Theft Security System

By Timothy Tomas
& Roman Geluz

Social Need

The IoT technology that we have decided to design is a theft security system that monitors and tracks a particular device. The goal of the product is to inform the user on when a device has been moved from its original location. A recent study at Kensington revealed that there were:

- At least one laptop stolen every 53 seconds
- 70 million smartphones are lost each year with only 7 percent recovered.
- 80 percent of the cost of a lost laptop is from data breach.
- 52 percent of devices are stolen from the workplace, and 24 percent from conferences.

(https://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches)

Based on this study, it reveals that there is a need for more security measures in the way we protect our devices from unsolicited threats. This product will improve on the implementation of security measures when a device is left unattended. The following diagram illustrates the components used within the system.

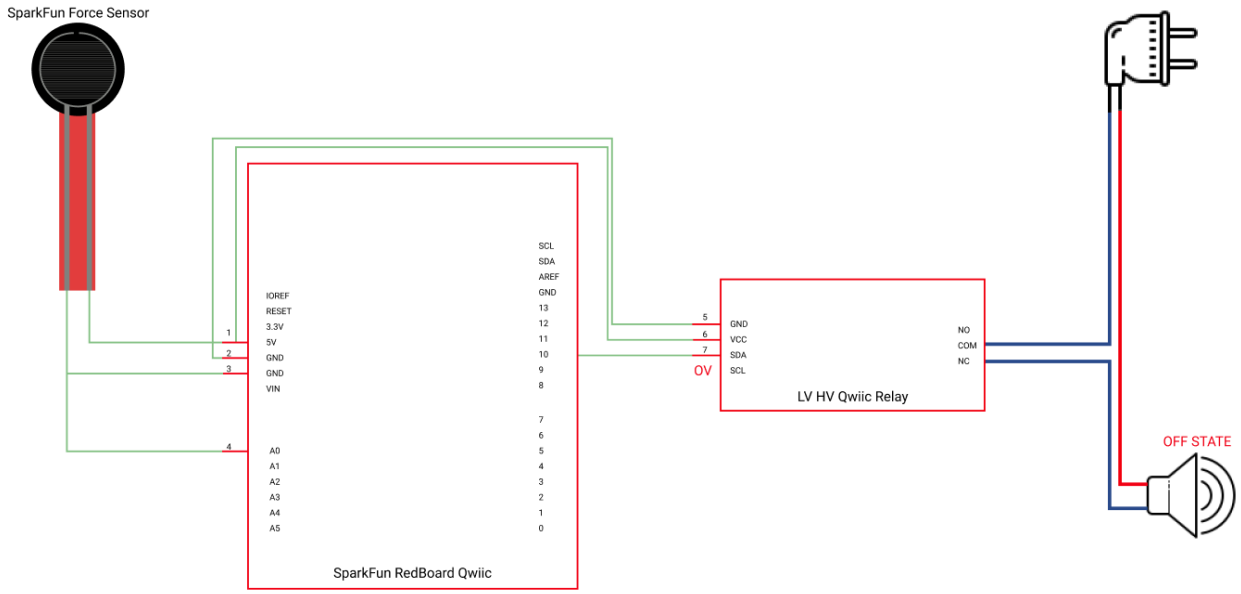

Fig. 1 Off State

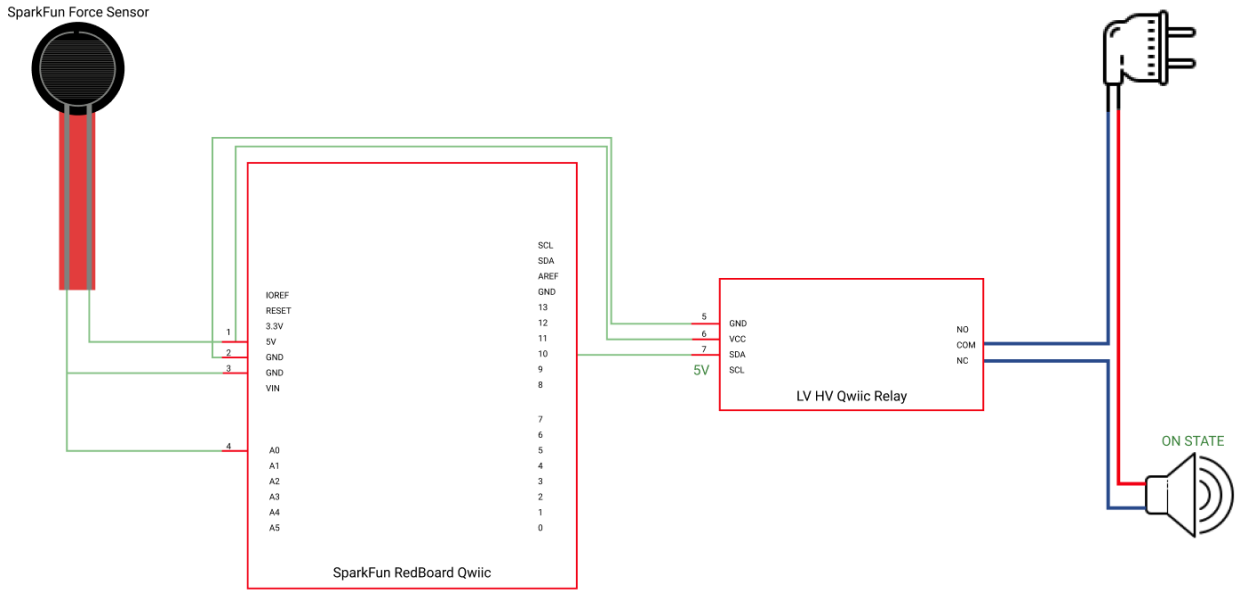

Fig. 2 On State

The system is comprised of the following components:

- 1x Sparkfun RedBoard Qwiic https://www.sparkfun.com/products/15123
- 1x SparkFun Force Sensor https://www.sparkfun.com/products/9375?_ga=2.62333864.580467825.1584202992-929296530.1584202992
- 1x Relay https://www.sparkfun.com/products/15093
- 1x Alarm Speaker https://www.sparkfun.com/products/13939

Figure one and two demonstrate the system in their OFF and ON states.

Competitive Analysis

In the current market there are a variety of competitors that use multiple types of security systems that deter against theft. One of those systems is used by Apple. Majority of their devices are kept on docking stations where each device is tethered to a security cable and is attached to an alarm that is tripped when the device is no longer connected to the security cable. Apple's security system is unique because it allows the user to hold and play with the device when shopping through their products. Apple strikes a balance between the experience of the shopper and the security of their devices.

Conversely, commercial stores use more subtle measures to ensure the safety of their products. For instance, Walmart and other big retailers use radio frequency systems to help deter shoplifting. Majority of their products have RF tags that are placed under the products label. When a person tries to walk out the store without paying for the item, the alarm sounds at the Entry/Exit way informing employees that an item has not been paid for. Our proposed technology is unique because it offers device protection that would be integrated into common

commercial facilities that are often visited amongst customers. One particular example would be libraries or coffee shops where they provide open seating for their customers.

The target audience that visit these facilities often bring a laptop to conduct their work. The problem that our design would solve that differs from our competitors is that we would implement our security device in the physical workspace of the environment without physically tethering a person's device to the system. As is the case with Apple and retail stores like Walmart, their devices are physically attached to a component within their security system. Our solution would embed the physical components into the environment itself. As illustrated in figure 3. the force sensor, RedBoard, relay, and alarm speaker are integrated into the table. When a customer sits down on the table they place their device on top of the force sensor. The customer will be given the option to utilize this security system through their smartphone where it will communicate the behavior and events of the device in case they walk away from the table. The rest of the security system is installed into the table invisible to the customers view. This system allows for seamless security protocols without physical tether requirements of the user, ultimately giving them protection, freedom, and control of their devices.

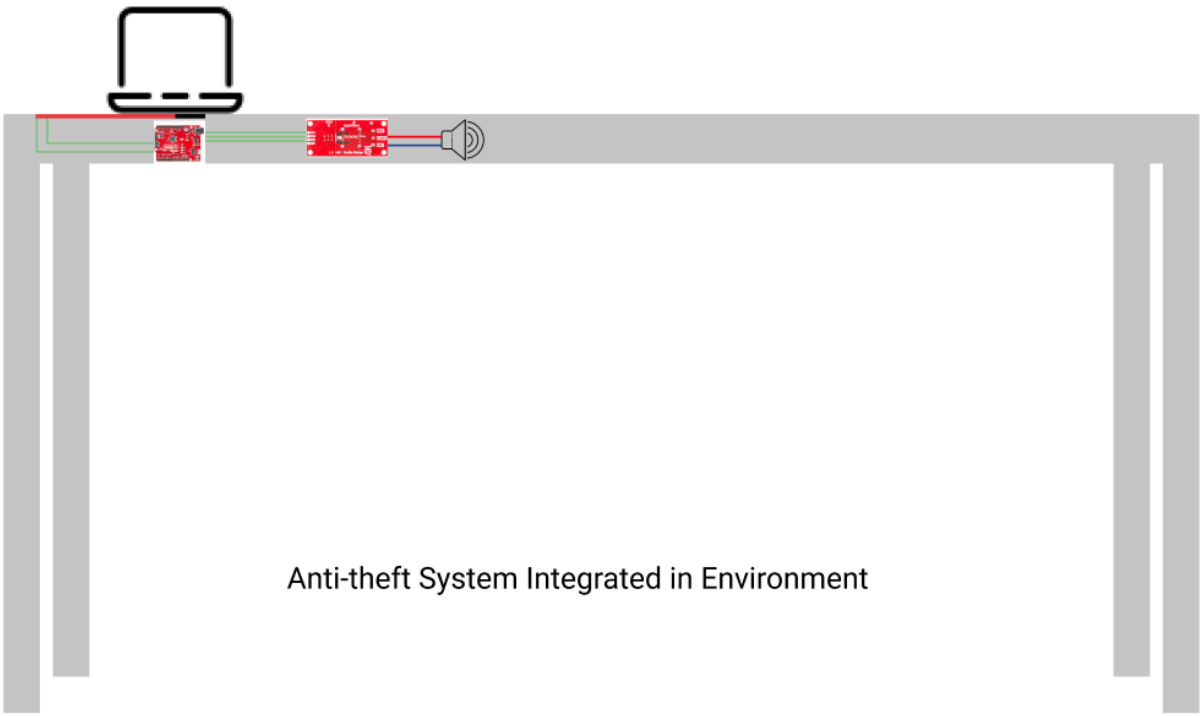

Fig. 3

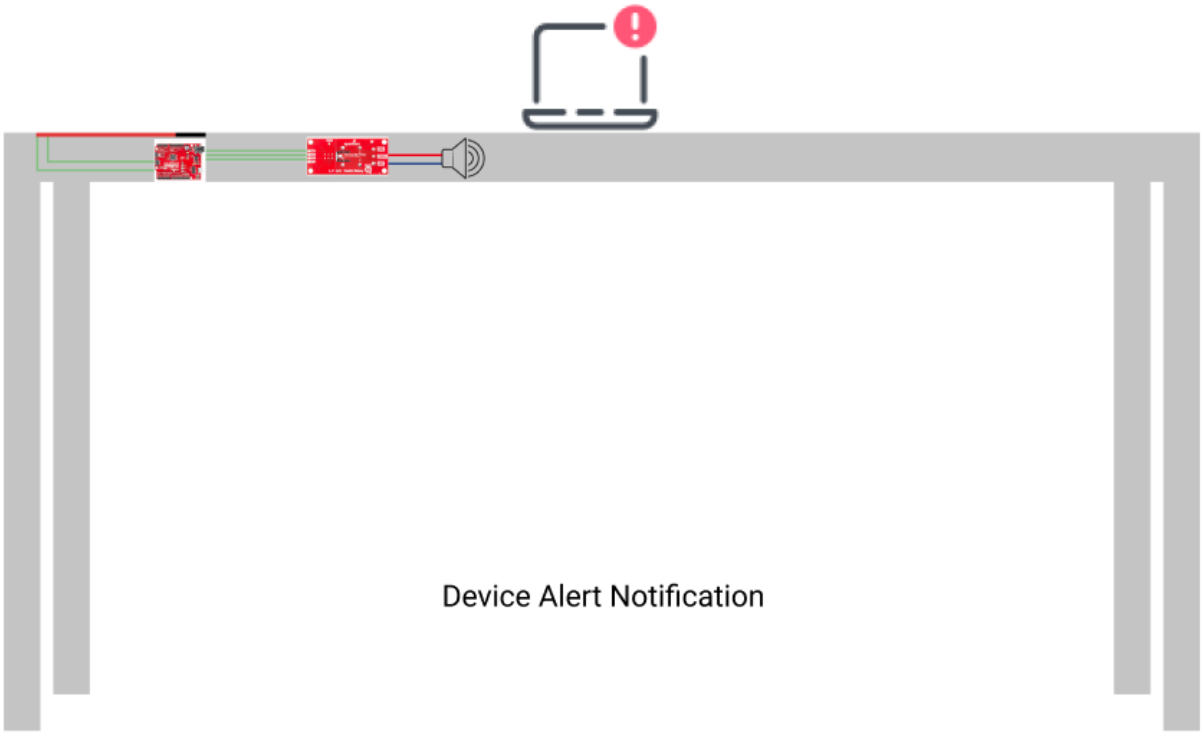

Fig. 4

Device Access and Data Transmission/Storage:

The Anti-Theft Security System optionally can be accessed via a security app which will work for Android and iOS devices including cell phones, smart watches and tablets. The app will allow customers to directly or remotely control the security system (either through usb cable or bluetooth), arm or disarm their system, view recorded security data, configure and receive alerts either by in-app or email notifications. For the premium service, recorded data can be transferred from the app and then stored onto an online cloud service, to archive event history.

In order to leverage and utilize mobile device security monitoring, the security system will require the use of Bluetooth protocol to be able to send and receive data to and from the smartphone and security system wirelessly. Data is transmitted via a 2.4 Ghz wireless link. It is a secured protocol and is designed for short-range, low-power, low-cost, wireless transmission between electronic devices. The security system will then need to connect a bluetooth module such as the Bluetooth SMD Module - BC127, to transmit and receive bluetooth signal.

The mobile app will receive and transmit data to and from the security system. The app will have a login screen to grant access to the security controls to users only with proper authorization through user authentication. The app will record all of the events of the system onto an internal log implemented by an embedded database. When an intrusion is detected, the security system will transmit the event data to the mobile app, and it will display a mobile alert. The app can also be configured to submit a notification alert to your configured email address.

Fig 5.

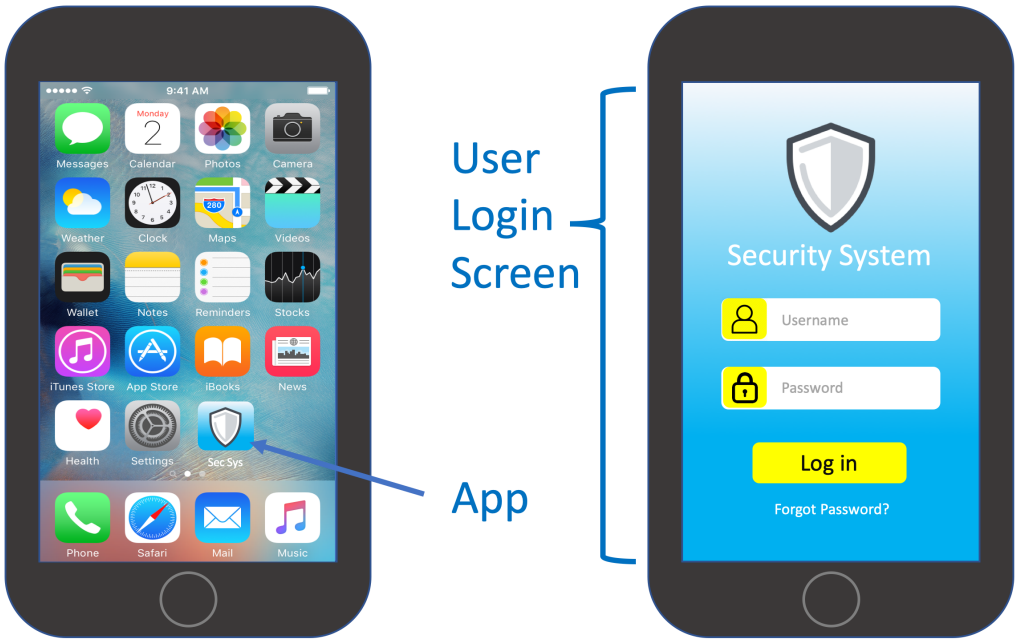
9:41 AM
Messages
Calendar
Photos
Camera
Weather
Clock
Maps
Videos
Wallet
Notes
Reminders
Stocks
iTunes Store
App Store
iBooks
News
Health
Settings
Sec Sys
Phone
Safari
Mail
Music
User
Login
Screen
App
Security System
Username
Password
Log in
Forgot Password?

Fig 6.

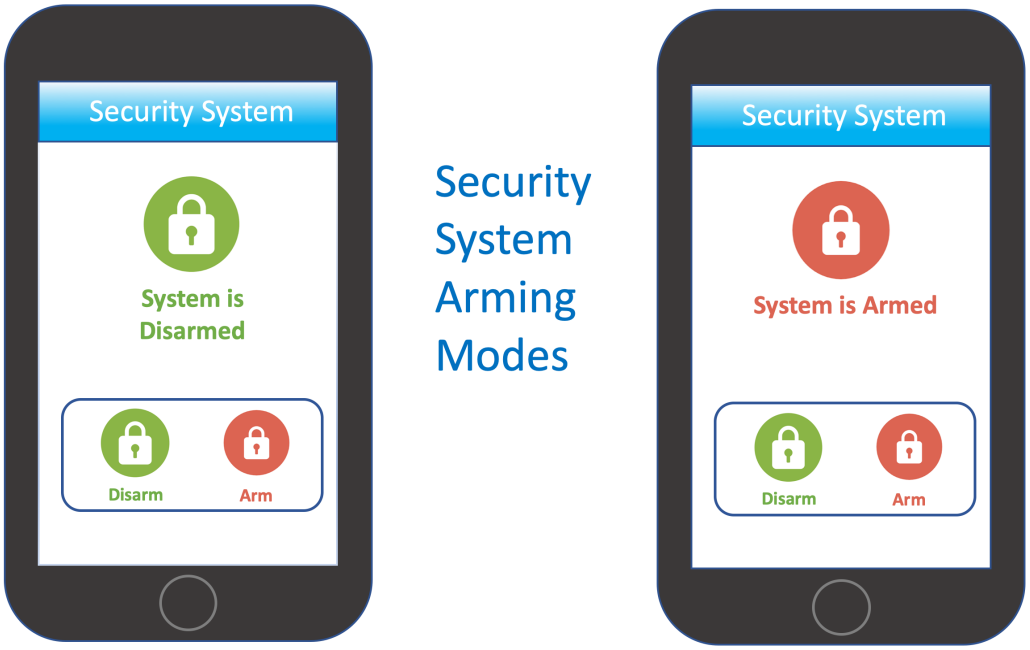
Security System
System is
Disarmed
Disarm
Arm
Security
System
Arming
Modes
Security System
System is Armed
Disarm
Arm

Fig 7.

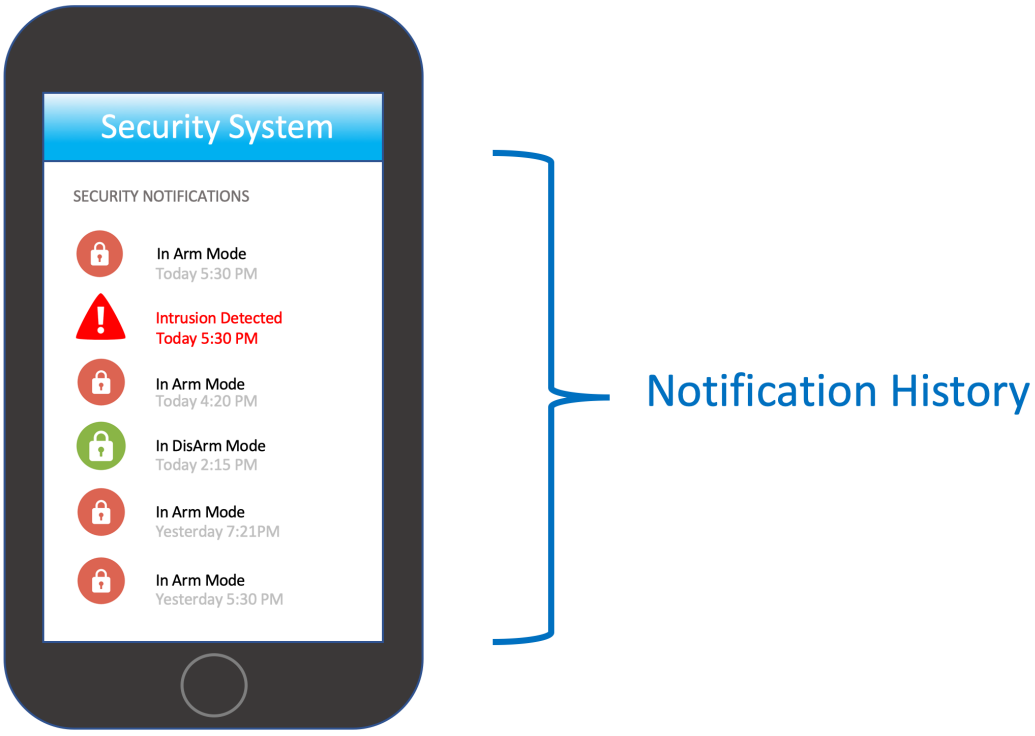
Security System
SECURITY NOTIFICATIONS
In Arm Mode
Today 5:30 PM
Intrusion Detected
Today 5:30 PM
In Arm Mode
Today 4:20 PM
In DisArm Mode
Today 2:15 PM
In Arm Mode
Yesterday 7:21PM
In Arm Mode
Yesterday 5:30 PM
Notification History

Fig 8.

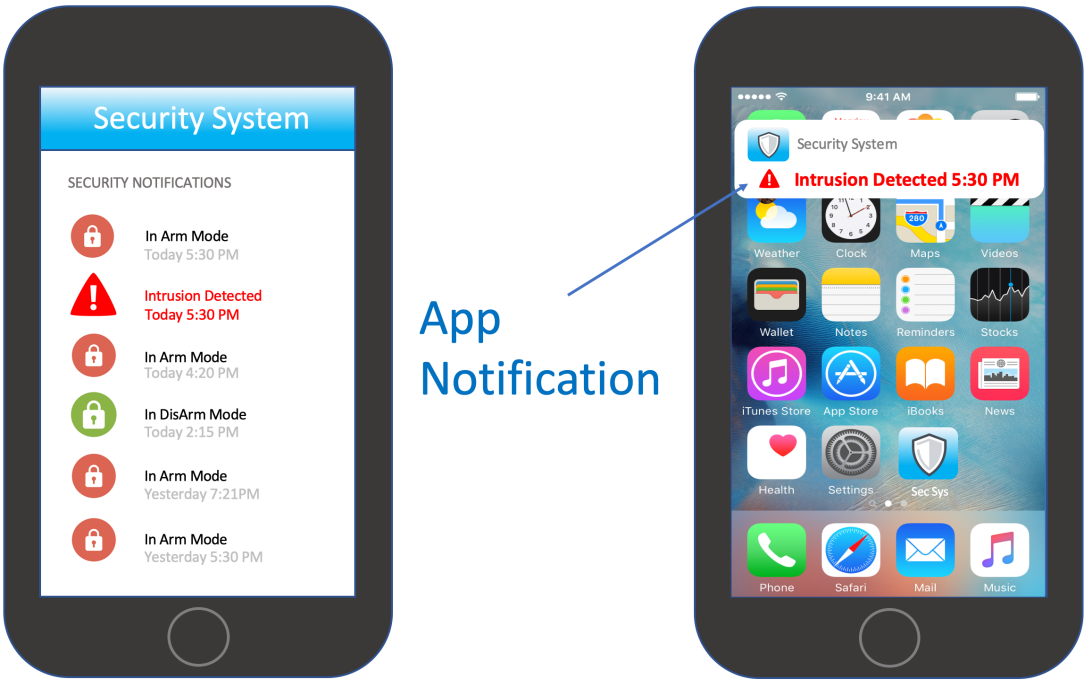
Security System
SECURITY NOTIFICATIONS
In Arm Mode
Today 5:30 PM
Intrusion Detected
Today 5:30 PM
In Arm Mode
Today 4:20 PM
In DisArm Mode
Today 2:15 PM
In Arm Mode
Yesterday 7:21PM
In Arm Mode
Yesterday 5:30 PM
App
Notification
9:41 AM
Security System
Intrusion Detected 5:30 PM
Weather
Clock
Maps
Videos
Wallet
Notes
Reminders
Stocks
iTunes Store
App Store
iBooks
News
Health
Settings
Sec Sys
Phone
Safari
Mail
Music

Fig 9.

Security Measures:

To prevent bypassing the force sensor detection from thieves who may use the swapping technique with dummy weight substitution, ala Indiana Jones' Golden Idol theft attempt with the use of a similar weighted bag of sand, a digital weight sensor can be coupled with the force sensor. The weight of the item to be secured, will be premeasured and be used as the target value for triggering intrusion. Weight calibration and recording can be handled through the security app. If the weight value being monitored deviates from this target value within a specified threshold, intrusion is detected.

If force and weight sensing is not sufficient, the use of a proximity sensor or an active RFID tag that responds to a ping from a transmitter or transmit data to a receiver can help reinforce intrusion detection. The item to be secured, will have the active tag, broadcasting signals. If the corresponding receiver fails to receive the life beat signal for a predefined time, intrusion detection will occur.

If intruders attempt to override control of the hardware or the smartphone app, through brute force attack where the intruder attempts to guess all possible passwords, two or multi-factor authentication can be employed to minimize intrusion. This can be combined with Login Failed Policy (for example 5 attempts) that can trigger a Account Lockout Policy which enforces a lockout duration (eg an hour) to the person with the exceeded failed attempts.

To further reinforce security, equipping the item to be secured, with gps/radio tracking, similar to that of LoJack or OnStar, with the use of GPS trackers such as "Real-Time 2G/3G/LTE Arduino GPS Tracker + IoT Dashboard" which has the capability to post tracking data to the cloud and view tracking data on a IoT Dashboard, can add more value to the theft detection system.

Summary of Work

Timothy Tomas:

- Social Need
- Competitive Analysis
- Figures 1 - 4

Roman Geluz:

- Device Access
- Security Measures
- Figures 5 - 9