Questions under observation:

- **Is compliance simply a liability shield? Is it actually useful?**

1. Are apps *talking about/advertising certifications?*
    a. Look into **websites, app descriptions on the Play Store**
        i. All ioXt-certified IoT apps (i.e., excluding VPNs and irrelevant apps), totalling at 11 applications
2. Are labs advertising who they have certified?
    a. Possible ways to analyze:
        i. Crawl the websites of all labs affiliated with ioxt
            1. Search the text content for titles, developer names, developer URLs, of iot apps from 37k (cosine similarity, bag of words, case insensitive)
        ii. OR just check manually the websites

Methodology & Results

PART 1

1. Are apps *talking about/advertising certifications?*
    a. Look into **websites, app descriptions on the Play Store**
        i. All ioXt-certified IoT apps (i.e., excluding VPNs and irrelevant apps)
            1. **Methodology:** Manual exploration of all 11 of the ioXt-certified applications. First off, I visited their Google Play Store page and checked for information regarding their certification on the descriptions (“about this app”). Next, I checked their “data safety” section to check if they mention they are certified. After checking the GPlay page, I get the developer’s website address from the GPlay page under “Developer Contact” and visit the developer’s website. I tried to keep the manual exploration of the GPlay page to less than 15 minutes for each app, as the GPlay page of the applications typically don’t have a lot of information on them and 15 minutes is adequate to analyze it. On the developer’s website, I start the index page and look if they talk about certification in the first page. If I can't find info on certifications or direct link for certification, I look under the menus to find any sub topic that may sound related to certification… Focus is on “Support and FAQ” “About Us” “data safety and privacy” “partners” pages or some pages in the website that are tailored for developers. If the website looks like it is advertising a primary product (for which the application is complementary, i.e. refrigerators being the actual product advertised but it also has an app), I look for pages in the website that seems to be related to the mobile app part of their business. If none of these work, I use the search functionality of the website (if it provides one) to look for keywords… such as ioxt, certification, certificates, certified, masa, mobile application, etc. For manual exploration of the websites, I tried to keep it to around 30 minutes.
            2. **Results:**
                a. **Apps that do mention that they are certified (4)**
                    i. Tuya, Midea Air, MSmartLife, Toshiba HA
                    ii. MSmartLife and ToshibaHA list the same developer website
                    iii. https://www.tuya.com/rule
                    iv. https://www.midea.com/us/msmarthome
                    v. https://msmart.midea.com/security
                    vi. https://msmart.midea.com/security
                b. **Apps that do not mention certification neither in their GPlay nor in their website (6)**

i. NetHome Plus, Eureka, GreenMAX DRC, Wyze, Dals Connect, Hubspace

c. **Apps that do not mention certification on their developer website but are certified and found on appdefensealliance.com/directory, also has a "security badge" on GPlay (1):**
   i. Google Home

d. I have also taken archive snapshots of the webpages for the certified apps:
   i. https://web.archive.org/web/20221230230823/https://www.tuya.com/
   ii. https://web.archive.org/web/20221230230943/https://www.eureka.com/us
   iii. https://web.archive.org/web/20221230231043/https://www.midea.com/us
   iv. https://web.archive.org/web/20221230231155/https://msmart.midea.com/
   v. https://web.archive.org/web/20221230231155/https://msmart.midea.com/
   vi. https://web.archive.org/web/20221230231326/https://www.leviton.com/en
   vii. https://web.archive.org/web/20221230231433/https://www.wyze.com/
   viii. https://web.archive.org/web/20221230231548/https://dals.com/
   ix. https://web.archive.org/web/20221230231650/https://www.google.com/intl/en_us/chromecast/built-in/
   x. https://web.archive.org/web/20221230231743/https://www.homedepot.com/b/Smart-Home/Hubspace/N-5yc1vZc1jwZ1z1pr0w?cm_sp=vanity-_-hubspace-_-APR21

PART 2

2. Are authorized labs advertising who they have certified?
    a. check manually the websites
        i. **Methodology:** Exploring the websites of each of the 8 authorized labs individually. Creating an archive snapshot of the website as I went through them. I found the links to these websites through https://www.ioxtalliance.org/authorized-labs. On each of the websites, they seem to announce their partnerships with ioxt either in a blog (like https://www.dekra-product-safety.com/en/dekra-authorized-ioxt-alliance-perform-security-testing-mobile-apps-and-vpn) or in a separate menu item under their services provided (like https://bishopfox.com/services/ioxt-certification-program). So in order to find these, I first start with a manual analysis of the index page to see if they have advertised talking about partnering with ioxt or if they have a direct link to their certified products. If not in the index page, exploring the menus were next. Specifically, I was looking for menu items that have likelihood of being related to certification, i.e. under menus like “services”, “partners”, “certification program” “about us” “security compliance/certification”. In finding the pages where they mention their certification, I was hoping that they also include a list of the products that they have certified through their certification program. This wasn’t the case however, and I had to look for other pages in the menus manually to find a list of their certified products or apps, just purely exploring most of their pages. Since I wanted to limit exploring each website to around 30 minutes, as a last resort, I also tried using the search function of the website, where I looked for keywords, i.e. list, certified products, certified applications/apps, ioxt, certification programs, etc.
        ii. **Results:** All 8 of the authorized lab websites talk about their partnership with ioxt, as mentioned earlier, either in a blog post or in a dedicated page in their menu items. However, only two websites (Dekra and NowSecure) have a page where they list their certified products, even though they are not for “ioxt" certified products/apps, but rather are for all kinds of generic certifications that they do. Rest (6) Do not have a list of their certified products, based on a manual exploration of 1 hour on the website. Some of these websites like bishop fox and onward security do mention some apps that have been certified/security tested but it is in a template of “customer stories” under their blog posts, or news section.
        iii. List of the authorized labs:
            1. Dekra
            2. NowSecure
            3. RedAlertLabs
            4. NCC Group
            5. Bureau Veritas
            6. BishopFox
            7. Onward Security

8. BrightSight

Complete Analysis:

Do authorized labs advertise who they have certified:

1. Beureau Veritas
    1. https://www.cps.bureauveritas.com/needs/ioxt-baseline-security-safer-iot-world
    2. Archive URL: https://web.archive.org/web/20221230225805/https://www.cps.bureauveritas.com/
    3. Couldn't find a visible list of certified apps
2. NowSecure
    1. https://info.nowsecure.com/ioXtAuthorizedLabReferralProgram_LP-FreeReport.html
    2. https://www.nowsecure.com/resource/infographic-mobile-iot-benchmark/
    3. List of certified apps: https://www.nowsecure.com/certified-apps/
    4. Archive: https://web.archive.org/web/20221230230156/https://www.nowsecure.com/
3. BrightSight
    1. https://www.brightsight.com/ioxt-alliance
    2. Archive: https://web.archive.org/web/20221230230100/https://www.brightsight.com/
    3. No visible list of certified apps, but in https://www.brightsight.com/psa-certified they have an external link to https://www.psacertified.org/certified-products/
4. Onward Security

1. https://www.onwardsecurity.com/

   https://www.onwardsecurity.com/news-detail/ioXt/

   2. Archive: https://web.archive.org/web/20221230230032/https://www.onwardsecurity.com/

   3. No visible list of certified apps

5. Dekra

   1. https://www.dekra-product-safety.com/en/programs/cyber-security

   2. https://www.dekra-product-safety.com/en/dekra-authorized-ioxt-alliance-perform-security-testing-mobile-apps-and-vpn

   3. https://www.dekra-product-safety.com/en/ioxt-alliance-certification-program

   4. Has links to search certified products:

      1. https://www.dekra-product-safety.com/en/about-dekra/certified-products

      2. https://www.dekra-checkme.com/search

6. Bishop Fox

   1. https://bishopfox.com/services/ioxt-certification-program

   2. https://bishopfox.com/services/mobile-application-assessment

   3. Archive: https://web.archive.org/web/20221230230215/https://bishopfox.com/

   4. No visible list

7. NCC Group

   1. https://campaign.cyber.nccgroup.com/ncc-group-ioxt-alliance-authorized-lab/

2. Archive: https://web.archive.org/web/20221230230349/https://www.nccgroup.com/

3. No visible list

8. Red Alert Labs

1. https://www.redalertlabs.com/

2. https://www.redalertlabs.com/iot-security-lab-evaluation

3. Archive: https://web.archive.org/web/20221230230439/https://www.redalertlabs.com/

4. No visible list

b. Crawl the websites of all labs affiliated with ioxt and Search the text content for titles, developer names, developer URLs, of iot apps from 37k
    i. First of all, I downloaded all the websites of each of the 8 authorized labs to work with them offline. For 5 of the websites, I used a tool called HTTrack which automatically crawls and downloads websites, with max internal depth of 5, and excluding image files like png, jpg, jpegs, gifs, and following the robots.txt rules for ethical purposes. For 2 of the websites, dekra and ncc group specifically, HTTrack could not download them, so I used another tool named Cyotek Webcopy, with the same configurations mentioned above. For the last one, redalertlabs, neither of the tools worked, so I had to write a custom python script that starts from the main index page, gathers all internal links (with the same domain), and iteratively goes through all the links, gathering all links in each of the pages and repeating this process. Just downloading the websites itself took about 1 day as the websites were quite large and the tools and scripts included delays to avoid being blocked by the websites.
    ii. After downloading the websites, Used 2 extensive techniques for doing this (I can't provide a concrete number of hours put on this, but definitely took a long time to write the scripts, cleanup the input, analyze the results and verify them, more than 100 hours, the scripts themselves ran for about 12 hours to find the results, some less some more). **Note** that this part of the analysis and research is heavily dependent on my own instinct of choosing sample results and also checking false negatives. I have not included this part of the research in the final paper. Below is the methodology:
        1. Searching for title of the application names and developer names
            a. **Methodology:** Wrote another python script that goes through all html files downloaded for each of the websites, and searches names of the 28k applications in them. List of the 28k applications can be found in the data subfolder of this repository. I first cleaned up the names, removing some unnecessary characters at the end, removing generic words like, free, app, etc, removing names less than 3 characters. Then in the actual script searching for the names, I first check if they may have a potential link to google play store which might indicate an app link. Then, I proceed to search for names. I first compare the name of the app against a blacklist of generic names that I observed among the app names, i.e. "iot", "link", "hover", "mobile", "smart", "grid", "flex", "element", "swap", "family", "privacy", "join", "device", "devices", etc. Then, I split the name of the app into words and if the name of the app is more than 3 words, I just search for the first three words of the app name. If the name of the app is a single word, I strictly look for that name as a whole to avoid cases when the name of the app can be a sub-string, i.e. app name "ion" can be substring for a name like "vision". If I hit a potential app name that was found in the html file,

I write the result into a txt result file. I employ the same methodology for searching for developer names.

   b. **Results:** The result file for each of the websites contained a vast number of false positives. Some result files hit around 300-500 hits, of which I manually checked all of them and they were false positives. Some result files hit more than 6000 hits, for which I chose a random sample of 500 hits and manually checked them, and they were false positives too. There were no indications of the searched apps being ioxt certified or the developers names being mentioned.

2. Searching for developer URLS
   a. **Methodology:** I first find the developer websites for all apps from the 28k subset, and then use urllib.parse netloc function to isolate the domain for each of the urls because the urls themselves in raw format contain subdirectories, or other subdomains. Furthermore, I also delete the prefixes like http:// and www as they don't necessarily affect the url. So at the end, I had a cleaned up list of dev websites in the format "something.com". Afterwards, I simply searched the urls in the html pages and if I hit a result, I recorded them in a result file.
   b. **Results:** Relatively few results were hit disregarding the generic domains like facebook.com, twitter.com, instagram.com, linkedin.com, youtube.com, github.com, etc. Those hits that were not generic, i.e. se.com, zoho.com, etc. I manually checked them to see in what context they are used in the authorized labs websites and all were used in a non-certification context, i.e. not related to our interest.