AAS – Email Security

Application Report

Wilmara Francisco
Nº 118019
Wilmara.francisco@ua.pt

1. Introduction

1.1 Background

Email security is a critical aspect of protecting users from phishing attacks and other malicious activities. This report discusses the implementation of an email security application designed to identify and flag suspicious emails based on predefined criteria.

1.2 Purpose

The purpose of the application is to enhance email security by identifying potentially malicious emails and notifying users to exercise caution.

2. Application Description

2.1 Features

The application employs the following features to analyze and identify suspicious emails:

- Extraction of email credentials
- Continuous monitoring for new emails
- Analysis of email headers and content for suspicious patterns
- Comparison with known phishing domains
- Identification of mismatch between displayed sender name and actual email address
- Utilization of a Bayesian spam classifier

2.2 Functionality

The application connects to the user's email account using the IMAP protocol, continuously monitors the inbox for new emails, and analyzes each email for potential security risks. It provides real-time alerts for suspicious emails based on predefined criteria. The Bayesian spam classifier, implemented in a separate file, enhances the accuracy of spam detection.

2.3 Implementation

The code utilizes the `imaplib` library for IMAP communication, the `email` library for parsing email content, and user input for email credentials. The main function orchestrates the connection to the email server, continuous email monitoring, and suspicious email identification. The Bayesian spam classifier function is located in a separate file and is imported for use in the main application.

3. Solution Description

3.1 Email Credential Input

Users are prompted to input their email address, password, and IMAP server address. This information is used to establish a secure connection to the email server.

3.2 Suspicious Email Identification

The application identifies suspicious emails based on various criteria, including specific keywords in the subject, urgency indicators, and comparison with known phishing domains. Additionally, it checks for mismatches between the displayed sender name and the actual email address. The Bayesian spam classifier, located in a separate file, adds an extra layer of sophistication to spam detection.

3.3 Continuous Monitoring

The application continuously monitors the inbox for new, unread emails, processing each one and providing real-time feedback on potential security threats.

4. Known Phishing Domains

4.1 Source

The list of known phishing domains is obtained from the Cloudflare blog post titled "50 Most Impersonated Brands to Protect Against Phishing" (https://blog.cloudflare.com/50-

most-impersonated-brands-protect-phishing). This source is reputable and regularly updated, making it a reliable reference for identifying potential phishing domains.

4.2 Integration

The list is integrated into the application's code, allowing it to cross-reference incoming emails with known phishing domains and enhance the accuracy of identifying potential threats.

5. Conclusion

In conclusion, the email security application provides an effective solution for identifying and flagging suspicious emails. By leveraging known phishing domains and analyzing email content, the application contributes to a more secure email environment.

6. Future Enhancements

Future enhancements may include:

- User-friendly alerts for suspicious emails
- Integration with machine learning algorithms for more advanced threat detection
- Regular updates of the known phishing domains list

This report provides an overview of the application, its features, and the source of the known phishing domains list, offering a comprehensive understanding of its functionality and security measures.