Merissa Tan

401 Written Assignment 1

In Daily Mail's article "Privacy fears over home security cameras as Wi-Fi signals can be hacked by criminals to tell when people are home or not", the author discusses privacy concerns surrounding home security cameras. The article highlights the concern that internet-connected security cameras that are used by many homeowners to monitor their houses and track potential burglars, such as Google's Nest Cam and Amazon's Ring range, can be interfered with by attackers. These cameras are usually triggered by motion and generate online traffic so that homeowners are able to remotely monitor the cameras online via a Wi-Fi link. This Wi-Fi link, when it is connected and activated, can be hijacked by attackers, even if the video content themselves are encrypted.

To investigate the extent to which a hacker could obtain information from these security cameras, UK and Chinese researchers obtained data from an undisclosed home internet protocol (IP) security camera provider. The researchers then assumed the role of an attacker and attempted to gather privacy-compromising information about the cameras' owners by tracking the uploaded data passively. They found that they were able to detect when the cameras were uploading motion without inspecting any of the video content, simply by looking at the rate at which the cameras uploaded data via the internet. In addition, the researchers discovered that future activity in the house could be predicted based on the traffic generated by the cameras. For example, a lack of traffic in the morning of a workday and a subsequent heavy traffic in the evening could reveal the homeowner's work schedule and allow the hacker to predict when the house is most likely to be empty, thus increasing risks of burglary.

With the continuous advancement of technology, it comes as no surprise that these internet-enabled security cameras, which were once only used in luxurious homes or commercial buildings and warehouses, are becoming more ubiquitous. As these types of technology become more accessible to the general public, more precaution needs to be taken by the manufacturers and programmers to ensure that the personal information and privacy of the consumers are protected. Understandably, this responsibility largely falls on the manufacturers—while everyone should be vigilant whenever it comes to sharing data online, we cannot expect every user to be an expert in privacy and security. Therefore, as software developers, we should put ourselves in the shoes of the users and consider the types of personal, identifying information that a user would expect to be protected when they use a product, such that said information would not be accessible to a malicious third-party.

With that being said, I was surprised to read in the article that there is currently no standard around the minimum data security and access requirements that Internet of Things (IoT) devices need to satisfy before they are released to the public. This lack of security guidelines and requirements is extremely concerning for obvious reasons. As the article points out, it does not take much for an attacker to derive pertinent information about a homeowner's daily routine from his or her security cameras. The lack of formal guidelines on the data protection requirements of these security cameras allows manufacturers to cut corners and neglect on investing in privacy protection in order to make the most profit. This also places the burden of monitoring and protecting the consumers' data on the consumers themselves. In fact, the lack of standard provides a loophole for manufacturers to escape liability should the system be misused to target unsuspecting consumers.

I hope that as I venture into the field of software engineering, I will find that even with the lack of formal rules and regulations, manufacturers and software companies will still serve the best interests of their consumers and do their part in developing secure systems. This is especially true when it comes to surveillance systems where the consumers' privacy could come under attack. Nevertheless, even the most skilled software engineer with the best intentions could miss a flaw in the system that they design. Therefore, I believe that there are a couple measures that could be taken to alleviate the concerns surrounding consumers' privacy for these home surveillance technologies.

The local government, or even the federal government, could establish comprehensive guidelines on the minimum data security requirements for these systems. For example, companies can be mandated to invest in cybersecurity measures to prevent attackers from hijacking a secure connection between the homeowner and their security cameras. I believe that the establishment of clear regulations on these systems will hold manufacturers accountable when there is a breach in their system and allow consumers to purchase these products with greater peace of mind. I have also experienced in my past internships that software companies would frequently hold a "bug bash" where developers gather as many users as possible to perform tests on a newly designed system in order to reveal bugs in a short period of time. I believe that a similar exercise would be extremely advantageous for manufacturers of surveillance technology—in addition to posing as users, developers could pose as hackers and attempt to find and exploit loopholes in the system to uncover previously undetected flaws. There are undoubtedly many more ways to ensure the privacy of consumers, but I believe that software developers should assume full responsibility when their systems are compromised due to a lack of security measurements. Therefore, developers should strive to minimize any misuse

of their products by consulting relevant parties for appropriate guidelines and conducting comprehensive testing on their systems.

With the rise of the popularity of home cameras, homeowners are able to monitor their houses more easily and exercise better control over their properties. At the same time, however, this benefit could backfire, and the homeowners could find themselves unwittingly making it easier for burglars to attack their homes. As the saying goes, with great power comes great responsibility—while this technology undoubtedly benefits many, manufacturers and software developers need to take measures to ensure that they protect the very users who are relying on their products for extra protection. As an aspiring software engineer myself, this article has opened my eyes to the ease at which technology can be abused and reminded me that I need to take the consumer's safety and privacy into consideration whenever I develop something that will be used by the general public.