CAB240: Risk Report for iPhone 12 Pro

Group 136: Ash Phillips, Sasha Le, Ethan Parkinson

Due Date:
31st October, 2021

Contents

1.0. Introduction

The client's organisation is SEA Photography, a small photography business in the creative arts industry sector. They are employed as the main wedding photographer and are therefore responsible for completing bookings, working with clients to understand their wants, and taking the photographs for clients. It is assumed they use a professional camera to take the photos so their phone, which is used for both personal and work use, is mostly used to store contacts of their clients, timetabling and event scheduling, temporary photo storage of inspiration pictures and test photos, etc. It is likely the user will use this for their personal activities

As the device is for both personal and work use, there is a high chance of this device containing sensitive data, including social media and/or bank accounts, personal and work messages, notes, emails, and contact details, etc. If this device was to be compromised, all three components of the CIA model could be broken.

Confidentiality - There would be email and messaging correspondence between each entity. Including sensitive data such as customers contact details, payment information and photos\videos.

Integrity - There is sensitive data on this phone with information that can be used for a spoofing attack and many active attacks where the attacker can intercept these communication channels and modify the messages (*Active and Passive attacks in Information Security - GeeksforGeeks*, 2021).

Availability - This device contains media files related to the organisation's operations. Applications that the organisation uses for storing their digital assets could be compromised resulting in accounts being stolen and access changed (Wong, 2021)

The purpose of this report is to understand the client's mobile device and its uses, review the client's mobile security through the means of assessing risks associated with installed applications, the device's operating system, the client's behaviour around device usage, and the physical security of their device. As well as determining the privacy of data in an installed application through a qualitative analysis with general findings that the application was mostly secure, possible risk treatment and countermeasures for mentioned risks, and also final recommendations for these risks.

Assumptions were made about how the client is using their device and how they may keep it safe; behaving as the average person does in regards to phone security. Also, by only researching and evaluating the risks and privacy issues with one application, Dropbox, the security of the device cannot be completely ensured as they use many other applications also. Due to this, there are limitations to how thorough this analysis can be; relying on assumptions made about the client, business, and phone usage.

2.0. Discussion

2.1. Context Establishment

2.1.1. Information Assets

The information asset possessed by the client is an iPhone 12 Pro. This device (iPhone 12 Pro) comes with an apple-design A14 bionic chip, 6.1 inch super retina XDR display and an IP68 rating. There are three cameras (Ultra Wide, Wide and Telephoto) with 12MP sensors that allow for HDR, 4k, 1080p and 720p recordings as well as high quality photo captures (*iPhone 12 Pro - Technical Specifications*, 2021).

The iPhone 12 Pro comes with 5G, LTE and supports WiFI 6 and bluetooth 5.0 for wireless communication. This device has a built-in GPS system as well as a NFC reader.

The battery capacity for this phone supports up to 17 hours for video playback or up to 11 hours for video playback streams and up to 65 hours audio playback. It has a built-in rechargeable lithium-ion battery that can be wirelessly charged. (*iPhone 12 Pro - Technical Specifications*, 2021)

This device runs on iOS with the latest version being iOS 14. This operating system comes packed with powerful features and built-in apps. The main preloaded application that is regularly used by the client are:

- Camera
- Photos
- Messages (most vulnerable)
- Phone
- Mail (most vulnerable)
- Maps
- Weather
- Contacts
- Calendar

The other applications that the client has installed are:

- Dropbox (most vulnerable)
- Adobe Lightroom
- Facebook
- Messenger

(*iPhone 12 Pro - Technical Specifications*, 2021)

Due to the nature of the client's work, there are a large volume of media files stored on their phone as well on some of the applications they use, such as dropbox.

The client will have sensitive contact information in regards to their customers in email and sms formats. Information includes:

- Name
- Addresses
- Phone numbers
- email address
- payment details (in some circumstances)
- Signed contracts

And also work related media files which includes:

- Photos
- videos

The client uses this device as their work and their personal phone. This would mean that not only would work related data and software be stored on this device, there are also applications installed for their personal use and also personal data such as:

- Personal contact information
- social media accounts
- music
- media files (photos, videos)
- emails and messages to family and friends as well as personal endeavours

2.1.2. Usage of the Device

This device is both the client's personal and work phone however, the main intended use of the device is for their organisation. It is a device for the client to communicate with their customers as well as have a portable means of accessing, editing and sharing their work as a photographer for SEA Photography. Any media files and information can\could be claimed as the organisation's property depending on the signed policy agreement made between the client and the organisation (SEA Photography).

The data on this device is critically important to the organisation as this contains sensitive customer data as well as access to the organisation's digital assets. If this device were to be breached, this could damage the organisation's image with their customers as well as losing important digital data that the organisation uses in their daily operations. Because of this high importance, the organisation will need have policy inplace to prevent the three components in the CIA model from being broken

Confidentiality - The client will need to follow policy to prevent this component from being breached. As the data contained on this device has sensitive information regarding the organisation's customers. Contact details, images , payment details will need to be kept safe and any unauthorised access will need to be denied.

Integrity - The integrity of the communication channel will need to be maintained, as stated above, this device is used as the main communication method.This device will have access to social accounts, email address and phone number attached to the organisation.

Due to this, the customers will initially assume any communication made from these accounts and numbers to be authorised.

Security policies will need to be followed to prevent this component from being breached to prevent any communication data from being altered.

Availability - The client will need to follow security policies to ensure and prevent the device being compromised. Security breaches on this device could lead to accounts relating to the organisation storage application,data files and contact information regarding the customers from being stolen and locked preventing the organization from access.Policies will need to be inplace to prevent this and also action plans if this does occur to avoid loss of operation.

Due to this device being both for personal and work, there are many other applications that the user uses. For personal applications, the client uses many entertainment applications relating to social, music and video applications.

However for their work, the main application the client interacts with on this device is Dropbox.

Dropbox is a tool for secure storage of files as well as providing a way to share these files and a convenient solution for project collaborations. Dropbox lets you store and access files from anywhere, brings all your content together and synces them across all devices using the account. Dropbox is advertised as a secure solution for your organisation that provides you with tools to protect the files you share. This application lets you choose and give access to the right people. This can be done with password protection, expiring links and editable download permissions. It has protection to avoid unwanted edits, deletions, hackers and viruses (*What is Dropbox - Features Overview - Dropbox*, 2021).

Email and SMS are another two main applications that the client uses.This is used to save contact information and correspondence made with the organisations customers. Can be used for scheduling , sending contracts and payment invoices as well as a communication method between the business and customer. Apple Mail is a pre-installed application that comes by default on all iphones. Allows for viewing and managing favourite mailboxes, searching for specific emails, view and sorting (*Use the Mail app on your iPhone, iPad, or iPod touch*, 2021).

iMessage is the default application for sms on an iphone. This application allows for collaboration with others in a conversation. You can send texts, photos, videos to other mobile phones as well as pin important messages to be viewed later. Sent attachments can be searched for if needed (*Use Messages on your iPhone, iPad or iPod touch*, 2021).

2.2. Risk Assessment

2.2.1. Article 1: Security Issue with a Mobile Device Application (Appx. 5.2.1.)

Title: Apple Has A New iMessage Challenge After Latest WhatsApp Update

Author: Zak Doffman

[**Reference Details:** Doffman, Z. (2021, September 18). Apple Has A New iMessage Challenge After Latest WhatsApp Update. Retrieved from: https://www.forbes.com/sites/zakdoffman/2021/09/18/apple-iphone-13-iphone-12-ios-15-users-stop-secret-access-to-your-imessages/ Date Accessed: October 21, 2021.]

Brief Summary: The article discusses a vulnerability in the mobile application 'iMessage' and how it interacts with the mobile application 'iCloud'. If a user stores iMessage backups on iCloud, the encryption key used to encrypt messages on the device will be stored in the Apple servers. This gives Apple employee's, or anyone using an employee's account, the potential to view private messages as they have access to the encryption key.

Information Asset: The information asset involved is the users private messages. As the encryption key has been stored elsewhere, anyone who has access to that key can compromise the security of these messages.

Security Issue:

Threat: This is an external threat involving a single action for an attacker to exploit the vulnerability. If an attacker were to breach an Apple employee's account, they would then have access to the encryption key and use it to view the message backups stored on iCloud, which is not end-to-end encrypted. This compromises the security goal Confidentiality as the user is under the impression their messages are secure and does not give consent for them to be shared.

Vulnerability: The vulnerability is the sharing of the encryption key by iMessage to the Apple servers. With this key shared, anyone who can access it can use it to decrypt the messages. Even if a user does not allow their messages to be backed up on iCloud, if the iCloud services are used at all on their device and are enabled this encryption key will still be shared.

Security Incident/Attack: The article describes the attack process simply; a person with access to an Apple employee account can access the users message backups, then use the encryption key to decrypt and view them. This active is an active attack as the attacker would still need to gain access to an Apple employee's account to exploit the vulnerability. But once the account is breached, the attacker can easily then compromise the messages.

This vulnerability has still yet to be patched by Apple, meaning any users of iMessage are still at risk if they have iCloud backups enabled.

2.2.2. Article 2: Security Issue with a Mobile Device Operating System (Appx. 5.2.2.)

Title: New iPhone WiFi Hack Becomes More Dangerous, Affects All iOS 14 iPhones

Author: Gordon Kelly

[**Reference Details:** Kelly, G. (2021, July 6). New iPhone WiFi Hack Becomes More Dangerous, Affects All iOS 14 iPhones. Retrieved from: https://www.forbes.com/sites/gordonkelly/2021/07/06/apple-iphone-wifi-security-hack-ios-iphone-upgrade/ Date Accessed: September 8, 2021.]

Brief Summary: The article focuses on a threat to all iOS 14 iPhones posed by malicious WiFi networks with symbol characters in their SSID. If the user connects to these networks their phone could be hit with a denial of service (DoS) attack or arbitrary code execution that will disable their phones WiFi or possibly add malicious code to the device.

Information Asset: The information asset involved is the iPhone's backup file. The attack attaches malicious content to this file to prevent the user from enabling the Wifi without a custom factory reset to remove and fix it. Due to the possibility of malicious code being added to the phone, any information on the device, or networks it connects to, could also be at risk of exploitation.

Security Issue:

Threat: This is an external threat created by attackers who wish to deliberately harness a bug in the WiFi setup of iOS 14. By using symbol characters in the SSID of the network they are able to exploit the format string vulnerability to disable the devices WiFi connection. This is done by tricking the system to read the characters as commands to cause the format function to fail and then potentially write arbitrary code onto the device/execute arbitrary code. This may compromise the security goal Confidentially as the arbitrary code could possibly target the users sensitive information; gain access without consent. The attack may also target Availability as by disabling the WiFi the user would no longer have access to any online personal/company data; for example, emails, cloud storage, company systems.

Vulnerability: The vulnerability was a format string bug present in how the WiFi connections work in iOS 14. If symbol characters were used in a network's SSID it could confuse the format function into thinking the symbols are commands that attackers could use to affect the device.

Security Incident/Attack: The article describes the premise of the attack, the attacker only needs to use symbol characters in their network SSID. They can also add these symbols in a way that users are not aware the symbols are there; for example, creating a long SSID so the symbols are not on the screen. Once a user connects, the attacker is then free to write/execute arbitrary code on the user's device. This is an active attack involving edits to the iPhone backup file. It has now been patched by Apple in the iOS 14.7 update.

2.2.3. Article 3: Security Issue with Mobile Device User Behavior (Appx. 5.2.3.)

Title: No, Your iPhone is Not More Secure than Android, Warns Cyber Billionaire

Author: Zak Doffman

[**Reference Details:** Doffman, Z (2021, May 16). No, Your iPhone Is Not More Secure Than Android, Warns Cyber Billionaire. Retrieved from: https://www.forbes.com/sites/zakdoffman/2021/03/16/iphone-12-pro-max-and-iphone-13-not-more-secure-than-google-and-samsung-android-warns-cyber-billionaire/ Date Accessed: September 9, 2021.]

Brief Summary: The article focuses on how Apple iPhones and their users approach security. Apple's security systems are much more closed off than Android's, so the users heavily rely on Apple to protect their devices rather than take action themselves. Because of this, many users do not follow basic security measures and are therefore at a high risk of being targeted by security attacks.

Information Asset: The information assets described in the article at risk of being targeted are any of the user's sensitive data stored on their phone, or any corporate information they may access with the device. As the article mainly focuses on users behavior and lack of phone security, it does not outline any statistics of corporate data being stolen; though it can be assumed that due to these attacks, and the vulnerability present, any threat that occurs has the potential to harm company data.

Security Issue:

Threat: This is an external threat to iPhone user's security caused by their lack of basic security precautions. The article states that 46% of companies in the United States had been the target of malicious software (malware) attacks introduced by an employee who used a phone that had been infected with it. These attacks may comprise the security goal Confidentiality as they leave the company's information assets at risk of being accessed without consent.

Vulnerability: The vulnerability is the lack of security precautions taken for work and personal mobile phones. The article states 95-99% of employees have no security software on the phones they use to access company systems, therefore any accessible data is at major risk of being targeted.

Security Incident/Attack: The article does not describe any specific attack process but does outline users need to be more aware of their phone's security and change their behaviour to reduce the risk of being targeted for attacks; for example, create secure passwords to unlock phone, pay attention to the apps they install to protect themselves against malware, etc. The malware attacks mentioned in this article would be considered active attacks, as they require the attackers to infect the user's device. These attacks would be considered by users to be a violation to their privacy.

2.2.4. Article 4: Physical Threat to a Mobile Phone (Appx. 5.2.4.)

Title: Apple Researching Battery Swell Detection with Internal Sensors on iPhone

Author: Wesley Hilliard

[**Reference Details:** Hilliard, W (2021, March 11). Apple researching battery swell detection with internal sensors on iPhone. Retrieved from: https://appleinsider.com/articles/21/03/11/apple-researching-battery-swell-detection-with-internal-sensors-on-iphone Date Accessed: September 16, 2021.]

Brief Summary: The article discusses new patents Apple has been researching to detect and prevent battery swelling. If a phone battery starts to swell, damage can be done to the device, putting it, and the user, at risk.

Information Asset: The information assets involved are the phone itself and any data that is stored on it; in this context say photos, contact details, schedule details etc. The article briefly mentions major damage to devices battery swelling has caused in the past; the Samsung Galaxy Note 7 battery casing was too small which led to their “violent destruction”. This potential of major damage puts all information assets on the device at risk.

Security Issue:

Threat: This battery swelling is an internal threat caused by the hardware of the device and/or user behaviours. As mentioned in the context, the iPhone 12 Pro uses a lithium-ion battery. Due to the chemistry of these batteries, charging may change the composition and produce by-products (for example, gas), causing the swelling. The security goal Availability may be compromised by this threat, as the user may need to have the issue fixed or replace the phone/battery, therefore they will not have access to the device and any contained data they may need. Also, if major damage was to occur to the device, the user would lose all access to the information assets on the device, further compromising Availability.

Vulnerability: The vulnerability is created by how the device is made and the components used. In the case of the Samsung Galaxy Note 7, the vulnerability was the casing being too small to account for any possible swelling/by-product secretion. Another vulnerability would be user behaviours, such as over charging the device causing by-products to be produced faster.

Security Incident/Attack: This is a security incident, as battery swelling is not purposely intended to occur by the manufacturer. If the device has a smaller battery casing, and the user tends to over charge the device, the resulting incident puts the device and information assets at risk.

Apple, by researching new technologies and hardware designs to detect and prevent these incidents, may keep future devices protected. The article states that the patent inventors also worked on the creation of the Apple Watch technology.

2.3. Privacy Analysis

2.3.1. Privacy Policy Summary

a) App Name: Dropbox (a free cloud storage app downloaded from the App Store with optional paid plans)

The details provided in the Privacy Analysis section were obtained from the Privacy Policy provided by the Dropbox developer on the Dropbox website, available at: https://www.dropbox.com/privacy

Date Accessed: 13 September, 2021

This app was specifically chosen as it is the most vulnerable app which the user has chosen to install on their device as well as one of the user's most frequently used apps.

b) Type of information collected: The information collected by Dropbox is composed of both personal and non-personal information.

- Personal data collected by Dropbox include account details (name, email address and phone number, credit card details, physical address, and phone contacts if the user chooses), file information (file size, upload date, collaborators and usage activity), information on how the users makes use of the app (sharing, editing, viewing, creating and moving files and/or folders), and even personal and sensitive device data such as IP Address and what web page the user visited before opening Dropbox. Dropbox may also collect social media account details, browser and/or device data, and advertisement conversion data if the user allows (Dropbox, 2019).
- Non-personal data collected by Dropbox include device information, such as the type of device used, unique device identifiers, and, depending on the user's settings, location.

c) Collection method: The Dropbox privacy policy (2019) states that personal information, such as name, email address, phone number, physical address and credit card details, are collected when the user signs up for an account, upgrades to a paid plan, and when they set up two-factor authentication. File information is collected when the file is uploaded to Dropbox, and user contacts and location are collected if the user allows the application access to their device's contact list and location. The privacy policy of Dropbox does not specify how it collects data such as device information or web usage activity, however, Dropbox's use of cookies and similar technologies document (2019) states that essential device information including unique device ID and browser information are collected by 'Strictly necessary' cookies while web usage data, social media account details and advertisement conversion data are collected through various non-essential cookies which the user can turn off.

d) When is the information collected? The privacy policy states that some personal information is collected when the user signs up to Dropbox, upgrades to a paid account, and enables two-step verification. The Dropbox use of cookies document (2019) states that device information and website usage data are only collected while the user is interacting with the Dropbox website or Dropbox services.

e) How relevant is the collected information to your use of the app? Seeing as Dropbox is primarily used to store and share files via the cloud, file information would be important for all involved parties, and certain personal information such as name and email address would help distinguish between users. Credit card details are only useful if the user is on a paid plan. Contacts and social media account details may be somewhat useful in sharing files, however they are hardly key to the app's functioning. Web usage data and advertisement conversion data are not immediately useful or necessary to store and share files.

f) How is the collected information used by the app providers? Dropbox states that they collect and use information such as name, email address, contacts, account activity and device information to "provide, improve, protect, and promote [their] Services". Data collected by cookies, such as website usage data, advertisement conversion data and social media account details, are used to "improve and customize services" as well as to personalise advertisements to the user's interests and "understand the effectiveness of [their] advertisements on social media services."

g) Information storage: Information relating directly to the user's account (i.e. name, email address, etc.) are retained indefinitely as long as the user's account remains active. If the user deletes their account, their information is retained for 30 days before being deleted. The policy states, however, that this information may be retained past the 30 day deadline if it is necessary to comply with legal obligations, resolve disputes or enforce their agreements. Data collected by cookies is lost when the cookies expire. Necessary cookies expire from a period of 30 days to 4 years, while the non-essential cookies expire after a period of 20 minutes to 2 or 3 years.

h) Use of encryption: The privacy policy makes no mention of encryption for data in transmission. The policy's only mention of encryption is "encryption of files at rest".

i) Information sharing: The Dropbox privacy policy (2019) mentions in its *With Whom* section that information may be shared with third parties in the following circumstances:

- Information may be shared with trusted third parties working for Dropbox to provide things such as customer support and IT services for "the business purposes of helping us provide, improve, protect, and promote our Services." The policy states that while these trusted third party companies will have access to the user's information to perform tasks on behalf of them, Dropbox still retains responsibility for their handling of it.

- Dropbox shares its infrastructure, systems and technologies with other Dropbox Companies. The policy states that the information is processed across these companies “as permitted by applicable law and in accordance with their terms and policies.”
- Dropbox shares information such as name, profile picture, email address, device, and usage information to other users who the user in question has collaborated with or chosen to share a file with.
- The user can choose to connect their Dropbox account with third party services and in doing so the policy states that the user is allowing Dropbox and the third party to exchange the information about the user and their data. The third party’s use of the data gathered from this exchange is then governed by their own privacy policy and terms of service.
- If the user is part of a Dropbox Business Team, the administrator of the business may be able to access and control the accounts of the Dropbox Business Team. If the user simply interacts with a Dropbox Business Team and is not a part of one, members of that organisation may be able to view the name, profile picture, IP address and email address associated with the user’s account at the time of interaction. If the user shares an item with a Dropbox team user, the administrator of that team may be able to access and edit what was shared
- Dropbox may share information to third parties if it is necessary to comply with legal processes, appropriate government requests, or to prevent fraud and protect the rights, property, safety and/or interests of Dropbox.

j) App user access to information: In the Dropbox privacy policy (2019), the *Your Control and Access of Your Data* section outlines what access a user has to their data. Users can delete files from their Dropbox and change their personal data held in their account, as well as ask for a copy of the user’s personal data that Dropbox collected, the business or commercial purpose for collecting it, the types of sources they drew from and the types of third parties the data was shared with. In addition, users can request to stop or limit the processing of their personal data for certain processing activities.

2.3.2. Privacy Risk Identification and Analysis

Which assets are most at risk? The assets most at risk when using Dropbox are the user's name and email address as these pieces of information are most readily shared with other users. Allowing any user to see the email address of someone who's chosen to share files with them opens up avenues to have that email exploited for scamming and phishing attacks which, if successful, could compromise the confidentiality of the user's more sensitive personal data. The lack of encryption in transferring data means that any data is unprotected and able to be read by any potential interceptor, meaning that any messages during a collaboration using Dropbox services could potentially be intercepted and read and potentially changed. The user's details may also be leaked if a third party company, which they have decided to link their Dropbox account to, experiences a cyber incident or data leak.

Risk analysis: The risks posed to the security of this app can be analysed using a qualitative scale. The more major the consequence, the higher the risk, in balance with the likelihood of a breach in security. For example, the risk of a user's name and/or email being seen and targeted by phishing or scam attacks is possible, however, depending on the user's response to the phishing/scam attack, the risk could become major for the user; this makes it a moderate threat. The risk of someone intercepting unencrypted data during a Dropbox collaboration is also possible but could have anything from minor to catastrophic consequences depending on the data being sent; whether it's a generic greeting or confidential business information, this constitutes a major risk. A third party company experiencing a data leak or cyber incident and leaking user data is somewhat unlikely, but could have major consequences for the user whose data was leaked and major or even catastrophic consequences for the company in both legal action taken against it and its future reputation. An unlikely occurrence with a potentially catastrophic consequence makes this eventuality a moderate risk.

Limitations and Difficulties: The risk analysis is limited by some of my inferences as the policies are vague and non-specific when it comes to third party companies and what the collected data is specifically used for. Such information is detailed to an extent, however it is only minimally done so in several separate documents which the privacy policy provides links to throughout the document, convoluting the information and providing the details to the few thorough readers who go through all the links in the policy.

How closely does this follow Australian Privacy Legislation? The privacy policy for Dropbox follows the Australian Privacy Legislation reasonably closely. Most of the information collected is reasonably necessary with the exception of some of the data collected by some of the non-essential cookies. Dropbox ensures that users consent to their data and Dropbox's uses for it and they allow the user to access and update their information at any time. However, the security of the information described in the privacy policy, or the lack thereof, leaves something to be desired.

2.4. Risk Treatment and Countermeasures

2.4.1. Mobile Device Application

Overview of Security Issue from Part A: Mobile Device Application

In Part A, a vulnerability that exists with Apple's default messenger application, allows Apple and its employees the ability to access users' private content (Doffman, 2021a).

Apple's iMessage application uses end-to-end encryption as a security measure to only allow the sender and receiver access to the contents. The security vulnerability of this application is that, if a user has iCloud Backups enabled, this opens up a security risk where user data can be accessed (Doffman, 2021a).

iCloud encrypts user data, such as iCloud messages, and stores it on Apple servers alongside the key used to encrypt the data (Hoffman, 2021). Anyone with access to Apple servers potentially has access to your data.

This vulnerability, if breached, will have an effect on the Confidentiality component of the CIA model.

Confidentiality - iMessage is one of the main applications the user will use to communicate with clients and peers. There will be confidential information in the messages as well as files being shared between users. Access to these messages which are unauthorised, is considered a confidentiality breach. This will affect the organisation image with their client that can affect the operational performance.

Treating the Risk

Suggested control measure and explanation:
A control measure for this scenario is to disable iCloud backups on the device entirely (Hoffman, 2021).

iCloud Backups are enabled by default and is the main exploit for this vulnerability. Disabling this will mitigate the security risk, as iMessage data will not be stored on Apple servers.

Due to the nature of the organisation, iCloud Backup is a useful application to store company data as well as backup of this data to avoid any operation downtime if there were any data-loss. However, because of the iMessage vulnerability it is recommended to not enable this but either look into using a third party data backup application or messaging application.

This approach was suggested in an article discussing the security issue with iMessage (Hoffman, 2021).

Type of Control Measure:
This is a preventive control measure to direct users away from the application's security risks. Disabling iCloud Backups or utilizing a different messenger application, allows users to bypass iMessage vulnerability, where the application data as well as the encryption key, gets stored on Apple servers (Hoffman, 2021).

This helps users prevent unauthorised access to their private data , allowing them to operate in a more transparent environment with their clients.

This is the main control measure suggested by Hoffman to fix the issue (Hoffman, 2021).

Degree of Protection Provided:
By following this control measure, the likelihood of unauthorised access to the users messaging data is greatly reduced. The control measure stops storage of the encryption key on Apple servers which will prevent unauthorised access by Apple and its employees as well as any security breaches made on Apple servers (Hoffman, 2021).

End-to-end encryption is used to protect iMessage data, disabling iCloud Backups ensures that no other access to this data can be made except the sender and receiver of this data. iMessage with end to end encryption is designed so that Apple can not read and access your messages in transit between the devices (*We're committed to protecting your data*, 2021).

This control measure aims to prevent the encryption key from being stolen from Apple servers. There are many other vulnerabilities with using iMessage such as SMS mobile threats and attacks that lead to theft of private data as well as spreading malware to other users. This control measure does not protect the user against SMS phishing, mobile malware or SMS scams (*SMS Attacks and SMS Mobile Threats*, 2021).

Limitations of this Control Measure:
The limitations of this control measure are, when you disable iCloud backups, data on your phone will not be backed up which can cause data loss if there are any malicious attacks to the phone or hardware and software failure (Hoffman, 2021). Disabling this will also mean that the user will be unable to access their messages from another device other than their mobile.

This control measure only secures against data breaches made from unauthorised access to the encryption key either by Apple or data breaches made on Apple servers (Hoffman, 2021). The device will not be secured from other malicious attacks such as SMS phishing, mobile malware or mobile scams.

2.4.2. Mobile Device Operating System

Overview of Security Issue from Part A: Mobile Device Operating System

In Part A, a vulnerability in the iOS 14 operating system that allows attackers to target WiFi connection (Kelly, 2021) was discussed. The vulnerability was a format string bug that allowed attackers to target the iPhone backup file. This vulnerability could be deliberately exploited by an external attacker to hit them with a denial of service (DoS) attack or perform arbitrary code execution to disable the phone's WiFi until a factory reset could be performed and/or potentially add arbitrary code to the device. To target this vulnerability, the attackers used symbol characters in their network SSID that then confuse the system to believe a command should be run, effectively disabling the WiFi and allowing them the potential to attach arbitrary code to the device/execute arbitrary code without the user knowing.

This attack compromises the security goals Confidentiality and Availability. Confidentiality is compromised as the attacker may gain access to the user's information assets present on the mobile device without the user's permission/consent, therefore violating the user's privacy; especially with the potential addition of arbitrary code to the device the attacker could use to access the device at a later date through remote execution. Availability is compromised as by disabling the device's WiFi capabilities, the user will no longer have access to any online systems needed for the company, e.g. company emails, web portals, etc.

Treating the Risk

Suggested control measure and explanation:
This WiFi bug was patched by Apple in the iOS 14.7 update, though control measures can still be taken to avoid this issue if it arises again in the future. A control measure for this scenario is to, in the device setting, turn off the Auto-Join feature and set "Ask to Join Networks" and "Auto-Join Hotspots" to "Ask"/"Ask to Join" (Doffman, 2021c). By changing these settings, the device will no longer transmit probes searching for open network connections that allow the device to connect to networks automatically. This measure will then prevent the device from connecting to these malicious networks without the user doing so themselves which should help to mitigate the connection issue.

This approach is suggested in an article covering this WiFi attack by Doffman (Doffman, 2021c).

Type of Control Measure:
This is a preventive control measure aiming to stop the user from encountering these attacks and lower the chances of the device connecting to a malicious network. With the auto-join feature turned off, the user must deliberately connect the device to a network themself. Due to this, the user can use their own judgment to decide if a

network is safe to connect to or not. While this should stop the majority of cases, as it should be easy for the user to spot a malicious network in this case as they use symbol character in their SSID, there may be some cases where these symbols are not clearly visible to the user (e.g. the network SSID is long, causing the symbol characters to not be shown on the screen).

This is the main control measure Doffman outlines to protect the device from these attacks (Doffman, 2021c).

Degree of Protection Provided:
By taking this control measure to protect the device, the likelihood of the attack occurring should be significantly reduced as connections are deliberate; the user can judge if a network looks to be malicious (if the SSID contains symbol characters).

While this control measure reduces the likelihood of malicious connections, as previously mentioned, there may be some cases where the user still connects to these malicious networks themselves either through accident or as they are unsuspecting of an attack; this measure does not prevent the user from connecting to malicious networks themselves. If a connection were to occur, the attack will still affect the device the same way as normal; this treatment will not affect the consequence of the attack if it occurs.

Limitations of this Control Measure:
As stated, though the malicious networks use symbol characters in the SSID, there are some cases where they may be difficult to detect by the user. Due to these cases, there are limitations as to how protected the device is. If the user does not take care when connecting to networks themselves by analysing the SSID for symbols or by connecting carefully/purposefully to avoid accidental miss-clicks their device may still be a target of these attacks. This control measure only helps to reduce the likelihood of connection through automatic connection, not manual.

2.4.3. User Behaviour

Overview of Security Issue from Part A: User Behaviour

In Part A, a vulnerability caused by the common user behaviour of people not taking precautions to ensure their phone's security (Doffman, 2021b) was discussed. As mentioned in part A, Apple's security systems are closed, so users generally rely on Apple to protect their devices and therefore don't take action themselves. Doffman states that 95-99% of employees access company systems with mobile devices that have no security measures in place, which creates a major vulnerability to the security of said systems. This vulnerability can lead to external attackers targeting company assets and any accessible data; as was also stated, 46% of United States companies have been targeted by malware attacks due to an employee's phone being infected.

These attacks may compromise the security goal Confidentiality. As company data is accessible via employee's devices that may themselves be compromised by malware, etc., there is the potential of this data being accessed without consent of the company by outside sources, therefore compromising Confidentiality.

Treating the Risk

Suggested control measure and explanation:
A control measure for this vulnerability is to enforce a BYOD (Bring Your Own Device) security policy (Australian Government, 2021). The suggested measure describes that this policy should include employee's installing security software and setting up a firewall to secure any mobile devices that will be used to access company data. Also, the policy should enforce employees to keep the devices' software up to date to protect against recent security flaws that may be patched in updates. By ensuring these policies are followed for each device used to access company data/systems, the safety of company assets can be better secured and employee awareness on mobile security, and possible risk factors involved caused by not ensuring security, can be increased. The policy should also ensure no employee will access company data with any unprotected device, including unprotected personal devices.

This approach is suggested in an article on protecting your business by the Australian Government (Australian Government, 2021).

Type of Control Measure:
This is a preventive control measure aimed at increasing security of employees' devices and therefore lowering any risks of security vulnerabilities that could affect company, and employee, safety. By increasing the security measures taken to protect mobile devices, it causes possible malware attacks to become less of an

issue, as the measures taken should prevent the user/decrease the likelihood of the user encountering such attacks.

This is the second of ten measures suggested by the Australian Government to protect a business from cyber attacks (Australian Government, 2021).

Degree of Protection Provided:
By increasing the security to protect the device the likelihood of any attacks occurring will be greatly reduced and, depending on the software installed, the severity of the attacks may also be reduced. The specific security software that the company recommends employees to install on their devices will change the degree of protection that can be provided to the device; the likelihood of being targeted by attacks will decrease no matter the software, but the scale it decreases by and the possible decrease in severity/consequence of said attacks will differ based on what software is used.

Ideally, a software that both decreases the likelihood of attacks occurring and also reduces the attack consequence should be chosen to provide the highest level of protection to the device and the accessible information assets.

Limitations of this Control Measure:
The security measures to take and the software to install is to be decided by the company and it should be up to them to ensure that security is kept at a high standard to protect their information assets, as well as protect their employees and customers. Depending on the softwares chosen, there may be limitations to what devices they can be installed on, e.g. different applications on Apple versus Android, so the company should take initiative to ensure the chosen measures are available to all employees, or put in place separate measures for each device. Also, as stated, regarding the degree of protection provided, different software will have different capabilities for protection against attacks and reducing the consequence the attacks may have. Again, it is up to the company to decide on a software that provides a high level of protection to ensure security is of high quality.

2.4.4. Physical Threats to Mobile Device

Overview of Security Issue from Part A: Physical Threats to Mobile Device

In Part A, a vulnerability in the iPhone 12 Pro hardware that allows battery swelling to occur was discussed (Hilliard, 2021). This vulnerability is caused by the components Apple used to build the device. As stated in part A, the iPhone 12 Pro uses a lithium-ion battery and, due to its chemistry, if it becomes overheated, by-products such as gas will build up in the battery, causing it to expand and break components around it. This expansion/swelling can be caused by damage to the battery unit, constant overcharging of the device, or, in the worst cases, general wear and tear of the materials within the battery (Barsch, 2018).

If the battery were to begin to swell within the device, the security goal Availability may be compromised. If this threat occured, the user would then have to take action to repair (i.e. replace the battery and any other components that may have been affected by the swelling) or completely replace the device, both outcomes causing a breach in Availability as the user would no longer have access to the device and its information assets (Hilliard, 2021). Availability would be compromised further if the device were to be destroyed as access the information assets would be lost to the user completely.

Treating the Risk

Suggested control measure and explanation:
A control measure for this scenario, which is one of few one can implement to control an essential piece of hardware, is to make sure that the user does not leave their device plugged into its charger; ensure the user does not regularly over-charge the device (*I have a swollen battery. What now?*, 2020). In the article by Battery World on swollen batteries, it is explained that lithium-ion batteries need to have the ability to discharge and recharge the by-products created through the charging of the device, so by leaving the device plugged into the charger/overcharging the device the battery cannot cycle through this process (*I have a swollen battery. What now?*, 2020). Therefore, ensuring the charger is unplugged from the device once the battery is fully charged, will allow the energy to be discharged and the build up of gas that causes the battery to expand will be minimised.

This approach is suggested in the article on battery swelling from Battery World (*I have a swollen battery. What now?*, 2020).

Type of Control Measure:
This is a preventive control measure, as the only other measure to take in this scenario would be to replace the battery either when the user detects that the battery has begun swelling or when the battery has already swollen to a point where it could be dangerous for the device and user themselves. This control measure relies

entirely on the user maintaining their responsibility to monitor their phone's battery and disconnect/reconnect the device from the charger only when necessary (i.e. when the device is fully charged/needs charging).

This is the first of four measures suggested in the battery swelling article from Battery World (*I have a swollen battery. What now?*, 2020).

Degree of Protection Provided:
This control measure would provide a minor degree of protection against this physical threat. While the control measure does decrease the likelihood of battery swelling, it is not very common in the first place, and this control measure only reduces one factor contributing to it. Furthermore, this measure does nothing to eliminate or decrease the consequence of battery swelling as if it were to occur the user would still need to take action against it.

This control measure may decrease the likelihood of the physical threat occuring by a small amount, but does nothing for the consequence.

Limitations of this Control Measure:
As previously mentioned, this control measure only mitigates one factor leading to battery swelling and does nothing to eliminate or decrease the consequence of the swelling. This control factor has no effect on factors such as damage to the battery or manufacturer defects, etc, creating some major limitations to its effectiveness. Generally, the likelihood of a battery swelling is not up to the user, as found in the article discussing the vulnerability, as it is due to how the device was manufactured as much as it is due to how the user handles the device (Hilliard, 2021). Due to this, the best option would be whenever the user was to purchase a mobile device, they look into how devices have been manufactured and if swelling was kept in mind when creating the them.

3.0. Recommendations

The recommendations that this organisation should take to improve the security of their digital assets are:

For the mobile device application, the organisation should implement a security policy for staff to comply with that ensures that the controls measures are taken.

Any staff who will use a phone for work will need to disable iCloud Backups and use Dropbox as an alternative for data storage as well as data back ups for the company assets. If users are using their own personal devices, iCloud Backup will also need to be disabled if not they are not authorised to use the device.

This control measure is critical to prevent any unauthorised access to company data. Messages are very important to the company as this is one of the main communication channels between the company and the client. This communication channel needs to be secure and reliable to ensure customer satisfaction as well as trust which will help the company image as well as operations.

These messages will contain sensitive data such as client personal contact information, payment details images and video, to prevent any unauthorised access to this information, the company should implement this control measure immediately.

All current company devices should be returned to the IT department so that the control measure can be implemented. New security policy should be distributed to companies for a better understanding of this new implementation and company digital assets on any staff personal devices that do not comply with the new policy will need to be removed. This implementation will take around a month to implement. The first couple of weeks is to write up the new security policy, hand to staff. The final week is for the company to act on the new policies.

The recommendation for the mobile device operating system is to include this control measure (refer to 2.4.2) in the company's new security policy. This is to ensure that users will follow the rules to prevent mobile attacks and reduce any threats.

Users who will use a mobile device for company work will need to turn off the Auto-Join feature and set “Ask to Join Networks” and “Auto-Join Hotspots” to “Ask”/”Ask to Join” (Doffman, 2021c). This will prevent the user's phone from auto-joining to malicious networks.

This control measure is critical to prevent unauthorised access to the company digital assets if a phone device or company account were to be breached in a malicious attack from this vulnerability. These phones contain sensitive data that needs to be protected. One of the main concerns is that if a phone were to be breached, any company accounts existing on that phone could also be compromised that could result in data loss as well unauthorised access to sensitive client information.

This policy is vital to keep the companys' digital assets secure and should be implemented as soon as possible. This can be done with most of these control measures given at once. This control measure will take around a week to implement. as the security policy has been written up from the first stages and have been distributed to staff

The recommendation for User Behaviour vulnerabilities is to include into the new security policy , that users will need to allow the company to install security softwares on their personal phones. As well as follow extra security procedures such as enable Multi Factor Authentication for company accounts.

Users will need to sign a statement that states that they will comply with all security policies.

Phone devices will need to be kept updated including application and operating system updates. This is to ensure any software vulnerabilities get patched up.

This control measure will take around a week to implement. as the security policy has been written up from the first stages and have been distributed to staff

The Recommendation for physical hardware vulnerabilities is to include into the new security policy, that users will and should not use their phones whilst it's being charged and to store the phones away for direct sunlight or storage that may heat up e.g. car dash units.

This is to prevent battery swelling on the users phone that can result in hardware damage as well data loss. There is critical information on the phone that is used for work that, if not backed up correctly, can result in data loss which will interfere with the company's operations.This control measure will take around a week to implement. as the security policy has been written up from the first stages and have been distributed to staff

These four control measures for Mobile device application, mobile device operating system, user behaviour and physical threats vulnerabilities, will need to be implemented as soon as possible. This can begin after you have received this report, and we recommend that you ensure your security policies include these amendments to ensure the safety of the company assets. The time frame to implement all these control measures is estimated to be around 1 month and 3 weeks.

4.0. References

Active and Passive attacks in Information Security. (2021). GeeksforGeeks. Retrieved September 18, 2021, from https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/

Australian Government. (2021, August 3). *Protect your business from cyber threats*. Business. Retrieved September 22, 2021, from https://business.gov.au/online/cyber-security/protect-your-business-from-cyber-threats#secure-your-devices-and-network

Barsch, E. (2018). *What to do with a swollen iPhone battery*. iFixit. Retrieved October 27, 2021, from https://www.ifixit.com/News/11211/what-to-do-with-a-swollen-iphone-battery

I have a swollen battery. What now?. (2020). Battery World. Retrieved October 27, 2021, from https://www.batteryworld.com.au/news/expert-advice/2020/i-have-a-swollen-battery-what-now

Doffman, Z. (2021, September 18). *Apple Has A New iMessage Challenge After Latest WhatsApp Update*. Forbes. Retrieved October 21, 2021, from https://www.forbes.com/sites/zakdoffman/2021/03/16/iphone-12-pro-max-and-iphone-13-not-more-secure-than-google-and-samsung-android-warns-cyber-billionaire/

Doffman, Z. (2021, May 16). *No, Your iPhone Is Not More Secure Than Android, Warns Cyber Billionaire*. Forbes. Retrieved September 9, 2021, from https://www.forbes.com/sites/zakdoffman/2021/03/16/iphone-12-pro-max-and-iphone-13-not-more-secure-than-google-and-samsung-android-warns-cyber-billionaire/

Doffman, Z. (2021, July 24). *Why You Should Change This 'Dangerous' iPhone Wi-Fi Setting*. Forbes. Retrieved September 19, 2021, from https://www.forbes.com/sites/zakdoffman/2021/07/24/apple-iphone-wi-fi-warning-as-dangerous-threat-hits/

Dropbox Privacy Policy. (2019, December 17). Dropbox. Retrieved September 13, 2021, from https://www.dropbox.com/privacy

Hilliard, W. (2021, March 11). *Apple researching battery swell detection with internal sensors on iPhone*. Apple Insider. Retrieved 16 September, 2021 from https://appleinsider.com/articles/21/03/11/apple-researching-battery-swell-detection-with-internal-sensors-on-iphone

Hoffman, C. (2021, July 30). *Apple's iMessage Is Secure … Unless You Have iCloud Enabled*. How-To-Geek. Retrieved 25 October 2021, from https://www.howtogeek.com/710509/apples-imessage-is-secure...-unless-you-have-icloud-enabled/

iPhone 12 Pro - Technical Specifications. (2021, August 25). Apple. Retrieved September 12, 2021, from https://support.apple.com/kb/SP831?locale=en_AU

Kelly, G. (2021, July 6). *New iPhone WiFi Hack Becomes More Dangerous, Affects All iOS 14 iPhones*. Forbes. Retrieved September 8, 2021, from https://www.forbes.com/sites/gordonkelly/2021/07/06/apple-iphone-wifi-security-hack-ios-iphone-upgrade/

McKeown, E. (2021, September 3). *What Is Multi-factor Authentication (MFA) and How It Works*. PingIdentity. Retrieved September 22, 2021, from https://www.pingidentity.com/en/company/blog/posts/2017/what-is-multi-factor-authentication-mfa.html

SMS Attacks and SMS Mobile Threats. (2021). Kaspersky. Retrieved 27 October 2021, from https://www.kaspersky.com/resource-center/threats/sms-attacks

Use Messages on your iPhone, iPad or iPod touch. (2021). Apple. Retrieved September 18, 2021, from https://support.apple.com/en-au/HT201287

Use of cookies and similar technologies. (2019, February). Dropbox. Retrieved September 13, 2021, from https://help.dropbox.com/accounts-billing/security/cookies

Use the Mail app on your iPhone, iPad, or iPod touch. (2021). Apple. Retrieved September 18, 2021, from https://support.apple.com/en-us/HT210511

We're committed to protecting your data. (2021). Apple. Retrieved 26 October 2021, from https://www.apple.com/au/privacy/features/

What is Dropbox - Features Overview. (2021). Dropbox. Retrieved September 18, 2021, from https://www.dropbox.com/features

Wong, J. (2021). *Stolen Dropbox passwords are circulating online. Here's how to check if your account's compromised*. Quartz. Retrieved September 18, 2021, from https://qz.com/771196/stolen-dropbox-passwords-are-circulating-online-heres-how-to-check-if-your-accounts-compromised/

5.0. Appendices

5.1. Context for Investigation

Team Member	Student Name	Student Number	Last Digit
1	Sasha Le	n10091378	8
2	Ethan Parkinson	n10761632	2
3	Ash Phillips	n10477659	9

Industry Sector: Creative Arts

Employee Type: Photographer - mostly weddings

Phone Type: Apple iPhone 12 Pro

Phone Owned By: Employee, Used for all personal use and for work use

5.2. Recent Articles Used in Risk Assessment

5.2.1. Article 1: Apple Has A New iMessage Challenge After Latest WhatsApp Update

Link:
https://www.forbes.com/sites/zakdoffman/2021/09/18/apple-iphone-13-iphone-12-ios-15-users-stop-secret-access-to-your-imessages/

Apple Has A New iMessage Challenge After Latest WhatsApp Update

Last Updated: Septemper 18, 2021
Zac Doffman

The battle between Apple and Facebook has just taken another twist. Hundreds of millions of iMessage users are caught in the midst of that battle, with shocking security and privacy issues at stake. If you're a daily iMessage user, then you need to understand these issues and what you need to do to stay secure.

This has been an awkward week for iMessage. An urgent security update to fix a serious security issue was released alongside glitzy PR promising iOS 15 feature updates. And then rival WhatsApp dropped its own surprise bombshell—the platform's biggest missing feature was suddenly here—as easy as that, a real game-changer.

WhatsApp has been hit by its own NSO exploits in the past, of course. But now, its surprisingly timed update exposes a different iMessage security vulnerability. If you back up WhatsApp from your iPhone to iCloud, then Apple can currently access that backup. It's the same with Android devices and Google Cloud. Now, WhatsApp is ending that vulnerability, cutting Apple's access. But that same vulnerability still remains by default in iMessage, undermining its end-to-end encryption.

WhatsApp's update was announced by Mark Zuckerberg himself—on Facebook. We knew it was in the works but had not expected this confirmation and technical detail so soon. The timing hitting the same week as the iPhone launch could be a coincidence, but Zuckerberg has called out iMessage's security vulnerability in the past. "Apple and governments have the ability to access most people's messages," he warned, as his privacy-focused battle with Apple intensified earlier this year.

With this update, WhatsApp ends its exposure to Apple's security. Its end-to-end message and call encryption is backed off with the same level of security for the chats and media you save to the cloud. It now presents a stark improvement over Apple's muddled approach to cloud encryption.

I reported on WhatsApp's update a week ago, and since then have fielded multiple questions from users as to how they secure iMessage against this vulnerability—you can find details below. It's a stupidly simple setting tweak that is little talked about.

WhatsApp's backup encryption is cleverly designed—it's clearly taken considerable work to provide a solution for 2 billion users across most of the world. Put simply, your backup is guarded by a

64-character encryption key. You can either create and store your own, manually, or protect one online in a third-party vault that is protected by a simple to remember password. The key being WhatsApp has no access.

And it's this concept of "access" that undermines iMessage security. Apple's encryption architecture for what it calls "Messages in iCloud" is also cleverly designed. It's the best multi-device, fully encrypted architecture available, beating WhatsApp's own multi-device update, given that it creates a circle of trusted devices without the concept of a master messenger to which all other devices are linked.

Apple provides you with an end-to-end encryption key that ensures that messages sent to and from your devices cannot be read by anyone but you and your counterparties. But it then stores a copy of that key in your iCloud Backup, and that iCloud Backup is not end-to-end encrypted, meaning Apple can access the backup, retrieve the key and then access all those "Messages in iCloud."

"iMessage users may wrongly believe that their communication is private," ESET's Jake Moore has warned, "but with access granted from just with a backup created, it somehow defeats its success in protection."

As Apple acknowledges, "Apple retains the encryption keys in its U.S. data centers. iCloud content, as it exists in the customer's account, may be provided in response to a search warrant issued upon a showing of probably cause, or customer consent."

This is all very timely. Apple came under fire for its plans to add a machine learning iMessage filter client-side (on your iPhone) that would warn minors sending or receiving sexually explicit images. Critical argued it was a potential backdoor. Apple denied this was the case but stalled its plans along with on-device CSAM screening.

This backup vulnerability, though, *is* a backdoor. "With access granted from just a backup created," Moore told me, "it somehow defeats its success in protection."

To understand the iMessage backup vulnerability, you need to think back to the evolution of iCloud and cloud services in general. What started as a means of automated or triggered off-device backups and data storage has become a seamless, always-on platform that drives apps and services in real-time.

In among the syncing iCloud services that keep your calendar and reminders and Safari data in sync across your devices, you have Messages in iCloud—a running backup of all the messages and which all your trusted devices can access.

But you also have the generic iCloud Backup, which primarily stores data from apps on your phone that don't rely on their own cloud services, plus your device settings and home screen layouts. You don't need this—you can run a direct transfer when you change device and most decent third-party apps offer cloud data backups of their own now, which is useful if you lose your device.

If you have Messages in iCloud enabled and also iCloud Backups enabled, then that iMessage encryption key is saved. Disable iCloud Backups and you're fine. Or, if you want to keep an iCloud Backup in place while maintaining fully encrypted messaging, then switch to WhatsApp or (better) Signal.

And the concept of "fully encrypted" messaging leads us to the other serious issue for iMessage, the lack of cross-platform interoperability. Those of you old enough will remember the early days of SMS, when it wasn't possible to message across networks. The current Apple/Google approach to messaging is sadly creating a similar paradox.

With iMessage you can send secure texts, but only to other Apple users; with Google Messages, you can now send secure RCS messages from your Android device, but not to iPhones. Crossing platforms (instead of networks, this time around) will see your messages revert to unsecured SMS, and that is best avoided.

Apple and Google are inadvertently making the case to switch from their own OS-based messengers to cross-platform over-the-tops. In recent months, WhatsApp has fixed its most serious issues—multi-device access and encrypted backups. Meanwhile, Signal continues to offer a more secure alternative that can do all the same.

As the shadow of Pegasus now recedes (Apple hopes), post iOS 14.8 and its welcome (albeit belated) transparency, Apple has serious iMessage questions to address. This backup anomaly needs to be fixed or at least more clearly communicated to users who should have the option to withhold encryption keys from being backed up. I asked Apple about this, but the company does not "comment or speculate" on future plans.

This is becoming a serious issue for Apple. iOS 15 was intended did to bring cool new iMessage features. But all we've talked about in recent months is iMessage security vulnerabilities. Apple needs to recognize that WhatsApp has now caught up and overtaken iMessage on the security front, while offering cross-platform and other secure features such as disappearing messages and view-once media.

With all this in mind, I can no longer recommend iMessage as a daily messenger for Apple users, and I suggest they opt for WhatsApp or Signal instead.

5.2.2. Article 2: New iPhone WiFi Hack Becomes More Dangerous, Affects all iOS 14 iPhones

Link:
https://www.forbes.com/sites/gordonkelly/2021/07/06/apple-iphone-wifi-security-hack-ios-iphone-upgrade/

New iPhone WiFi Hack Becomes More Dangerous, Affects All iOS 14 iPhones

Jul 6, 2021,07:13 PM EDT
Gordon Kelly

Over the weekend, iPhone owners worldwide were warned about the potentially serious implications of an obscure new iPhone hack. Now new developments strongly suggest those fears are about to come true.

The Increased Damage

The first development came via Carl Shou, the reverse engineer who initially discovered the hack. Shou found that joining WiFi networks with specific symbols in their name (SSID) could disable any iPhone's WiFi until the phone's network settings were reset. Shou has subsequently managed to increase the damage this hack does, with WiFi only being restored from a custom factory reset where the iPhone backup file is manually edited to remove malicious entries.

Fears had already been expressed that this hack - known as a format string flaw - could be amplified. The end game being to use it to inject and execute malicious code onto devices and even whole networks.

The Hidden Threat

The flip side to this escalating threat, was that iPhone owners would have to join a strangely named WiFi network to be hacked. But the second development suggests this may no longer be the case.

Speaking to me, Amichai Shulman, CTO of wireless security specialist AirEye, revealed that "Our research team was able to construct the network name in a way that does not expose the user to the weird characters, making it look like a legitimate, existing network name."

Amichai warns that their research is still ongoing, but if hackers are able to spoof popular WiFi hotspots then iPhone owners would struggle to tell if the hotspot they join is about to nuke their device or plant software which could later infiltrate their home or work network.

"Since the attack traffic is not part of the corporate network, Firewalls, NACs and Secure WLANs do not protect against this type of attack and most traditional network security solutions remain completely oblivious to it," Amichai explains. "Attack traffic can be sent over channels that are not used for corporate network traffic. Consequently, the attack goes undetected by network security solutions and does not leave any trace in the forensics and networking logs."

Amichai says that AirEye's testing indicates MacBooks may also be vulnerable while format string flaws can also be written for Android, Windows and Linux devices. "Airborne attacks are new and an as-yet unaddressed threat vector. Given their stealthy nature we're bound to see more such attacks," he concludes.

More immediately, Apple needs to patch this specific flaw in iPhones and I would expect to see a priority fix released either in iOS 14.7 (which is currently in beta testing) or a dedicated iOS 14.6.1 security update. At which point a new and potentially high stakes game of Whack-a-mole is likely to develop between hackers and big tech companies.

Joining a WiFi network may never be the same again.

5.2.3. Article 3: No, Your iPhone is Not More Secure than Android, Warns Cyber Billionaire

Link:
https://www.forbes.com/sites/zakdoffman/2021/03/16/iphone-12-pro-max-and-iphone-13-not-more-secure-than-google-and-samsung-android-warns-cyber-billionaire/

No, Your iPhone Is Not More Secure Than Android, Warns Cyber Billionaire

Mar 16, 2021,08:30 AM EDT
Zak Doffman

One of the world's leading cybersecurity experts has just warned that the alarming new surge in malicious apps is a much more serious threat to iPhone users than you might think. iPhones, he says, have a surprising security vulnerability.

"We're all wide open," the billionaire founder of Check Point tells me. "And attackers are not missing that." I last talked to Gil Shwed just before the world was struck down by Covid-19. Everything has changed, he tells me now. "The attack surface has greatly expanded. We've seen this huge surge in mobile and malicious apps."

Android's reputation for securing its fragmented ecosystem is not good—the widely held view is that iPhone's are much safer. But you can buy an Android and lock it down fairly easily. Not so with an iPhone. Apple makes its devices harder to attack, but also harder to protect. You are reliant on Apple to do the work for you—and so, for users and companies now under attack, Shwed warns that this has become a serious issue, that the security risks between the two platforms are now "balanced."

Before Covid-19, the world was relatively simple. "If you're easy to attack," Shwed told me then, you will be attacked. "So, just make your network and systems harder to penetrate than those around you." But now, he says, "with half the companies in the world, there's evidence that [at least one] employee has a malicious application and therefore may be susceptible to attack from the outside."

A year ago, we talked nation state cyber, the threats from China, Russia and Iran. Now, despite Solar Winds, to say nothing of the Microsoft Exchange nightmare that hit just after our meeting, the security implications of the world's companies throwing open their systems to newly remote workforces are even more front of mind.

Everything is mobile, remote, and we're still *not* ready for that. "All our systems are now accessible by external entities—first and foremost, our employees, but then our suppliers, our vendors, they all do remote monitoring, remote work on our systems. The hackers didn't lose sight of that and they are taking advantage of that."

Shwed sells security software—his latest innovation is Harmony, a multi-platform solution to safeguard a whole person, not just a few of that person's specific machines. "The security of the user wasn't the number one [CISO] priority a year ago. Now it is. Because we all realized how that creates a huge vulnerability in our infrastructure. And the hackers are really taking advantage. There is no doubt—we see that every day."

Shwed is fresh from his company's annual flagship CPX 360 event—held virtually this year. "With the sudden shift to remote work," the company said, promoting its event that included Chris Krebs amongst the speakers, "we learned the value of being able to adapt. Your cyber security strategies must also change."

And this is Shwed's theme as we speak now. Unsurprisingly, the man who sells security software wants to sell more security software. But he's definitely got a point. Most of us know we should run software to protect our PCs and even our Macs. A well-run organization wouldn't enable its myriad employee laptops to access its core systems without any protection. But with our phones, it's all very different.

"On the PC side, that awareness level is quite high," Shwed says. "On the mobile it's still very low. What we are trying now to do with Harmony is actually address that by saying it's all going to be together. So it's not going to be the decision of saying our focus is now on the PC, because that's what we know, or because that's the highest priority. But rather saying your focus should be on the users."

Today's mobile security situation is a disaster. How many of the smartphones accessing core enterprise systems don't currently carry security software? "95% of them don't," Shewd says, "or even 99% don't." And this is his key takeaway. There's an urgent game of CISO catch-up to be played. If you want to use your smartphone to access enterprise systems, then you need to be secure. "And it's very simple. I access the company portal, it tells me: 'If you want to keep using that, download this software from here. Click here and use it.' And that's very simple."

Back to those numbers. Maybe as few as 1% of cell phones carry security software, but 46% of companies found themselves infected by a malicious app brought into their ecosystem on an employee's phone. The mobile threat vector has become much more critical in recent years. And that risk was catapulted by coronavirus.

And Shwed raises another parallel with Covid-19. "Looking at what we call a cyber pandemic is an important element," he tells me. "We need to understand that cyber attacks can behave like a pandemic and do behave like pandemic, except that they are much, much faster than a biological pandemic. So, we need the tools to prevent them and stop them and these tools needs to be super-fast... AI based autonomous threat prevention that will see the attacks and stop them. Not see the attacks and do nothing or wait until next week, because it's now Friday evening and nobody's in. The system should move, it should run by itself because the hackers are working 24/7."

Check Point's 2021 security report warns that this mobile threat is now coming at us from every angle—banking trojans, mobile remote access trojans, deployed by both nation state threat actors and criminal enterprises, arms-length espionage by state intel agencies on overseas targets. All enabled by social engineering, our relative lack of security awareness when it comes to our phones, and no security software.

"Companies need to take very seriously the need to build a unified cyber architecture," Shwed warns, "to consolidate as much as possible. The fact that you have one place that detect the virus or the pandemic in one side of the enterprise, but on the other side of the enterprise, nobody knows what to do with it, is not helpful enough... You see something bad, you stop it. If the damage remains outside, great. If there's damage inside—let's take SolarWinds—it's a typical pandemic. You found the victim, you found the patient, in the Coronavirus world, you found somebody infected. Now quarantine them and the damage is going to be very, very limited. You don't quarantine them, within a few minutes or few hours, your entire enterprise is not working.”

Check Point’s 2020 recap is bleak. “More than 400 weaknesses in a Qualcomm chip that affects a large portion of the entire mobile market... Weak points in Android phone hardware that can be exploited to result in a full takeover... Instagram reported to have an RCE zero-click vulnerability in its JPEG decoder. Apple’s ‘sign in’ system vulnerability can allow remote attackers to bypass authentication and take over targeted accounts. Additional vulnerabilities in WhatsApp, Facebook, and more.”

There have been many more mobile vulnerabilities targeting and exploiting Android devices than iPhones in the last year—unsurprisingly; iPhones are much more secure, right? No, Shwed, tells me. “I think the risks are for both. There are zero-day attacks and there are malware on both platforms. I think it's actually very balanced.”

His point here is interesting. If you use an Android, then the onus is on you, the user, to secure your device. There are plenty of security platforms available from leading vendors. And they can wrapper the device. If you’re an enterprise user, then your company can do the same for you. This overcomes the issues with Android’s fragmented ecosystem, the lag in deploying security patches and general updates, the relative lack of security on the Play Store compared to Apple’s equivalent.

But with iPhone, the onus is on Apple to keep you safe. And two urgent OS updates in the last few weeks, with some admission of exploits being caught in the wild, clearly shows that the threat is real. “iPhone is a much more closed system,” Shwed says, “and Apple regulates much more what's on the platform, which theoretically or practically make it a little bit more secure. On the other hand, there is also limitation about what security software can do an iOS. So the balance may be the same.”

The extent and severity of those risks are *not* balanced, though. “With Android, it's much easier to develop software, to use software, and that software can be more malicious than on iOS. But at the same time, on Android, you can build much better security software because the same openness exists also towards security systems.”

All of which presents a dilemma for CISO’s handling the new normal, hybrid workforce, which will prevent reverting to walled garden, no external access, enterprise solutions anytime soon. “In the past, you can work remotely—in the past, it was fun to say that and we did it small part of the time. Today it's 100% of the time.”

For Shwed, this means another new normal—no security software on your phone, no access to your company systems. “It's not very difficult,” he says. “In Check Point, everybody using your own phone, you're doing whatever you want. But once you want to access the corporate email or the corporate systems, it checks that you have our threat prevention software on your mobile phone. If you don't have it, you can't access the system. That's very simple. Everybody installed that software. And if they don't, they can't access the system. And they don't risk it.”

The risk of a cyber pandemic is real—you'll see ever more warnings over the coming months. What we've seen recently with expansive attacks, allied to a still fragmented workforce and new supply chains has left huge vulnerabilities.

The need for cybersecurity "is now bigger than ever,' Shwed warns. "That's clearly something that we need to deal with... Before, security people were saying, 'you can't come in because it's unsafe.' Today, we're all forced to say everything is open because that's the only way we can work. So I think that the task that we have for next year, and then beyond that, is not to close these doors, but to secure them."

Indeed. But with just 1% of phones secured and mobile malware surging at an unprecedented rate, that's significantly easier said than done.

5.2.4. Article 4: Apple researching battery swell detection with internal sensors on iPhone

Link:
https://appleinsider.com/articles/21/03/11/apple-researching-battery-swell-detection-with-internal-sensors-on-iphone

Apple researching battery swell detection with internal sensors on iPhone

Mar 11, 2021
Wesley Hilliard

Apple is researching how to use new sensing methods to detect the early signs of a swelling battery, and how to not just tell the user that it's happening, but how to prevent it.

Apple filed two patents pertaining to battery technology that will reduce device size and allow the device to detect battery swelling. These technologies go hand-in-hand for creating ever-smaller devices while keeping them safe for the user.

Both of these patents are important for Apple's goal of achieving smaller devices that users carry or wear on a daily basis. For example, the battery casing was too small on the ill-fated Samsung Galaxy Note 7, which resulted in the eventual expansion and violent destruction of these devices. If Apple seeks to reduce the battery casing size, it also needs to account for possible battery swelling.

Even Apple's iPhone is not immune to battery expansion since it is a side-effect of the battery chemistry in lithium-ion. Detecting and preventing battery expansion, or at least warning users of an exhausted battery, would go a long way for user safety.

Small Metal Battery Casing

The first patent describes a system for positioning components internally surrounding a battery. This new system will allow for larger batteries in the device enclosure without damaging components.

Currently, batteries must be physically separated from the rest of the components since the external battery container may contain an electrical charge. This results in wasted space and a smaller battery.

The patent says that using a new system in which a metal shell is placed around the battery housing, then grounded, would allow for components to be packed closer to the battery. In some cases, components could come into contact with the metal shell and not be damaged.

The drawing represents the old battery container (figure 1) and the patent's new design (figure 2). The old battery had wasted space to separate components represented by the dotted line, the new battery's external casing can more safely touch components.

The patent lists seventeen inventors, several of which were previously credited with working on Apple WatchApple Watch technology. It was originally filed on May 26, 2020 and came to the attention of *AppleInsider* on March 11, 2021.

The second related patent describes multiple solutions to detecting and mitigating battery expansion. The need to determine if a battery is expanding is present regardless of the device, be it a car or smartphone.

Once an expansion has been detected a processor coupled to the sensor would determine how to slow expansion or prevent it. This would be accomplished by adjusting charge or discharge of the battery depending on the cause of expansion.

One detection method would use a capacitor to determine the physical distance between the battery case and the device case. If this distance shrinks, the capacitance will change and alert the battery processor.

Distance could be measured between several different surfaces like the internal and external battery casing using capacitance. The patent also describes using several different sensors that determine strain, acoustic resonance, photo interruption, contact, or pressure.

Regardless of the sensor used any change in the physical boundaries of the battery would result in triggering a sensor. This in turn would tell the battery processor to alter charge or discharge to extend battery life and mitigate swelling.

The patent lists twelve inventors and was originally filed on November 16, 2020, and came to the attention of *AppleInsider* on March 11, 2021.

Apple files numerous patent applications on a weekly basis. While the existence of a patent filing indicates areas of interest for Apple's research and development efforts, they do not guarantee the concepts will appear in a future product or service.

AppleInsider has affiliate partnerships and may earn commission on products purchased through affiliate links. These partnerships do not influence our editorial content.