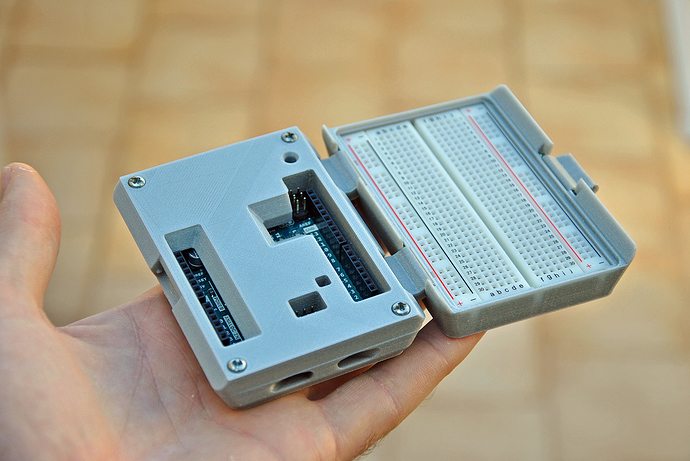
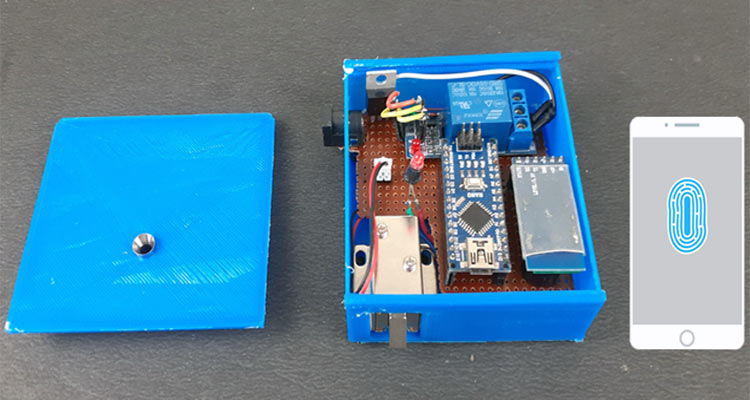
**Arduino Yun project Security**

There are so many security risks in 2021 more and more often we seem to hear about security breaches and people’s personal information being compromised. These days everything seems to be connected to the internet so it is important we look at what security we can implement to our project in the future to avoid any security attacks or limit some of the vulnerabilities available to target. The best and possibly most obvious place to start would be with your home Wi-Fi changing from the default password will limit access to any unauthorized users and limit some of the opportunities to attack the Arduino project or the code. Another good option would be to use DCHP where possible to reserve the mac address to avoid the Yun being unable to access the network. It would be a smart option in my opinion to use camel casing and numbers and symbols to ensure your password is as difficult as possible for anyone to try and guess. Example Pa$sw0Rd this makes the password difficult for anyone to figure out and its recommended you do not share your password with anyone else. The Arduino Yun address 192.168.240.1. can be accessible through the hotspot so it is a good idea to make sure another strong password is used on the interface configuration website and is not left as the default password. one other way to add some protection to the project would be the use on online debugger software such as visual micro which is a plug in available via Microsoft that is used to Create cross platform programs on Arduino. The next step I would introduce to avoid any physical security breaches such as resetting to default factory settings by pressing the WLAN RST button for longer than thirty seconds. To avoid this, I would place the Arduino Yun itself in the box pictured below then I would place it in a larger box secured with a lock to avoid any unauthorised access other than the user themselves. Project Two: For further security we have sourced the two-factor authentication on the Arduino website. This allows you to scan a QR code which gives you an authentication code that changes every thirty seconds. You will then be required to enter the code and once this is done you receive a recovery code which you must keep safe as you will need this to restore your account should you forget your password. This adds an extra layer of security which requires both your password and a six-digit pin sent to your authentication app on your mobile phone. This means should someone get your password they still need the code sent to your mobile, without this they cannot log in. we have also sourced some code which allows us to send a http request to a client and can receive data back from the client. For added security as http is not fully secure, we have a code encryption which encrypts any data received but decided against adding it to the current project as we are only reading in light levels and not personal information or data. Some other security available is the Arduino security primer which gives access to the Arduino IoT cloud, this allows you to store code. The security primer requires a hardware element to guarantee authenticity and confidentiality and provides two further elements. Unfortunately, this requires an upgrade to a premium account as the Arduino Yun is not compatible with a basic account. For the project two as we are using a smart bulb, we are required to make commands across the internet it is very important that we use secure protocols which is why we use the https protocol when calling the light trigger from the Arduino Yun. As previously mentioned in project one it is just as important that we change all default passwords. As the smart bulb is controlled by IFTTT (If not this then that) for added security it would be best to use the correct protocols and a strong IFTTT password for your account. It would be best to register with your google or apple account as this would inform you of any log in or activity on your account and may even need authentication to access the account. Now that we have these new steps in place, we would be more confident with the security of our project. Further security be added in the future, but we are confident that the further security we have added is a step up from the security we had in project one.

Example cases for physical security

References:

<https://docs.google.com/forms/d/e/1FAIpQLSflkD2mEYdRsqyPBUQxaViIpyXmHT5KD8856fzpqEnpT3sRrA/viewform?c=0&w=1>

<https://blog.arduino.cc/2020/07/02/arduino-security-primer/>