Rogue Wi-Fi Access Point Detection and Identification

Find and identify unwanted WIFI AP's

Born and raised in B2B connectivity, we combine innovation, expertise, and great talent into (mobile) connectivity solutions that will make both businesses and society grow. 0G to 5G. Citymesh is the European leader and expert in the construction of private 4G & 5G networks and WiFi as a Service, with +50 MPN's deployed

The goal

The Rogue Wi-Fi Access Point Detection and Identification project aims to develop a system that can automatically detect and identify rogue Wi-Fi access points within an organization's network infrastructure. Rogue access points pose a significant security risk by potentially providing unauthorized access to the network, leading to data breaches and other security incidents. This internship project will focus on creating a proof-of-concept solution to address this critical security concern.

Objectives:

1. **Rogue Access Point Detection**: Develop algorithms and mechanisms to continuously monitor the network environment for the presence of unauthorized Wi-Fi access points. This includes identifying access points that are not part of the organization's approved infrastructure.
2. **Identification and Profiling**: Create a system that can differentiate between legitimate and rogue access points. For rogue access points, gather as much information as possible, such as MAC addresses, SSIDs, signal strength, and location data.
3. **Alerting and Reporting**: Implement real-time alerting mechanisms to notify network administrators when rogue access points are detected. Additionally, create comprehensive reports detailing the rogue access points discovered, their attributes, and any associated risks.
4. **Integration**: Ensure that the solution can integrate with existing network management and security tools, such as intrusion detection systems (IDS) and security information and event management (SIEM) systems, to enhance the organization's overall security posture.
5. **User Interface**: Develop a user-friendly web-based interface for network administrators to view real-time alerts and reports, configure detection parameters, and take appropriate actions when rogue access points are detected.
6. **EXTRA: Machine Learning Integration**: Investigate the potential use of machine learning algorithms to improve the accuracy of rogue access point detection and reduce false positives.
7. EXTRA: Methodology for walk-testing in a venue: Network administrators mobile device may need to walk around the venue to search for rogue Wi-Fi access points. A protocol should be developed to scan the space and assist in potential triangulation of the problem, considering how often this should be done.

8. **Documentation and Training**: Create comprehensive documentation and training materials for network administrators to effectively use and maintain the rogue access point detection system.
9. **Testing and Validation**: Conduct thorough testing, including both lab testing and real-world simulations, to validate the system's effectiveness and reliability in different network environments.

Expected Deliverables:

- Functional rogue Wi-Fi access point detection and identification system.
- User-friendly web interface for network administrators.
- Comprehensive documentation and training materials.
- Validation reports and performance analysis.
- Integration with existing network security tools (if applicable).

This internship project will provide valuable experience in network security, software development, and machine learning, while also addressing a critical security concern for organizations. It will require strong problem-solving skills, programming expertise, and a deep understanding of networking concepts.

Our approach

We strive to provide comprehensive coaching and furnish students with supplementary resources and training as required. Our interns benefit from the constant support of a dedicated mentor who is readily available to offer assistance. Joining us means being part of a vibrant and youthful team, working in a cutting-edge technological environment.

Student profile

Background and Education:

- Undergraduate or graduate student pursuing a degree in Computer Science, Information Security, Network Engineering, or a related field.
- Strong academic record with coursework in networking, cybersecurity, and programming.

Technical Skills:

- Proficiency in programming languages such as Python, Java, or C/C++.
- Familiarity with networking concepts, including TCP/IP, routing, and wireless protocols.
- Basic understanding of cybersecurity principles and threats.
- Knowledge of machine learning and data analysis (preferred but not mandatory).

Skills and Qualities:

-
- Strong problem-solving and analytical skills.
- Attention to detail and a methodical approach to tasks.
- Ability to work independently and as part of a team.
- Good communication skills to convey technical concepts effectively.
- Eagerness to learn and adapt to new technologies and challenges.

- Commitment to ethical behavior, as this role involves monitoring network activity and data.

Interested?

Contact Jens Buysse (jens.buysse@citymesh.com) with your CV. We have other internships available as well! Don't hesitate to contact us.