
1) System Context Diagram (C4-Model Level 1) of the Wi-Fied Platform
Own presentment
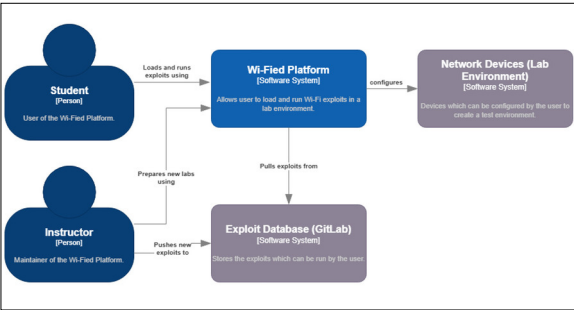
2) Primary Stakeholder Groups of the Project
Own presentment
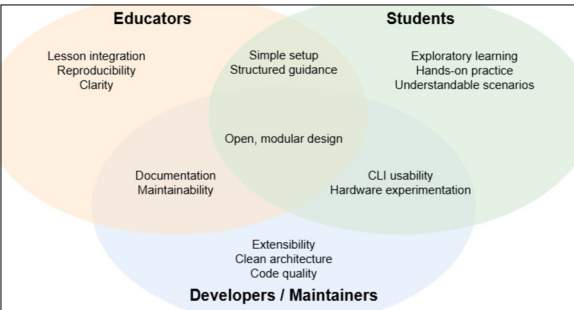
3) Real-life Setup of Lab-Devices
Own presentment

Advisor
Dr. Daniel Tschudi

Co-Examiner
Dr. Bernhard Tellenbach, Cyber-Defence Campus, Zürich, ZH

Subject Area
Networks, Security & Cloud Infrastructure