SNiFi

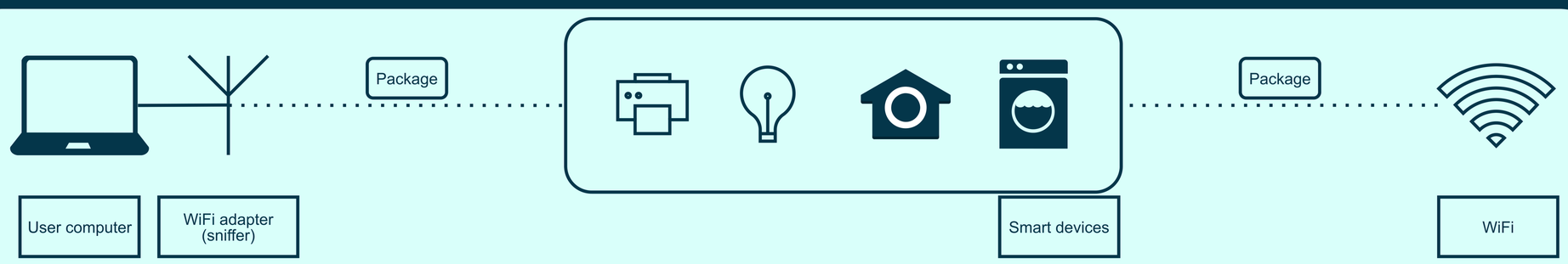
Marcin Kielar
markie9@st.amu.edu.pl

Kacper Dawidowicz
kacdaw@st.amu.edu.pl

Damian Judek
damjud@st.amu.edu.pl

Abstract

SNiFi is easy to use solution that aims to increase safety of small and medium sized networks. Its main goal is to provide network security insight to people with lesser technical knowledge by monitoring network traffic, detecting abnormal activity and notifying user about incidents in an easy to understand and informative format focused around educating user about current threats and possible mitigations.

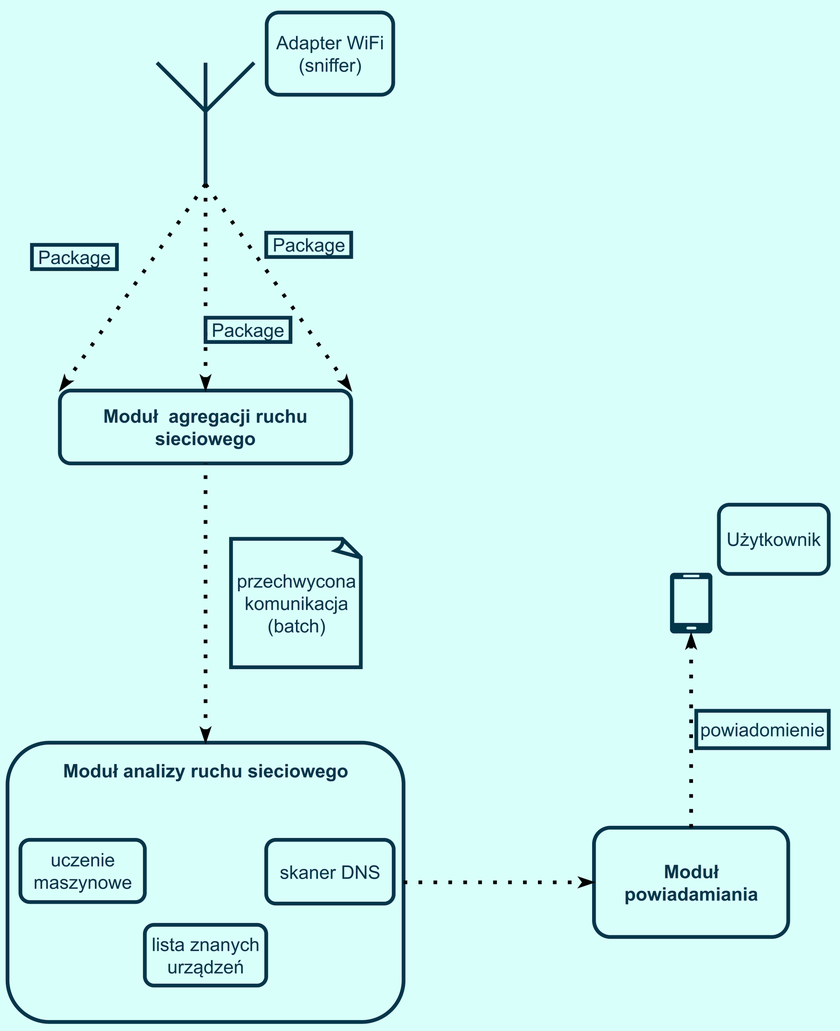


System Architecture

This project's system architecture integrates a traffic aggregation module, an analysis module with machine learning for traffic classification, active network scan module, and intuitive user interface for configuration and real time monitoring.

Packet Analysis

Custom machine learning model is utilized in the Packet Analysis module alongside conventional solutions to identify and classify malicious network traffic. Increased capabilities of a such hybrid detection module ensures fast and effective operation.

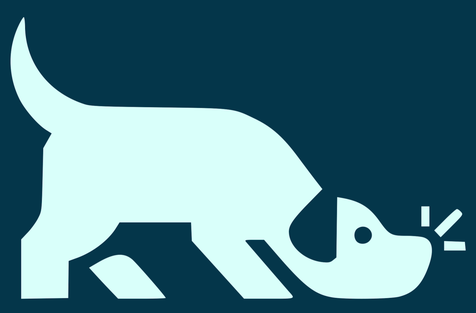


Network Scans

Active scans are conducted to evaluate security of each device attached to the network, identifying risks and changes in devices presence and behavior. These scans are crucial for notifying the user about possible vulnerabilities and threats before they become a serious problem.

Notifications

The Notification module alerts users about abnormal activity. It offers customizable alerts through popular messaging platforms like Discord and Telegram, keeping users informed about their network's security status in a easy to understand format that informs and educates user about current threat.



The project aims to partner with an OEM in order to create product that can be used out of the box. Such a device will be shipped with preinstalled Debian based operating system with SNiFi software included. This approach ensures a hands-off experience for non-technical users.