**CAB240 Information Security - Semester 2, 2016.**

**Marking Criteria Sheet for Mobile Security InvestigationPart II submission (due Friday 28 October)**

|  |  |  |  |
| --- | --- | --- | --- |
| Student Name: | YeongJe Park | Student Number: | N8923108 |

Include your name and student number in the header of your report. Include this page at the front of your submission.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Report component** | **You have completed this component of the task outstandingly, with:** | **You have completed this component of the task well, with:** | **You have completed this component of the task satisfactorily, with:** | **Your attempt to complete this task is satisfactory in the following ways:** | **Your attempt to complete this component of the task is not satisfactory, as:** | **Mark:** |
| **5** | **4** | **3** | **2** | **1/0** |  |
| **Information security asset description and usage overview** | Excellentconcise description withcomprehensive details of:  □ the device hardware,  □ the operating system and version,  □ application software installed,  □ types of stored data  □ level of criticality of all items/applications and data, and sensitivity of the data items included in description with respect to CIA | Very good concise description providing details for each of the following:  □ the device hardware,  □ the operating system and version,  □ application software installed,  □ types of stored data  □ level of criticality of all items/applications and data, and sensitivity of the data items included in description with respect to CIA | Description providing some details for each of the following:  □ the device hardware,  □ the operating system and version,  □ application software installed,  □ types of stored data  □ level of criticality of all items/applications and data, and the sensitivity of the data items included in description with respect to CIA | Description providing some details for at least 3 of the following:  □ the device hardware,  □ the operating system and version,  □ application software installed,  □ types of stored data  □ level of criticality of all items/applications and data, andthe sensitivity of the data items included in description with respect to CIA | Your description lacks details of the following aspects:  □ the device hardware,  □ the operating system and version,  □ application software installed,  □ types of stored data  □ level of criticality of all items/applications and data, andthe sensitivity of the data items included in description with respect to CIA | /5 |
| **Article 1 (O/S related) Name:** | | **iPhone vulnerability used to target journalists, aid workers** | | | | |
| **Control measures to deal with issue identified in**  **Part I**  **Article 1:**  **Mobile device operating system** | □ Identifies a relevant control measure  □Comprehensive article summary that correctly and clearly explains how the control measure applies to this issue,  □ correctly categorises the control measure, and  □ clearly explains the limitations of the selected control measure. | □ Identifies a relevant control measure  □Good article summary that clearly explains how the control measure applies to this issue,  □ correctly categorises the control measure, and  □ explains the limitations of the selected control measure | □ Identifies a relevant control measure  □Satisfactory article summary that explains how the control measure applies to this issue, and  □ correctly categorises the control measure, and  □ identify the limitations of the selected control measure | □ Identifies a relevant control measure  □ Article summary attempts to explain how the control measure applies to this issue, and  □ categorises the control measure, and  □ identifies the limitations of the selected control measure | □ Does not identify a relevant control measure, or  □ Article summary does not attempt or correctly:  □ explain how the control measure applies  □ categorise the control measure  □ identify limitations of the selected control measure | /5 |
| **Article 2 (App related):** | | **Minimizing security risk of playing Pokemon Go** | | | | |
| **Control measures to deal with issue identified in**  **Part I**  **Article 2:**  **Mobile device application** | □ Identifies a relevant control measure  □ Comprehensive article summary that correctly and clearly explains how the control measure applies to this issue,  □ correctly categorises the control measure, and  □ clearly explains the limitations of the selected control measure. | □ Identifies a relevant control measure  □ Good article summary that clearly explains how the control measure applies to this issue,  □ correctly categorises the control measure, and  □ explains the limitations of the selected control measure | □ Identifies a relevant control measure  □ Satisfactory article summary that explains how the control measure applies to this issue, and  □ correctly categorises the control measure, and  □ identify the limitations of the selected control measure | □ Identifies a relevant control measure  □ Article summary attempts to explain how the control measure applies to this issue, and  □ categorises the control measure, and  □ identifies the limitations of the selected control measure | □ Does not identify a relevant control measure, or  □ Article summary does not attempt or correctly:  □ explain how the control measure applies  □ categorise the control measure  □ identify limitations of the selected control measure | /5 |
| **Article 3 (User behaviour related):** | | **The threat in downloading new mobile apps.** | | | | |
| **Control measures to deal with issue identified in**  **Part I**  **Article 3: User behaviour** | □ Identifies a relevant control measure  □ Comprehensive article summary that correctly and clearly explains how the control measure applies,  □ correctly categorises the control measure, and  □ clearly explains the limitations of the selected control measure. | □ Identifies a relevant control measure  □ Good article summary that clearly explains how the control measure applies to this issue,  □ correctly categorises the control measure, and  □ explains the limitations of the selected control measure | □ Identifies a relevant control measure  □ Satisfactory article summary that explains how the control measure applies to this issue, and  □ correctly categorises the control measure, and  □ identify the limitations of the selected control measure | □ Identifies a relevant control measure  □ Article summary attempts to explain how the control measure applies to this issue, and  □ categorises the control measure, and  □ identifies the limitations of the selected control measure | □ Does not identify a relevant control measure, or  □ Article summary does not attempt or correctly:  □ explain how the control measure applies  □ categorise the control measure  □ identify limitations of the selected control measure | /5 |
| **Conclusion** | Excellent conclusion relating the application of the control measures to the identified information security issues in the three Part I articles, and summarising the information security status of your mobile device. | Good conclusion relating the application of the control measures to the identified information security issues in at least 2 of the three Part I articles, and summarising the information security status of your mobile device. | Satisfactory conclusion relating the application of the control measures to the identified information security issues in at least 2 of the three Part I articles, and summarising the information security status of your mobile device. | Attempts to relate the application of the control measures to the identified information security issues in at least 2 of the three Part I articles, and/or to summarise the information security status of your mobile device. | Does not relate the application of the control measures to the identified information security issues in at least 2 of the three Part I articles, or summarise the information security status of your mobile device. | /5 |
| **Articles to support selected control measures:** | For all three articles,  □ Comprehensive and correct reference details  □ In text citation  □ Reference appears in bibliography | For all three articles,  □ Mostly correct reference details  □ In text citation  □ Reference appears in bibliography. | For all three articles,  □ References provided, but some details missing  □ In text citation  □ Reference appears in bibliography | For all three articles,  □ References provided but many details missing OR  □ No in text citation | □ No reference details  □ Missing many important details  □ No in text citation | /5 |
| **PART I total** | | | | | | /30 |

**Mobile Security Investigation Part II**

This report will show basic explanation about the information assets and security issues associated with iPhone 6. Furthermore, this report describes real security issues in detail by citing some articles.

First of all, there are various kind of hardware for iPhone 6. For instance, input device shows a tablet pencil, keyboard, and scanner while output device shows a printer, monitor and so on. The most essential element is A8 chip which is a part of CPU in iPhone 6. The A8 chip is foundation to operate the iPhone. It can also offer the Secure Enclave which is a great function for information security. The Secure Enclave provides all cryptographic operations for data protection key and retain the integrity of data, if hackers can successfully attack the kernel. Furthermore, there is also helpful a hardware which is Touch ID sensor to improve security. It is one of locking method to use iPhone by utilising fingerprint. Thus, there are some hardware to prevent security problems.

Secondly, there is a iOS platform which is designed by Apple for mobile device. OS is the most important software to manage hardware and application. If there is no OS in mobile device, this device is just useless tool. The iOS provides some powerful security features to protect data in regard to confidentiality, integrity and availability. Many people believe that this OS is always safety from external attack. For example, iOS can prevent unauthorized users when they try to access to device, and enable remote wipe if the iPhone is stolen or lost. In addition, the development team in Apple always try to improve the iOS to make better features. Therefore, when Apple company release the new version for iOS, people can immediately update the latest iOS.

Thirdly, there are many useful installed and installable application software on iPhone. For instance, people can see basic application such as calendar, photo, contact, music, safari, app store and so on when people buy new iPhone. Some application have the sensitive data. The contact application shows friend's information such as phone number, email address, picture and so on. There is the Applocker application which is the locking tool to protect their information in respect to confidentiality and integrity. People can lock each significant application by using the Applocker. Furthermore, when application developers want to release new application on App store, the new application should be examined by Apple company for security. iPhone users can install new application on formal app store

without anxiety about virus or hacking.

Lastly, there are various data types such as music, photos, video, messages and so on for Apple mobile products. People can conveniently save the data on safari which is internet application without connecting computer. For example, when people want to watch movie or read fantasy novels, they can download a movies and novel directly from internet to mobile device. Furthermore, Apple's user can share the saved data to other Apple products

by utilising iTunes. For instance, If people saved some music and photo files in iPad on iTunes, the user can download these files on iTunes to iPhone or other products. People can also recover last data by using iTunes when people initialize every data and system.

Semester 2 2016

**Mobile Security Investigation Part II**

**First submission article:**

**Title:** iPhone vulnerability used to target journalists, aid workers

**Author:** Kelly, Heather

**Reference details (if online article, give URL and date accessed):**

Kelly, H. (2016, Aug 25). iPhone vulnerability used to target journalists, aid workers.*CNN Wire Service* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1813993584?accountid=13380

**Security goals compromised:**

This article shows that dangerous security goal is confidentiality. The iPhone malware approved hackers to access virtually every data on iPhone. Therefore, attackers could see and control saved application and information on iPhone without the user's consent.

**Threat/vulnerability/attack details:**

Ahmed Mansoor who is human rights activist received a suspicious SMS text message on his iPhone for the first time. Manssor sent the suspicious message to Citizen Lab laboratory. The Citizen Lab which is an interdisciplinary researcher discovered security problem on iPhone. The link included a zero-day iPhone remote jailbreak. It was unknown exploits and usedto avoid IOS security measures until a recent date. The vulnerability was known as "Trident". It could provide opportunity to install spyware on iPhone, when people click malicious links in text message. After spyware was installed by clicking this link, attacker could monitor and control everything on virtual. For example, hackers could send messages in chat application and track their movements by Google map. They could also record content of telephone conversation.

**This submission: treating the risk**

**Suggested control measure and explanation:**

A control measure for this scenario shows the Apple company cooperate with various international security company such as Citizen Lab. The Citizen Lab and Lookout security team shared the discovered vulnerability with Apple to notify this security issue(Bill & John, 2016). Apple is now offering very safety security on iOS to users. But, some unknown vulnerabilities can make dangerous situation to Apple mobile devices. Therefore, the collaboration can improve iOS security to prevent problem early. For example, when attackers make malignant code or find vulnerability on iPhone, Security company and Apple can upgrade new iOS version by sharing discovered problem to prevent security issue.

**Limitations of this control measure:**

Even though Apple provide secure iOS version to users, the new iOS cannot protect exposing their information if they click suspicious link or download application on unofficial app store. But, If users recognize the importance of information security, the improved iOS can provide very safer environment for security. Periodic patch of iOS can offer the lowest likelihood of an incident and prevent negative consequence. Therefore, Users should often check the newest version of OS system to update.

Semester 2 2016

**Mobile Security Investigation Part II**

**First submission article:**

**Title:** Minimizing security risk of playing Pokemon Go

**Author:** [Hudson, Laura](http://search.proquest.com.ezp01.library.qut.edu.au/indexinglinkhandler/sng/au/Hudson,+Laura/$N?accountid=13380)

**Reference details (if online article, give URL and date accessed):**

Hudson, L. (2016, Jul 14). Minimizing security risk of playing pokemon go. *International New York Times* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1803635387?accountid=13380

**Security goals compromised:**

A successful attack of hacker compromises the confidentiality on security goals. The Niantic company could get authority of their Pokemon Go user's Google account when users log in Pokemon Go game application by Google account. Therefore, The Niantic company could access to email, photos, calendars, stored documents and everything on Google account.

**Threat/vulnerability/attack details:**

This article shows the vulnerability of Pokemon Go which is the most popular mobile virtual reality game.The vulnerability is permitting for access of user's account on Google when people play Pokemon Go game. This vulnerability can show huge security risk. For example, the Niantic company can invade user's privacy by watching stored data on Google and live information since users should utilise the camera and GPS function to play Pokemon GO. Furthermore, Andrew Stroms who is vice president of security services at the security company said the company could get a lot of data about your habits and what you are doing on your phone. The Niantic company also can sell the great amount of data by collecting data to other marketers.

**This submission: treating the risk**

**Suggested control measure and explanation:**

The suggested control measure is change of authority about access to user's Google account to protect user's privacy. In other words, the Niantic company should change from the setup of feasible access to Google account to the setup of impossible access to account. But, the Google now curtailed the Pokemon Go's authority of access to only basic information on Google account(Ruiz, 2016). Therefore, after users update the Pokemon Go application to prevent disclosure of personal information, they can play this game without any anxiety.

**Limitations of this control measure:**

The alteration of authority about access to Google account will not invade the user's private life. But, before the Niantic company change the setting, this company already gathered a lot of information on their database system. The Niantic responded our company does not has any plans to sell Pokemon Go user's aggregated data to other third party(Conger, 2016). But, their users cannot know how Niantic did this obtained information. Furthermore, the company can still access to data about user's location and camera as this game is virtual reality game. People need to take the possible care for theemselves.

Semester 2 2016

**Mobile Security Investigation Part II**

**First submission article:**

**Title:** The threat in downloading new mobile apps.

**Author:** [Chowdhary, Sudhir](http://search.proquest.com.ezp01.library.qut.edu.au/indexinglinkhandler/sng/au/Chowdhary,+Sudhir/$N?accountid=13380); [Sen, Monalisa](http://search.proquest.com.ezp01.library.qut.edu.au/indexinglinkhandler/sng/au/Sen,+Monalisa/$N?accountid=13380)

**Reference details (if online article, give URL and date accessed):**

Chowdhary, S., & Sen, M. (2016, Jul 11). The threat in downloading new mobile apps.*Financial Express* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1802682316?accountid=13380

**Security goals compromised:**

This article shows that the most serious security goal is confidentiality from attack. The personal information about people in living India are usually exposed by permitting access to data when people try to install new application on mobile devices.

**Threat/vulnerability/attack details:**

This article describe Indian people did not have idea about importance of information security as many people used to install free application by providing their personal information. This behaviour is very serious vulnerability as attackers can easily invade their privacy. This vulnerability can be deliberately exploited when hackers can hide malignant code on free application to attack their mobile device. In India, mobile users think that some serious security problems are some threats associated with misuse of credit card or fraudulent access and hacking or leaking of individual data. For instance, after people download new application by offering their mobile data and personal information, attackers can access to mobile bank to gain bank account, bank password and bank statements. Furthermore, attackers can sell obtained data to some companies or third parties for money.

**This submission: treating the risk**

**Suggested control measure and explanation:**

The story of control measure is education about information security for India people to recognize the importance of security. People should know the risks of their behaviour to download free application by permitting personal information on mobile devices. These behaviour will cause various security issues. Information security education is one of the most simple method to prevent various type of security issues(Jeffrey, 2016). This control measure can support the decrease of leaking of personal information and protection against the attackers. Actually, people do not need to know technical knowledge to protect their information. When they use mobile devices, they need to be careful in their behaviour.

**Limitations of this control measure:**

The main limitation of this control measure shows that there are some education centres to teach knowledge of information security. Furthermore, generally people will not go this centre to learn by paying money. Even if there is free education school, some people probably will go this school to learn. But, after some people study a basic of concept about security, they can prevent active attacks by recognising them. Furthermore, they can consider some situation again when they receive a suspicious message.

In conclusion, there are some basic information about hardware, operating system, application software and some types of data. Furthermore, there are main three articles about information security to show security issue and control measure.

First article shows a vulnerability of the last iOS 9.3.5 version. After iPhone user received a suspicious message including distrustful link, attackers could virtually access to every data and control every application on iPhone when people click the suspicious link. To solve this issue, the Apple company directly released the newest iOS version to iPhone users. At this time, Apple received the discovered vulnerability to solve the vulnerability from the Citizen Lab and Lookout security team. Thus, the control measure is collaboration of Apple with reliable security companies as other security teams can support Apple for better safer environment for security.

Secondly, the vulnerability of the Pokemon Go game shows that the Niantic company could access to every stored data and functions on Google account when people play Pokemon Go game. Furthermore, the Pokemon Go company could invade their user's privacy in real time as users should use the GPS and camera functions to play game. Therefore, the company could also know their user's moving route. The control measure of this issue is reduction of the authority to access to Google account. Namely, Pokemon Go company can access to only basic information on account to check authorised use.

Thirdly, the article shows that threat of behaviour of Indian people. Many people in living in India provide their personal information when they try to download free application on their mobile device. Thus, their important information are already exposed to dangerous situation as hackers can easily get personal information by spreading free application. The control measure for this issue is offering the free education centre to teach idea about information security. After people learn the knowledge about security, they can recognize a mistake of giving personal information to install free application.

Lastly, in terms of my iPhone, there is no any security problem after I bought. I install always application on only official app store. When I receive the notice about new update for iOS, I directly update the latest version for better security setting. In fact, there is no opportunity to attack my iPhone as I usually use my mobile phone to communicate with my family or friends. Furthermore, Apple provide a credible security environment without antivirus program.

**Reference List**

Kelly, H. (2016, Aug 25). iPhone vulnerability used to target journalists, aid workers.*CNN Wire Service* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1813993584?accountid=13380

Bill, M. & John, S(2016, August). The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. *The Citizen LAB* Retrieved from https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Hudson, L. (2016, Jul 14). Minimizing security risk of playing pokemon go. *International New York Times* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1803635387?accountid=13380

Ruiz, R. (2016, Jul 14). Pokémon go update fixes google security issues.*University Wire* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com.ezp01.library.qut.edu.au/docview/1803664889?accountid=13380

Conger, K. (2016, Sep 1). Niantic responds to senate inquiry into pokémon Go privacy. *TechCrunch* Retrieved from

<http://social.techcrunch.com/2016/09/01/niantic-responds-to-senate-inquiry-into-pokemon-go-privacy/>

Chowdhary, S., & Sen, M. (2016, Jul 11). The threat in downloading new mobile apps. *Financial Express* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1802682316?accountid=13380

# Jeffrey, R. (2016, Oct 4). To Minimize Cyber Risk, Organizations Should Focus on Education. *INSURANCE JOURNAL* Retrieved from http://www.insurancejournal.com/news/east/2016/10/04/428338.htm