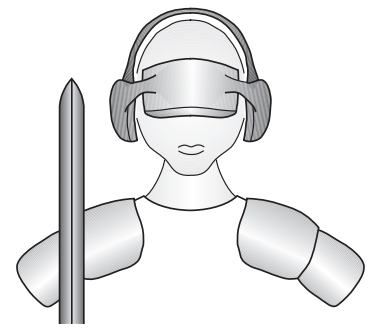


AN8: Tamper Protecting A Kiosk System

JoyWarrior24F8 - Applications For Acceleration Sensing



Code Mercenaries

Theft And Tamper Proofing Kiosk Systems

Kiosk systems can easily become targets for theft and tampering. Their very advantage of being able to operate unattended also makes them good targets for those with bad intentions.

The task for the kiosk designer is to make it as hard as possible for a perpetrator to steal or open the kiosk without significantly driving up the system cost. Since many kiosk systems are connected to the internet a good approach to protect the system is to detect suspicious activities and send an alarm if necessary.

Types Of Threats And How To Identify Them

A kiosk can be either stolen completely, or forced open to steal goods and money or tamper with the internal electronics.

An attempt to steal the complete kiosk can be detected by sudden movements or tilting of the cabinet. In most cases it will be necessary to tilt the kiosk to load it onto some transport device.

Attempts to break into the kiosk can be either by brute force or by lock picking. Lock picking can be defeated by using door contacts in combination with some secure identification. Opening of a door without first identifying as an authorised person results in an alarm.

Brute force usually results in violent vibrations of the cabinet, detecting this and differentiating from normal vibrations could be used to generate an alarm.

How To Send An Alarm

To be able to use the internet connection to send an alarm it is necessary to set up the kiosk in a way that it is blocking the access to the power and internet cables, so the connections can not be cut before the kiosk detects the attack. If the kiosk uses WLAN or mobile internet and has an UPS (uninterruptible power supply) internally it is even

easier to assure that it can get its alarm message to some security center.

The actual mechanism for sending an alarm depends on the available infrastructure. If the kiosk is communicating to some central system at all times it should be simple to add an alarm message. Using email may not be practical since transmitting email takes relatively long and the delay until it is received and then acted upon may also be significant.

Detecting Multiple Threats With One Sensor

The JW24F8 is a three axis acceleration sensor with USB interface and eight aux inputs for digital signals like switches.

It allows to detect multiple events, like tilt angle, movement, shock, and with the aux inputs it can support up to eight signals like door switches or other status or alarm indicators.

The small size and low cost of the JW24F8 allows it to be integrated in all kinds of applications.

Sample Software

Code Mercenaries provides a sample software for the JW24F8 demonstrating the basic principles of various attack detections. The sample software can detect movement, tilt angle and hard hits.

For real applications the software will have to be adapted to the actual properties of the kiosk system.

Detecting Tilt

To move a kiosk it usually has to be tilted first to load it onto a trolley or other transport device.

The JW24F8 is excellently suitable to detect the tilt angle of the system.

When mounted horizontally inside the cabinet the X and Y axis of the JW24F8 are used together to calculate the tilt angle. To get the resultant tilt off the horizontal the pythagorean theorem is used:

$$\text{tilt}^2 = x^2 + y^2$$

The tilt angle is the $\sin(\text{tilt})$.

To differentiate tilt from horizontal acceleration the Z axis should also be used to calculate the tilt angle, if the two results do not match a horizontal acceleration can be assumed.

After installing the system the final position should be stored as a reference to detect attempts to move the cabinet. Any significant variation from the installation position lasting longer than a few dozen milliseconds should be considered an attempt to move the cabinet.

A person bumping into the cabinet should not activate the alarm. Using a low pass filter for tilt detection can help to discern such events from real attempts to tilt the cabinet. Any signal that lasts less than maybe 100ms could be ignored.

The threshold for activating an alert due to tilt detection should be set individually depending on the design of the cabinet.

Detecting Movement

Movement detection can be a bit more tricky due to possible interfering signals. If the cabinet is set up in an environment where vibrations are present movement detection may not be practical.

Typical acceleration values for movement detection are specific to the design and size of the cabinet and should be tested.

A low pass filter is used to discern movement from shock transients.

Detecting Mechanical Intrusion Attempts

Hitting a cabinet with a metal tool generates a distinctive transient that can be discerned from a blow with a fist or a kick. By using a high pass filter on the acceleration data and then triggering on a certain threshold allows to detect violent blows with hard materials.

The threshold level and necessary cut off frequency for the filter can depend on the material and construction of the cabinet. Testing with a target system is required to optimize the trigger

levels to the individual cabinet design.

Door Contacts

In addition to the acceleration based sensing JW24F8 also offers eight digital inputs that can be used to connect door contacts to detect opening of access doors on the cabinet.

If the door contacts are combined with some identification process, like a password protected maintenance mode, unauthorized access to the cabinet can be detected.

Conclusion

Adding the JW24F8 and some software can allow your kiosk system to call for help in many attack szenarios. It can not outright prevent the attempt of stealing or opening it. But sending an alert to a security center, or activating a web cam to take pictures of the perpetrators does increase the risk of getting caught significantly, which will scare off many of those looking for booty.

AN8: Tamper Protecting A Kiosk JoyWarrior24F8 - Applications For Acceleration Sensing

Our Demo Setup

Following is the description of a demo unit we are using to showcase the security application of JoyWarrior24F8.

By using relatively simple filtering algorithms on the data stream of the sensor tilting, moving, and hitting the enclosure can be detected. This allows to detect when somebody tries to remove the cabinet or break into it. To prevent false alerts due to a person bumping into the cabinet or giving it a slap with the hand, the transients of hits are

analyzed to discern between hits with soft and hard objects.

The additional digital inputs of the sensor can be used to detect opening of access doors. In the demo one of the inputs is used to disable the alarm when the door is properly unlocked with a key.

The sensor can be seen at the lower front structure of the cabinet, mounted firmly on the structure to transmit movements and shocks. On the right is an IO-Warrior24 which is used for demo purposes only to drive LEDs to illuminate the interior of the box and show red light for the alert status.

