Dipen Delvadiya

Research Paper 2

ITMS – 478

Ray Trygstad

11/03/2016

Increasing Insecurity in the Internet of Things (IoT)

Industries have been trying their best to launch new technology that can be more useful to people in this competitive market. Just two years ago, appearance of Internet of Things (IoT) was seemed far away, but those days are gone. Nowadays, IoT has become really useful technology in our daily life. According to ABI's research, there are 10 billion wirelessly connected devices in the market by today, and there will be more than 30 billion expected devices by 2020 ("More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020", 2013). Apple and Google had made this IoT an increasingly real business opportunity. According to Cicso estimation, "IoT has possible value of the $14 trillion" (Vermesan & Friess).

First let me explain what IoT is! Internet of Things is an internetwork of the computing devices, vehicles, buildings, phones, and objects through internet with unique identifiers, which is capable of transferring data over internet without any human-human or human-computer interactions. It has become so obvious that we don't even notice how we have been using this technology since long time. For example, listening to music through Bluetooth in your car is definitely IoT. IoT has gained such a global popularity that IoT had become the most growing field of attraction, popularity, and usage. Bluetooth, Wi-Fi, cellphones, RFID, and many other technologies play major role in expanding this technology worldwide. However, some people think that IoT has reached the peak of this century. It is not true at all. In reality, we have just came across our hope and it is just the beginning. For example, by today in India, more than 50% percent people do not even use internet (Barcena & Wueest, 2015). That is why Facebook have been trying to build up internet system in India and can implement IoT technology in this developing country. On the other side, we are creating a new threat for ourselves. In this paper, I am going to discuss why IoT is so useful and few threats related to this emerging technology.

1. Why IoT is so important?

IoT simply wants to connect all the devices to interact with each other to provide secure and better lives to us. Just imagine a life where you wake up, lights get turned on, and coffee machine stats brewing coffee. This is what IoT is capable to do! The IoT may have limitless possibilities, but following are few applications that are significant:

1) Home Network Topology: Mostly everyone's network is made up off a router giving internet access to all the devices in certain range. The devices connect to this network are mostly laptops, phones, and desktop computers. These connected devices can communicate with each other through same network. Most of the devices support any of these communication methods: Z-wave, RFID, Bluetooth, Powerline, and Zigbee (Matho, 2015).

2) Environmental Observing (Matho, 2015): Everyone might have noticed that when you go on internet, you would see interesting things like hotels, food, and restaurants. It also keeps track of your interests and shows you matching categories. These are really common advantages, but there might be some really useful application in the future like earthquake prediction or tsunami prediction before people have to suffer through any damage (Matho, 2015).

3) Tracking: It is possible to for tracking any problems in the bridge and railways. It can reduce the high amount of risk of danger and alarm to aware management to repair it (Matho, 2015).

4) Energy Management (Matho, 2015): Energy Management is a management that is responsible to reduce energy. Basically it has some sensor that sense the sunlight in the

house and reduce the power consumption by either turning off the lights or changing the brightness of the lamps.

5) Medical Systems: Medical systems have the most advanced IoT systems, which are really useful in case of emergency. There are smart tablets that can monitor the amount of dowse needed for any patient to get better.
6) Transport Technology (Matho, 2015): This technology is already in use for detecting any crimes in covered area. It tracks the timings and location of the trains. Also it has automatic configurations of lights, and camera to monitor the traffic and speeds of vehicles.

2. **Insecurity in the IoT**

Just two months ago, Distributed Denial of Service (DDoS) attacked a major Internet domain name server, and blocked the number of popular websites including Twitter and The New York Times (Hagemann, 2016). This is a type of attack in which multiple connected systems get infected with a Trojan and can hack those devices that are connected to the infected systems. Although IoT has some incredible advantages and performance, there are still security breaches that need to be fixed. These breaches might put millions of people at risk of cybercrimes.

1) DDoS attacks and Authentication: As I just mentioned, DDoS attacks can inject high amount of traffic that would be impossible to handle for any website. If high amount of traffic tries to access the data that is not available, customers would be unhappy and enterprise have to go through loss and customer dissatisfaction. It can be injected through any devices that is connected to the network. Hence it is essential to keep track of lost or stolen devices or block them out as soon as possible.

   Easy passwords and hint are the possible reason for the authentication breach. People have to understand their responsibility as a user in enterprise or any group network.

As I mentioned earlier, large companies have been trying to implement these technologies in developing countries like India because of large amount population and huge market. They also need to explain people their roles before assigning them any responsibility. I have stayed in India for almost 18 years, and I have seen people sharing their passwords on phishing mails or phone calls. Unawareness of users is a major breach in this growing technology.

2) New Car Technologies: Ford and GM have been increasing their offers in Wi-Fi. Now anyone can turn their car into hotspot using any passengers' internet (Geer, 2014). But, it has same security vulnerabilities as personal hotspot; it has no firewalls. It is possible to get into this internet really easily, and steal the owner's sensitive information like credit cards and data.
3) mHealth application (Geer, 2014): This always have been a field of attraction to hackers. Any medical system would definitely have large amount of sensitive information. According to Jonathan Collins, Lead Analyst of ABI Research, "mHealth will have 171 million devices by 2018" (Geer, 2014). Hackers have been attacking systems with windows, because non-traditional devices usually use windows.
4) Smart systems but less security: Windows have been launching extremely intelligent and fast systems, but it has less safety because of open source codes. According to Joffe, "There is no patching mechanism for windows on these devices" (Geer, 2014). Windows are really easy to get infected when they connect to the internet.

3. Possible Solutions

As we saw how important data we send through IoT, we need to have extra layer of security to protect our information. The level of security required for any device changes depending upon the functions it going to perform. For example, military communication need way higher security level than regular cell phones communication satellite. Following are the possible solutions:

- Secure Cloud Infrastructure: Cloud infrastructure supporting IoT technologies needs security at variety of layers ("Securing the Internet of Things: Seven Steps to Minimize," n.d.). At application layer, they need to have security protections to prevent anyone to access that data directly ("Securing the Internet of Things: Seven Steps to Minimize", n.d.). Also data need to be always backed up.
- ISO/IEC certification: Any cloud-based systems must have these standards to make sure that service providers have control for managing security of IoT technologies.
- Secure IoT devices: Anyone must have strong passwords for local users. Systems should have strong encryption and device authentication using unique keys ("Securing the Internet of Things: Seven Steps to Minimize", n.d.).
- Simple but most responsible person is user. They always need to be aware of surroundings and have updated software
- Secure boot and using firewalls would kill some low level viruses

There is no doubt that IoT is the future of modern technology. Even today, embedded devices using IoT technologies perform critical functions. Security at network level is as critical as device level. It is important to understand that these possible solutions are not the best way of approaching difficult cybersecurity problems. Companies should consider the safety of these technologies first and implement it in the design process. The challenges and intelligence of hackers in the future will surely be far more expansive, but we can still at least be prepared and learn from our mistakes.

Bibliography

1) More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020. (2013, May 09). Retrieved November 03, 2016, from https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/

2) Vermesan, O., & Friess, P. (n.d.). Internet of Things Applications – From Research and. Retrieved November 3, 2016, from, http://www.internet-of-things-research.eu/pdf/IoT-From%20Research%20and%20Innovation%20to%20Market%20Deployment_IERC_Cluster_eBook_978-87-93102-95-8_P.pdfIndia Internet Users. (2016, July 1). Retrieved November 03, 2016

3) Barcena, M. B., & Wueest, C. (2015, March 12). Www.symantec.com. Retrieved November 3, 2016, from https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things-en.pdf

4) Mahto, J. (2015, November 18). Why We Need IoT (Internet of Things) ??? | Jugeshwar Mahto ... Retrieved November 3, 2016, from https://www.linkedin.com/pulse/why-we-need-iot-internet-things-jugeshwar-mahto

5) Hagemann, R. (2016, October 24). Internet of Things or Internet of Insecurity? - Niskanen Center. Retrieved November 03, 2016, from https://niskanencenter.org/blog/internet-things-internet-insecurity/

6) Geer, D. (2014, January 09). The Internet of Things: Top five threats to IoT devices. Retrieved November 03, 2016, from http://www.csoonline.com/article/2134265/network-security/the-internet-of-things--top-five-threats-to-iot-devices.html

7) Securing the Internet of Things: Seven Steps to Minimize ... (n.d.). Retrieved November 3, 2016, from https://www.ptc.com/~/media/Files/PDFs/Services/PTC_IoT_CloudSecurity_WP.pdf?la=en