
# Privacy in Mobile Apps. Enterprise Opportunities

*YURY CHEMERKIN*

*DefCamp 2014*

# [ YURY CHEMERKIN ]

- MULTISKILLED  SECURITY RESEARCHER
- Work for Advanced Monitoring
- EXPERIENCED IN :
  - *REVERSE ENGINEERING & AV, DEVELOPMENT (IN THE PAST)*
  - MOBILE SECURITY, & CLOUD SECURITY
  - IAM, COMPLIANCE, FORENSICS
  - PARTICIPATION & SPEAKING AT MANY CONFERENCES

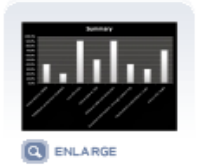


# AGENDA

- Wild Animals :: < Facts about insecurity of Mobile Apps >
- Wild Tools :: < Forensics Tools, Data/Backup Tools >
- Wild Security Concepts :: < Data Protection Concepts, Best Practices >
- Wild Environment :: < OS: iOS, Android , BlackBerry, WinRT >
- State of Facts :: < Application Security Examination >
- Wild Security Solutions :: < OS Security, EMM Solutions >
- Recommendations :: < MAM, Development Advices, etc >
- Other Salvation Ideas :: < BlackPhone >

# 40% of iOS Banking Apps Leak Sensitive Data Through System Logs

SHARE: 8+1 10 Like Share 51 Tweet 93 Adjust text size:




**IOActive researcher Ariel Sanchez has analyzed a total of 40 mobile banking applications for iOS devices to see if they're secure or not. The apps belong to the 60 most important banks from all over the world.**

The expert has found that 40% of the tested apps are vulnerable to Man-in-the-Middle (MitM) attacks because they don't validate the authenticity of SSL certificates.

Around 20% of them have the Position Independent Executable (PIE) and Stack Smashing Protection disabled, which makes them susceptible to memory corruption attacks.

90% of them don't have jailbreak detection. The same percentage contain a number of non-SSL links when surfing the app, allowing cybercriminals to intercept traffic and inject arbitrary code for phishing purposes.

Cybercriminals can also abuse insecure UIWebView implementations in over half of the tested apps to inject JavaScript.

When it comes to two-factor authentication, which is a great mechanism to protect against impersonation attacks, the h a system.

hrough log files, such as crash reports. The data leaked

# App Makers May Be Exposing Your Sensitive Data to Hackers

By Megan Geuss, PCWorld Aug 8, 2011 6:00 PM

Some popular apps store sensitive data such as user names and passwords and credit card information in plain text on your phone's memory, making the data an easy target for hackers. A Chicago-based mobile forensics company called viaForensics recently found as much after completing an audit of dozens of the most popular apps on both iOS and Android platforms.

Some of the biggest-name apps--such as Android Mail for Exchange and Hotmail, Foursquare, and Groupon--stored the user's passcode and portions of the information that the user accessed through the app, in clear text on the phone's memory for versions of the apps released around the beginning of 2011.

# Android Coupons App Leaks Your Personal Information To Everyone

Jan 06, 2014 2:24 PM EST | 0 Comments

By Max Eddy

We've looked at several apps for Android that gather, to paraphrase John Hodgman, more information than they require. We've also looked at severa apps that handle that information badly, allowing it to be easily extracted or intercepted. This week, Appthority shows us an app that does both, and also transmits your information to any other server it contacts.

# Banks Rush to Fix Security Flaws in Wireless

Email Print Comments A A

By SPENCER E. ANTE

Updated Nov. 5, 2010 12:01 a.m. ET

A number of top financial companies and banks such as Wells Fargo WFC -0.12% & Co., Bank of America Corp. BAC +1.06% and USAA are rushing out updates to fix security flaws in wireless banking applications that could allow a computer criminal to obtain sensitive data like usernames, passwords and financial information.

**Audio**

- **Listen:** You're probably not looking to have your banking information stolen but, unfortunately, there are apps that do that.

The central problem is that the apps, which run on Apple Inc. AAPL +0.19% 's iPhone and Android-based devices from Google Inc., GOOG -0.64% are storing a user's information in the memory of a cellphone, a basic lapse that the security researcher who found the flaws said could allow a cybercriminal to access a person's financial accounts.


# Executives Confirm Starbucks App Stores Passwords in Plain Text

Like 0 Tweet 3 8+1 0

*WRITTEN BY Casey Houser*
*January 18, 2014*
*Tags: iOS, starbucks*

Starbucks executives confirmed Tuesday that their company's mobile app stores various types of sensitive data in plain text, according to a recent analysis of the issue posted by Computerworld. Specifically, the Starbucks app retains username, password, and geolocation data on users' mobile phones, leaving them vulnerable.

# Instagram 3.1.2 For iOS, Plaintext Media Information Disclosure Security Issue

- Vendor: Instagram
- Product: Instagram 3.1.2
- Tested on: iPhone 4 (iOS 6.0)
- Vendor notification: Nov 11, 2012.
- Risk level: Low
- Link: Secunia Advisory SA51270

Instagram 3.1.2 for iPhone (released on Oct 23, 2012) is vulnerable to partial eavesdropping and man in the middle attacks that could lead an evil user to delete photos and download private media without the victim's

# Mobile iOS banking apps are miserably insecure leaky messes

By Darlene Storm
January 13, 2014 12:15 PM EST 2 Comments

Share 24 +1 Like 121 More

Dear iPhone/iPad device owners, do you use mobile banking apps? If so, then you might like to know that most of the iOS mobile banking apps for the top 60 leading banks are miserably insecure; in fact, most are leaky messes that leave users vulnerable and at risk of attack.

IOActive Labs researcher Ariel Sanchez tested 40 mobile banking apps from the "top 60 most influential banks in the world." Initially, Sanchez was skeptical about finding flaws in iOS bank
the banks failed to implement
notified of vulnerabilities.

## Vulnerability Summary for CVE-2014-0647

**Original release date:** 01/27/2014
**Last revised:** 02/24/2014
**Source:** US-CERT/NIST

### Overview

The Starbucks 2.6.1 application for iOS stores sensitive information in plaintext in th
(/Library/Caches/com.crashlytics.data/com.starbucks.mystarbucks/session.clslog), v
that reads session.clslog.

### Impact

**CVSS Severity (version 2.0):**

**CVSS v2 Base Score:** 2.1 (LOW) (AV:L/AC:L/AU:N/C:P/I:N/A:N) (legend)

**Impact Subscore:** 2.9

**Exploitability Subscore:** 3.9

**CVSS Version 2 Metrics:**

**Access Vector:** Locally exploitable

**Access Complexity:** Low

**Authentication:** Not required to exploit

**Impact Type:** Allows unauthorized disclosure of information

# Want to Protect Your Emails? Don't Use these 11 Android and iPhone Email Apps

Comment / Shares / Tweets / Stumble / Email More+

*Last Updated Feb 2, 2011 10:32 AM EST*

Want your email to be secure? Of course. But if you lose your smartphone or tablet, you might be out of luck, if it runs **Google's**

Safari

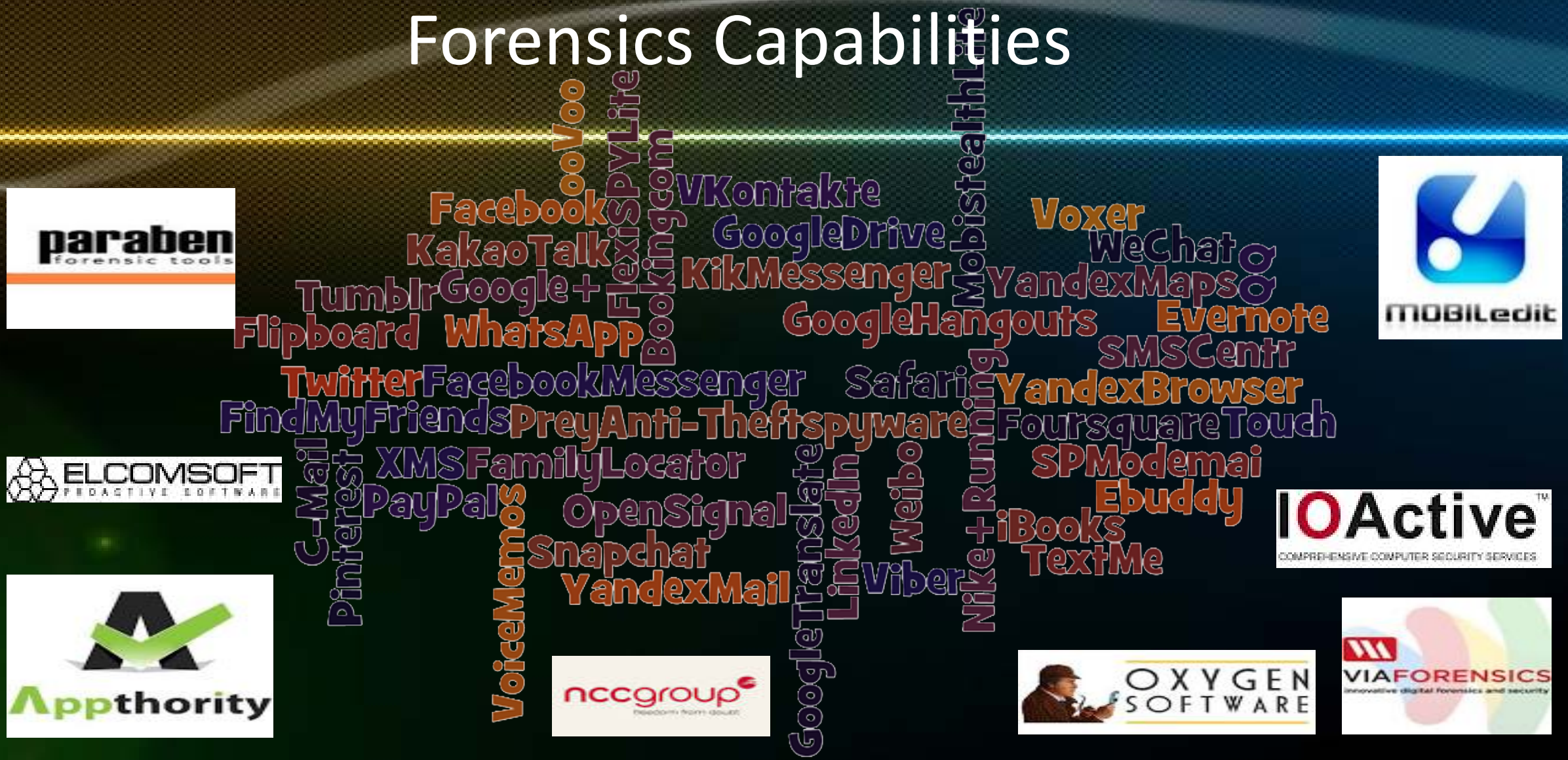
# Mobile Threat Monday: Tax Time Android Threats

Apr 14, 2014 3:03 PM EST | 0 Comments
By Max Eddy

Tomorrow is the last day to file your taxes in the U.S. without an extension, and many of you probably forgot. I know, I've been there. Fortunately, there are lots of handy electronic helpers here to make paying up to Uncle Sam a little easier. Unfortunately, not all of them are equally secure. This week, Appthority examines three tax and finance apps that, while not malicious, have security issues that might make you think twice.

**TaxSlayer GO**

# Forensics Capabilities



# DATA PROTECTION CONCEPTS

- Data-at-Rest (DAR) protection
- Data-in-Use (DIU) protection
- Data-in-Transit (DIT) protection
- Data-in-motion (DIM) protection (~DIT)
- Data-in-action (DIA) protection (~DIU)
- App Disablement (~ DIU & DAR)
- Geo-fence (~ DIT & DIM)

# Data-at-Rest (DAR): iOS

- SQLite storage
  - any type of data
- Binary cookies
  - depends, usually, credentials, tokens
- Keyboard Cache
  - auto correction, word list  counts 600
- Snapshot Storage
  - any preview info, like email from Banks
- File Cache
  - attachments, files from clouds, etc.
- Error logs
  - any data, even credentials
- iCloud
  - all data backup to cloud, even credentials

# Data-at-Rest (DAR): Android

- Where & What stores :: /data/data/<package>/…
  - App
    - analytics, dump, misc
  - Cache
    - up/downloaded files
  - Databases
    - history, chat, bank info
  - Files
    - attachments, crypto-keys
  - Shared_prefs
    - credentials, token, history

- How does it store
  - Shared preferences (lightweight XML format)
  - Internal storage (/data/data/ + shared docs & media)
  - External storage (cache, debug, db, maps)
  - SQLite (DB, discussed earlier)
  - Network (logs/event, datestamp, credentials)

# Data-at-Rest (DAR): BlackBerry

- BlackBerry Backup
  - What :: app, app data, app config, all documents, etc.
  - How :: ElcomSoft, any other that works with BB backup
- Shared folders
  - What :: docs, media, backup with credentials may happen
  - How :: live access, spyware, rarely encrypted
- Remotely accessed data
  - What :: device entirely plus SD-Card
  - How :: BB Link should authorized PC before gaining access
- The rest data protected except you got an access to backup or find a way how to root/jailbreak OS ☺
- Android application data files
  - What :: cached files, any other like Android App
  - Where :: Device/misc/android/Android/data)
  - How :: like a shared folders or remote access
- Misc tracks
  - Device/Misc
    - What :: Misc files, backup like whatsapp,
    - How:: like a shared folders or remote access
  - Device/Android except android data
    - What :: any data Android and Android apps usually store on SD card
  - How :: like a shared folders or remote access
  - Not all android app data found on these paths (!)

# Data-at-Rest (DAR): WinRT

- <Local>
  - Data that exists on the current device and is backed up in the cloud.
- <Roaming>
  - Data that exists on all devices on which the user has installed the app.
- <Temporary>
  - Data that could be removed by the system at any time.
- <Localcache>
  - Persistent data that exists only on the current device.
  - If your app is removed, these data stores are deleted.

# Data-in-Use (DIU): All OS

- Data-in-Use (DIU)
  - Partial vendor code obfuscation
  - Custom tools for a code obfuscation (WinRT)
  - Once time all data appear in plaintext (user can't read encrypted text ☺)
- Data-in-action (DIA)
  - Clipboard & Screenshot activities are under restriction while phone is enabled for an enterprise policy
  - Clipboard & Screenshot activities are usually disabled for all applications




# Data-at-Transit/Motion (DIT/DIM): All OS

- Data-in-Transit (DIT)
  - HTTP/HTTPS
  - Post/Get, Rest API
  - JSON, Soap, XML
  - Gzip, Base64
  - WebViews
  - Custom connections schemes & custom P2P
- Data-in-motion (DIM)
  - Networks encryption wrappers
  - Networks policy wrappers
  - App-level VPNs
  - Other corporate stuff




# Geo-fence/App Disablement: All OS

- Enterprise app disablement depends on custom EMM capabilities
- **iOS**
  - Restrict geo-location per each app or service
  - There is no option “All-in-one” to restrict geo-location for all apps/services
- **BlackBerry**
  - Restrict geo-location per each app or service
  - “All-in-one” to restrict geo-location for all apps/services
  - Can’t restrict geo-location for Android apps (*probably, can do it in future*)
- **Android**
  - Can’t manage permissions per app separately except Firefox OS
  - There is no option “All-in-one” to restrict geo-location for all apps/services
- **WinRT**
  - Restrict geo-location per each app
  - “Flight mode” is kind of “All-in-one” option to block any connection

# Examination :: What

# Examination :: How


**40-40-20**

# Results :: Notes of Research Limits

- Researched cross-platform apps updated prior one month before HH event, but may
  - not available to download or pretend to the latest version due to countries restrictions
  - not available for all platforms
  - not refer to analytics sdk like flurry or similar
- Any app data presented here
  - stored in shared folders too if it is possible and need for export feature (like BlackBerry)
  - stored in memory as is at least one time
    - You can do anything in run-time, even repack an application & install on the device
  - stored locally in case of Android-app running on any Android-based OS
  - Stored in keychain on iOS is not additionally encrypted
  - transferred via https or http without any additional protection
    - may be under the simple MITM attack via ProxyTools except
      - native services of iOS, BlackBerry, Google & Windows Markets
      - most of all native BlackBerry Apps & apps like Yandex Disk, Dropbox, Evernote
  - stored in snapshots folders on iOS if user swiped down his app
    - by default developers never turn off that feature even for bank apps
    - apps that have inactive this feature are highlighted additionally

# [ Results :: 4talk ]


- Phone Number
- Login (phone@4talk.im)
- Sms code
- Https Auth (login, pass)
- Device Model
- Device Type
- Message
  - From/to ID
  - Time
  - Body
  - Device-type + OS
- Avatars
- Addressbook (Name,Phone,Email)
- 4talk vCards
- Jabber client
- Log-file stored locally contains all network sessions (see above)

# [ Results :: Whatsapp ]

- Account
  - country code, phone number
  - Pw.dat – seems encrypted but not a token definitely
  - login / tokens Facebook wasn’t revealed
  - Avatars :: phone+@s.whatsapp.net.j (jfif)
- Address book
  - No records of address book were revealed…
  - Check log-file and find these records (!)
- Messages
  - Date & Time
  - content of message
  - ID :: phone@s.whatsapp.net
  - Attachments (as is)

# [ Results :: Viber ]

- Account
  - country code, phone number
  - Device Hardware Key
  - login / tokens of Twitter & Facebook
  - Calls history
  - Name + internal ID
  - Duration + date and time
- Address book
  - Quantity of contacts / viber-contacts
  - Full name / Email / phone numbers
- Messages
  - Conversations
    - Quantity of messages & participants per conversations
    - Additional participant info (full name, phone)
  - Messages
    - Date & Time
    - content of message
    - ID
    - Attachments & Preview (as is)
    - VoiceMessages
  - Media
    - Snapshots (iOS only)
    - Snapshot of active chat
  - Stored locally
    - Common paths to stored data refer to know environments …
    - .. like %Documents%, %AppFolder%

# [ Results :: Facebook & FB Messenger ]

- Media
  - User images/avatar (first of all, of those who're on messenger/chat)
  - Snapshot of app screen (iOS only)
  - Pic/avatar URL,
  - Image cache .jfif
- Conversation
  - Thread ID, Name , Date & Time
  - Quantity of Messages
  - Message / body
  - ID of sender/recipient
  - Status :: Unread/archived/can reply
- Account
  - Tokens, incl. private
  - Lot of configs
  - Numeric ID of account (100001827345335.plist)
- Address book / Synchronized
  - Full Name, Email , Phone number
- Users
  - User ID, User Name , User NickName
  - Has a mobile messenger? Is a Friend ?
  - Email
- FB Messenger
  - configs
  - User Phone Number
  - Friend avatars
- Credentials found in traffic
  - Username & password,
  - For rest interaction token only

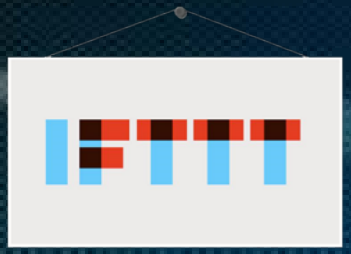
# [ Results :: Connect ]

- Device Info
  - Device ID, Version
  - Carrier
  - System name (OS), Platform, Model
  - Orientation
- User/Credentials
  - Connect username
  - FB token incl. private token
  - FB permissions (groups, photo, geo, friend_checkins, email, basic info, friend all info, birthday)
  - email
- Credentials
  - Nothing revealed
- Captures in traffic
  - Fb token from iOS
  - Lot of analytics trackers (device root/jail type, device environment, network+carrier type, etc.)
  - Has a testflightapp analytics too
  - Raw data (maps, event, history, etc.)

# [ Results :: Cloack ]

- Media
  - Snapshots
  - PNG map shots of friends
- User/Credentials found locally
  - FB token
  - FB permissions (public profile, user friends, friend photos, stream, geo, friend_checkins, email, basic info, friend all info, birthday)
- Credentials found in traffic
  - Fb token grabbed from iOS
  - 4squre token grabbed from 4squre app
  - Login, pass, tokens from Twitter, because Cloack performs ‘login’ action via Safari
  - Login, pass, tokens from Instagram, because Cloack performs ‘login’ action via Safari

# [ Results :: IFTTT ]




- Receipts (local & traffic)
  - What to do (create link in Evernote Notebook, post to Facebook, etc.)
  - Numeric ID & Text Name of receipts
  - Source link , Headline of ‘news’
  - Location notification for iOS if you leave/enter area – postal code, street, city
  - Public ID of social profile URLs
  - Internal ID/Tokens (?) of the storages like Dropbox
- Credentials captured in traffic
  - Username, password, tokens
- Credentials when assigning new services
- Full receipts details belong to the different services like folder in dropbox, etc.

# [ Results :: Vkontakte ]

- Media
  - Snapshots
- Messages time
  - Conversations
  - Attachment Info, URL
- Friends
  - Full Name
  - Profile URL Avatar
  - Birthday
  - Misc tokens (?)
- Credentials
  - Nothing revealed

- Data-in-Transit
  - Uploading attachments in plaintext (all platforms)
  - Sending messages in plaintext (iOS only)
  - Android has a feature ‘allows https connections’ turned off by default
  - iOS doesn’t provide https feature

# [ Results :: Linkedin ]

- Media
  - Snapshots
  - Cached friend avatars
- Notifications
  - Date and time
  - View profile + quantity
  - Invitation request/acceptance
  - Endorsed (who) for skills
  - Full name of actor
- Friends
  - Search request per each contact record from your address book
  - Full Name , company are result of the search
  - Profile Friend URL + avatar URL
  - Level of connection (1st, 2nd, 3rd )
- Connections
  - Full Name, ID, avatar
  - Email, Phone, birthday if available
  - Latest three job positions
  - Job Title
  - Profile Info (Summary, skills ,etc)
- Profile
  - Full name + user ID, Twitter ID
  - Picture URL
  - Job Title
  - Configs
- What captured in traffic
  - Login, password, token
  - Address book
  - Mails, news …
  - ….and everything mentioned above

# [ Results :: 4square/swarm ]

- Media
  - Snapshots
  - PNG map shots of friends & check-ins
  - Uploaded photos via app on check-in event
- User/Credentials
  - Search request info by name/location/etc.
  - Like, Comments + friend username per check-ins
  - Badges + description and who unlocked it
- Credentials captured in traffic
  - Username & password on first registration
  - Password on ‘change password’ event
  - Tokens to access foursquare & swarm
  - Swarm grabbed most data from 4square

# [ Results :: Instagram ]


- Profile Info
  - Friend profile URL + Full Name + Photo
  - Twitter User name
  - FB Permissions – publish stream
  - FB token key & expiration
  - Login name
- Actions
  - Comments & profile name of those who comment photo
  - Cache of uploaded photos plus date & time
  - Stored on Amazon S3 ☺
- Network (in-transit)
  - Profile Name + URL
  - Friends' Name + Url
  - Upload /Download photos
  - Comments
  - Seems everything except credentials
  - Username, password, fb token
  - Address book, tokens
  - Photo & video stream

# [ Results :: Aeroexpress ]

- Account & Credentials  (traffic, locally)
  - Register key (traffic only)
  - User UID (locally only)
  - Device ID (traffic only)
  - Email address = login
  - Password (locally on Android & iOS)
  - Phone Number
- Products (locally & traffic)
  - Tickets number & QR-ticket
  - How to use e-Ticket ☺
  - What time train departs & arrives ☺
- Payment Info  (traffic, locally on Android & iOS)
  - Full Name
  - Card number
  - Expiration Data
  - CVV (only in traffic)
- Many analytics libraries

# [ Results :: App-in-the-Air ]

- Account & Credentials
  - FB Token & numeric username, nickname/login
  - Oauth Secret token
  - FB Permissions
    - Edu / Work history, Basic info, public profile, email,  User geo, friends, about_me,
  - Twitter token/secret/Oauth, NickName/login
- some extra data encoded in base64 (probably flurry libraries) ::
  - jailbroken/rooted, vendor / install id, os info
- Data
  - Flight info (port/gate, airline, flight # per depart / arrival place)
  - Miles per flight
- User Full Name/EmailTrip Info (login, username, email)
  - Delay status (low, moderate, high)
  - Date & time of the latest info per terminal)
- Device Info
  - Device ID, Version, Carrier, System name (OS), Platform, Model

# [ Results :: AnywayAnyday ]

- Credentials
  - Login, Password, token
  - userID, userProfileID, passenger ID
- Loyalty
  - Bonus level
  - Loyalty id & types
- Geo - suggest for looking the nearest airports
- Payment – card number, owner Name, CVV not request to type (cards are locally stored only)
- Orders details
  - OrderID, orderNumber, date of order, status (canceled/captured)
  - Route, depart &arrival dates, price & currency, bonus points
  - ScoreForOrder, payment method, ticket number
  - trip gate, airline, geo location of cities, stopovers,
- Passport
  - Passport number & expiration, document type, gender, Name, nationality, birthdate, age
- Everything found locally and captured in traffic

# [ Results :: British Airways ]


- Account
  - ID is locally stored
  - Password (is on Android, in captured traffic)
- Loyalty (locally & traffic)
  - card number, card & membership expiration
  - Loyalty bonuses
- Device info – OS & version (in captured traffic)
- Customer Info
  - UID, Birthday, preferred email, plus see “Loyalty”
- Recent transaction (locally & traffic)
  - Booking ref, bonus balance per transaction, date
- Tracked Flights Info (iOS)
- Full Name (iOS), Email (iOS)
- Cached images with exif (like NY SkyBridge) if you have stopover there or it’s your arrival/departure city

# [ Results :: Aeroflot ]

- Number user ID (network), Login
- Session IDs (local only)
- Password (local only)
- Password (Network) – salted hash, PBKDF2 alg
- Flight – no info, because I don't use this app last year ☺
- Loyalty ID
- Date of birth
- Phone number
- Passport details
  - Number
  - Expiration
  - Type
  - Bonuses activity history (amount, day, activity info like store, flight – incl. airports codes)
- All PASSPORT INFO (not only travel data)
- Home Address (network & local), even you never type it!
- Work Address (network & local) , even you never type it!
- Company name and job title

# [ Results :: Delta ]

- Login ID,  Password, Name, Birthday, gender, username
- Loyalty
  - ID, Bonus balance, Expiration date
  - Phone, Home address, Email
- Payment
  - Alias name per card
  - Last 4 digit, Payment system (visa, American express)
- Passport data
  - Number, program name, Expiration date
- Flight
  - Absolutely detailed information (traffic)
  - Barcode stored locally in base64

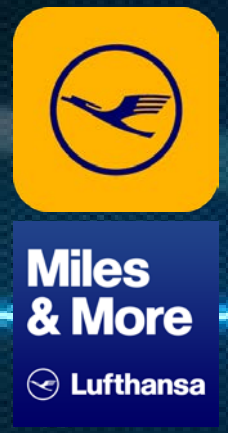
# [ Results :: Booking.com ]

- Account & Credentials
  - Crash analytics UID
  - Email/login info
- Media
  - Cached Hotel Images
  - Upload to Google Image Search
  - Push Search Button
  - Get Hotel Info (!)
- Device OS + Version, SessionID - stored locally plus some extra data encoded in base64 (probably flurry libraries) ::
  - jailbroken/rooted, vendor id, install id, os info
- Device os&version, carrier name, device token, auth token, fb ID, hashed user ID & passw
- Last searches (full details) stored locally and captured in traffic
- UID, phone, Name, email, City, login, password, longitude & latitude, network type, device ID
- No reservation info – not booked yet ☺

# [ Results :: IHG ]


- Reservation (local & network)
  - Reservation ID, Status (confirmed or another one), Check-in & Check-out Time
  - Hotel Code & Hotel Image URL, Address & Phone & Name, Country Code & Country Name, Latitude & longitude
  - Number of Rooms / Adults / Children, Guest Last Name / No info about optional guest (2nd guest, etc.)
- Misc (local)
  - Flurry UID, Platform ID
- Device ID, Version, Carrier, System name (OS), Platform, Model
- Cached (local)
  - Geo data - city, street, country, postal code, lat & lng
  - Room Facilities, Hotel Info (see previous) , Room/Hotel photos (JFIF)
- loyaltyID, loyalty balance, phone number, home address, Name, email, Room preferences,
- last 4 card digits, payment system (visa), encrypted card number & exp.date
- Encryption key is a kind of token (local & network),
- Login & password are captured in traffic

# [ Results :: Lufthansa ]




- Lufthansa
  - Account
    - ID ,bonus card number, password stored in plaintext is not revealed
    - Session ID, secret token & expiration date, encrypted login & password (local & network)
  - Information
    - Date of birth
    - Passport details
  - History (airlines, city, flight number only)
- Miles & more
  - ID M&M inbox email stored in .PDF locally & capture as html in traffic
  - Customer , Home Address, birthday, card #, (both, locally & traffic)
  - Name, award miles, activity history (see Lufthansa) - (both, locally & traffic)
  - M&M number and pin captured in traffic

# [ Results :: Yandex Disk ]


- Locally
  - Cached Files
  - Login ID
- Network
  - Warn on simple MITM attack like a proxy tools that decrypt ssl
  - Flurry & Yandex analytics (not yet examined)
  - Client ID, Secret, password, token, Name, uid
  - storage quota, used size, available size, avatar

# [ Results :: Dropbox ]

- Logs
  - iOS version as a log-file-name
  - Settings like upload_over_cell or geofence_state
  - User_id (numeric)
  - Perms like “permission.photos.granted”
  - Extension
  - Connection time – WiFi, Cellular
  - Size
  - Download info (started, finished, failures)
  - Device ID
  - Nothing captured in traffic, Dropbox detects simple MITM attacks
- Uploads
  - Images, resized images
  - Other files
  - Cached PDF as separated jpg pages
- Media
  - Snapshots (iOS only), profile photo
- Credentials
  - Nothing revealed

# [ Results :: Evernote ]

- Account Info
  - Account database name
  - Current account name
  - Camera settings
  - Numeric ID account info
- Data/Content
  - Linkedin invites & profile via ‘Scan Business card’ Premium feature
  - Grabbed data from Business cards
  - Html note + attaches
  - Html notes with embedded files/content like image or pdf/docx
- Media
  - Snapshots (iOS only)
- Nothing captured in traffic, Evernote detects simple MITM attacks

# [ Results :: Onedrive + business, office mobile, onenote ]

- OneDrive + OneDrive for Business
  - Uploads
    - Images, resized images
    - URL to download (have to login via liveID)
    - Full url to download file
    - Full user name, Permissions info
    - Downloaded files as is
    - PDF stored NOT as separated jpg pages
  - Credentials
    - Nothing revealed
- Captured in traffic for all apps
  - XML wrapped documents, media (photo)
  - Token & email
- Office Mobile
  - login name (= email)
  - cached files w/o name
  - Images, resized images
  - Sharepoint URL even it's not public
- Media
  - Snapshots (iOS only)
  - holiday inn reservation pdf as a jpeg
- OneNote
  - login name (= email)
  - Cached notes

# [ Results :: eFax ]

- Account Info
  - Efax message ID like 442030700520@messages.efax.com
  - Email, Full Name
  - Efax ID Numeric 442030700520
  - Premium or not / expiration date
- Content
  - Faxes as separated image (black&white)
  - ‘pageCount’ File
- Misc
  - Country, Region, TimeZone (Russia, EU, GMT+4)
- CrashAnalytics IDs
- Captured in traffic
  - Username, password, handset token
  - Faxes as jpg

# [ Results :: Amazon Store ]


- Locally
  - downloaded apk-files in local or shared folders (like downloads or SD cards)
- Network
  - Network type, carrier, device manufacturer
  - display size, device build & name & OS (full device info)
  - API level, all hardware capabilities plus emulator checker
  - direct URL, APK
  - Run on BlackBerry too, captured “guardian.blackberry.com” request per install (a kind of Antivirus from McAfee)

# [ Results :: Alfabank ]

- Locally
  - Latest used geo location unless it wiped
  - Latest phone number used to transfer money
- Network
  - Geo
  - Numeric ID & pin code, session ID, timeframe for session id
  - Card info
    - First 6 and last 4 digits, card name, card description, amount, currency
    - Linked phone number (country code, two digit of local code, last 4 digits)
    - Virtual card info, payment categories, account number linked to card
    - Payment history (not appeared for Android app run on BB)

# [ Results :: Sberbank ]

- Locally
  - Guid, Amount & linked card (first 6 & last 4 digits), card info
  - Card, amount and linked account number
- Network
  - Numeric login and guid in response, sms code and token in response, pin code and new token in response, login and one more token (!) in response
  - Each request contains GUID & device ID
  - Name, date, last IP, amount, loyalty info
  - Amount & linked card (first 6 & last 4 digits), card info
  - Card, amount and linked account number, payment history

# [ Results :: RSB ]

- Locally
  - Numeric login, encrypted pass (seems HMAC, need to check), uid, session id
- Network
  - Tracker ID (mobileapptracking.com) – not researched yet
  - Numeric login, encrypted pass (seems HMAC, need to check), OS, Vendor, imei
  - Card (first & last 4 digits) and linked account number plus amount, last transactions
  - The same password over several platforms

# [ Results :: RBK Money / CitiMobile ]


- RBK Money
- Captured in traffic
  - Account & Credentials :: Email = login , Password, session ID, Name, useraccount_ID, amount
  - Payment Info
    - Masked bank card number like xxxx****xxxx
    - Payment /Transaction History
- Locally stored as is:
  - Login/email, password, pin, payment info
- CitiBank
- Captured in traffic
  - Account & Credentials
    - Username, password, sms, last 4 digits of phone number
    - Amount info, transaction history, account number (fully detailed)
  - Device name, screen resolution, OS & version, carrier name
- Nothing special stored locally

# [ Results :: CitiMobile ]


- Captured in traffic
  - Account & Credentials
    - Username, password, sms, last 4 digits of phone number
    - Amount info, transaction history, account number (fully detailed)
  - Device name, screen resolution, OS & version, carrier name
- Nothing special stored locally

# [ Results :: Megafon/MailRu.Money ]

- Megafon Money
- Captured in traffic
  - Account & Credentials
    - Username = phone number, password, token,
    - Transfer details
- Token stored locally
- Mail.Ru Money
- Captured in traffic
  - Account & Credentials
    - Username = login, password, token, payment password, account id
    - Transfer details, linked credit card number (first 6 & last 4 digits)
- Stored locally
    - linked credit card number (first 6 & last 4 digits)


# Outlines: Fails


| App Type/Protection | In-Rest | In-Memory | In-Transit |
|---|---|---|---|
| **Built-in apps** | Plain-Text | Plain-Text | Rarely Encrypted / SSL/HTTPS |
| **IM apps** | Plain-Text | Plain-Text | Weak Encryption |
| **Social app** | Plain-Text & Rarely Store some data | Plain-Text | SSL/HTTPS |
| **Geo Apps** | Plain-Text | Plain-Text | SSL/HTTPS |
| **Office Apps** | Plain-Text | Plain-Text | SSL/HTTPS |
| **Travel Apps** | No/weak encryption | Plain-Text | SSL/HTTPS |
| **App with payment features** | Plain Text / Weak Encryption | Plain Text | SSL/HTTPS |
| **Bank apps** | Rarely Store data / Good Encryption | Plain-Text | SSL/HTTP / Encrypted |

# Outlines: BlackBerry

- BlackBerry Apps & Services prevent transferring data via untrusted connection even
- System protection storage couldn’t be easily access
- Apps usually store data in shared folders (docs, audio, etc.) are available to read/write for all
- Quite difficult to make BlackBerry trust to the proxy-certificates
- Android apps running on BlackBerry don’t differ from other Android apps neither network, nor local

# Outlines: Android

- Credentials stored or transferred in plaintext locally.
- OS does not provide any protection like a keychain in iOS
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption that helps to quickly decrypt data (depends on dynamically linked libraries)
- Data stored in SQLite databases usually not encrypted
- Data stored on external memory (SD card) rarely encrypted
- Keys may be hardcoded or put in data folder

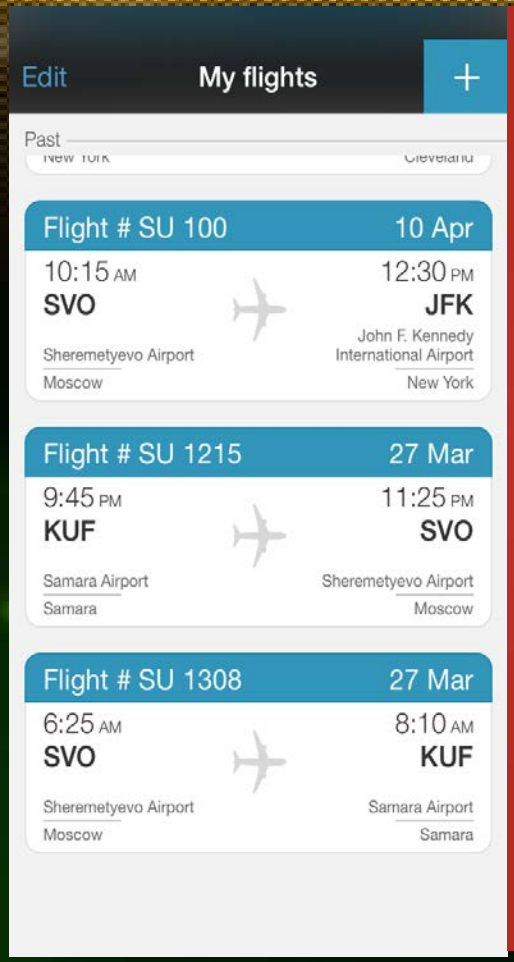
# Outlines: Store data everywhere

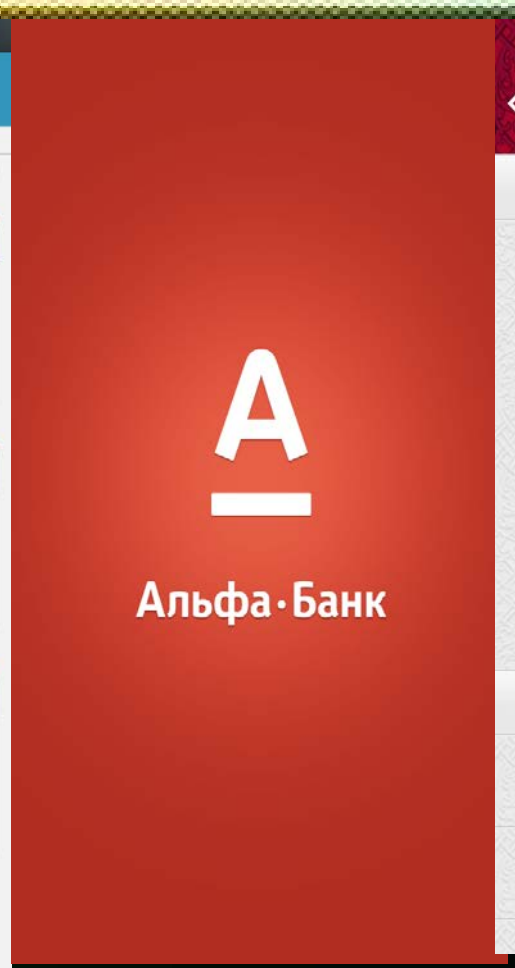
```
/data/data/ru.lynx.aero/shared_prefs/activities.main.MainActivity.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="phone">9851719122</string>
    <long name="cardExpiryDate" value="1472723015507" />
    <long name="scheduleChangesDate" value="1411638096257" />
    <long name="scheduleLastUpdateDate" value="1411638096692" />
    <string name="password">XXXXXXX</string>
    <string name="cardHolder">Yury Chemerkin</string>
    <string name="email">xxxxxxxxxxxxxx@gmail.com</string>
    <string name="userId">7-7011656</string>
    <string name="layout">phone</string>
    <string name="login">xxxxxxxxxxxxx</string>
    <string name="language">ru</string>
    <string
name="deviceId">bEBDPM1dCdDAPA9……K7iF9_lnAFKLgEE7VHdDCXbyww</string>
    <string name="cardNumber">1234567890123456</string>
</map>
```

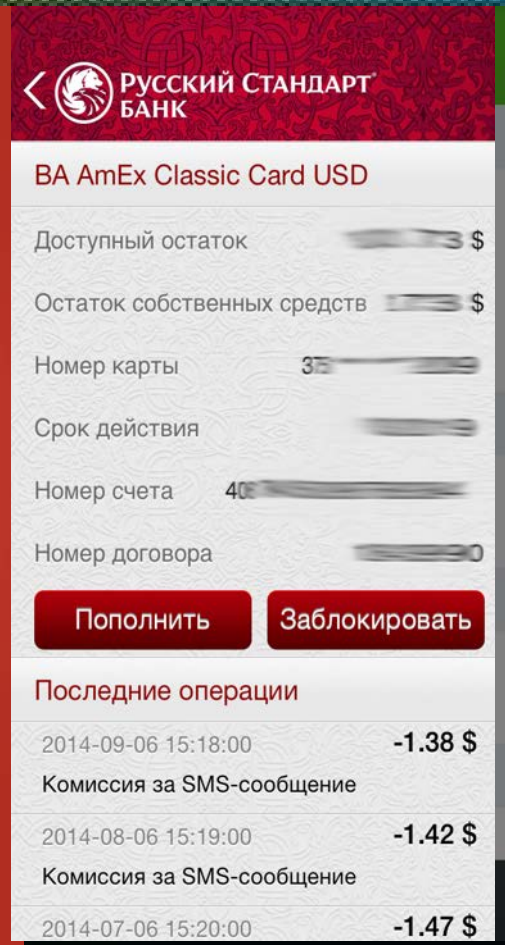
# Outlines: iOS

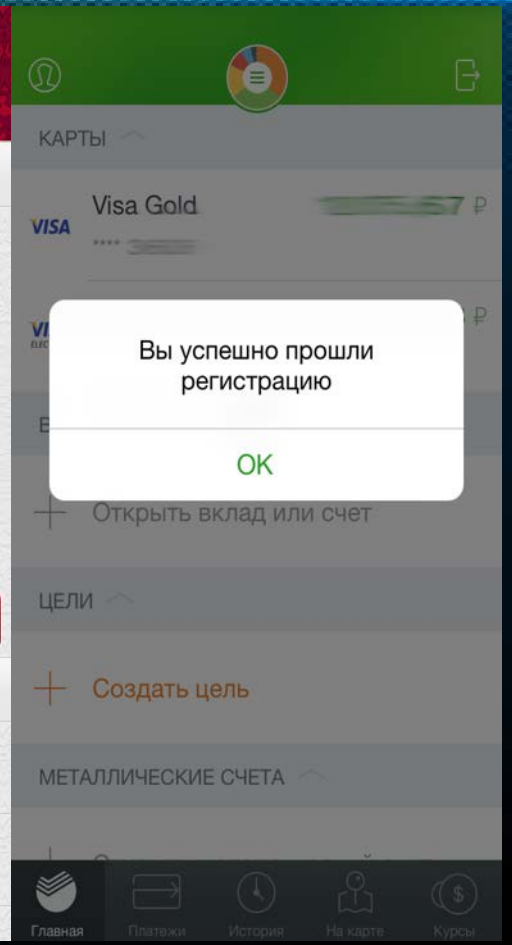
- Credentials stored/ transferred in plaintext locally.
- Data stored in a keychain without additional protection or encryption
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption that helps to quickly decrypt data
- Avoiding protection mechanism in iOS that leads to pure protection eventually
- Data stored in SQLite databases usually not encrypted
- Application data could be access without jailbreak
- Keys may be hardcoded

# Outlines: Snapshots in iOS



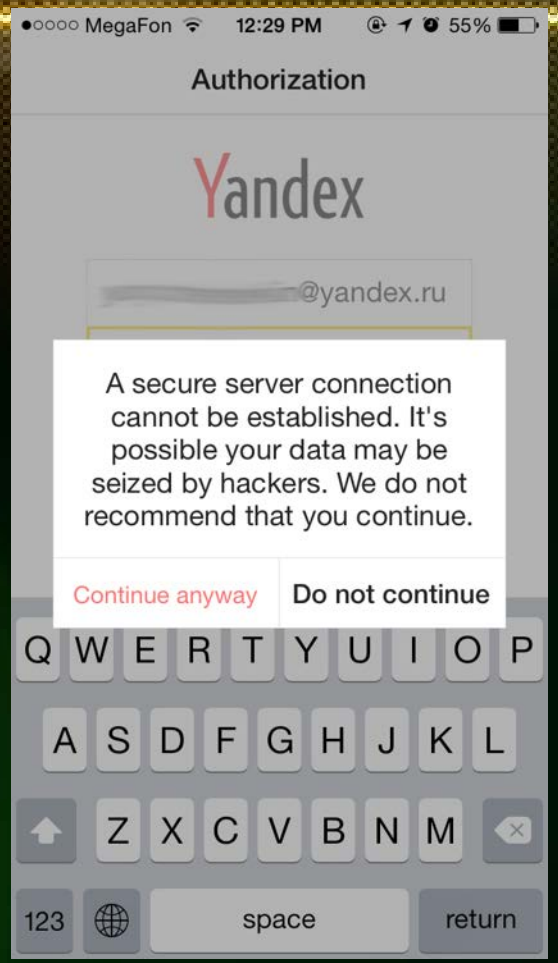



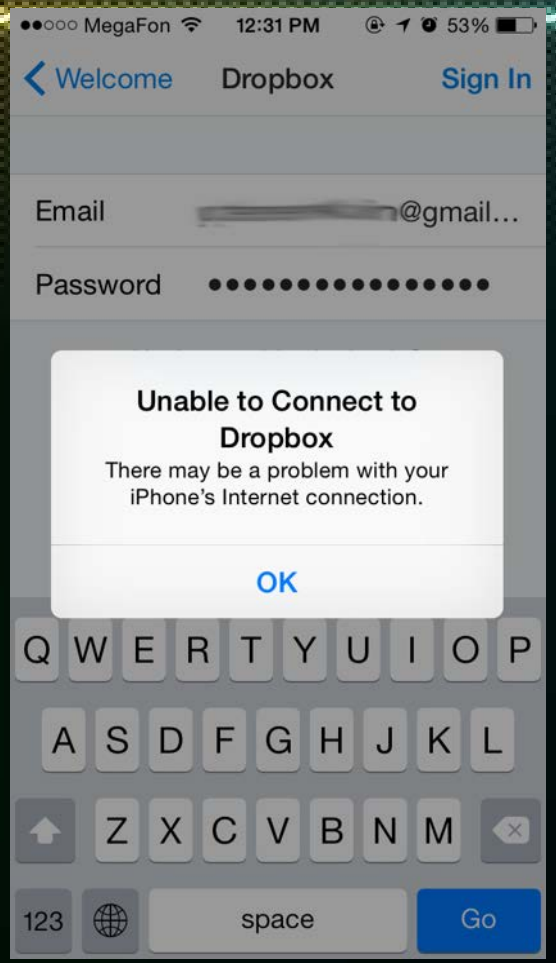



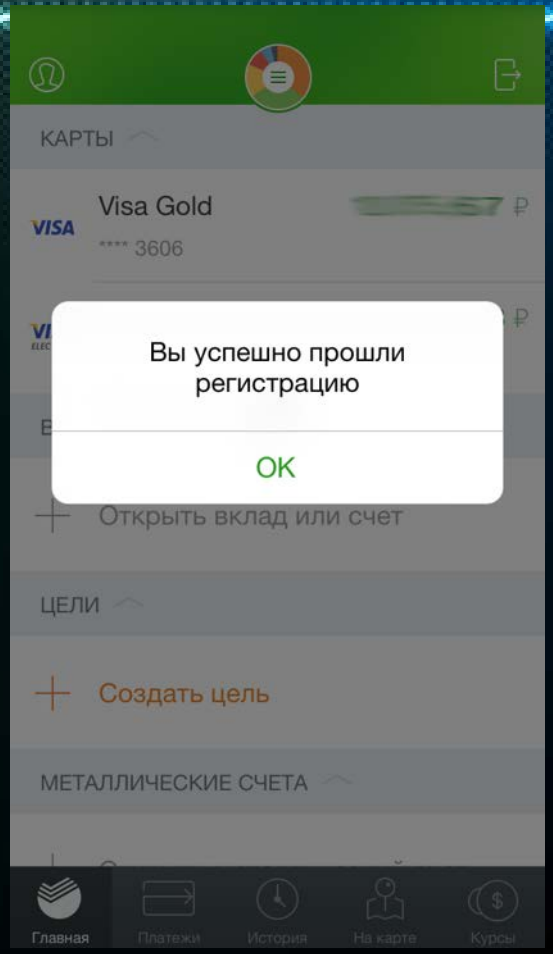
# Outlines: WinRT

- Credentials stored or transferred in plaintext locally.
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption helps quickly decrypt data (depends on dynamically linked libraries)
- Data stored in SQLite databases usually not encrypted
- Keys may be hardcoded or put in data folder
- Applications could be analyzed on Windows 8 (full edition rather than WinRT that’s only mobile OS edition) via known methods like a desktop applications

# Outlines: Network / Sniffing the traffic



# EMM FEATURES : Vendors

# [ EMM FRAMEWORK ]

## EMM (Enterprise Mobile Management)

- MDM: Mobile Device Management
- MAM: Mobile Application Management
- MEM: Mobile Email Management
- MIM: Mobile Information Management
- Devices: Smartphones, Tablets

## 3rd Party Solutions to EMM

- NAC: Network Access Control (Management)
- AV: Antiviruses Solution
- Mobile SIEM: Log Management Solution
- DLP: Data-Leakage Prevention
- COMPLIANCE: Standards, Best-Practices, Guidelines, etc.

# EMM FAILS :: MDM

- HIGH LEVEL DEVICE MANAGEMENT
- OPTIMIZED FOR CONFIGURATIONS DELIVERY
- OPTIMIZED FOR PERMISSIONS DELIVERY
- OPTIMIZED FOR INTERGRATION WITH AN INFRASTRUCTURE
- OPTIMIZED FOR CONFIGURATION DELIVERY
- LACK OF GRANULAR CONTROLS
- SECURITY CONTROLS DEPEND ON MOBILE OS

# EMM FAILS :: MAM

- PACKAGED/WRAPPED APPLICATIONS
- QUANTITY OF APPLICATION CHALLENGE ( OBVIOUSLY > 100 ☺ )
- COOPERATION WITH APPLICATION VENDOR
- SEPARATION OF PERSONAL, WORK, AND SUSPICIOUS APP
- SERIOUSLY DIFFERENCE ON APP INTERFACES PER EACH OS WITH THE SAME APP
  - VPN
  - ENCRYPTION
  - ACCESS RESTRICTION (GEO, CREDENTIALS)

# EMM FAILS :: MIM

- LACK OF TYPE FILES' MANAGEMENT
- LACK OF STORAGE SERVICES' MANAGEMENT
- LACK OF DEVICE FILES' MANAGEMENT
- LACK OF VENDOR SUPPORT
- NEED OF A ROOT ACCESS TO DEVICE IN CERTAIN CASES
- MOBILE OS INCAPABILITIES TO BE INTEGRATED WITH MIM SOLUTIONS

# EMM :: WHO IS GOOD FOR ?

| | |
|---|---|
| AirWatch | an MDM and MAM specialist that helped Lowes deploy and manage iPhones |
| App47 | which offers a platform that allows enterprises to deploy their own App stores (hot opportunity alert) |
| AppBlade | which supports application deployments and management across iPhone iPad BlackBerry and Android platforms. |
| AppCentral | which also helps enterprises to develop app stores |
| BlackBerry (BES/Fusion) | is good for MDM partially MIM & MAM. Supports all mobile OS |
| MaaS360 | is good with BlackBerry together |
| Kony | which has a platform that allows partners to build enterprise app stores for customers. |
| MobileIron | focused heavily on MDM |
| Nukona | another provider of enterprise app store technology |
| Partnerpedia | the former builder of channel partner communities; now focused on private labeled app stores. |
| WorkLight | now owned by IBM; focused on mobile development tools middleware and management |
| Terria Mobile | which offers a platform for app management. |
| Good Technology | supports application deployments and management across modern OS |

# GENERAL REMEDIATION/ISSUES

**WinRT, iOS & Android & BlackBerry apps have the same behavior & logic issues**

- ❑Insecure Data Storage
- ❑Poor AAA (Authentication Authorization Accounting)
- ❑Log Leakage
- ❑Weak Cryptography & Communication Protection
- ❑Sensitive Information Disclosure
- ❑**In general, iOS, Android, BlackBerry, WinRT apps have the same behavior & logic issues**

# Remediation: BlackBerry

- ❑Follow security programming guide from BlackBerry
- ❑Don’t store credentials in shared folders
- ❑Encrypt data stored in shared folders
- ❑Use implemented protection mechanism in BlackBerry…
- ❑But … add extra protection layer beyond just in case
- ❑Don’t forget to encrypt SQL databases
- ❑Don’t develop Android app-ports
- ❑Try to avoid using ported or Android native app under BlackBerry
- ❑Develop more and use native apps for BlackBerry ☺

# ANDROID-SPECIFIC REMEDIATION

- ❑Follow security programming guide from Google
- ❑Call ‘setStorageEncryption’ API for locally stored files (new Android OS v4+)
- ❑Encrypt externally stored files on SD Card or Cloud (any OS)
- ❑Define when encryption signature doesn’t matter, else avoid it
- ❑Reduce using of ‘MODE_WORLD_READABLE ’ unless it really needs
- ❑Avoid hardcoded and debug tracks as much as possible (it’s easy to decompile)
- ❑Add extra protect beyond OS (encryption, wiping, etc.)

# Remediation: iOS

- ❑Follow security programming guide from Apple
- ❑Never store credentials on the phone file system. Use API or web scheme instead
- ❑Define when encryption signature doesn’t matter, else avoid it
- ❑Use implemented protection mechanism in iOS…
- ❑But … add extra protection layer beyond OS protection in case of jailbreak
- ❑Use any API and protection mechanisms properly but never default settings
- ❑Don’t forget to encrypt SQL databases

# Remediation: WinRT

- ❑Follow security programming guide from Microsoft
- ❑Don’t try store credentials elsewhere system keystorage
- ❑Define when encryption signature doesn’t matter, else avoid it
- ❑Don’t forget to encrypt SQL databases
- ❑Remember, that all folders to store data are public accessible
- ❑Note, that WinRT apps could easily be reversed & debugged under desktop OS (Windows 8) even on Tablet
- ❑App’s code is one of set: C++, .Net, Silverlight, XAML, JavaScript
- ❑Try to implement a code obfuscation (it’s possible to do and not restricted)

# MAM SPECIFICS

## APP WRAPPING :: ADVANTAGES

- Is a secure bubble around each corporate application and its associated data
- Helps in creating an encrypted space, or folder, into which applications and data may be poured
- Newer, more granular approach in which each app is enclosed in its own encrypted policy wrapper, or container.
- Allows administrators to tailor policies to each app.
- Small vendors with proprietary approaches dominate the market like Symantec.

# MAM SPECIFICS

## APP WRAPPING :: DISADVANTAGES

- A Binary/Source application modification
  - Implementation of missing features
  - Interception of API & other call-methods
- Tech Limits of wrapper approach
  - Preinstalled, & built-in apps
  - Access to binary codes depends on OS
- Org Limits of wrapper approach
  - License limitation
  - Consuming mobile device resources to gather information
  - Many app-agents & app-agents management

# One More Salvation – Black Phone (?)


# Black Phone – Paranoid Phone or BlackBerry Clone?

The Blackphone is an announced smartphone developed by SGP Technologies, that will provide encryption for phone calls, emails, texts, and internet browsing.

**Zimmerman said,**
I had to wait for the rest of the technology infrastructure to catch up to make it possible to do secure telephony. PGP was kind of a detour for me while waiting for the rest of the technology to catch up to make really good secure telephony possible

**Technica states,**
Blackphone will run a custom built Android OS called PrivatOS. The operating system essentially “closes all backdoors” which are usually found open on major mobile operating systems. Some major features of PrivatOS are anonymous search, privacy-enabled bundled apps, smart disabling of Wi-Fi except trusted hotspots, more control in app permissions, private communication (calling, texting, video chat, browsing, file sharing and conference calls)

**Mike Janke, CEO clarifies,**
The Blackphone allows unsecure communications are certain calls you'll want to encrypt, but "if you're ordering a pizza or calling your grandma", it's unlikely you'll feel the weight of the NSA on your shoulders. "This is why Blackphone is so unique—it gives the user the chance to choose the level of privacy."

**The Verge states,**
The Blackphone looks like a fairly standard Android phone. It has a 4.7-inch HD (the exact resolution has yet to be announced) IPS display, a 2GHz quad-core processor, 16GB of storage, an 8-megapixel camera, LTE—pretty much everything you'd want in a smartphone, and very little you wouldn't. Produced by Silent Circle, a company with an existing portfolio of security- and encryption-related software

# Black Phone Device: Rumors

Website offers no details on how those extra levels of security will be implemented, but..

- Silent Circle is U.S. based company
- Zimmermann is cofounder of mobile privacy software firm Silent Circle
- GeeksPhone is a Spanish smartphone hardware company/start-up
- GeelsPhone sells open Android phones and developer devices of Firefox OS.
- SPG Technology is a Switzerland-based join venture
- IntelliJ IDEA is used to build applications

# Black Phone Software: Rumors & interviews

- How was the idea for the Blackphone conjured up?
  - Large market of folks who didn't want to build their own car, but they wanted a good car
- Why should users want to have a Blackphone? Security Center
  - At $629 is the total package.
  - Lot of security magic to stop leaks out
- Who is buying the Blackphone?
  - 45 percent of orders have come from Europe and 38 percent from North America
  - Blackphone is gathering as little information as possible on who is buying its product
- Who should be buying a Blackphone?
  - There are clearly industries that are already predisposed to seek privacy, such as stockbrokers, attorneys, senior executives
- Why is this phone safer than what's currently out there?
  - It's safer because it's more usable
  - Every bit of information the phone sends out is encrypted whether it's a call or a text No one can offers it now
- BYOD/Enterprise?
  - Absolutely, even MDM tools
- How secure is the Blackphone?
  - Anybody who claims that anything is hackproof is clearly selling snake

# Black Phone - Software

The Blackphone is an announced smartphone developed by SGP Technologies, that will provide encryption for phone calls, emails, texts, and internet browsing.

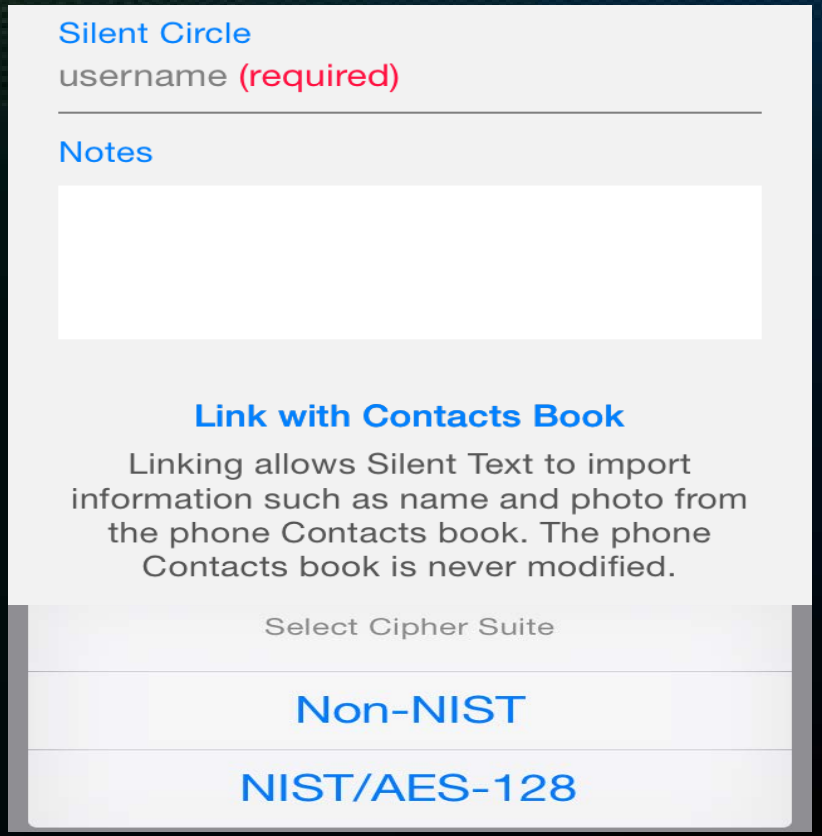
- Silent Circle Apps
  - Silent Phone
  - Silent Text
  - Silent Contacts
- Blackphone-built Apps
  - Blackphone Security Center
  - Blackphone Activation Wizard
  - Blackphone Remote Wipe
- 3rd-party Apps
  - Disconnect Secure Wireless
  - SpiderOak Blackphone Edition
  - Kismet Smart Wi-Fi Manager
- Misc
  - PrivatOS
  - International Power Adapter Kit

# Black Phone - Examination

Servers of its custom-built network are located in Canada

Also Supports iOS, Android, Windows Desktop

- Silent Phone: Encrypted voice and video calls on iOS and Android, it can be used with Wi-Fi, EDGE, 3G or 4G cellular. Encrypted VoIP from Windows computers.
- Silent Text: Encrypted text messaging and secure cloud content transfer with “burn notice” feature for permanently deleting messages from devices.
- Silent Mail: Discontinued August 9, 2013 Encrypted e-mail on Silent Circle’s private, secure network and compatibility with popular e-mail client software.
- Silent Contacts: App is prebuilt with all previous



# Black Phone - Examination

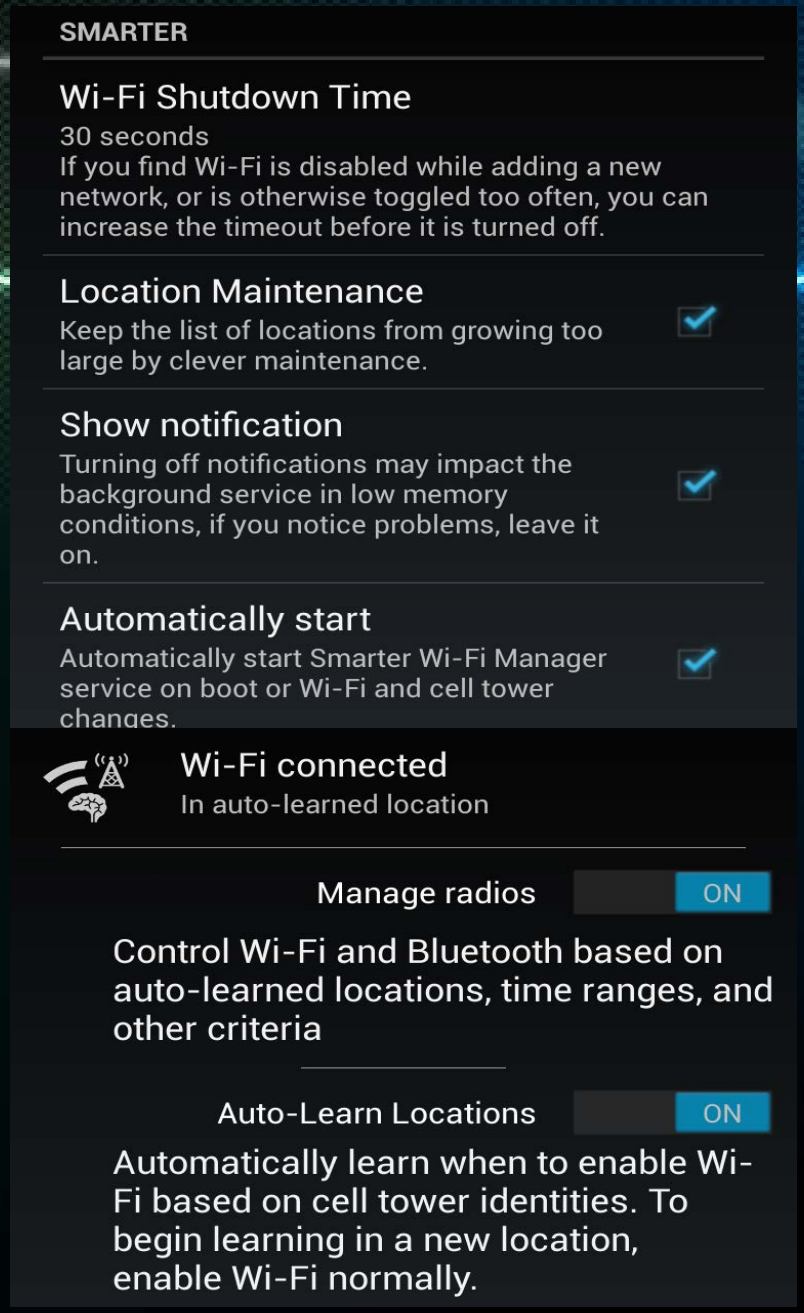
The company's products enable encrypted mobile phone calls, e-mail, text messaging, and video chat. Servers of its custom-built network are located in Canada

- Silent Phone/Text/Contact: available for iOS & Android with source code on GitHub
- Remote Wipe: Provides no centralized cloud service to manage device
- Private OS: Android 4.4 KitKat
- International Power Adapter Kit: Android 4.4 KitKat
- Disconnect Secure Wireless: its custom-built VPN client
- Kismet Smart Wi-Fi Manager: Public Wi-Fi Manager
- SpiderOak: Encrypted Cloud Storage

# Black Phone / Smart Wi-Fi Manager

Is that secured ?

- It manages Android phone Wi-Fi connection by automatically learning where you use networks. Wi-Fi is only enabled when you are in a location have previously used Wi-Fi, increasing battery life, security, and privacy.
- It is a paid app in Google Play but fully open source under the GPLv2 license.
- It aims to be smart, invisible and will manage Wi-Fi state in the background.
- Airplane mode and Wi-Fi Tethering modes are detected and respected
- Since Wi-Fi will be turned off, your phone won't be broadcasting your home network name everywhere you go! It prevents spoof attacks
- Successfully installed on BlackBerry 10



# Black Phone / SpiderOak

## Why not Box or Mega?

- It is US based online backup tool to back up, share, sync, access and store data using an off-site server.
- It is accessible through an app for Windows, Mac and Linux computer platforms, and Android, N900 Maemo and iOS mobile platforms
- It uses encrypted cloud storage and client-side encryption key creation, so even employees of SpiderOak cannot access users' information
- It provides automatic de-duplication of data

# Black Phone / SCMC (MDM)

Oh, God ☺

- It can be incorporated to the typical policy and management tools in a business environment
- A web-based console which grants a nominated customer administrator “super user” status within his or her own network.
- Create, organize and bulk distribute via email to provide team members with Silent Phone, Silent Text, and Out-Circle Access.
- Create groups and sub-groups to reflect your company’s organization and allocate encrypted mobile apps accordingly.
- Dynamically manage and control (enable/deny access) for all users under your administration.
- Enable outliers, contractors, and third parties to communicate securely with your team on the fly.

# Black Phone: Pros & Cons

## Fully protected (no any PoC yet)

- ❑Encrypted Contacts, splitted for personal & business uses
- ❑Encrypted Text, Media Messenger
- ❑VoIP for encrypted Calls
- ❑Smart WiFi Manager to prevent attacks
- ❑Disconnect Secure Wireless VPN
- ❑Privat OS is Android 4.4 KitKat
- ❑MDM w/o MAM, MIM, MEM
- ❑BlackPhone gathers little info on who is buying it

## Impractical & too commercial

- ❑Alike any other app on AppStore or GooglePlay,WorkBalance MDM Solution
- ❑TextSecure, CryptoCat, BBM, iMessage, etc?
- ❑VoIP is everywhere for the less price ☺
- ❑Gather Geo, Network Data, AutoLearn
- ❑VPN is everywhere too
- ❑GeeksPhone offers a root access …
- ❑Impractical, MAM need at least
- ❑Name, Address, Payment method, Personal or Enterprise

# Black Phone: Pros & Cons

| Storages | SpiderOak | Is that only one? |
|---|---|---|
| **Provider** | **Encrypted storage** | **Personal Encryption2** |
| Amazon S3 / AWS | + | + |
| Box (PreBuild on BlackBerry) | + | + |
| CrashPlan | + | + |
| ElephantDrive | + | + |
| Handy Backup | + | + |
| IASO Backup | + | + |
| Jungle Disk | + | + |
| KeepVault | + | + |
| MediaFire | + | + |
| MEGA | + | + |
| Norton Zone | + | + |
| OwnDrive | + | + |
| SpiderOak | + | + |
| Sync | + | + |
| TeamDrive | + | + |
| Wuala | + | + |

# Black Phone: Pros & Cons

| | PrivatOS Enhancement | Android Default | BlackBerry | iOS |
|---|---|---|---|---|
| **Web Search** | Anonymous | Trackable | Both & Flexible | Both |
| **Bundled Apps** | Few, and all privacy-enabled | Many, with privacy disabled by default | Least privilege access control | On-Demand Access |
| **Wi-Fi usage** | Smart disabling of all Wi-Fi except trusted hotspots | Always on for geolocation and user tracking | Separate + Per Apps | Global + Separate Per App |
| **App permissions** | Fine-grained control in a single interface | All-or-nothing | Fine-Grained Control | On-Demand Access |
| **Communication tools** | Private calls, texting, video chat, file exchange up to 100MB, browsing and conference calls | Traceable dialer, SMS, MMS, browser. Vulnerable to spoofed cell networks and Wi-Fi | Both, need VPN configuration | Both, need VPN configuration |
| **Updates** | Frequent secure updates from Blackphone directly | Supplied infrequently after carrier blessing | Frequent secure updates from BlackBerry directly | Frequent secure updates from Apple directly |
| **Remote Wipe & Anti Theft** | Anonymous (??) | Requires use of centralized cloud account | Cloud account | Cloud account |
| **Business Model** | Delivering privacy as a premium, valued feature | Personal data mining for tracking and marketing | Delivering secure & privacy as a default valued feature last 20+ years | Music, App, Games :) |
| **Management** | MDM | Weak MDM Features/Samsung enhanced | MDM, MAM, MEM, MIM,… | MDM, MAM, MEM, MIM,… |

Y.O.B.A. hacking