The Internet of Things

Introduction

Assume that you have been appointed to a task force of 5 or 6 computing professionals within your organization. You have been asked to examine the current issue outlined in the article below. Your team has not been asked to make specific recommendations to solve the problem. Rather, you have been asked to make recommendations that will help the Government decide what next steps they should take.

Prompts

1. What is/are the problem/problems here? Is there an underlying fundamental problem?
2. Who are the major stakeholders and what are their perspectives?
3. What are the major ethical, legal, and security aspects associated with the problem?
4. What are the intended and unintended consequences of existing computing solutions? Consider the consequences on individuals, organizations and society within local and global contexts.
5. What recommendations do you propose that may lead to potential solutions?

The Internet of Things (IoT) is a developing business of connecting objects and making everyday objects smart. Individual objects are connected and networked to applications and the Internet. This enables, for example, your car to communicate with other cars and with your house. Things can be networked to applications and the Internet by firstly connecting one product, with a single chip and an Internet connection, then linking that to an application to connect with other products. This idea dates from 1999 and some predict by 2020 we may have 20.4 billion connected devices. The IoT can be applied to houses, cars but more widely to the urban environment, and Dubai aims to be the first Smart City in the Middle East through its Smart Dubai Plan 2021. In areas such as transport and power Dubai has made progress, for example by connecting all traffic lights to a central system that changes the light timings according to the flow of traffic. By 2030 Dubai plans to power the city through solar panels and manage electricity use through smart meters, to store and direct power according to demand.

With so many devices becoming connected, how secure will these devices be? Up to 70% of IoT products are open to attack, highlighting issues about security and standards. Some examples were a baby video monitor that let hackers view live feed, a security system that could be turned off remotely, a Samsung security system which

was blocked so the owner couldn't access it, and the I-Spy Tank that allowed a remote hacker to access and control it. A flying drone was also disabled in mid flight by accessing the operating system remotely and smart TVs have been hacked to intercept data and allow the attacker to post to the user's social media. While some of these security breaches are simply annoying, the implications of others such as the drone could be more dangerous and far reaching. It's clear the use of connected things has outpaced security, and many devices have little or no security built in. Once Dubai has made power, transport and health systems in the city smart, security may be a challenge.

However, rather than prioritizing the security of networked things, companies are continuing to put their energies into the development of connected devices. After a hole was discovered in a flying drone's operating system, the company issued a patch that didn't address other security vulnerabilities of the device. The car industry is another example; GM claims to already have one million connected cars in America. Researchers demonstrated hacking cars such as Jeep and Dodge with mobile connections. Students took over an electric car, and caused the doors to fly open, the wipers to work and the horn to honk, and an earlier hack stopped brakes from working, turned the steering wheel, and tightened the seatbelts, all from a laptop. Yet car companies continue to produce vehicles with the same features. It's clear the security aspect of connected devices is an issue so why is it not of primary importance to developers?

The security around the IoT is often not taken seriously by consumers, as people wonder why hackers would want to gain access to a fridge for example. However security researchers have demonstrated that gaining access to one product could enable a hacker to read emails, perhaps reset passwords and even steal identities. At the moment not many people own IoT devices, and the small size of connected devices with limited processing power could cause challenges to developing good security measures. The low cost and fact that many devices are disposable means that updating them or providing a security patch is difficult. Adding more security features requires more powerful processors, so more weight and battery power. Producing IoT chips may also not be a lucrative business, and so the companies are not so motivated. Finally, the Internet is not totally secure so how can IoT devices be secure?

Standards bodies also do not seem overly concerned about the security of IoT. There are no rules applied to drones that are not secure, unlike planes, and security companies hope that the regulations related to planes would be extended to all things that fly. If drones were required to be more secure then the companies producing drones would be forced to spend resources on improving the security while developing the product. The standards body related to smart TVs is also not concerned and a patch to address the security breach in smart TVs has not even been issued.

In Dubai, IoT is expected to make the city seamless, safe and efficient in a personalized way as a global example of a smart city. Smart buildings, energy, traffic and healthcare will improve the living experience for the predicted population of 3.4 million by 2020. For the moment the responsibility lies with the consumer to update passwords and maintain as much security as possible around their connected devices. It is expected companies and authorities will start to address the security more as more security issues arise. Certainly if consumers demand more security when their fridge starts sending out spam, everyone involved in the IoT will respond, from the technology giants to individual developers.

Bibliography

Dingman, S. (2015, October 18). *Why consumers should take the Internet of Things and the lack of security more seriously.* Retrieved April 10, 2016, from The Globe and Mail : http://www.theglobeandmail.com/technology/why-consumers-should-take-the-internet-of-things-and-the-lack-of-security-more-seriously/article26865804/

Dingman, S. (2015, June 14). *Internet of Things a playground for hackers.* Retrieved April 11, 2016, from The Globe and Mail : http://www.theglobeandmail.com/technology/internet-of-things-a-playground-for-hackers/article24953037/

Gartner. (2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016.* Retrieved May 2, 2018, from https://www.gartner.com/newsroom/id/3598917

Gulf Business. (2017). *Dubai's ruler launches new Internet of Things strategy*. Retrieved May 2, 2018, from http://gulfbusiness.com/dubais-ruler-launches-new-internet-things-strategy/

Hajdarbegovic, N. (n.d.). *Are we creating and insecure Internet of things .* Retrieved April 10, 2016, from Toptal: https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things

Ismail, N. (2018). *The Internet of Things: The security crisis of 2018?* Retrieved May 4, 2018, from Information Age: http://www.information-age.com/internet-things-security-crisis-123470475/

Smith, J. (2016, February 16). *Dubai's smart city ambitions .* Retrieved May 28, 2016, from The National : http://www.thenational.ae/arts-life/the-review/dubais-smart-city-ambitions