



**SECON**

ассоциация разработчиков

# БЕЗОПАСНОСТЬ ДАННЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ.

МИФЫ И РЕАЛЬНОСТЬ

**ЮРИЙ ЧЕМЁРКИН**

*MULTI-SKILLED SECURITY EXPERT*





# ЗАО «ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ»

Компания «Перспективный мониторинг» была создана в 2007 году как исследовательское подразделение группы компаний «ИнфоТеКС».

Сегодня в компании развиваются направления:

Коммерческий Центр мониторинга информационной безопасности (SOC).

Threat Intelligence и разработка правил для средств защиты информации.

Разработка средств мониторинга и аналитики.

Практики безопасной разработки ПО.

Исследования защищённости информационных систем.

**Безопасность мобильных устройств, приложений и сетей.**

<http://amonitoring.ru>



# PENTESTER & DEVELOPERS



<https://youtu.be/Nh11A41kL4?t=50s>

# APP INSECURITY. WARNING



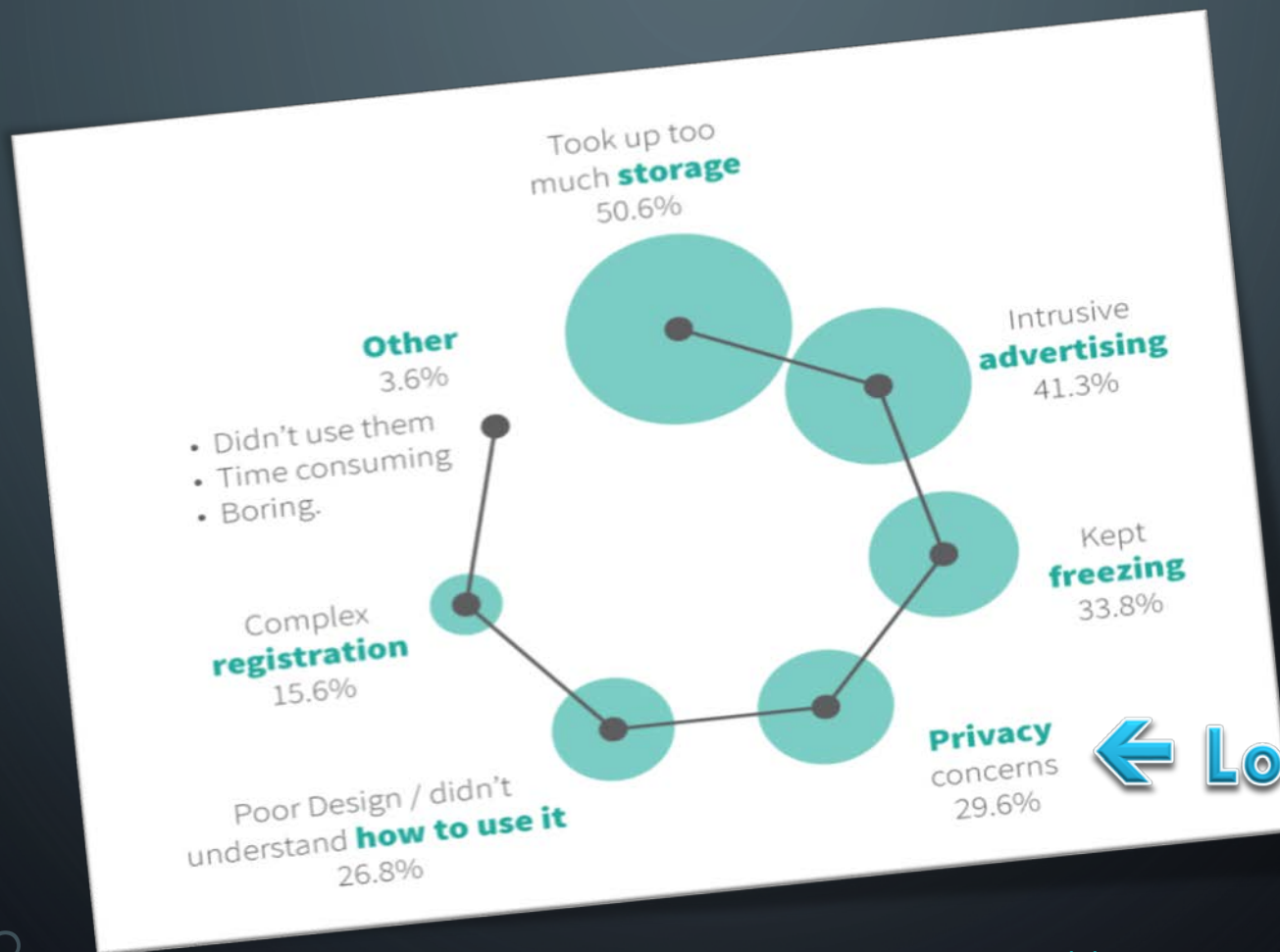
Everything presented further contains information for educational purposes and only with using only your data & licenses. Moreover, to each app presented here was not applied any techniques and actions such as:

- modifying, decompiling, disassembling, decrypting and other actions with the object code of any Program, aimed at obtaining source codes of any Program

Also, as known,

- the User may make a modification of the Software solely for his or hers own use and reverse engineering for debugging such modifications.

# ITR RESEARCH RESULTS. WHY CONSUMER UNINSTALLED MOBILE APPS



← Look Here

# MOBILE APPS BING BANG – Y2011 - Y2014 - Y2017

**Y2011** – viaForensics, which runs the appWatchdog web page, checked whether an app encrypted passwords, user names, or actual email content before storing it on the phone. A full pass meant that all three were stored in encrypted form. An app received a warning if the user name was left in plain text but password and content were encrypted. If either the password or content was stored in plain text, the app failed

<http://www.cbsnews.com/news/want-to-protect-your-emails-dont-use-these-11-android-and-iphone-email-apps/>

**Y2014** – Researchers find data leaks in Instagram, Grindr, OoVoo and more. By sniffing out the details of network communications, University of New Haven researchers have uncovered a host of data-leakage problems in Instagram, Vine, Nimbuzz, OoVoo, Voxer and several other Android apps. The problems include storing images and videos in unencrypted form on Web sites, storing chat logs in plaintext on the device, sending passwords in plaintext, and in the case of TextPlus, storing screenshots of app usage that the user didn't take

All in all, the researchers estimate **968 million people total use the apps.**

<https://www.cnet.com/news/researchers-find-data-leaks-in-instagram-grindr-oovoo-and-more/>

**Y2017** – 76 Popular Apps Confirmed Vulnerable to Silent Interception of TLS-Protected Data. According to [Apptopia](#) estimates, there has been a combined total of **more than 18,000,000 (Eighteen Million) downloads of app versions** which are confirmed to be affected by this vulnerability

For **33 of the iOS applications**, this vulnerability was deemed to be low risk (All data confirmed vulnerable to **intercept is only partially sensitive analytics data about the device, partially sensitive personal data such as e-mail address, and/or login credentials which would only be entered on a non-hostile network**).

For **24 of the iOS applications**, this vulnerability was deemed to be medium risk (Confirmed ability to **intercept service login credentials and/or session authentication tokens** for logged in users).

For **19 of the iOS applications**, this vulnerability was deemed to be high risk (Confirmed ability to **intercept financial or medical service login credentials and/or session authentication tokens** for logged in users).

[https://medium.com/@chronic\\_9612/76-popular-apps-confirmed-vulnerable-to-silent-interception-of-tls-protected-data-2c9a2409dd1#.ea21dxqmw](https://medium.com/@chronic_9612/76-popular-apps-confirmed-vulnerable-to-silent-interception-of-tls-protected-data-2c9a2409dd1#.ea21dxqmw)

# MOBILE APPS VS. SECURITY/PRIVACY MYTHS OF DATA PROTECTION



- No weakness in normal activity in compare to vulnerabilities
- Complex issues. We guarantee the confidentiality of your data and we developed our apps in compliance to Apple/Google guides, PCI DSS, so on...
- Weirdness and Worseness are coming
- [Dev.:] My app is good protected! “Data is stored in an unencrypted format because the both iOS and Android provide data isolation ... This is considered standard ... is completely safe“
- Crafted certificate is not a wild attack and it’s an user fault only
- We will update it soon!
- Lack of Protection of data items is an issue over several apps
  - One app might be risky and has a quite bad data protection – OK
  - One risky app over several dozens apps is a betrayer that lead to leaks – NOT OK

# NO WEAKNESS IN NORMAL ACTIVITY

Data Leakage is data that becomes available when you perform typical activities. Instead, Vulnerability is a weakness of program. Thus, Vulnerability  $\neq$  Data Leakage, because no weakness in normal activities...

So, shut up and install our application



# COMMON WEAKNESS OR VULNERABILITIES IN DATA PROTECTION. EXCERPTS

## Sensitive data leakage [CWE-200]

- ✓ Sensitive data leakage can be either inadvertent or side channel
- ✓ Protection can be poorly implemented exposing it:
  - Location; Owner ID info: name, number, device ID; Authentication credentials & tokens
  - Target App Information is also sensitive (out of scope of CWE-200)**

## Unsafe sensitive data storage [CWE-312]

- ✓ Sensitive data should always be stored encrypted so that attackers cannot simply retrieve this data off the file system, especially on removable disk like micro SD card **or public folders (out of scope of CWE-312)** such as
  - banking and payment system PIN numbers, credit card numbers, or online service passwords
- ✓ **There's no excuse for sandboxing without encryption here**

## Unsafe sensitive data transmission [CWE-319]

- ✓ Data be encrypted in transmission lest it be eavesdropped by attackers e.g. in public Wi-Fi
- ✓ If app implements SSL, it could fall victim to a downgrade attack degrading HTTPS to HTTP.
- ✓ Another way SSL could be compromised is if the app does not fail on invalid certificates.
- ✓ **There's no excuse for partial SSL validation here**

# OWASP MOBILE PAST vs. NOW

## Code Protection

### Top 10 Mobile Risks 2012-2013

- **M1:** Insecure Data Storage
- M2: Weak Server Side Controls
- **M3:** Insufficient Transport Layer Protection
- M4: Client Side Injection
- M5: Poor Authorization and Authentication
- M6: Improper Session Handling
- M7: Security Decisions Via Untrusted Inputs
- **M8:** Side Channel Data Leakage
- M9: Broken Cryptography
- **M10:** Sensitive Information Disclosure

## Code Protection & Dev fails

### Top 10 Mobile Risks 2014-2015

- M1: Weak Server Side Controls
- **M2:** Insecure Data Storage
- **M3:** Insufficient Transport Layer Protection
- **M4:** Unintended Data Leakage
- M5: Poor Authorization and Authentication
- M6: Broken Cryptography
- M7: Client Side Injection
- M8: Security Decisions Via Untrusted Inputs
- M9: Improper Session Handling
- M10: Lack of Binary Protections

## Data Protection & Dev fails

### Top 10 Mobile Risks 2016-2017

- **M1:** Improper Platform Usage
- **M2:** Insecure Data Storage
- **M3:** Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

[https://www.owasp.org/index.php/Projects/OWASP Mobile Security Project - Top Ten Mobile Risks](https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks)

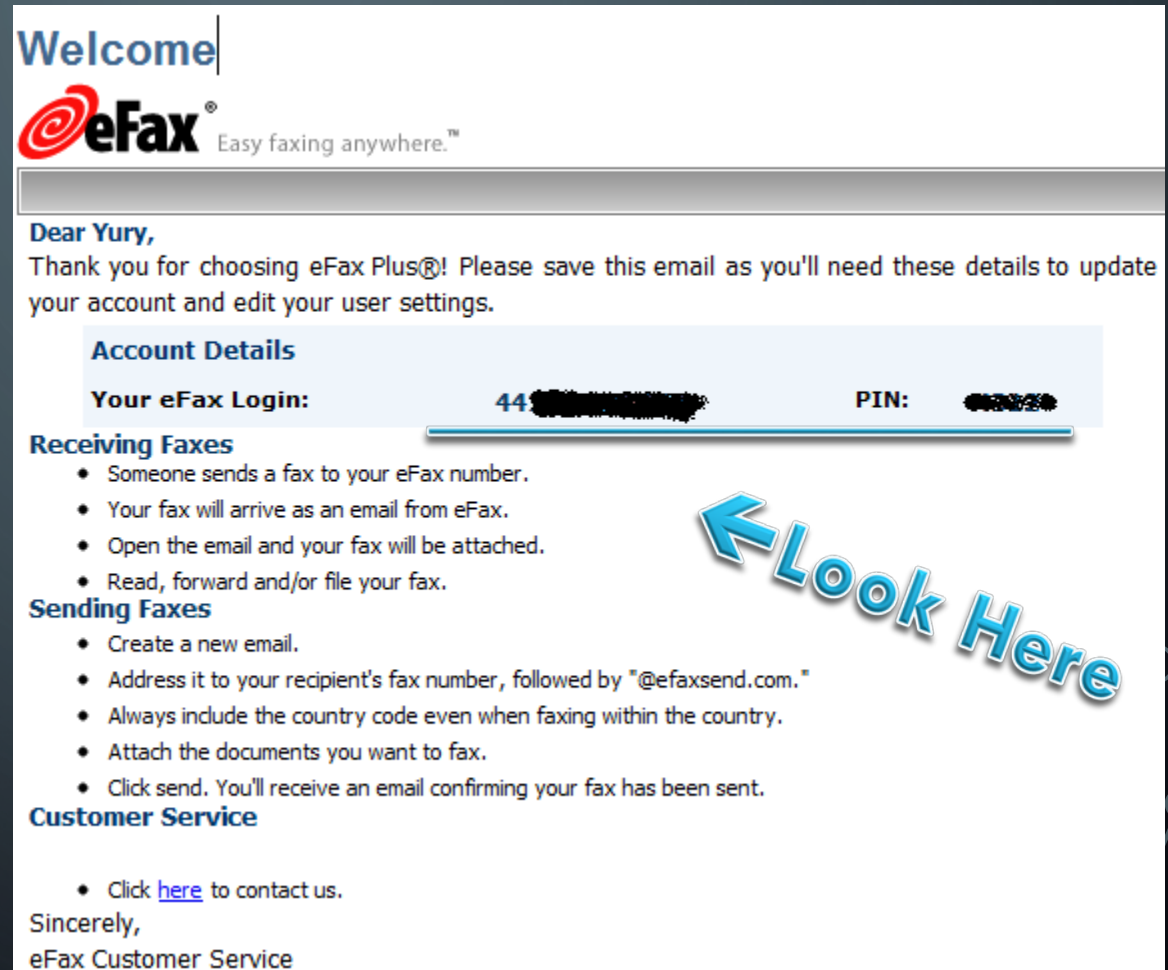
[https://www.owasp.org/index.php/Mobile Top 10 2016-Top 10 Y2017's Top 10 is upcoming](https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10_Y2017's_Top_10_is_upcoming)

# COMPLEX DATA LEAKAGE WE GUARANTEE THE CONFIDENTIALITY OF YOUR DATA

Don't trust email  
applications?

Signed up for  
account on popular  
services and got a  
confirmation email?

Here we go!



**Welcome**

**eFax**® Easy faxing anywhere.™

---

**Dear Yury,**  
Thank you for choosing eFax Plus®! Please save this email as you'll need these details to update your account and edit your user settings.

**Account Details**

<b>Your eFax Login:</b>	44 [REDACTED]	<b>PIN:</b>	[REDACTED]
-------------------------	---------------	-------------	------------

**Receiving Faxes**

- Someone sends a fax to your eFax number.
- Your fax will arrive as an email from eFax.
- Open the email and your fax will be attached.
- Read, forward and/or file your fax.

**Sending Faxes**

- Create a new email.
- Address it to your recipient's fax number, followed by "@efaxsend.com."
- Always include the country code even when faxing within the country.
- Attach the documents you want to fax.
- Click send. You'll receive an email confirming your fax has been sent.

**Customer Service**

- Click [here](#) to contact us.

Sincerely,  
eFax Customer Service

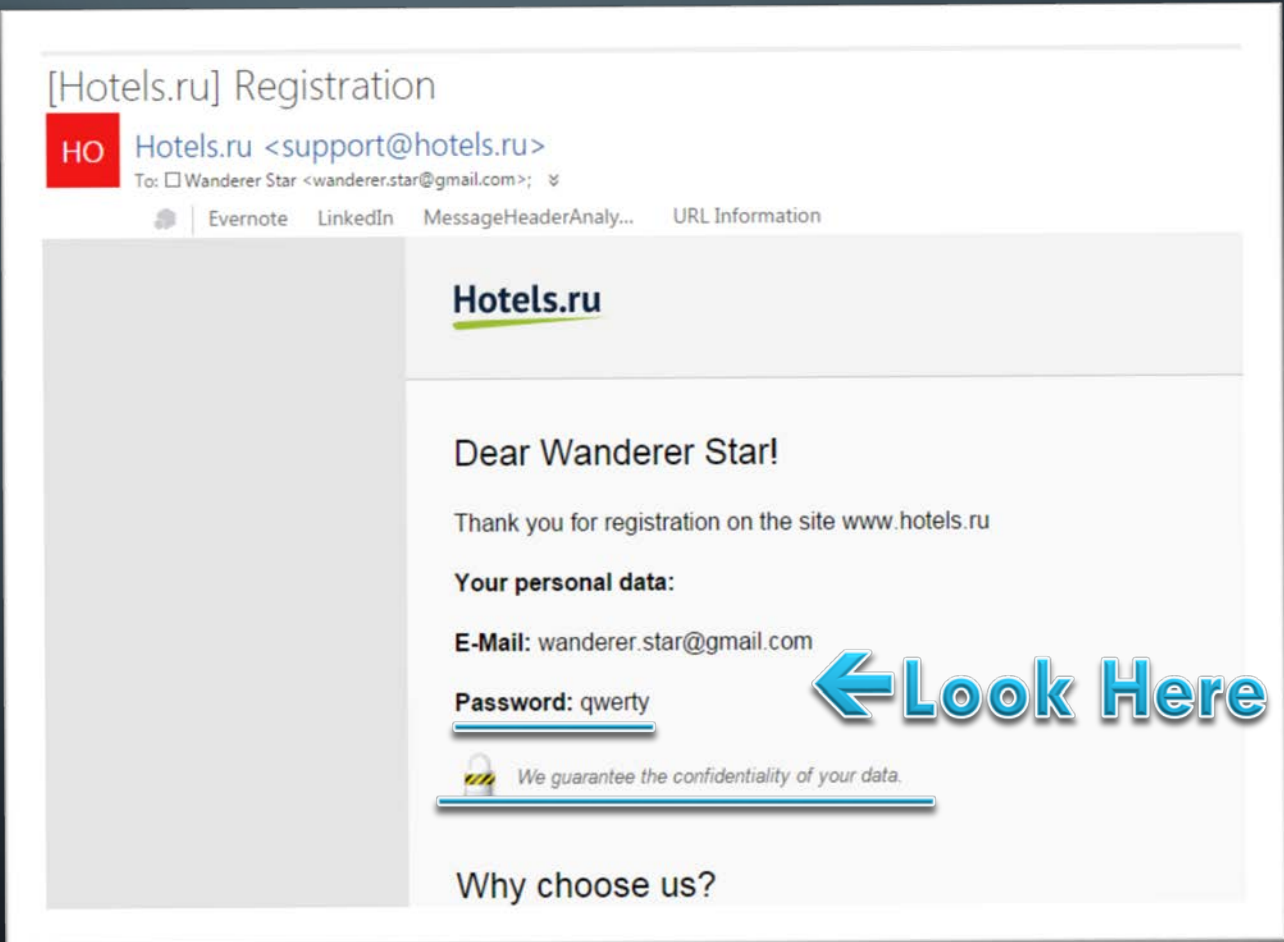
**← Look Here**

# COMPLEX DATA LEAKAGE WE GUARANTEE THE CONFIDENTIALITY OF YOUR DATA


Don't trust email  
applications?

Signed up for  
account on  
popular services  
and got a  
confirmation  
email?

Here we go!



[Hotels.ru] Registration

**HO** Hotels.ru <support@hotels.ru>  
To:  Wanderer Star <wanderer.star@gmail.com>; 

[Evernote](#) [LinkedIn](#) [MessageHeaderAnaly...](#) [URL Information](#)

---

**Hotels.ru**


Dear Wanderer Star!

Thank you for registration on the site [www.hotels.ru](http://www.hotels.ru)

**Your personal data:**

**E-Mail:** wanderer.star@gmail.com

**Password:** qwerty

 We guarantee the confidentiality of your data.

Why choose us?

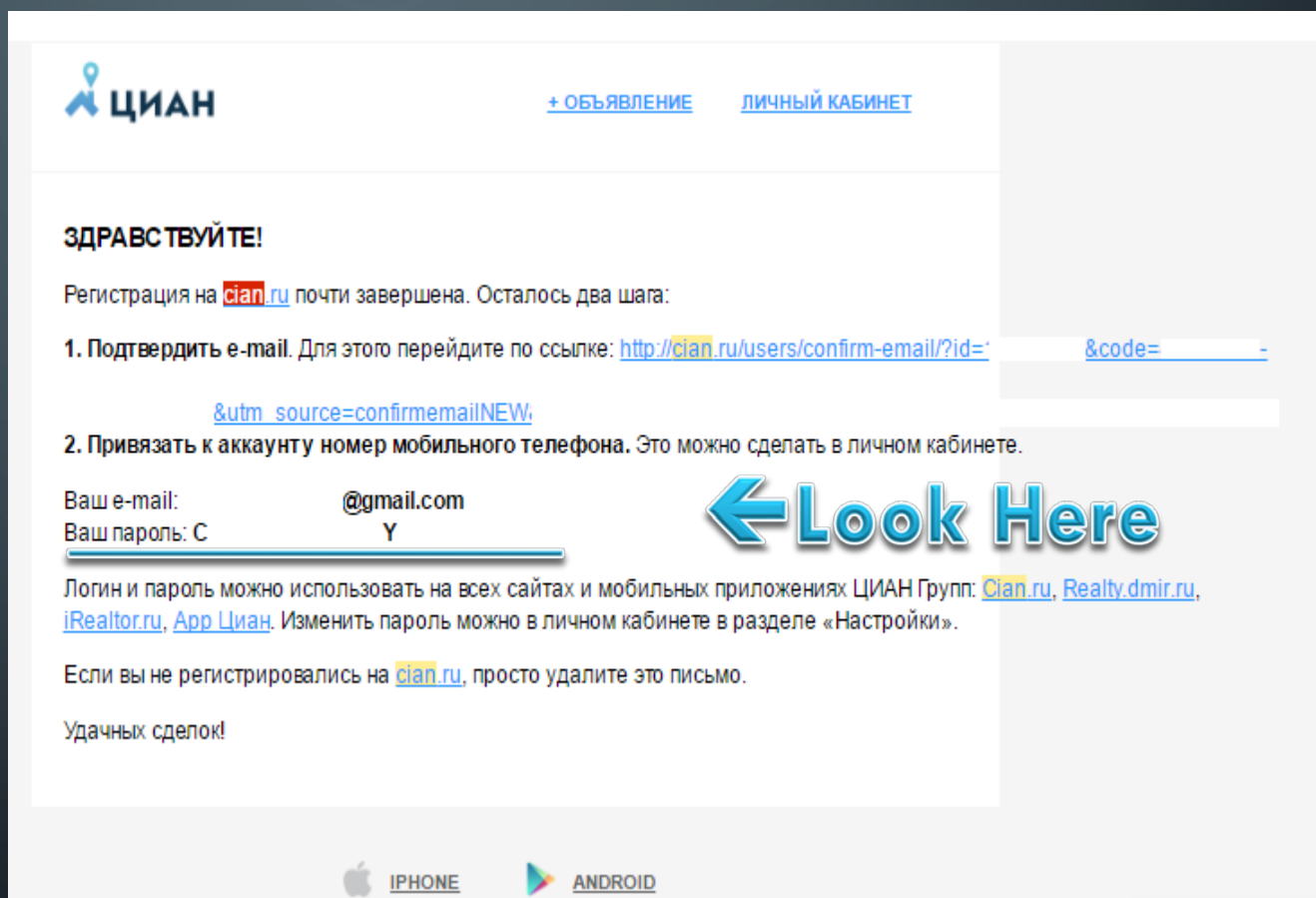
**← Look Here**

# COMPLEX DATA LEAKAGE WE GUARANTEE THE CONFIDENTIALITY OF YOUR DATA

Don't trust email  
applications?

Signed up for  
account on  
popular services  
and got a  
confirmation  
email?

Here we go!



The screenshot shows a confirmation email from CIAN.ru. At the top, there is the CIAN logo and navigation links for '+ ОБЪЯВЛЕНИЕ' and 'ЛИЧНЫЙ КАБИНЕТ'. The main text reads 'ЗДРАВСТВУЙТЕ!' followed by 'Регистрация на [cian.ru](http://cian.ru) почти завершена. Осталось два шага:'. Step 1 is 'Подтвердить e-mail. Для этого перейдите по ссылке: [http://cian.ru/users/confirm-email/?id=\\_\\_\\_\\_\\_&code=\\_\\_\\_\\_\\_&utm\\_source=confirmemailNEW](http://cian.ru/users/confirm-email/?id=_____&code=_____&utm_source=confirmemailNEW)'. Step 2 is 'Привязать к аккаунту номер мобильного телефона. Это можно сделать в личном кабинете.' Below this, the email address is shown as '@gmail.com' and the password as 'Y'. A blue arrow points to the password field with the text 'Look Here'. At the bottom, there are links for 'Cian.ru', 'Realty.dmir.ru', and 'iRealtor.ru', and a note about deleting the email if not registered. The footer contains 'IPHONE' and 'ANDROID' logos.

# AEROEXPRESS 2.1.3 for iOS

## AEROEXPRESS 3.1.3 for Android



Apps didn't have a SSL Validation over years until Apr 16<sup>th</sup>, 2017. Now a certificate is need to MITM

~20-25 data items per each application

### Data-in-Transit Data Items

'Credentials Info' Group: Credentials (IDs, Activation IDs, Password)

'Loyalty Info' Group: Account Details

'Payment Info' Group: **Card Full Information**, Shorted Passport Data

'Orders Info' Group: Orders Details & History, Media Data (QR Ticket, URL for Ticket, Address Data - Railways Station), Shorted Passport Data

'Account Info' Group: Tracked Data & Favourites

### Data-at-Rest Data Items (same data items)

According to PCI DSS docs, app is required:

- prevent MITM, does a validation SSL
- does not store payment details

February Y2015

Aeroexpress has passed its PCI DSS certification. Now it is even safer for passengers to pay for online services provided by this express carrier.

In early February, Aeroexpress passed its PCI DSS certification, which is aimed at ensuring the secure processing, storage and transfer of data about Visa and MasterCard holders. Given the PCI DSS certified security level, Aeroexpress passengers can pay for tickets via the website or the company's **mobile app using bank cards and can be confident that their personal data and funds are safely secured.**

Press Release:

[https://aeroexpress.tickets.ru/en/content/safety\\_payments.html](https://aeroexpress.tickets.ru/en/content/safety_payments.html)

Press Release:

[https://aeroexpress.ru/en/press\\_releases/news20090589.html](https://aeroexpress.ru/en/press_releases/news20090589.html)

[https://www.pcisecuritystandards.org/documents/Penetration\\_Testing\\_Guidance\\_March\\_2015.pdf](https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf)

# ROCKETBANK, ROSINTER, DELIVERYCLUB



## App facts

All Apps' Data items are vulnerable to MITM with crafted certificate (Credentials, Payments, Account Info and so on...)

**RocketBank:** Payment Card's Pin Code = Application Password

## Privacy Policy facts

ROSINTER – no Privacy Policy

DeliveryClub

We implement **a variety of security measures** to maintain the safety of your personal information when you place an order. We offer the use of **a secure server**. All supplied sensitive/credit information is **transmitted via Secure Socket Layer (SSL)** technology and then encrypted into our Payment gateway providers database only to be accessible by those authorized with special access rights to such systems, and are required to keep the information confidential.

[http://www.delivery-club.ru/google\\_privacy.html](http://www.delivery-club.ru/google_privacy.html)

RocketBank 2013-2015: User agrees that (among other statements... most important)

Unique codes and phone number are enough to perform authenticated actions over internet

<https://goo.gl/zVcgnD>  
<https://goo.gl/MQmzNc>

Rocketbank Team doesn't give a shit about risks

The client is only responsible for everything happened with him and his data over internet.

RocketBank 2016 - now: Nothing about security or protection

<https://rocketbank.ru/open-rules#offer>  
<https://goo.gl/e9eecf>

# WORST APPS. TAXI APPS

All apps below transmit and store data in plaintext

## Meridian (RO)

'Geolocation Info' Group: Geo, Address Data

'Credentials Info' Group: Credentials (Tokens, IDs, Password)

'Account Info' Group: Account Data

'Application Info' Group: URLs (URL to binary installer files)

'Social Info' Group: Account Data, Credentials (Tokens, IDs, Password), Device Environment

## Cris Taxi Bucuresti (RO)

'Geolocation Info' Group: Geo, Address Data

'Travel Info' Group: Geo, Address Data

'Account Info' Group: Account Data

'Orders Info' Group: Orders Details & History

## Taxi 777 (Ru), FixTaxi (Ru, Android only)

'Geolocation Info' Group: Geo, Address Data, Place Details, Favourites Addresses

'Account Info' Group: Account Details

'Credentials Info' Group: Credentials (IDs, Tokens, Activations IDs)

'Financial Info' Group: Card Short Info (no CVC/CVV), Favourites Cards

'Browser Info' Group: Card Full Info (with CVC/CVV)

'Orders Info' Group: Orders Details & History



# WEIRD PROJECTS: FACEBOOK, FACEBOOK MESSENGER, AND FACEBOOK PAGE MANAGER APPS

From time to time some parts of app are worse protected than others  
~60 data items per each application

Application Information – **MITMed, crafted cert is needed**

- Transaction History & Contact Short Profile

- Credentials (IDs), Credentials (Passwords) and Credentials (Tokens)

Browser Information

- Preview

Message Information

- GEO Data

- GEO Snapshots

The rest *Data-in-Transit* data is **SSL Pinned** & *Data-at-Rest* data is in **backup**

- Account Information, Address Book 'n' Contact Information, Analytics 'n' Ads Information, Application Information, Credentials Information, Device Information, Events Information, Location 'n' Maps Information, Media Information, Social Information

Media Data are in **plaintext** (**Facebook Messenger**)

- Cached profile images



# THE BEST 'WORST' APPS



**AlterGeo** 4.6 for iOS / 3.13 for Android

No updates since Spring Y2014. Everything in plaintext including Credentials



**Weather Street Style** 1.9.0

Everything in plaintext including Credentials. Sending Credentials & Geo to the server each 30 second



**IHG & Marriott**

Limited access by a time (no longer 180 days) - Booking Info: Orders History

Encrypted Credentials Information: Passwords - IHG only

Doesn't make a sense if it's only way to give an access to the user account

Makes a sense if it's data that stored locally if it's out of backup even



**WeChat**

Awesome protected (many security fails fixed by now), encrypted but Location data is still out of protection

Location 'n' Maps Information: Contact Media

Message Information: GEO & Address Data, GEO Snapshots, Place Details



**Maxim Taxi (iOS & Android)**

Everything in plaintext

Credentials (any), Geo-Location & Address Data, Device Info, Favourite Geo Data & Trips

No Credit card is supported (?)



# APPs FOR NEWS, ENTERTAINMENT AND SO ON...

**SSL but no validation exists at the same time, except recently updated iOS App**

Many of them might have a bad protection

iFunny 😊 – SSL but no validation exists at the same time

Credentials (IDs, Password, Token)

Social Credentials (IDs, Password, Token)

Account Data, URLs, Account Media URLs, so on...

Account Media, Media Stream – in plaintext (http)

Password is not saved locally (token instead)

**iOS app was recently updated (Apr 16<sup>th</sup>, 2017)**

Now it requires a crafted certificate is needed to MITM network data



# PureVPN v5.4.0 for iOS

## PureVPN v5.6.0 for Android

iOS App's data items protected by SSL pinning\_ Android App's data item MITMed by preinstalled certificate

### Account Information

| Account Details, Settings 'n' Configs, Credentials IDs+Passwords, Account Media, Tracked/Favorites

### Analytics 'n' Ads Information

| Analytics Configs, Device Data, Environment

### Application Information

| Application Certificates 'n' Profile + Configs, Credentials (IDs+Passwords+ Tokens)

### Device Information

| Device Data **but network data is available by preinstalled certificate**

### Location 'n' Maps Information

| GEO & Address Data

### VPN Information

| Application Configs

All Data-at-Rest items are stored in plaintext (credentials in backup as well)



# PureVPN. EULA/PRIVACY

Personally Identifiable Information (PII) includes all such information which can be directly linked to an individual e.g. Name, telephone number or email address.

This information may include, **but not limited to:**

Names (For account creation purpose)

Email address (For the creation of an account and/or to contact you with offers and discounts)

Phone number (For particular users from certain countries ONLY)

We Are Data Superheroes

**All PII, public and private keys, passwords are stored in encrypted format**, using strong cryptographic algorithms.

<https://www.purevpn.com/privacy-policy.php>



# CYBERGHOST v6.7 for iOS

# CYBERGHOST v6.0.1.65 for Android

License, credentials, app passwords, settings can be MITMed with crafted/stolen/installed certificate

## Account Information

- | Account & License Details

## Analytics 'n' Ads Information

## Application Information

- | Application Certificates 'n' Profile

## Browser Information

- | Credentials IDs, Password, Tokens

- | Account & License Details, GEO Data, Environment, Application Config

## Credentials Information

- | Credentials (IDs, Tokens, Access IDs, App Passwords, PreShared Secret)

## Device Information

- | Environment & Network Details

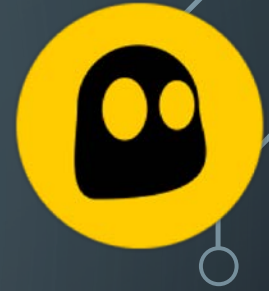
## Location 'n' Maps Information

- | GEO Data & Address Data

## Log Information (supposed to be logs) – out of backup files, jailbreak/root required

- | Log Data, Credentials IDs, Tokens, Access IDs, App Passwords, PreShared Secret

- | GEO Data & Address Data, Account Details & License Details, Network Details



# CYBERGHOST. EULA/PRIVACY

Personal data: CyberGhost collects and uses no personal data, such as e-mail addresses, name, domicile address and payment information.

If you register for the Premium-Service of CyberGhost VPN, we store a fully anonymous User ID, an encoded password and your pay scale information (activation key, start and end). The stored e-mail addresses are not linked to a User ID.

Log data: CyberGhost keeps no logs which enable interference with your IP address, the moment or content of your data traffic. We make express reference to the fact that we do not record in logs communication contents or data regarding the accessed websites or the IP addresses.

In March 2012, CyberGhost had successfully passed an audit and verification conducted by QSCert for the implemented Information Safety Management System (ISMS) according to the international industrial standards ISO27001 and ISO9001.

The certification confirms the high quality of the internal safety processes and is renewed yearly ever since.

<http://www.cyberghostvpn.com/en/privacypolicy>

# PUBLIC RESEARCH

## “AN ANALYSIS OF THE PRIVACY AND SECURITY RISKS OF ANDROID VPN PERMISSION-ENABLED APPS”



The **BIND\_VPN\_SERVICE** permission is a powerful Android feature that allows the requesting app to intercept, manipulate and forward all user's traffic to a remote proxy or VPN server of their choice or to implement proxies in localhost [93].

Android generates two warnings to notify user's whenever an app creates a virtual interface using the VPN permission:

- (i) a system dialog seeking users approval to create a virtual interface, and
- (ii) a system-generated notification that informs users as long as the VPN interface remains active [60].

**Third-party user tracking and access to sensitive Android permissions:** 75% of them use third-party tracking libraries and 82% request permissions to access sensitive resources including user accounts and text messages.

**(Lack of) Encryption and traffic leaks:** 18% of the VPN apps implement tunneling protocols without. 84% and 66% of the analyzed VPN apps do not tunnel IPv6 and DNS traffic due to lack of IPv6 support, misconfigurations or developer-induced errors.

**TLS interception:** Four of the analyzed VPN apps compromise users' root-store and actively perform TLS interception in the flight. Three of these apps claim providing traffic acceleration services and selectively intercept traffic to specific online services like social networks, banking, e-commerce sites, email and IM services and analytics services

<https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf>



# SOLUTIONS. FORENSICS SOFTWARE

Isn't easy to adopt for you needs.

You still don't know how good or bad it was protected

But you know how much data can be extracted by these tools

Common features (example, Oxygen Software) <http://www.oxygen-forensic.com/en/events/news>

Social Networks. Extraction from Kate Mobile (30.1) from Android OS devices.

Messengers. Extraction from WhatsApp (2.16.1) including encrypted messages.

Messengers. Extraction from Skype (6.15.0.1162) from Blackberry 10 devices.

Business. Extraction from Yandex.Money (4.4.1) from iOS devices.

Messengers. Extraction from Telegram (3.7.0) from Android OS devices.

Messengers. Extraction from Viber (5.8.1) from iOS devices.

Social Networks. Extraction from LinkedIn (9.0.9) from iOS devices.

Social Networks. Extraction from Instagram (7.19.0) from Android OS devices.

# COMPANIES' QUOTES

## WHAT THEY THINK ABOUT INSECURITY

The Kik logo is displayed inside a white speech bubble with a black outline. The word "kik" is written in a lowercase, green, sans-serif font.

"Message data is stored in an unencrypted format because the operating systems (both iOS and Android) provide data isolation that prevents apps from having their storage read by other apps. This is considered standard in the industry, and is completely safe," the Kik said.

<https://www.cnet.com/news/researchers-find-data-leaks-in-instagram-grindr-oovoo-and-more/>

A small photograph of a man wearing a brown tweed jacket and a matching hat, looking down at a smartphone he is holding in his hands.

Oxygen Forensics releases a maintenance version of Oxygen Forensic® Detective. Version 9.0.1 offers functionality and interface improvements of Oxygen Forensic® Cloud Extractor, Oxygen Forensic® Maps and Export Engine. It also adds data parsing from Video Locker and KeepSafe applications and updates support for popular messengers: **Kik Messenger**, Facebook Messenger, Viber, WhatsApp, etc. The total number of **supported apps versions exceeds 2400!**

Applications. Messengers. Updated support for **Kik Messenger (10.16.1.9927) for Android OS** devices.

<https://www.oxygen-forensic.com/en/events/news/739-oxygen-forensic-detective-adds-support-for-new-applications-and-devices>

# EXTRACTING LOCAL DATA. EXAMPLES

Common OS techniques

Public tools incl. rooting scripts

Forensics solutions

Cellerite

OxygenForensics

Elcomsoft

And more...

# FORENSICS CLOUD FEATURES

## Cellebrite

UFED Cloud Analyzer provides access to **more than 25 private cloud data sources** to help you attain the critical case evidence that often hides in cloud application data. See the full list below: Facebook, WhatsApp, Twitter, Gmail, Google Location History, Google My Activity, Google Photos, Google Chrome, Google Calendar, Google Contacts, Google Drive, Google Bookmarks, Google Tasks, Mail (IMAP), Dropbox, iCloud App, iCloud Calendar, iCloud Contacts, iCloud Drive, iCloud Photos, OneDrive, Instagram, KIK, VK, Telegram, iCloud Notes, iCloud Reminder, iCloud Location <http://www.cellebrite.com/Pages/ufed-cloud-analyzer>

## Oxygen Forensic® Detective

Oxygen Forensic® Detective acquires data from **more than 30 cloud storages**: iCloud contacts and calendar, Google Drive, Google Location History, Live contacts and calendar, OneDrive, Dropbox and Box as well as from a wide range of social media including Twitter and Instagram <https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective/detective/cloud-data-extraction>

## Elcomsoft Cloud eXplorer

Acquire information from users' **Google Account** with a simple all-in-one tool! Elcomsoft Cloud Explorer makes it easier to download, view and analyze information collected by the search giant, providing convenient access to users' search and browsing history, page transitions, contacts, Google Keep notes, Hangouts messages, as well as images stored in the user's Google Photos account.

<https://www.elcomsoft.com/ecx.html>

## Elcomsoft Phone Breaker

Cloud acquisition is an alternative way of retrieving information stored in mobile backups produced by Apple iOS, and the only method to explore Windows Phone 8 and Windows 10 Mobile devices. Elcomsoft Phone Breaker can retrieve information from **Apple iCloud and Windows Live!** services provided that original user credentials for that account are known.

The Forensic edition of Elcomsoft Phone Breaker enables over-the-air acquisition of iCloud data without having the original Apple ID and password. Password-free access to iCloud data is made possible via the use of a binary authentication token extracted from the user's computer.

Elcomsoft Phone Breaker supports accounts with Apple's two-step verification as well as the new two-factor authentication. Access to the second authentication factor such as a trusted device or recovery key is required. You will only need to use it once as Elcomsoft Phone Breaker can save authentication credentials for future sessions.

<https://www.elcomsoft.com/eppb.html>

# CELLEBRITE UNLOCKING CAPABILITIES

Cellebrite Advanced Investigative Services (CAIS) experts provide law enforcement agencies with forensically sound, early access to sensitive mobile digital intelligence.

Advanced Technical Services provide:

Unlocking and extraction of Apple iPhone 4S, 5, 5C, 5S, 6, 6 Plus, iPad 2, 3, 4, iPad Air, iPad mini 1, 2, 3, 4, iPod touch 5G, 6G

Unlocking and decrypted physical extraction of Samsung Galaxy S6, S6 edge, S6 edge+, S6 active, A5, A7, A8, J1, J7, Note 5, S7, S7 edge, S7 edge, S7 active

Decrypted Physical extractions available for most models

Limitations may apply based on iOS/Android version and Security patch level

[http://go.cellebrite.com/cais\\_unlock](http://go.cellebrite.com/cais_unlock)

# OXYGEN FORENSIC DETECTIVE

Oxygen Forensic® software retrieves all vital application data from mobile devices running **iOS, Android OS, BlackBerry 10, Windows Phone 8**. The program is able to decrypt apps databases even if they securely encrypted.

Currently **370 unique applications and 2760+ app versions** are supported.

| Social Networks, Dating, Messengers, Web Browsers, Navigation, Travel, Finance, Productivity, Health, Games

**Android Rooting** add-on grants an access to: **Full file system, Applications data, Geo-location information, Deleted data**

| No 100% successful rooting is guaranteed. The procedure is available for the most of Android devices with versions 1.6 - 2.3.4 and 3.0 - 5.1

The Jet-Imager module allows to create full physical dumps from Android devices on average up to 25% faster. **The extraction speed depends on how much data the device has. For example, 16GB can be extracted in 5-7 minutes, 32Gb – in 8-10 minutes.**

Currently there are two extraction methods in the Jet-Imager module:

| **physical extraction via custom forensic recovery (Samsung)**  
| **physical extraction of pre-rooted devices**

<https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective/detective/jet-imager>

<https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective/analyst/android-rooting-addon>

<https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective/analyst/applications>

# ELCOMSOFT iOS FORENSIC TOOLKIT

## Support for 32-bit and 64-bit iOS Devices

**All devices:** Logical acquisition is available for all devices regardless of jailbreak status / iOS version. Supports lockdown files for accessing passcode-protected devices.

**Legacy:** Unconditional physical acquisition support for legacy devices (iPhone 4 and older) regardless of iOS version and lock status

**32-bit:** Full physical acquisition support of jailbroken 32-bit devices running all versions of iOS up to and including iOS 9.3.3 (iPhone 4S through 5C, iPad mini)

**64-bit:** Physical acquisition for jailbroken 64-bit devices running any version of iOS for which a jailbreak is available (iPhone 5S, 6, 6S and their Plus versions, iPad mini 2 through 4, iPad Air, Air 2)

**iOS 9.3.4, 9.3.5, iOS 10.x:** Logical acquisition only for iPhone 7, 7 Plus and all other devices running iOS 10 or versions of iOS 9 **without jailbreak**. Device must be **unlocked with passcode, Touch ID or lockdown record**

**Locked:** Limited acquisition support for jailbroken 32-bit and 64-bit iOS devices that are locked with an unknown passcode and cannot be unlocked

## Compatible Devices and Platforms

The Toolkit completely fully supports the following iOS devices, running **all iOS versions up to iOS 7; no jailbreaking required, passcode can be bypassed** or quickly recovered:

iPhone (original), iPhone 3G, iPhone 3GS, iPhone 4 (GSM and CDMA models), iPad (1st generation), iPod Touch (1st - 4th generations)

**Physical acquisition** is available for the following models (**requires jailbreak with OpenSSH installed**)

iPhone 4S, iPhone 5, iPhone 5C, iPod Touch (5th gen), iPad 2, iPad with Retina display (3rd and 4th generations), iPad Mini

The following (64-bit) models are supported via **physical acquisition for 64-bit devices, regardless of iOS version (up to 9.3.3):**

iPhone 5S, iPhone 6, iPhone 6 Plus, iPhone 6S, iPhone 6S Plus, iPad Air, iPad Air 2, iPad Mini 2/3/4, iPad Pro

All other devices including **iPhone 7/7 Plus as well as devices running iOS 10.x, 9.3.4 and 9.3.5** are supported via **logical acquisition** (must be **unlocked with passcode, Touch ID or lockdown record**).

## Supported operating systems:

iOS 1-5

iOS 6.0-6.1.2 (with evasi0n jailbreak)

iOS 6.1.3-6.1.6 (with p0sixspwn jailbreak)

iOS 7.0 (with evasi0n jailbreak)

iOS 7.1 (with Pangu 1.2+ jailbreak)

iOS 8.0-8.1.2 (with TaiG, PanGu or PP jailbreak)

iOS 8.1.3-8.4 (with TaiG 2.0 jailbreak)

iOS 9.0-9.1-9.2-9.3.3 (with PanGu jailbreak)

iOS 9.3.4-10.x (via logical acquisition only)

## Decrypt keychain items, extract, device keys (32-bit devices only)

Keychain is extracted but cannot be decrypted with 64-bit device except the known / empty backup passcode; passcode must be removed in iOS settings

## Passcode is not required

**iOS 1.x-3.x:** passcode not required. All information will be accessible. The original passcode will be instantly recovered and displayed.

**iOS 4.0-7.x:** certain information is protected with passcode-dependent keys, including the following:

Email messages; Most keychain records (stored login/password information);

Certain third-party application data, if the application requested strong encryption.

**iOS 8.x through 10.x:** most information is protected. Without the passcode, only very limited amount of data

Call log that includes all incoming and outgoing calls (including FaceTime), Voicemail, All settings and options,

List of installed apps, Many log files including download and update histories, service launch logs and many other system and application logs, Various temporary files

Simple 4-digit passcodes recovered in 10-40 minutes

<https://www.elcomsoft.com/eift.html>

<https://www.elcomsoft.com/eift.html>

# SSL ISSUES: Apps, Mozilla, WoSign, Apple, Google

Applications handle SSL connection in different ways:

- ❑ Some don't validate SSL certificate during the connection
- ❑ Many trust to the root SSL certificates installed on the device due to SSL validating
- ❑ Some have pinned SSL certificate and trust it only

Trusting root certificate might not be a good idea (Mozilla reports):

- ❑ Between 16th January 2015 and 5th March 2015, WoSign issued 1,132 SHA-1 certificates whose validity extended beyond 1st January 2017
- ❑ Between 9th April 2015 and 14th April 2015, WoSign issued 392 certificates with duplicate serial numbers, across a handful of different serial numbers
- ❑ It is important background information to know which WoSign roots are cross-signed by other trusted or previously-trusted roots (expired but still unrevoked)
- ❑ Eventually **Apple removes SSL certificate from iOS, perhaps from iOS 10 only**

<https://support.apple.com/en-us/HT204132>, <https://support.apple.com/en-us/HT202858>

<https://threatpost.com/google-to-distrust-wosign-startcom-certs-in-2017/121709/>



# DESPITE REVOKED CA'S, STARTCOM AND WOSIGN CONTINUE TO SELL CERTIFICATES

Once in a while, Certificate Authorities misbehave. They might have bugs in their validation procedures that have lead to TLS certificates being issued where the requester had *no* access to. It's happened for Github.com, Gmail, ... you can probably guess the likely targets.

When that happens, an investigation is performed -- *in the open* -- to ensure the CA has taken adequate measures to prevent it from happening again. But sometimes, those CA's don't cooperate. As is the case with StartCom (StartSSL) and WoSign, [which in the next Chrome update](#) will start to show as *invalid certificates*.

Google has determined that two CAs, WoSign and StartCom, have not maintained the high standards expected of CAs and will no longer be trusted by Google Chrome, in accordance with our Root Certificate Policy.

This view is similar to the recent announcements by the root certificate programs of both [Apple](#) and [Mozilla](#).

[Distrusting WoSign and StartCom Certificates](#)

So Apple (*Safari*), Mozilla (*Firefox*) and Google (*Chrome*) are about to stop *trusting* the StartCom & WoSign TLS certificates.

<https://ma.ttias.be/despite-revoked-cas-startcom-wosign-continue-sell-certificates/>

# SYMANTEC API FLAWS REPORTEDLY LET ATTACKERS STEAL PRIVATE SSL KEYS & CERTIFICATES SYMANTEC KNEW OF API FLAWS SINCE 2015



Stealing Symantec  
SSL Certificates

A security researcher has disclosed critical issues in the processes and [third-party API](#) used by Symantec certificate resellers to deliver and manage Symantec SSL certificates. The flaw, discovered by Chris Byrne, an information security consultant and instructor for Cloud Harmonics, could allow an unauthenticated attacker to retrieve other persons' SSL certificates, including public and private keys, as well as to reissue or revoke those certificates. Even without revoking and reissuing a certificate, attackers can conduct "man-in-the-middle" attack over the secure connections using stolen SSL certs, tricking users into believing they are on a legitimate site when in fact their SSL traffic is being secretly tampered with and intercepted.

Symantec has responded to this API flaws and provided the following statement to The Hacker News:

"We have looked into Chris Byrne's research claim and could not recreate the problem. We would welcome the proof of concept from the original research in 2015 as well as the most recent research. In addition, we are unaware of any real-world scenario of harm or evidence of the problem. However, we can confirm that no private keys were accessed, as that is not technically feasible."

<http://thehackernews.com/2017/03/symantec-ssl-certificates.html>

# GOVERNMENT AND NETWORK SECURITY

## Online surveillance. Microsoft may be accidentally helping Thailand's government spy on its citizens

A new report from Privacy International entitled "Who's That Knocking at My Door? Understanding Surveillance in Thailand" says a Microsoft policy involving root certificates enables the state to monitor encrypted communications sent via email or posted on social media sites. Microsoft says that the certificate meets the company's standards.

While Apple's macOS does not include the Thai root certificate by default, Microsoft Windows does, and Privacy International says this leaves users of that operating system open to attack or surveillance. Windows accounts for over 85 percent of the desktop computing market in Thailand, according to [StatCounter](#).

<https://news.vice.com/story/microsoft-may-be-accidentally-helping-thailands-government-spy-on-its-citizens>

## Kazakhstan is going to start intercepting HTTPS traffic via "man-in-the-middle attack" starting Jan 1, 2016

The law was accepted in December, but now one of our providers announced information for small and medium business how to install government-provided root SSL certificate: [https://www.beeline.kz/b2b/sme/ru/press\\_centers/10040](https://www.beeline.kz/b2b/sme/ru/press_centers/10040)

### Update, Contribution with Mozilla:

[Mozilla bug report – Add Root Cert of Republic of Kazakhstan](#)

[Mozilla CA Program \(in pdf\)](#)

[Gov Cert of Kazakhstan](#)

[https://www.reddit.com/r/sysadmin/comments/3v5zpz/kazakhstan\\_is\\_going\\_to\\_start\\_intercepting\\_https/](https://www.reddit.com/r/sysadmin/comments/3v5zpz/kazakhstan_is_going_to_start_intercepting_https/)

# BYPASSING NETWORK SECURITY FOR \$0

How To: Use mitmproxy to read and modify HTTPS traffic

| <https://blog.heckel.xyz/2013/07/01/how-to-use-mitmproxy-to-read-and-modify-https-traffic-of-your-phone/>

Use SSLsplit to transparently sniff TLS/SSL connections – including non-HTTP(S) protocols

| <https://blog.heckel.xyz/2013/08/04/use-sslsplit-to-transparently-sniff-tls-ssl-connections/>

How To: DNS spoofing with a simple DNS server using Dnsmasq

| <https://blog.heckel.xyz/2013/07/18/how-to-dns-spoofing-with-a-simple-dns-server-using-dnsmasq/>

Rogue AP Setup

| <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-invisible-rogue-access-point-siphon-off-data-undetected-0148031/>

Kali Linux Evil Wireless Access Point

| <https://www.offensive-security.com/kali-linux/kali-linux-evil-wireless-access-point/>

Bettercap – mixed features

| <https://www.bettercap.org/docs/proxying/http.html>

| <https://www.bettercap.org/docs/servers/dns.html>

| <https://www.bettercap.org/docs/proxying/custom.html>

... and so on 😊

# ANDROID 7. REPACK APK TO BYPASS A SYSTEM-WIDE ANTI-MITM TECHNOLOGY

Google introduced on Android 7.0 new network security enhancements. Those new enhancements prevents 3rd party to listen to network requests coming out of the app. More info:

- 1) <https://developer.android.com/training/articles/security-config.html>
- 2) <http://android-developers.blogspot.com/2016/07/changes-to-trusted-certificate.html>

This script injects into the APK network security exceptions that allow 3rd party softwares, like Charles Proxy / Fiddler to listen to the network requests and responses of the app.

Download the script and the xml file and place them in the same directory. You will need apktool and android sdk installed. I recommend using brew on Mac to install apktool (brew install apktool)

The script take 2 arguments:

- 1) Apk file path. 2) keystore file path (optional - Default is: `~/.android/debug.keystore` )

## Examples

```
./addSecurityExceptions.sh myApp.apk ./addSecurityExceptions.sh  
myApp.apk ~/.android/debug.keystore
```

<https://github.com/levyitay/AddSecurityExceptionAndroid>

```
<?xml version="1.0" encoding="utf-8"?>  
<network-security-config>  
  <base-config>  
    <trust-anchors>  
      <certificates src="..." />  
      ...  
    </trust-anchors>  
  </base-config>  
  
  <domain-config>  
    <domain>android.com</domain>  
    ...  
    <trust-anchors>  
      <certificates src="..." />  
      ...  
    </trust-anchors>  
    <pin-set>  
      <pin digest="...">...</pin>  
      ...  
    </pin-set>  
  </domain-config>  
  ...  
  <debug-overrides>  
    <trust-anchors>  
      <certificates src="..." />  
      ...  
    </trust-anchors>  
  </debug-overrides>  
</network-security-config>
```

# iOS MASQUE ATTACK WEAPONIZED: A REAL WORLD LOOK

FireEye has recently uncovered **11 iOS apps within the Hacking Team's arsenals** that utilize Masque Attacks, marking the first instance of targeted iOS malware being used **against non-jailbroken iOS devices**.

These apps are reverse engineered and weaponized versions of popular social networking and messaging apps, including: **WhatsApp, Twitter, Facebook, Facebook Messenger, WeChat, Google Chrome, Viber, Blackberry Messenger, Skype, Telegram, and VK**.

**Unlike the normal versions of these apps**, they come with an **extra binary designed to exfiltrate sensitive data and communicate with a remote server**. Because all the bundle identifiers are the same as the genuine apps on App Store, they can directly replace the genuine apps **on iOS devices prior 8.1.3**.

[https://www.fireeye.com/blog/threat-research/2015/08/ios\\_masque\\_attackwe.html](https://www.fireeye.com/blog/threat-research/2015/08/ios_masque_attackwe.html)

# AN EXAMPLE OF THE RUNTIME BEHAVIOR OF THE REPACKAGED FACEBOOK APP



Fig. 5: Runtime behaviors of the repackaged Facebook app

[https://www.fireeye.com/blog/threat-research/2015/08/ios\\_masque\\_attackwe.html](https://www.fireeye.com/blog/threat-research/2015/08/ios_masque_attackwe.html)



# UPDATES DON'T WORK!

MOBOMARKET (ANDROID APP STORE), BEST ONE IN CHINA & INDIA

○ App v2

○ **SSL worked but MITM was possible (preinstalled cert?)**

○ Privacy Policy

“We encrypt our services and data transmission using SSL”

“You’re responsible for privacy”. Just do it yourself

On March, 2016

Slide #48, <http://goo.gl/wPfmqM>

○ App v3

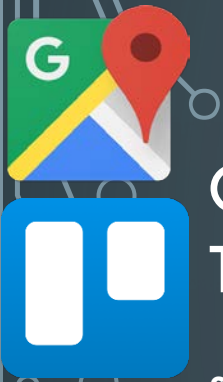
○ **Everything is in plaintext by HTTP, even app installers (APK)**

○ Privacy Policy

We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information, username, password, transaction information & data stored on Site

Official Website <http://goo.gl/FYOXiE>





# GOOGLE MAPS TRELLO



SSL Pinned to Not Pinned (MITM is available by crafted certificate)

Google Maps: ~24-31 data items per each application for iOS & Android

Address Data (what you're typing in search field)

Other items are still MITMed with crafted certificate

Trello: ~25 data items per each application for iOS & Android

'Credentials Info' Group: Credentials (IDs, Password)

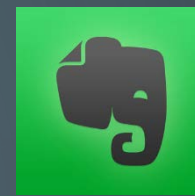
'Account Info' Group: Account Data, Media Data (Profile Images)

'Tasks Info' Group: Tasks, Sync Docs, Doc List, URLs

'Contact Info' Group: Contact Short Profile + Media (Profile Images)



# UPDATES DON'T WORK!



eFax – weird SSL Pinning

Evernote – downgraded from Pinning

Evernote for Android (March, 2017)

– Pinned everything

○ Before Summer/Autumn 2016

eFax

Media Data (faxes) are PINNED, but

Media URL of faxes, Credentials & rest data are MITMed (Cert)

Evernote

Everything is PINNED, except Social credentials of LinkedIn

Locally stored data

Accessible via iTunes incl. all DBs

○ Since Autumn 2016

eFax

MITM with preinstalled/crafted/stolen CERT

Applies to all data items

Evernote

Everything is MITMed with preinstalled/crafted/stolen CERT

Location data is not protected

Documents & Location Info: GEO Data & Address Data

○ Since March 2017

eFax

MITM with preinstalled/crafted/stolen CERT

Applies to all data items

Evernote (Android only)

Everything Pinned

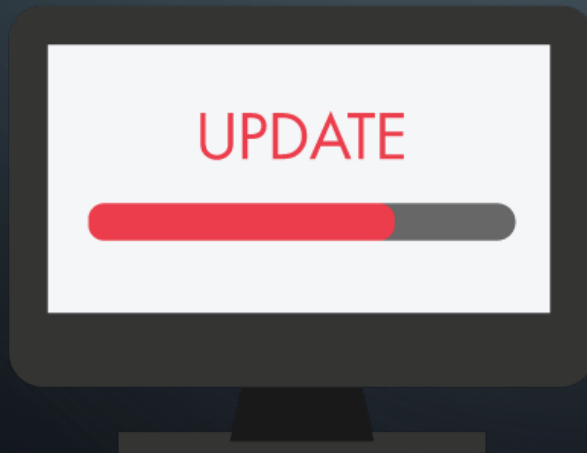
Location data is Pinned (Android)

Documents & Location Info: GEO Data & Address Data

# UPDATES. IT WORKS!

**UNBELIEVABLE**

- OS updates / Vendors (Apple, Google, Asus, HTC,...)
- App updates
- Updates fix the issues sometimes
- But keep an eye on a vendor activity





# FIX TAXI

## iOS

**Data-in-Transit: No SSL Validation  
(Weak Protection) on March 30th**

**Geo data requires a CERT on April 20<sup>th</sup>**

'Geolocation Info' Group: Geo, Address Data, Place Details, Favourites  
Addresses

'Account Info' Group: Account Details

'Credentials Info' Group: Credentials (IDs, Tokens, Activations IDs)

'Financial Info' Group: Card Short Info (no CVC/CVV), Favourites Cards

'Browser Info' Group: Card Full Info (with CVC/CVV)

'Orders Info' Group: Orders Details & History

## ANDROID

**Data-in-Transit: Plaintext (No  
Protection)**



**FIXED**

# VKONTAKTE – iPHONE, iPAD, ANDROID



## VK for iPhone/Android

- on fly MITM (no preinstalled cert need)
- HTTPS was turned off by default, everything except credentials were transferred by HTTP
- Updated in Autumn – now preinstalled cert is needed to MITM

## VK for iPad (last update 2016 Sept 14<sup>th</sup>)

- on fly MITM (no preinstalled cert need), https was turned off by default

June 5<sup>th</sup>, 2016

VK DBs records for just 1 Bitcoin  
(approx. US\$580)

VK.com HACKED! 100 Million Clear  
Text Passwords Leaked Online

<http://thehackernews.com/2016/06/vk-com-data-breach.html>



# FOURSQUARE & SWARM APPS

iOS got fixes, Android didn't

~30-40 data items per each application

## Foursquare - Non-protected Media Data

- 'Account Info' Group: Media Data (Profile Images) – iOS & Android not fixed
- 'Media Info' Group: Place Details (Place & Building photos) – Android, iOS fixed
- 'Geolocation Info' Group: Place Details (Place & Building textual) – Android, iOS fixed
- 'Geolocation Info' Group: Media Data (City photos) – Android, iOS fixed

## Swarm - Non-protected Media Data

- 'Account Info' Group: Media Data (Profile Images) - Android, iOS fixed
- 'Contacts Info' Group: Media Data (Friends' Profile Images) – Android, iOS fixed
- 'Media Info' Group: Place Details (Place and Building photos) – Android, iOS fixed



# PLAZIUS

Random fixes

~20-25 data items per each application

All Data Affected

'Geolocation Info' Group: Geo data

'Credentials Info' Group: Credentials (ID, Activation IDs, Tokens)

'Loyalty Info' Group: Credentials (ID, Activation IDs, Tokens), Geo Data, Place Details, Order, Buyer's Check

'Account Info' Group: Account Details

'Payment Info' Group: Card Short Number, Card Full Information

Apps written for iOS < 10 **DO NOT HAVE** a SSL validation

Apps written for iOS 10+ only got fixes (MITM with crafted certificate still works)

Android Apps **HAVE** a SSL Pinning





# INSTAGRAM: “LONG ROAD TO SECURITY” FROM INSECURITY TO SECURITY THOUGHT THE SECURITY & INSECURITY



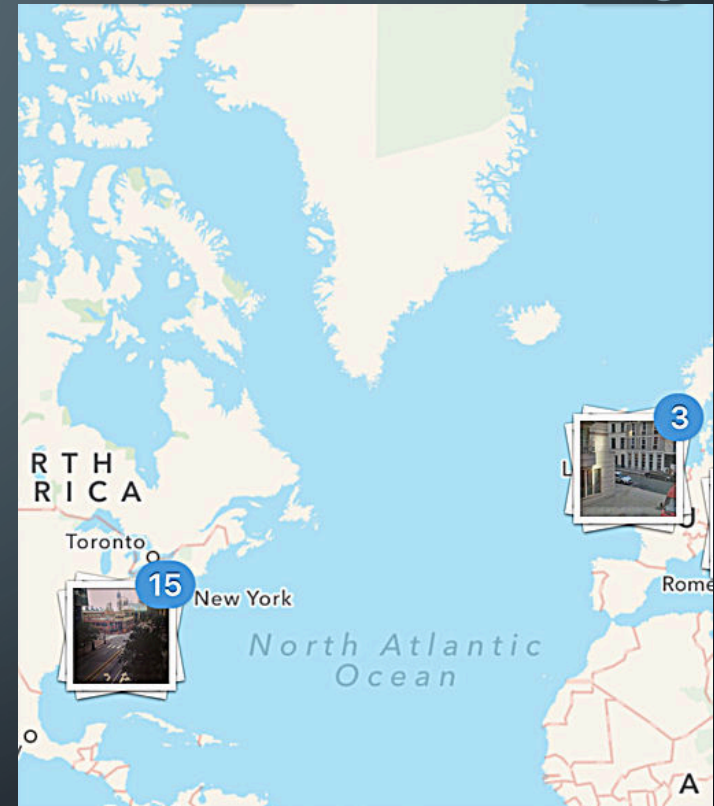
Metadata is usually technical data that is associated with User Content. For example, Metadata can describe how, when and by whom a piece of User Content was collected and how that content is formatted.

Users can add or may have Metadata added including

- a hashtag (e.g., to mark keywords when you post a photo),
- geotag (e.g., to mark your location to a photo), comments or other data.
- It becomes searchable by meta if photo is made public

Details: (1), (2)

<https://goo.gl/1lxKUg> <https://goo.gl/LPh07C>



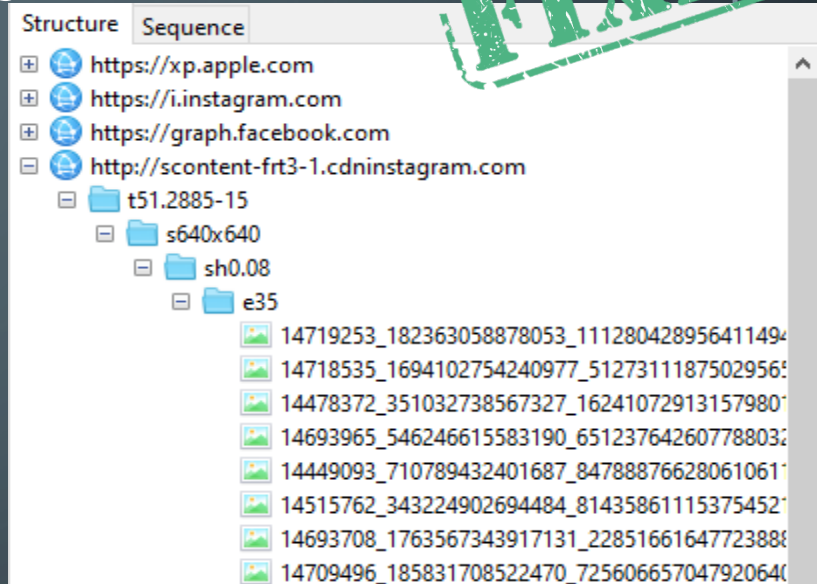




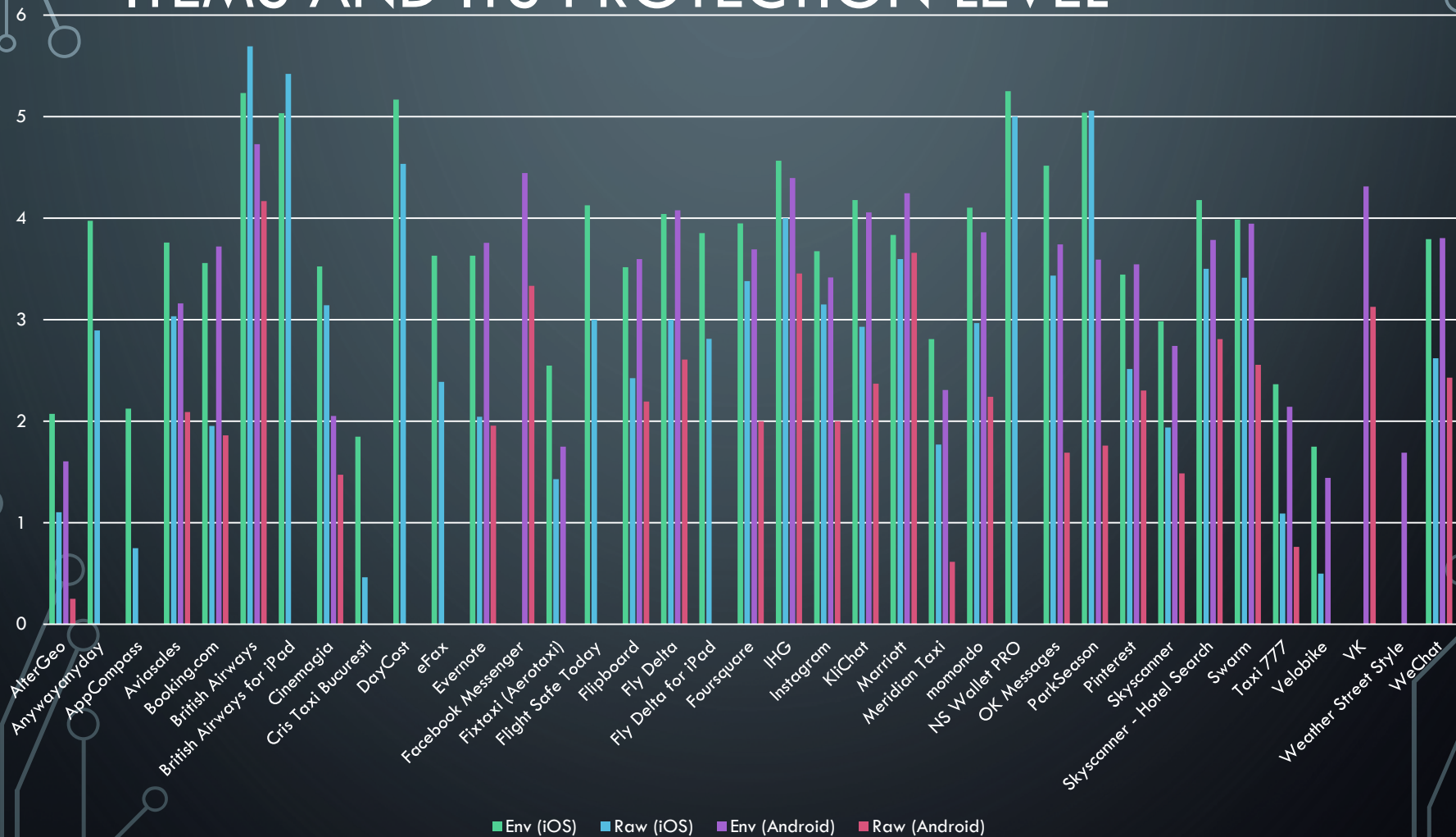
# INSTAGRAM: “LONG ROAD TO SECURITY” FROM INSECURITY TO SECURITY THOUGHT THE SECURITY & INSECURITY



- Media Data includes Advertisement, Profile images, your photos and so on...
- Y2014:** Media data transferred as is **without protection**; hosted on AWS S3
  - Instagram said it's moving to encrypted communications for its images by moving to HTTPS, the secure version of the standard used to transfer Web data over the Internet.
- Y2015:** Media data transferred **over HTTPS** and hosted on Amazon Storage Service (AWS S3); **Crafted cert to MITM needed**
- Y2016:** Media data transferred as is **without protection** and hosted on own Instagram storages
- Y2017 - iOS:** Media data transferred **over HTTPS**; **Crafted cert to MITM needed**
- Y2017 - Android:** Media data transferred as is **without protection**; the rest data is SSL PINNED



# APPS WITH WORST PROTECTED DATA ITEMS AND ITS PROTECTION LEVEL



# APPS WITH WORST PROTECTED DATA ITEMS AND ITS PROTECTION LEVEL

Many of applications reveal something in plaintext 8 groups, 16 data items, 30 pairs of group + data items

- Account Information: Account Details, GEO & Address
- Contact Information: GEO + Profile + Social + Media URLs + Place Details + Stream
- Analytics 'n' Ads Information: Device Data & Environment
- Credentials Information: Credentials IDs & Passwords
- Events Information: Stream
- Location 'n' Maps Information: GEO & Address, Media Data, Messages, Place Details
- Loyalty Information: Account Data, GEO & Address, Place Details
- Media Information: Place Details

## ISSUE:

# SAME DATA ITEMS, DIFFERENT PROTECTION LEVEL

Same data items (one password, card data, passport, etc. over several apps)

Different protection level of these apps means the worst one burns your security down

'Account Info' Group: Account Data, Account Details

'Application Info' Group: URLs (URL to binary installer files)

'Browser Info' Group: Card Full Info (with CVC/CVV)

'Credentials Info' Group: Credentials (Tokens, IDs, Password, Activations IDs)

'Financial Info' Group: Card Short Info (no CVC/CVV), Favourites Cards

'Geolocation Info' Group: Geo, Address Data, Place Details, Favourites Addresses, Media

'Orders Info' Group: Orders Details & History

'Travel Info' Group: Geo, Address Data, Trips Info

'Social Info' Group: Account Data, Credentials (Tokens, IDs, Password), Device Environment

# CONCLUSIONS

- App designed in compliance to Apple and Google Security Guidelines means the minimal level of protection if it is done in a right way
- There is nothing alike data leakage beside vulnerabilities. OWASP strongly disagree
- I believe my app has a good protection. Okay, don't forget to check it on the forensics web-site 😊
- Privacy Policy and other statement about security don't guarantee anything
- It works only with root/jailbreak.
  - There are backup copies that keep a plenty awesome data inside itself
  - Tell that to forensics teams and check it on the forensics web-site again 😊
- Crafted SSL certificate to perform MITM is not a global issue. What about stolen, revoked and government root certificates then?
- Android 7 prevents MITM attacks. Yes, but only in align to other requirements (No alternative AppMarket, No Repackaged Apps, No Root, No Any Apps from Unknown sources)
- Next update is going to bring fixes?** No, it is possible to get worse protected release even
  - But we keep an eye on new releases**
- Many apps are not good protected, should I ignore it? No, keep an eye on security update news

# SOLUTIONS: FOR DEVELOPERS

- Secure Mobile Development Guide *by NowSecure*

- Coding Practices
- Handling Sensitive Data
- iOS & Android Tips
- etc.

<https://books.nowsecure.com/secure-mobile-development/en/index.html>

# RESEARCHES TO READ

2014

Included ~200 apps results, for Cross OS apps provide - *protection concepts, OS specifics per concept, outlines & remediation, EMM specifics*

**“We know Twitter & Dropbox are better secured than bank apps!”**

<http://www.slideshare.net/EC-Council/hh-yury-chemerkin>

[http://defcamp.ro/dc14/Yury\\_Chemerkin.pdf](http://defcamp.ro/dc14/Yury_Chemerkin.pdf)

2015

Current Research ~700 apps (iOS, Android, BlackBerry, Windows, Mac OS apps)  
+ Bonus – Security & Privacy Project (demo)

<http://def.camp/wp->

[content/uploads/dc2015/Chemerkin\\_Yury\\_DefCamp\\_2015.pdf](http://def.camp/wp-content/uploads/dc2015/Chemerkin_Yury_DefCamp_2015.pdf)

2016

Refined by iOS and Android Only

+ Bonus – Report + Security Project (beta)

[https://def.camp/wp-content/uploads/dc2016/Day%202/Yury\\_Chemerkin.pdf](https://def.camp/wp-content/uploads/dc2016/Day%202/Yury_Chemerkin.pdf)



# БЕЗОПАСНОСТЬ ДАННЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ. МИФЫ И РЕАЛЬНОСТЬ



**YURY CHEMERKIN**

SEND A MAIL TO: [YURY.S@CHEMERKIN.COM](mailto:YURY.S@CHEMERKIN.COM)

**HOW TO CONTACT ME ?**



**ADD ME IN LINKEDIN:**

[HTTPS://WWW.LINKEDIN.COM/IN/YURYCHEMERKIN](https://www.linkedin.com/in/yurycchemerkin)