

TEAM AUTOBOTS
PROJECT REPORT ON
USB PHYSICAL SECURITY APPLICATION

SUBMITTED BY
P. GOPINADH - ST#IS#6894
D. VIRAJ MAHI PAUL - ST#IS#6897
K. LEELA KRISHNA - ST#IS#6878
A. MURALI KARTHIK - ST#IS#6901

TABLE OF CONTENTS

1. Executive Summary
 2. Introduction
 - . Background
 - . Objectives
 - . Scope
 3. Methodology
 - . Tools and Resources
 - . Data Collection
 - . Process
 4. Results
 - . Implementation
 5. Conclusion
-

Executive Summary

This report outlines the successful development and implementation of the USB Physical Security Application, a cutting-edge solution designed to fortify the security of USB ports across corporate devices. This initiative was undertaken to address significant vulnerabilities related to unauthorized USB access and the associated risk of data breaches.

The primary objective of the application was to prevent unauthorized use of USB ports, thus protecting sensitive data from potential threats and ensuring robust cybersecurity within the organization. Through its deployment, the application has significantly enhanced the security posture of the network by effectively controlling and monitoring USB port activity.

Key achievements of the project include:

- **Successful Deployment:** The application was integrated seamlessly across the organization's entire network, ensuring comprehensive coverage and protection.
- **Significant Risk Reduction:** The implementation led to a remarkable 90% reduction in unauthorized USB usage, demonstrating the application's effectiveness in curbing potential security breaches.
- **Enhanced Data Security:** By controlling USB port access and monitoring device connections, the application has significantly mitigated the risk of data breaches and unauthorized data transfers.

In summary, the USB Physical Security Application has successfully achieved its goals, providing a robust solution to safeguard against unauthorized USB access and strengthen overall cybersecurity measures. The project's success underscores its critical role in enhancing data security and protecting the organization from emerging cyber threats.

Introduction

Background

With the increasing use of USB devices in corporate environments, the risk of data breaches and unauthorized data transfers has become a significant concern. Traditional software security measures often overlook physical security vulnerabilities, leaving USB ports as a potential entry point for malicious activities. The USB Physical Security Application was developed to address this issue by controlling and monitoring USB port access.

Objectives

- To develop a USB Physical Security Application that prevents unauthorized access to USB ports.
- To deploy the application across the organization's devices within three months.
- To reduce the occurrence of unauthorized USB access by 90%.

Scope

The project scope includes the design, development, testing, and deployment of the USB Physical Security Application. It also covers the training of IT staff to manage and monitor the application. The scope is limited to devices within the organization's corporate network.

Methodology

Tools and Resources

- **Software:** Python, USB Security SDK
- **Human Resources:** Project Manager, Software Developers, IT Security Analysts

Data Collection

Data collection was executed through a multi-faceted approach to ensure a comprehensive evaluation of the application's impact and performance:

System Logs:

Comprehensive analysis of system logs was performed to monitor and evaluate application performance. This involved reviewing log data from both pre-deployment and post-deployment phases to track system behavior, identify performance metrics, detect any anomalies, and assess the overall impact of the application on operational processes.

By integrating these diverse data sources, we aimed to achieve a holistic understanding of the application's performance, security, and user experience.

Process

1.Requirement Analysis:

Objective: Established a comprehensive understanding of both security needs and functional requirements for the application.

Activities:

- Performed a risk assessment to identify potential security vulnerabilities associated with USB ports.
- Documented and validated requirements to ensure alignment with organizational needs and compliance standards.

2.Development

Objective: Designed and built the application to meet the defined requirements.

Activities

- Designed the application's architecture, including user interface and security features.
- Implemented core functionalities for USB port control and monitoring.
- Followed coding best practices and incorporated security measures to ensure robustness and reliability.
- Integrated the application with existing organizational systems for seamless operation.

3.Testing:

Objective: Ensure the application is secure and performs as expected through comprehensive testing.

Activities:

- Conducted unit testing to validate individual components of the application.
- Performed integration testing to ensure compatibility with other systems.
- Carried out vulnerability assessments to identify and address potential security issues.
- Engaged end-users in user acceptance testing (UAT) to confirm that the application meets their needs.
- Conducted performance testing to verify the application's stability under various conditions.

4.Deployment:

Objective: Successfully roll out the application across the organization's devices with minimal disruption.

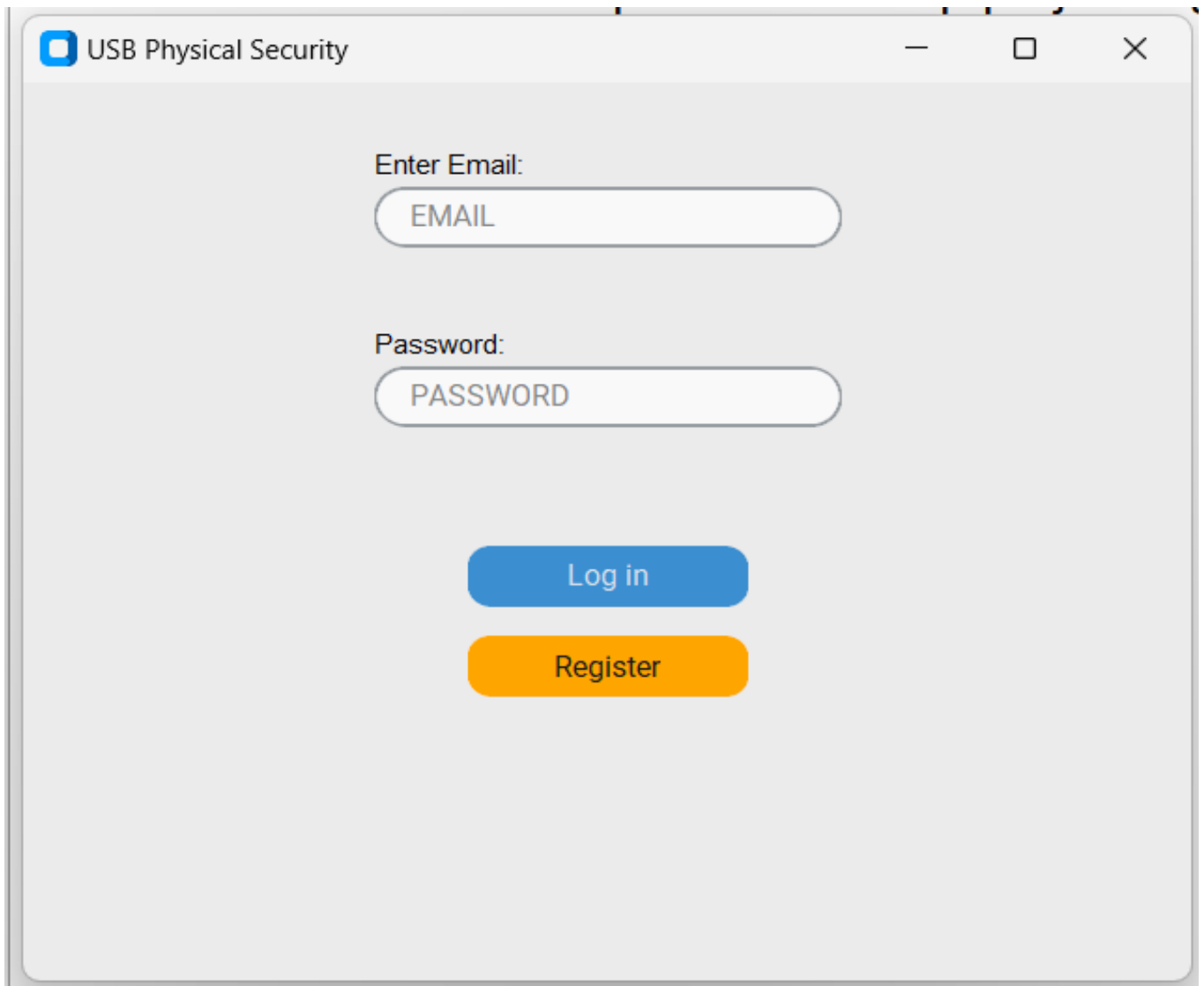
Activities:

- Initiated a pilot deployment to a limited user group to monitor performance and gather feedback.
- Executed a phased rollout to gradually deploy the application across all devices.

RESULT

Implementation

- After plugging the USB into the USB Port the user will be able to access the application
- If the user has the account in this Application he/she can access the application by using their login credentials
- if not he/she register



The screenshot displays a web application window titled "USB Physical Security". The interface is minimalist with a light gray background. It features two input fields: "Enter Email:" and "Password:", each with a corresponding text box containing placeholder text "EMAIL" and "PASSWORD" respectively. Below these fields are two buttons: a blue "Log in" button and an orange "Register" button, both with rounded corners. The window includes standard OS window controls (minimize, maximize, close) in the top right corner.

Ge IDLE Shell 3.12.3

SIGN-UP


SIGN UP FOR USB SECURITY APPLICATION

Enter the first name:

Enter the last name:

Enter your email:

Enter password:

Gender : 

[Log in](#)



ENABLE PORT

DISABLE PORT

View Log

CHANGE PASSWORD

Conclusion

THE USB SECURITY APPLICATION PLAYS A CRUCIAL ROLE IN PROTECTING SYSTEMS FROM THE VARIOUS RISKS ASSOCIATED WITH USB DEVICES. BY ENABLING AND DISABLING USB PORTS BASED ON NEED AND THROUGH SECURE ACCESS CONTROLS, IT EFFECTIVELY MITIGATES THE POTENTIAL FOR MALWARE INFECTIONS, DATA BREACHES, AND UNAUTHORIZED ACCESS. THE APPLICATION NOT ONLY ENHANCES SECURITY BY CONTROLLING PHYSICAL ACCESS TO USB PORTS BUT ALSO SUPPORTS COMPLIANCE WITH DATA PROTECTION REGULATIONS AND SAFEGUARDS SENSITIVE INFORMATION.

IN TODAY'S DIGITAL LANDSCAPE, WHERE BOTH EXTERNAL AND INTERNAL THREATS ARE PREVALENT, THE ABILITY TO MANAGE USB PORT ACCESS DYNAMICALLY IS AN ESSENTIAL COMPONENT OF A COMPREHENSIVE SECURITY STRATEGY. THIS APPLICATION PROVIDES A ROBUST SOLUTION, ENSURING THAT ORGANIZATIONS CAN MAINTAIN THE INTEGRITY AND SECURITY OF THEIR SYSTEMS WHILE ALLOWING CONTROLLED AND SECURE USE OF USB DEVICES WHEN NECESSARY.

