**SG/MMP/5CS024/Open Day KIOSK**

**Date:** Tuesday April 29, 2025

**Location:** University of Wolverhampton

**Tested By:** Satish Desurkar

**Security Test Report**

**Introduction:**

This report details the security testing conducted on the University of Wolverhampton Open Day KIOSK (MMP). The KIOSK is designed to provide visitors with information, including event schedules, QR code access details, and university information, triggered by visitor proximity and button selection. The testing aimed to identify potential security vulnerabilities and assess the KIOSK’s resilience against common threats.

**System Description**

**The KIOSK comprises the following components:**

* Arduino UNO Microcontroller
* TMP36 – Temperature Sensor
* HC-SR04 – Ultrasonic Distance Sensor
* LCD Display Screen (16 x 2)
* 3 Push Buttons
* Potentiometer
* Resistors
* Jumper Wires

**The system logic functions as follows:**

**Proximity-Based Greeting:** When a visitor is within a specific range of the distance sensor, the LCD displays a greeting, event schedule and temperature. When the visitor is outside the range, the LCD displays “Welcome to University of Wolverhampton.”

**Pushbutton-Triggered Information:**

* **Pushbutton 1:** Displays event schedule and current temperature.
* **Pushbutton 2:** Displays QR code access details.
* **Pushbutton 3:** Directs the visitor to the University of Wolverhampton website URL (simulated on the LCD).

**Scope of Testing**

**The security testing focused on the following areas:**

* **Unauthorised Access:** Testing the potential for unauthorised manipulation of the KIOSK hardware or software.
* **Data Integrity:** Verifying the accuracy and consistency of the information displayed.
* **Denial of Service:** Assessing the KIOSK’s ability to withstand attempts to disrupt its functionality.
* **Input Validation:** Ensuring that user inputs (pushbutton presses) are handled correctly and do not lead to errors.
* **Information Disclosure:** Checking if sensitive information (if any) is adequately protected.

**Testing Methodology**

**The following testing methods were employed:**

* **Black Box Testing:** Testers had no prior knowledge of the internal working of the KIOSK.
* **Functional Testing:** Verifying that the KIOSK functions as intended.
* **Interface Testing:** Checking the interaction between different hardware components.

**Test Results**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Serial No.** | **Test Scenario** | **Simulated Distance (cm)** | **Expected Behaviour** | **Actual Behaviour** | **Test Result Pass/Fail** | **Observations** |
| 1 | On Clicking Push Button 1 |  | Display “Current Temperature & Event Schedule “ | Displayed  “Current Temperature & Event Schedule “ | Pass | Correctly displayed the current temperature & event schedule. |
| 2 | On Clicking Push Button 2 |  | Display  “QR Code Access Details “ | Displayed  “QR Code Access Details “ | Pass | Correctly displayed the QR code access information. |
| 3 | On Clicking Push Button 3 |  | Display  “University of Wolverhampton URL “ | Displayed  “University of Wolverhampton URL “ | Pass | Correctly displayed the URL of University of Wolverhampton. |
| 4 | Denial of Service Test - Button Spamming: Repeatedly pressing push buttons as fast as possible for an extended period. |  | Display the relevant information correctly | Displayed the relevant information correctly | Pass | The system remained responsive and did not crash. |
| 5 | Minimum Distance | 2.73 | Display “Schedule”  message | Display “Schedule”  message | Pass | Sensor reading was stable |
| 6 | Maximum Distance | 331.22 | Display “Name of University” | Display “Name of University” | Pass | Sensor reading was stable |
| 7 | Rapid Fluctuations | Changing between 20 - 80 | Message changes smoothly | Message changes smoothly | Pass | LCD message changed without flickering |
| 8 | Out of range value | 2.32 | Display default message | Display default message | Pass | Serial monitor provided out of range value |
| 9 | Out of range value | 332 | Display default message | Display default message | Pass | Serial monitor provided out of range value |

**Ultrasonic Distance Sensor Testing:**

The distance sensor was evaluated to see how it behaved under different conditions, particularly with close and very far distances, and with rapid changes in distance.

**Extreme Value Testing:** We evaluated the sensor at its closest and farthest simulated distances.

**Fluctuation Testing:** We rapidly changed the simulated distance to see if the sensor’s readings were stable.

Here are the results of the distance sensor testing:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Serial No.** | **Test Scenario** | **Simulated Distance (cm)** | **Expected Behaviour** | **Actual Behaviour** | **Test Result Pass/Fail** | **Observations** |
| 1 | Minimum Distance | 2.73 | Display “Schedule”  message | Display “Schedule”  message | Pass | Sensor reading was stable |
| 2 | Maximum Distance | 331.22 | Display “Name of University” | Display “Name of University” | Pass | Sensor reading was stable |
| 3 | Rapid Fluctuations | Changing between 20 - 80 | Message changes smoothly | Message changes smoothly | Pass | LCD message changed without flickering |
| 4 | Out of range value | 2.32 | Display default message | Display default message | Pass | Serial monitor provided out of range value |
| 5 | Out of range value | 332 | Display default message | Display default message | Pass | Serial monitor provided out of range value |

**LCD (16 x 2) Display Testing:**

The LCD display was tested to ensure it could handle various types of messages, including long text and special characters. The tests aimed to check if the display showed information correctly and if the code prevented any errors.

**Long Message Testing:** Messages longer than the LCD’s display width were sent to the LCD to see how it handled them.

**Special Character Testing:** Attempts were made to display symbols and characters that might not be standard on the LCD.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Serial No.** | **Test Scenario** | **Message Sent** | **Expected Display** | **Actual Display** | **Test Result Pass/Fail** | **Observations** |
| 1 | Long Message | “Welcome to the University Open Day! We have a very long schedule for you.” | “Welcome to the Uni…” (scrolling or truncation) | “Welcome to the Uni…” (truncated) | Pass | Display truncated the message |
| 2 | Special Character | “Temperature: 25oC” | “Temperature: 25oC” | “Temperature: 25?C” | Fail | Degree symbol not displayed correctly |
| 3 | Standard Message | “Campus Tour” | “Campus Tour” | “Campus Tour” | Pass | Message displayed correctly |

**Discussion of Issues:**

The LCD handled long messages by truncating them, meaning it cut of the extra text. This is expected behaviour for a standard LCD. To display the whole message, scrolling would need to be implemented in the code.

The LCD did not display the degree symbol (o). This indicates that the LCD’s character set does not include the specific symbol, or that the code was not using the correct character code. If special characters are critical, a LCD that supports them would be used, or a custom character would need to be created.

All normal messages are displayed as expected.

**Temperature Sensor (TMP36) Testing:**

“The temperature sensor was tested to evaluate its performance under extreme conditions and potential failure scenarios. Tests were conducted to verify the sensor’s accuracy and the code’s ability to handle unexpected readings.

**Extreme Value Testing:** The simulated temperature was set to minimum and maximum values allowed within Tinkercad’s simulation range.

**No Value Testing:** The sensor was, in the code, virtually disconnected, by setting the sensor reading variable to a null value, to simulate a sensor failure.

The results of the temperature sensor testing are summarized in the following table:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Serial No.** | **Test Scenario** | **Simulated Temperature (o C)** | **Serial Monitor Reading (o C)** | **Expected Behaviour** | **Actual Behaviour** | **Test Result Pass/Fail** | **Observations** |
| 1 | Minimum Value | -40.86 | -40.86 | Display correct minimum value | Display correct minimum value | Pass |  |
| 2 | Maximum Value | 113.62 | 113.62 | Display correct maximum value | Display correct maximum value | Pass |  |
| 3 | Rapid Fluctuations |  |  | Responsive | Responsive | Pass |  |

**Conclusion:**

The security testing performed within the Tinkercad simulation environment demonstrated the project’s overall robustness in handling various input scenarios. The distance sensor, LCD display, temperature sensor, and potentiometer all functioned as expected under tested conditions, including extreme and fluctuating values.

It is important to acknowledge the inherent limitations of the Tinkercad simulation. Real-world deployments may encounter more complex scenarios such as physical tampering, or unexpected environmental conditions.

**Potential Vulnerabilities**

Given the nature of the KIOSK and its components, the following potential vulnerabilities have been identified:

**Physical Tampering:**

* **Component Damage:** Visitors may attempt to damage or disconnect components such as the temperature sensor, distance sensor, or LCD Display.
* **Wire Manipulation:** Jumper wires could be disconnected or short-circuited, leading to malfunction or unintended behaviour.
* **Device Theft:** The entire KIOSK or individual components could be stolen.
* **Button Jamming:** The push buttons could be physically jammed or held down, disrupting the intended functionality.

**Software Exploitation:**

* **Input Manipulation:** Although the system relies on physical buttons, there might be potential vulnerabilities if the Arduino code is not robust enough and someone tries to send malicious signals.
* **Code Modification:** If the Arduino’s firmware can be accessed, it could be modified to display incorrect information or cause other issues. This is less likely in a closed KIOSK system but should be considered.

**Information Disclosure:**

**Display of Sensitive Information:** We must ensure that the displayed schedule, temperature, or URL does not inadvertently reveal any sensitive or non-public information.

**Denial of Service:**

**Resource Exhaustion:** Although less likely with this simple setup, a malicious actor could try to cause a denial of service by rapidly and repeatedly pressing the buttons.

**Potential real-world security concerns include:**

**Power Supply Issues:** Inconsistent or interrupted power could lead to instability. Implementing a backup power supply or ensuring a stable power source would address this concern.

**Environmental Factors:** Extreme temperatures, humidity, or dust could impact the system’s performance. Designing the kiosk with appropriate environmental protection and testing under various conditions would be necessary.

**Sensor Failure:** Malicious actors could potentially interfere with sensor readings, or the sensor

While the simulation provided valuable insights into the project’s behaviour, a thorough rea-world security assessment would be necessary prior to actual deployment to fully address these and other potential vulnerabilities.