Task 1a - Project Specification LSEPI Analysis

Analysis into Project Specifications of the Legal, Social and Professional impact of computing and the IT Industry.

Project Specification 6 LSEPI

Within the project most of the issues were centred around the Social and Ethical issues particularly in privacy and tracking with phone technologies, although some do appear in the form of legal issues. Since the application requires a large amount of data to be collected through location, people often become conscious of where the data is going and what it is being used for.

Issue 1

One of the main issues the developer will face with this project is the use of data needed for the application to function, in this instance both Location and Time data is required. The heavy usage of location data can present numerous issues when developing the project due to the ethical implications of storing the data, and risks of data breaches. Secure storage of this data on encrypted servers must be ensured due to GDPR regulations being enforced to protect consumers. Meaning only data that is necessary for the functionality of the application is used, and no further data is required from users. Whilst also getting full consent that is in an easily accessible form and easily readable with the intended purpose of data attached onto the consent. (EU GDPR.ORG, 2019).

An example of this is in 2018, Strava opened their data to allow users to discover new places to run or bike. Strava didn't realize that members of the US military were using GPS-enabled wearables, and their activity exposed the locations of bases and patrol routes in Iraq and Afghanistan. (Loukides, Mason, & Patil, 2018). This data could then be viewed by enemy combatants and then used to plan attacks, if this data was secured properly and not shared any risk presented to these soldiers would have been minimal.

Issue 2

Another potential issue of development comes from Android wear devices and possible vulnerabilities against malware and hacking, and to make sure the application is secure and safe from these risks extensive development may be needed. Failure to secure the application and fix any potential bugs and loopholes may lead to theft of data or a spread of malware, which could cost thousands to millions to repair any damages. To work around this more time may be needed when developing and debugging the application for android wear to plug up vulnerabilities or he/she may need to forgo using them altogether. Kuang Do and colleagues have performed various tests on the security and vulnerabilities of Android and have discovered that one such flaw with Android Wear devices is within the bootloader. Which allows untrusted OS's to be launched to extract sensitive user data from third-party applications and other files from the device using customized boot images.(Do, Martini, & Choo, 2017)

Issue 3

A potential vulnerability the developer may have to adapt to comes from the implementation of QR codes to allow users to log their attendance. QR codes, especially those used for logging in are vulnerable to being hijacked and gain data (like banking and login details), performed by an attackers QR code to trick a victim into scanning it. These types of attacks can even affect applications such as WhatsApp or Alibaba to gain access to the wide variety of data hidden behind them. To secure them the developer should check and change them regularly to ensure that they haven't been highjacked. Alternatively, the developer may have to implement Session Confirmation where confirmation messages and session information is sent between the user and server can be used to improve the security on these QR codes. (Baset, 2019)

In China a recent spate of scams involving QR codes has shone a spotlight on the issue of security in mobile payments. In Guangdong province, about 90 million yuan has reportedly been stolen via QR code scams. According to other reports, policemen in Foshan, recently arrested a man on suspicion of pocketing 900,000 yuan through QR code frauds. According to one senior official, almost a quarter of Trojans other viruses are transmitted though QR codes. (Tao, 2019) Proving the potential vulnerabilities of QR Codes, victims will have no idea that the QR code is a scam when the scan the code and their data stolen unknowingly.

Issue 5

Mobile applications must be allowed access to certain phone features in order to function properly, it does this by alerting the user to what it needs access to with the user allowing/denying as they see fit. For example, access to the camera is required to scan QR codes. If the user doesn't allow access to these features, then the application will not be able to function properly and be essentially useless to its intended purpose. To overcome this a minimum and recommended access will need to be developed into the application, with the minimum access be to the phone's location and time data and further access to the camera be useful for further functionality of the application. When developing the application, access must be requested to the user and it should not attempt to access data in the background with failure to do this resulting in a breach of GDPR regulations, which again could result in fines if not followed.

This is shown in a case with the Spanish soccer's premier league, LaLiga, which has netted itself a €250,000 fine for privacy violations of the GDPR. The smartphone app does more than show commentary of football matches — but can use the microphone and GPS of fans' phones to record their surroundings in a bid to identify bars which are unofficially streaming games. (Lomas, 2019)

Researchers from the International Computer Science Institute (ISCI) discovered that 1325 Android apps harvest user data despite being denied permission. Researchers identified third party online provider—Baidu—collect this information. 153 apps, including Hong Kong and Shanghai Disney theme park apps, Samsung Health and Samsung Browser, transmit data without permission. (Huffington Post India, 2019)

Bibliography

Baset, M. A. (2019, 10 14). *QRLJacking - Your QR Based Session Belongs to us*. Retrieved from Seekurity: https://seekurity.com/blog/2016/11/04/admin/phishing-analysis/qrljacking-your-qr-based-session-belongs-to-us

Do, Q., Martini, B., & Choo, K.-K. R. (2017). Is the data on your wearable device secure? An Android Wear smartwatch case study. *Software: Practice and Experience*, 391-403.

EU GDPR.ORG. (2019, 10 14). *Key Changes with the General Data Protection Regulation - EUGDPR*. Retrieved from EU GDPR.ORG: https://eugdpr.org/the-regulation/

Huffington Post India. (2019, 10 15). *Android Apps Steal Your Data - Even if You Deny Permission*. Retrieved from Huffington Post India: https://www.huffingtonpost.in/entry/android-apps-steal-your-data-even-if-you-deny-permission_in_5d91c74ae4b0e9e7604f86b3

Lomas, N. (2019, 10 15). *Laliga Fined 280K for Soccer Apps Privacy Violating Spy Mode*. Retrieved from TechCrunch: https://techcrunch.com/2019/06/12/laliga-fined-280k-for-soccer-apps-privacy-violating-spy-mode/

Loukides, M. C., Mason, H., & Patil, D. (2018). Ethics of Data Science. In *Ethics of Data Science (1st Edition).* O'Reilly Media, Inc.

Tao, L. (2019, 10 15). *QR code scams rise in China, putting e-payment security in spotlight*. Retrieved from South China Morning Post: https://www.scmp.com/business/china-business/article/2080841/rise-qr-code-scams-china-puts-online-payment-security