Mentari School Bintaro in Indonesia

Instructor: Misael Joel Vera (**:** misaeljoelvera@gmail.com)

Feedback from 10 Students

Alvin Ghossan (Alvin) Adhitya

alvin.adhitya@yahoo.co.id

Hello my name is Alvin and I like to comment lol. In general I believe that that IoT has no significant benefits to the society. Sure the concept has justify some of the believed benefits especially to the sustainability, efficiency and economy of the community, however in my point of view, representing all the normal non-techy citizens of the world; The concept of IoT does not solve the BIG problems of the world. It only solve for small things like "Showering shorter". Like what the hell are humans getting that lazy, lets not depend our lives too much on technology shall we?

In context to the IoT framework alliance, I want to ask the following questions:

1. Are we mature enough to adopt the new IoT framework?
2. What Is the value of online privacy facing IoT?
3. Will IoT revolutionize future criminal activities?

In a different context, I want to ask does humans really need IoT in their system? From What I understand, IoT is a system, a program, a set of functions. I believe that human nature has its value in its randomness. We are not suited to be in such automatic system. Like IoT. However I also believe in changes, and probably the best thing to do for all citizens is to go with the flow if the progress of IoT is unstoppable.

Dehan Alhany

d_alhany@yahoo.com

1. How can the IOT devices preserve its integrity and security in the network? Besides connected to one local network, which belongs in the customer's house, there must be a network service that protects the network of the IOT devices, the house network and the cloud in which the devices receive information to and from. It could be a 3rd party service or a cloud service. They could employ a 3rd party cloud service to protect the IOT connections and network within the host home, the host's smartphone and the devices network.
2. Manufacturers must conspicuously disclose all personally identifiable data types and attributes collected.
    a. They have to be specific with the type, amount and variety of data each IOT peripheral collects and sends to the company. Instead of prompting every device to ask for permission to collect data, the smart home software should group every peripheral with its role (kitchen devices, toilet devices) and then ask for data collection. The user can choose to go deeper to change the settings on each device for further flexibility.

3. Default passwords must be prompted to be reset or changed on first use or uniquely generated.
    a. Device must prompt password change after first use, requiring the use of a capital letter and numbers. Smart home software must have a password manager which contains the password of the software, cloud service, and discrete peripheral groups.

Quirina Kintan Cemara Daeng

kintancmra@gmail.com

Article #8 -- Default passwords must be prompted to be reset or changed on first use or uniquely generated. Where possible, separate passwords should be required for administrative vs user access and not permit password reuse. Ideally passwords should be randomly generated.

In my opinion, passwords that are uniquely generated would prove to be too long and one the user has to write down to remember; passwords are also a way in which shows involvement of humans as a form of identification, although, in most IoT devices, there are no human involvement, so these uniquely generated would seem a tad bit irrelevant.

Ghiffari Fardhana

ghiffari.fardhana@gmail.com

Online Trust Alliance or OTA developed the IoT framework in which they are required to follow a list of standards such as the disclosure all personally identifiable data types and attributes collected, the term of the duration the data or default passwords and the likes.

Manufacturers must conspicuously disclose all personally identifiable data types and attributes collected. For example a health or fitness band would potentially disclose physical location, tracking and personal vitals (heart rate, pulse, blood pressure), as well as user profile data. The problem with this very brief proposed regulation is its vagueness. The fact that OTA don't really elaborate on how they actually achieve such disclosure shows the potential danger and the obvious flaw of this regulation. They should've said more details regarding where all of the identifiable data types and attributes are originally stored before getting disclosed as it really endangers confidentiality and privacy of the user, which is another issue that is regulated in a different regulation that is much more specialized for privacy settings.

The term and duration of the data retention policy must be disclosed. In general, data should be retained for as long as the user is using the device, or to meet legal requirements. It is acceptable for the policy to state data will be retained as long as a customer uses the product or service and must be deleted upon expiration or account termination. Again, another vague statement that is also very briefed, which gives an unclear view to which OTA is flawed. The data that users are retaining after using a certain device should be backed and kept as long as possible until the user decides to delete them, but the durability of the data should be convincing so that users would not have to deal with unfortunate data loss just because of the IoT's inconvenience.

Default passwords must be prompted to be reset or changed on first use or uniquely generated. Where possible, separate passwords should be required for administrative vs user access and not permit password reuse. Ideally passwords should be randomly generated. Default passwords are one of the biggest reasons why users usually have trouble in the accessability of the system in which OTA should have restrain from using default passwords as the keygen for creating those randomize passwords can be hacked as compared to the much more personal password. The fact that they will prompt the user first is a positive note, however the use of security question can also be utilized instead of uniquely generated passwords.

Putri Gusti

putrig298@gmail.com

1. On Issue #1, it states that the privacy policy must be readily available to review prior to product purchase. The IOT must state an approximate time frame prior before the release of the product.
2. With the use of multiple family members and the creation of individual profiles, information that is accessible through parental and administrative controls are not listed.
    a. What kind of information is able to be accessed by parental/administrative controls?
    b. Following the hierarchy, does the child have any control over the personal information being shared?
    c. If users with administrative or parental controls are breached, information of other family members are also able to be accessed. Thus, decreasing the level of integrity.
    d. Determine if all of the multiple users are able to access all smart devices connected.
3. On Issue #21, information regarding the time-frame and the warranty are not listed in detail.
    a. How much time is given to the users prior to replacing an older version and purchasing a newer one?
    b. Are there any benefits presented for being a loyal user (i.e. those that have been using it for a certain amount of years)
    c. In regards to those who opt not to replace with a newer version, would the framework be compatible and be able to support older versions? Does the user have an option to downgrade from a newer version to the older version by choice?
4. If a hierarchy of smart technology were to be established, the amount of information that can be accessed by the technology should be disclosed. The amount of information that is allowed to be accessed by the technology, should be controlled by the user.
5. On Issue #14, with consideration of administrative control, determine the following:
    a. Control of who are able to access multi-factor verification. Is this limited to administrative controls? Are users able to access multi-factor verification as well?
    b. If passwords for multiple devices differ from one another to increase security.

Michael Heyzer

michaelheyzer@gmail.com

The IOT trust framework is something that is developed by the Online Trust Alliance that provides a standard and a sort of framework for manufacturers who are operating in the IOT industry; in an attempt to provide the privacy required for the consumers of this niche market. The Online Trust Alliance framework is mainly focused upon establishing the trust and reputation amongst the companies and the consumers.

Amongst the things discussed, the framework encouraged the manufacturers to sustain the privacy of the data that the product that the manufacturer produces collects from consumers. This is not so much a case of sustaining the privacy of data of current products that are still being manufactured, as usually manufacturers already have a high standard of encryption for the data that is being collected. The thing that needs to be discussed is the sustainability and protection of the data after the product becomes obsolete. The data itself will become vulnerable to attackers, as the same level of encryption if not any at all might not support the data. The problem with the products that are constantly being released by technology manufacturers is that sometimes the hardware changes are so immense and the architectural framework becomes so different that the problem starts when the data used by previous product becomes incompatible for its successor. This is a problem of backwards compatibility when a new product is released; manufacturers tend to not have any support for the products that were the predecessor of the current lineup. An easy example would be the Sony Smart watch 1st Generation; when the second generation Sony Smart watch came out, the support for the 1st generation ended; meaning that no new software updates rolled out for the watch. This increased hacking vulnerability of the device as this gives the hackers time to develop codes that would actually be able to infiltrate the device software itself and since there are no more software updates; the consumers themselves are defenseless against these hackers.

A solution that I would offer in addition to the things mentioned is to advise manufacturers to not only do a certain act that would improve privacy such as advising to have different passwords on each account and devices but also the extent of the complication of the password to actually truly improve the privacy and safety of the consumers.

Kiral Jura (Kiral) Katoppo

kiralkatoppo@yahoo.com

Issue #13, how extensive should the safety notification be? What are the criteria within the plan?

Issue #11 how are the penetration test done? How extensive should it be? The company that are utilizing the IoT framework should perform numerous scenarios. This also begs the question on how accountable are companies with regards to safety issue.

How does the IoT framework interact with one another in case user output contradicts each other?

How will the IoT framework support older models? Some updated products make drastic changes that not all their customers agree with. How will the company support it and how liable are the companies when older products are vulnerable to newer security breaches.

Abe Manyo Nainggolan

abemanyo@gmail.com

1. The issue of Sustainability and Backward Compatibility.

    In the event that the hardware turns obsolete and can't support the software-security upgrade, a compatibility configuration should be provided for said obsolete hardware to allow the software-security upgrade.

    As IoT allows almost all items to be able to connect to the internet, even an old car or an old Ps2 or and old trophy could be connected. What if the hardware, which has invaluable sentimental value, was to be compromised due to the lack of security that is evident in older versions of hardware? What if the old hardware was used as a gate to connect to customer's IoT networks seeing that its defenses are minimal compared to newer hardware?

    The problem are items with sentimental value, they can't just be discarded. The customers would want, instead, for these invaluable items to be given up-to-date security: and the IoT should be able to do that. After all, the right to keep obsolete hardware(s) is in the user's discretion, and regardless of the reason why, the option to allow said hardware to have safety measures that are still eye-to-eye with the latest ones should still be available.

2. How can IoT deal with devices that cannot be upgraded?

    Items belonging to the generation before the IoT framework – items with novelty values or items that, for whatever reasons, will not be thrown away; what will be done to them to ensure that they are a part or not a part of IoT? How will the framework ensure that these items, when adapted to IoT, can be upgraded into the latest technology software to ensure they are truly secure and do not provide a risk to the network? Is it possible? Or will this option simply be discarded, leaving the pre-IoT items unconnected to the rest of the world's network, forever obsolete?

M. Kahari (Ari) Pranata

this.is.not.an.email007@gmail.com

Overall, I agree with the proposed minimum requirements. But here are my concerns regarding to the proposed minimum requirements:

- On issue #3, will the local government be able to collect any data that they want? If so, in what sort of way will the government collect the data, but at the same time, make the users feel secured?
- On issue #8, is there any specific length of password, as well as the password strength?
- Regarding to issue #11, I would like to suggest to give out penetration test every time the device received a software or hardware update, and in order to make the strong result, I

would like to suggest to do the test more than three times, in order to get a good conclusion.

- For issue #16, I would like to suggest that the IoT devices must be verified through different people, possibly a company that verifies devices. That's because, if the one who verify is either the developers themselves or has a close relationship with the developers, the verification will be bias.
- For issue #18, how should the manufacturers know that the one who contact them is the actual owner of the device, instead of a thief?

The last issue would be the number of proposed requirements. I would like to suggest making it less, but at the same time, covers every requirement that is currently proposed. I understand that more requirement means better result. But by making it less, it would be easier to understand it.

Lorenzo Miguel Valencia

Gio3a_dragon@yahoo.com

The person who purchases one of the IOT device should buy it directly from the company or at least from a place with good reputation in order to prevent the use of RATs being used before reselling it. If the customer chooses to buy an IOT device anyway they should be made aware of the risks that could occur with the purchase of the IOT devices and have a specialist check the product completely for any kind of virus at all to reaffirm the safety of the product.

This is because sometimes a device that has been bought from a person with little credibility like say, a friend or a workmate, might have been infected with a rootkit that allows a hacker from miles away to anonymously track and record data about a person to steal their identity or to utilize their cameras to photograph the person in any situation where the camera is present.

In my opinion the IOT devices shouldn't be able to connect everything at once in the first place because it would leave major security flaws and release an insane amount of data on different people regarding sensitive information. Even if we were to raise the penetration passing test to 90% there is still a 10% that's vulnerable for black hat hackers to exploit and use for malicious purposes.

Companies who create IOT devices should be made to constantly update the security of these devices and have a way of checking and finding the most difficult rootkits with the consent of the user. These devices should be as much as possible, dummy-proof in order to reduce the chance of careless people from releasing confidential information that could harm both the user and those around them.

Also, For the IOT devices there should be certain levels of security for the IOT devices because it is unrealistic to apply all the framework items to every single device. An example would be how a dumb or simple device with only a few functions is supposed to have an extremely long password with email capabilities and privacy settings is too much and unrealistic. How much computing power would a shoe rack really need? Thus the security of the shoe rack should be quite low and should be specifically stated and readable for the user in comparison to the modem or heart of the network where every device is connected to. That device should have the highest security system in order to better protect the users

from possible invasions of privacy and safety. Thus the simplest devices would have a low security and the more functions or complexity the device has the security level should increase exponentially as well.

In my opinion the smartest IOT devices shouldn't be able to connect everything at once in the first place because it would leave major security flaws and release an insane amount of data on different people regarding sensitive information. Even if we were to raise the penetration passing test to 90% there is still a 10% that's vulnerable for black hat hackers.