CIRCL Technical Report on

SECURITY OF iOS BASED DEVICES

Executive Summary

The integration of iOS[1] based devices in a governmental environment introduces several risks that were discovered during the research done for this report. It is essential to understand that iOS based devices are powerful links to internal and probably sensitive information of the organisation. Most of these additional risks can be reduced by adequate policies, procedures, proper configuration, awareness of the users and the implementation of additional security measures, **but the overall risk level increases compared to a situation without iOS based devices.**

Introduction

The introduction of iOS based smart devices like Apple's iPhone or iPad seems inevitable[2] for ministries and businesses in general. One reason for this might be the market penetration in the consumer market.

Assuming that iOS based smart devices like Apple's iPhone or iPad are to be run in professional or governmental environments **special considerations regarding information security have to be made to protect the assets of the** organisation, especially sensitive information being accessed by the device (locally or remotely) needs careful attention.

This report is based on a collection of security related papers covering mobile phones, smart devices in general and particularly iOS based devices, as well as CIRCL conducted tests. It highlights **risks** and gives **recommendations** on how to increase security in an organisational environment.

Limitations

The report is addressing the current situation (iOS version 4.2.1 on iPhone and iPad). Changes to the design of iOS, the discovery of vulnerabilities in the operating system as well as the usage of other Apple or 3rd party software or hardware can modify the risk exposure. These aspects will be monitored and kept up to date in the technical annex (annex B) of this report.

[1] APPLES' IOS MOBILE OPERATION SYSTEM USED IN THE IPAD AND IPHONE DEVICES

[2] LATEST REPORT FROM DELOITTE ABOUT THE 10 EMERGING TRENDS IN ICT

Report

iOS devices integrate several security aspects quite well, for instance automated backup, memory encryption (since iPhone 3GS), making the remote wipe more effective, and the way App store applications are reviewed.

On the other hand, there is a multitude of risks of which many are generic or at least not limited to the iOS platform, others are specific to it. These are briefly discussed here. A more detailed list of the risks and possible mitigation scenarios are given in annex B.

General smart devices security

Lost, stolen or decommissioned devices store confidential information or have low access security barriers granting access to sensitive information and/or internal networks.

General Phone security

The GSM encryption (A5 GSM Encryption) is weak and SMS should not be considered for secure information exchange. Remote access to the voicemail should be secured by a strong password or strong PIN code. Data roaming costs are to be considered.

Network security

Accidentally using rogue access points, set up in a malicious intent, might reveal login credentials to attackers if an insecure transport layer[3] is used. Bluetooth might give access to the device if configured badly.

Cloud computing security (data stored and processed on 3rd party servers on the internet)

Information security does not solely rely on the quality of the software used on the device, but also on data storage, the transport- and authentication-security as well as the trustworthiness of the cloud service used.

Software installation security

Accidental or deliberate data leakage or theft through the installation of third party applications is possible.

Software restriction circumvention risks

Jail-breaking the device (removing vendors' restrictions) opens the device for remote access (ssh) with default user name and password and the user might install un-reviewed and potentially malicious software.

[3] OMISSION OF SSL/TLS ENCRYPTION

Malware risks

The infection with dialerware (cost producing malicious software calling premium numbers or sending SMS to such), phishing and financial malware is possible, partially even through the vendors' App store as it was proven by researchers[4].

All these aspects need to be considered and mitigated through behavior or information security policies, before dealing with sensitive information on the smart devices (inevitable in business or governmental use cases).

Conclusion

Almost all of the risks can be reduced by the proposed mitigation methods detailed in annex B. One of the main issues you have no control over, is the use of Apple's App Store for 3rd party Application installation. Even if these applications have to follow strict development guidelines, researchers have shown that they can abuse the system and implement malicious behaviour.

The complexity of such a system as well as the inter-dependencies between the different security methods should be kept in mind. An example is the memory encryption. The encryption is implemented in software rather than a TPM[5] hardware module, hence the key can be extracted. Is the device not secured by good pass-codes or if the pass-code is stolen, the device memory can be dumped and read.

It is vital that the right policies, the necessary procedures and the correct configurations are put in place. Adequate training to all the users is a must do too. Additional security measures might be necessary depending on the use case of the iOS smart devices and the sensibility of the data handled.

[4] IPHONE PRIVACY - HTTP://SERIOT.CH/RESOURCES/TALKS_PAPERS/IPHONEPRIVACY.PDF

[5] TRUSTED PLATFORM MODULE

ANNEXES

Annex A - References

- http://www.itnation.eu/forum/topics/deloitte-identifie-dix
- http://developer.apple.com/appstore/resources/approval/guidelines.html (authentication required), for a copy see: http://images.worldofapple.com/appstoreguidelines_9910.pdf
- http://www.enisa.europa.eu/media/press-releases/security-is-there-an-app-for-that-eu2019s-cyber-security-agency-highlights-risks-opportunities-of-smartphones
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/MobilEndgeraete/mobile_endgeraete_pdf.pdf?__blob=publicationFile
- http://www.contextis.co.uk/resources/white-papers/smartphones/Context-Smartphone-White_Paper.pdf
- https://www.bsi.bund.de/cae/servlet/contentblob/487520/publicationFile/30774/oefmobil_pdf.pdf
- http://www.funkyspacemonkey.com/spyphone-ni
- http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf
- Enterprise iPhone and iPad Administrators Guide, Charles Edge, Apress 2010

Annex B - Technical details and recommendations

iOS smart device advantages

- Backup integrated
- Memory encryption since iPhone 3GS - Note: Encryption is not done in hardware and key and can be retrieved from the device
- Remote wipe integrated - Note: since iPhone 3GS within seconds, on older models within hours
- Applications are reviewed based on strict guidelines

Smart devices security considerations

- General Smartphone considerations
    - Lost, stolen or decommissioned devices storing sensitive information or with low access security barrier granting access to sensitive information and/or internal networks
- General Phone considerations
    - Weak GSM encryption (A5 GSM Encryption)
    - SMS is not a secure information exchange method
    - Cost trap Data roaming
    - Remote access to Voicemail
    - Network
    - Risk of using rogue access points and revealing credentials to various network services to the attacker when using insecure transport layer (e.g. plain HTTP)
    - Risk of insecure Bluetooth configuration
    - Cloud computing
    - Information security not only managed on the device, but also influenced by:
        - Data storage security in "the cloud"
        - Transmission security to "the cloud"
        - Authentication security for "the cloud"
    - Software installation capabilities:
        - Accidental data leakage through third party applications (e.g. social network applications revealing the current geo-location information
        - Deliberate data leakage/theft by malicious third party applications
        - Cost producing malicious software (calling or sending SMS to premium numbers)

- Software restriction removal risks (Jail-broken devices)
    - Comes with remote access enabled with default user/pass
    - Has access to untested software
- Other malware considerations
    - Phishing
    - Financial malware
    - Smart devices are used for dual authentication, e.g. via SMS
    - A lot of specific banking software is available with weak security implementation

Recommendations for the consumer market

- Physical security
    - In case of loss/theft:
        - Get the device remotely wiped immediately
        - Get the SIM card blocked
        - Don't leave the phone unattended
        - Don't lend the phone to anybody you do not trust fully
    - Device access security
        - Use a PIN to unlock the SIM
        - Use at least a numerical code, better an alphanumerical pass-code to unlock device
        - Make sure shoulder surfers cannot watch you entering the codes
    - Remote access
        - Only enable network interfaces you need (e.g. turn off Bluetooth or WLAN if not used)
    - Software security
        - Install updates
        - Do not jailbreak
        - Backup frequently
    - Disposal/Selling considerations
        - Securely wipe the device before selling/dumping it

Recommendations for the organisation

- Strict usage of VPN and/or usage of transport layer security
- Do not allow/configure applications using clear text transmission of data or authentication process
- Policies for loss, theft
    - Loss/theft should be reported immediately and 24/7 staff should be granted the power to remotely wipe device
    - Policies for lifecycle, decommission and media sanitization
    - Track device from start to end-of-life by serial number/IMEI
    - Only dispose/re-assign device after complete secure wipe
- Policy/Configuration for data roaming
    - Consider the necessity of data roaming and turn-off by policy if not needed
- Policy/Configuration for reasonable strong pass-codes
    - Policy/Configuration for automated device locking after reasonable time
    - Reasonable time is considered around 3 minutes
- Policy/Configuration for storing data (e.g. emails) on server only (no local copy)
    - Limit time of cached mails
- Policy for iOS software updates
    - To clarify how to automate this
- Policy for private smart devices on corporate network or accessing corporate resources
    - Do not allow private/unmanaged smart devices on the network
- Policy for physical security (see 'Considerations for the private user')
- Policy for Modifications and Software installation (including Jail-breaking)
- Policy/Configuration for allowed App Store applications
- Have the employee report any suspected modification of the phone (wiretapping)
- Do not allow and periodically check for Jail-broken devices
- Policy for necessary network interfaces and remote access
    - Turn off Bluetooth for instance
- Usage-Policy
    - Beware of shoulder surfing/ - espionage by photographing the display while working on the road