



RISKWARE BETRAYER

WHO IS THE BIGGEST ONE?

YURY CHERMERKIN

MULTI-SKILLED SECURITY EXPERT

INTRO: RISKY MOBILE APPS



- Mobile applications store data locally and transfer it over networks (at least)
- Data - not only binary protected or non-protected. Quality of protection matters
- Reverse engineering gives an answer how it works and is protected (slowly)
- Pentesting the data protection gives an answer 'what happened' and 'why' (faster)
- Developers never tell and never admit they fail but they does
- Privacy Policy might be pure, high detailed or misleading even
- 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

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

- **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](https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10)

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]

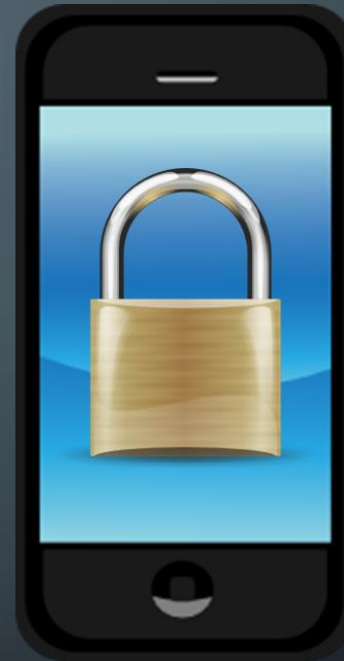
- ✓ Sensitive data should always be stored encrypted so that attackers cannot simply retrieve this data off the file system, especially on removable disk like micro SD card **or public folders (out of scope of CWE-312)** such as
 - banking and payment system PIN numbers, credit card numbers, or online 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**

SOLUTIONS

- PrivacyMeter (will talk a bit later)
- Vulnerability databases
- Security scanners
- Forensics software
- Privacy Policy



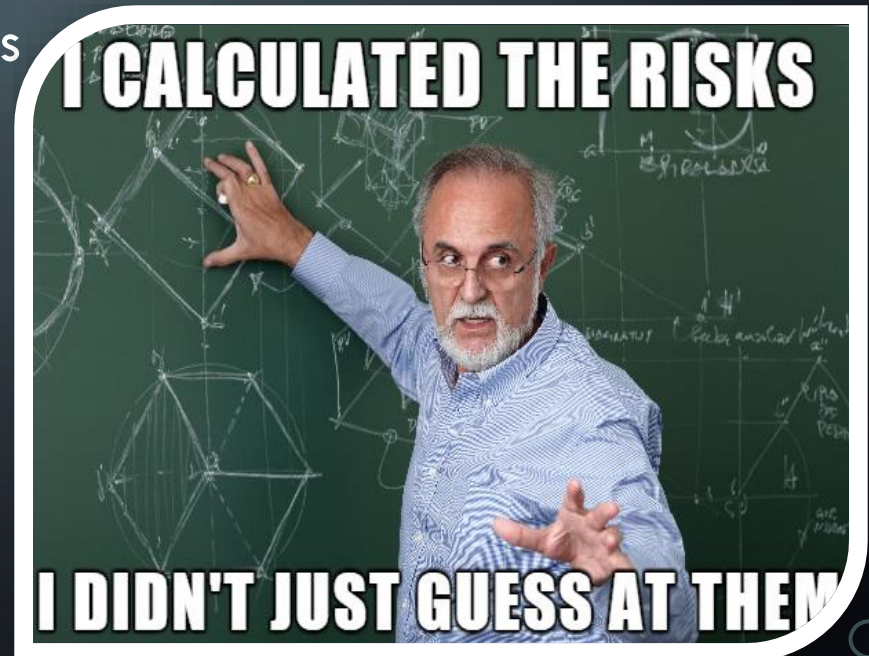
SOLUTIONS. VULNERABILITY DBs

- CVE, CWE, CVSS, NVD, and so on...
- Put 100 vulns into the report – be ready to prove it works
- Vulnerabilities are everywhere



SOLUTIONS. SECURITY SCANNERS

- Incorporated into EMM, MDM, MAM solutions
- Pure & High detailed at the same time
- Based mainly on auto-scanners
- Based on idea
 - | API/System Calls \leftrightarrow Data Item
 - | That \neq any info how's protected
- Built like a checklist 'be up-to-date'



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.

SOLUTIONS. PRIVACY POLICY

Privacy Policy is a 'longread' doc filled by scaring buzzphrases like:

- We request all permissions & information we need
- Do not guarantee the confidentiality of information and data
- Participant is obliged to observe safety measures & care security
- Under no circumstances be liable of business interruption, loss of business, or other data or information ...
- Certified by PCI DSS... and use SSL
- Everything is 100% protected because of SSL
- Keep yourself inform about security.. by yourself



SOLUTIONS. SUMMARY

- ✗ • Vuln. DBs make sense for known vulnerabilities. Vuln. Scanner is like
 - ✗ • 1st day: “Device is not checked yet! Check now! Congrats – 100% Secure”
 - ✗ • 2nd day: “Oops, device is 50% protected”. Wait for developer’s update
 - ✗ • ... 364th day: “Finally, updated. Now 86% protected”. Another app is bad. Wait for update
- ✗ • Security Scanner is mainly based on app code scanner. Lack of useful details
 - ✗ • “This application has vulnerabilities”. See a section above (Vuln. DBs)
 - ? • “This application has a HTTP”. It’s bad app!
 - ? • “This application encrypt your traffic”. It’s good app!
 - ✗ • “This application request your Device ID, IMEI,... and ACCESS to FILE SYSTEM”
 - ✗ • Very detailed about device & lack of details about files? **This is API ← → DATA**
 - ✓ • “Device is jailbroken/rooted”. Don’t do that! Fix it!
 - ✓ • “Malware detected”. Remove it!

PANDA SM MANAGER IOS APP - MITM SSL CERTIFICATE VULNERABILITY

IT TOOK 6 MINOR RELEASES & 8 MONTHES TO FIX 'MITM' ISSUE

- **"Panda Systems Management is the new way to manage and monitor IT systems."**

Issue

The Panda SM Manager iOS application (version 2.0.10 and below) does not validate the SSL certificate it receives when connecting to a secure site.

<http://osdir.com/ml/bugtraq.security/2016-03/msg00018.html>

Impact

An attacker who can perform a man in the middle attack may present a bogus SSL certificate which the application will accept silently.

Usernames, passwords and sensitive information could be captured by an attacker without the user's knowledge.

Solution

Upgrade to version 2.6.0 or later

Timeline

July 19, 2015 - Notified Panda Security via security@xxxx, e-mail bounced

July 20, 2015 - Resent vulnerability report to corporatesupport@xxxx & security@xxxx

July 20, 2015 - Panda Security responded stating they will investigate

July 31, 2015 - Asked for an update on their investigation

August 3, 2015 - Panda Security responded stating that the issue has been escalated and is still being reviewed

August 14, 2015 - Asked for an update on their investigation

October 16, 2015 - Asked for an update on their investigation

March 1, 2016 - Panda Security released version 2.6.0 which resolves this vulnerability

ANSWERS ARE LOOKING FOR?

What questions are usually asked by customers when they see a security report?

Which security holes are important and may lead to the leakage?

What data may leak through the particular hole?

Do updates help? And when it will be fixed?

At a customer level:

Does app need access to emails in address book, or handles & display names?

Does browser process need access to the home directory, or just downloads directory?

What does media player need write access to?

Does any solution answer any questions? Not really.



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>

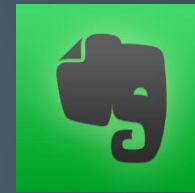
○ App v3

○ **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>



UPDATES DON'T WORK!

eFax – weird SSL Pinning

○ 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

Evernote – downgraded from Pinning

○ 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

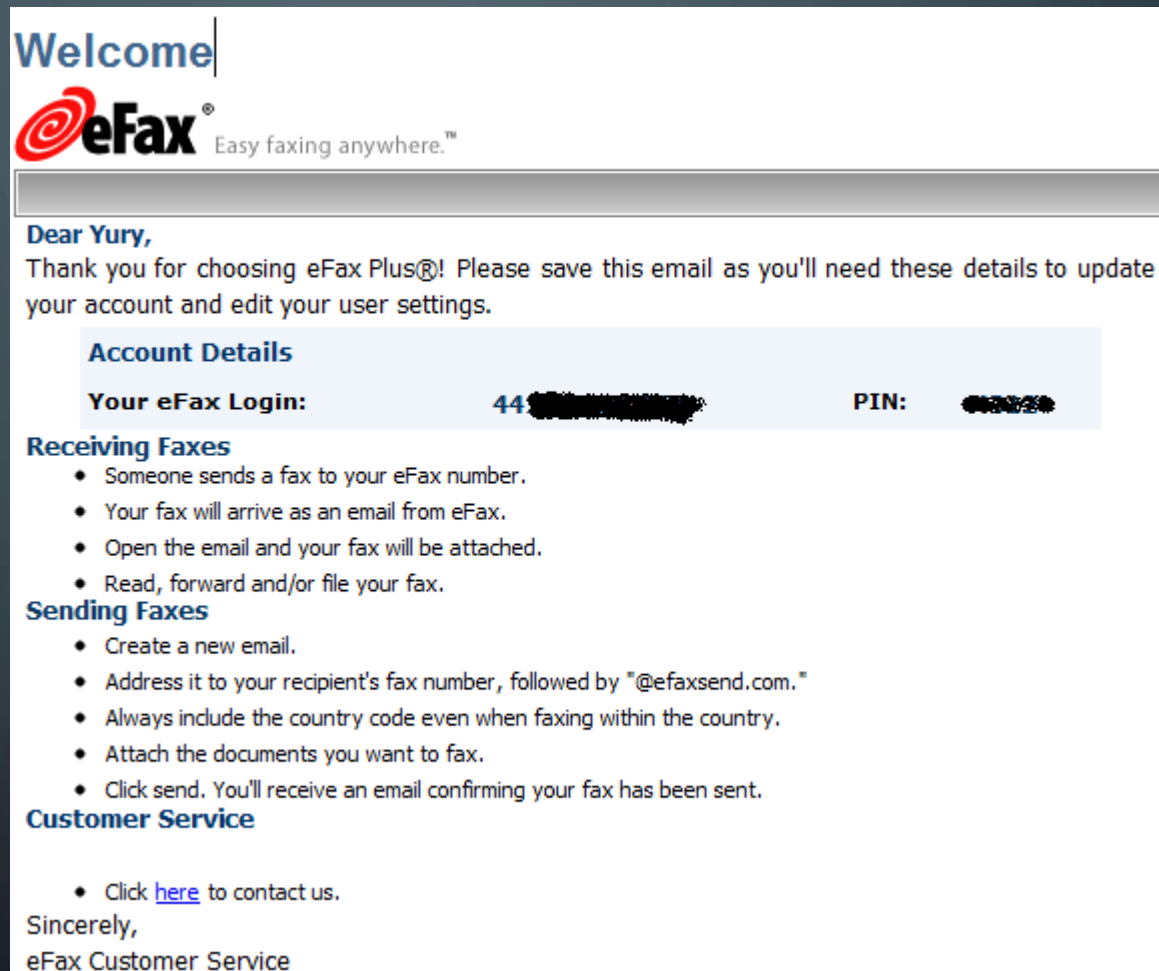
Documents & Location Info: GEO
Data & Address Data

COMPLEX DATA LEAKAGE


Don't trust email applications?

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

Here we go!

A screenshot of a welcome email from eFax. The email is addressed to 'Yury' and thanks them for choosing eFax Plus. It provides account details, including a login ID of '44' and a PIN, both of which are redacted with black boxes. The email also includes instructions for receiving and sending faxes, and a link to contact customer service.

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

Your eFax Login:	44 [REDACTED]	PIN:	[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

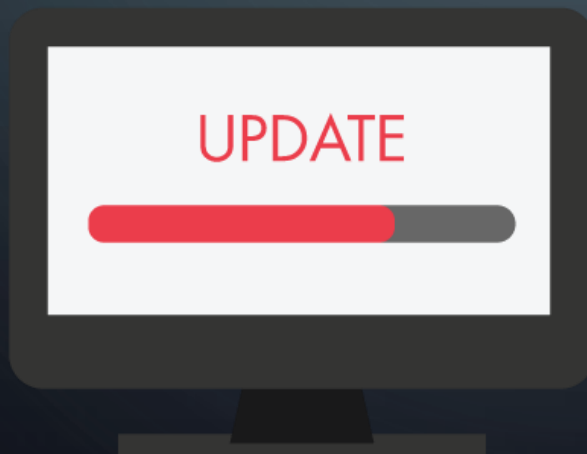
- Click [here](#) to contact us.

Sincerely,
eFax Customer Service

UPDATES. IT WORKS!



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



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 need to MITM

VK for iPad

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

June 5th, 2016

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

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

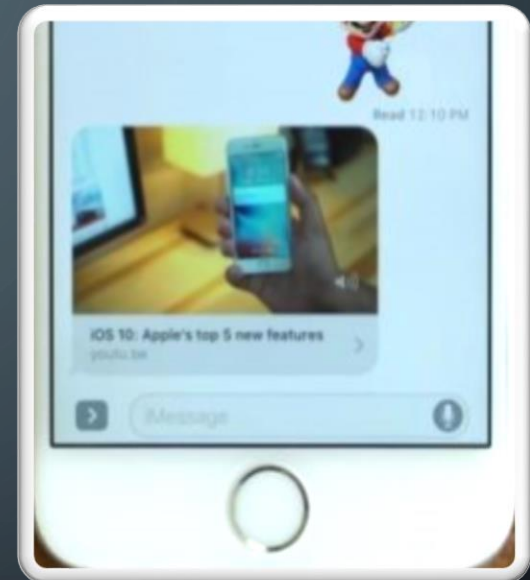
<http://thehackernews.com/2016/06/vk-com-data-breach.html>

Apple iMessage EXPOSES USER IP ADDRESS AND DEVICE DETAILS

FIXED

- When the user opens iMessage to see the message, even if he never clicks the link and accesses it, iMessage would connect to the URL automatically, and retrieve the necessary preview data plus user's IP address, OS version, and device details.
- Preview & device data issue is not iMessage only issue.
- Preview, device data and media have a weaker protection issue is also known for many mobile apps even if the rest data is good protected

<http://news.softpedia.com/news/apple-s-imessage-exposes-user-ip-address-and-device-details-to-spammers-508948.shtml>



APP IN THE AIR

Flight manager & notification app:

- In-App, SMS, stats, history, so on

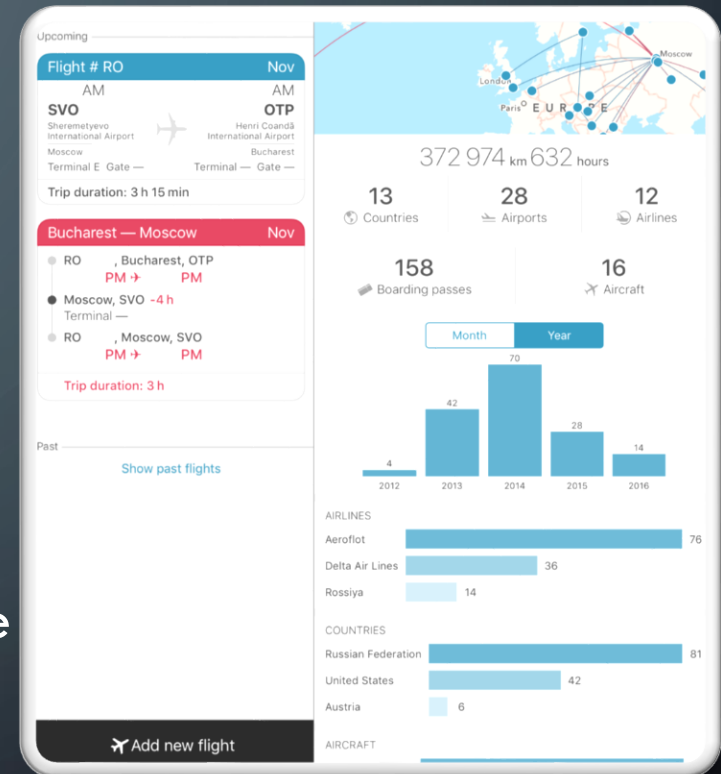
Y2014: HTTP

- Simple notification app

Y2015+: HTTPS

- Fake/Crafted/Preinstalled certificate to perform MITM

FIXED



INSTAGRAM: FROM INSECURITY TO INSECURITY THOUGHT THE SECURITY

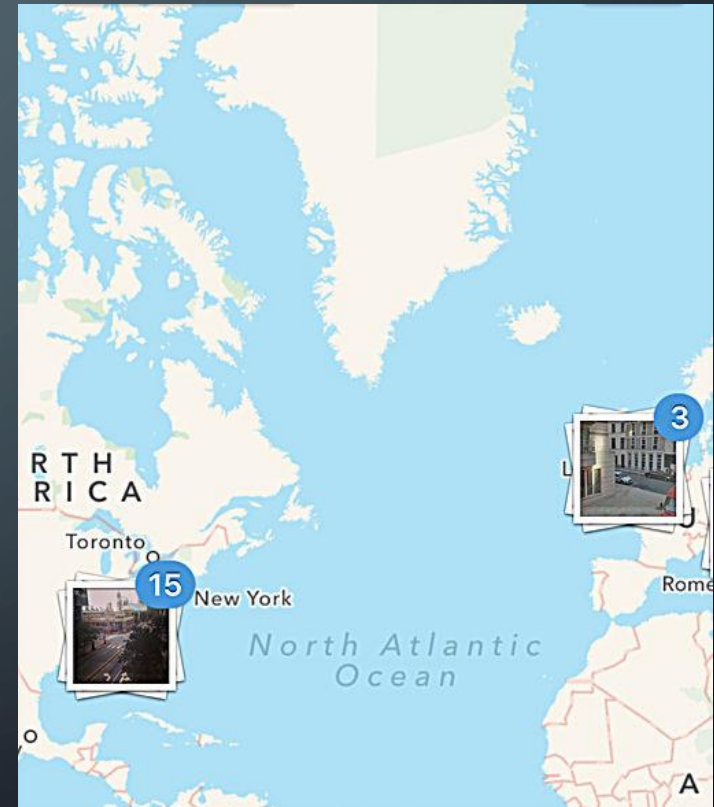
Metadata is usually technical data that is associated with User Content. For example, Metadata can describe how, when and by whom a piece of User Content was collected and how that content is formatted.

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

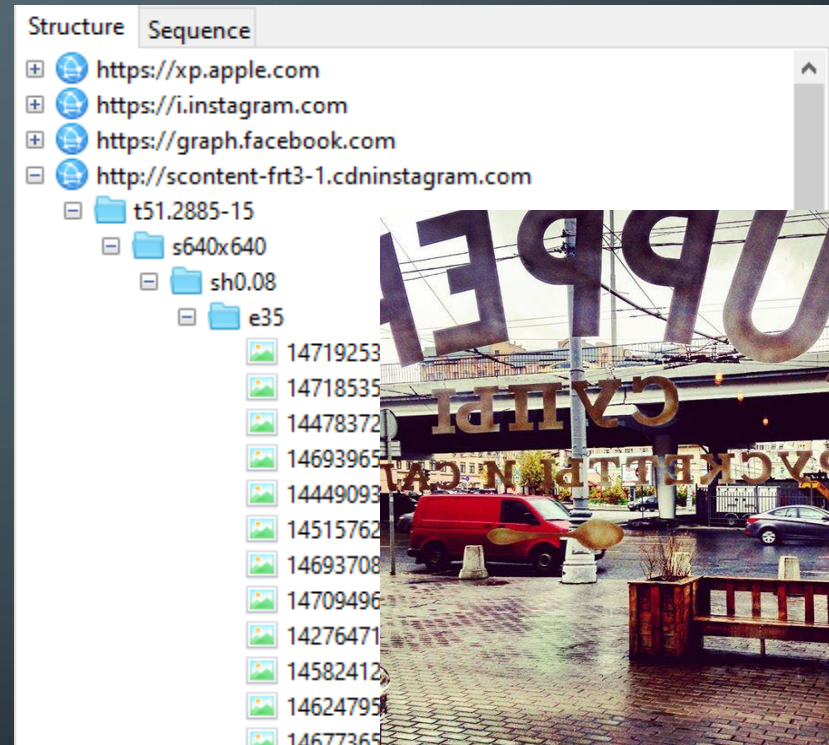
Details: (1), (2)

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



INSTAGRAM: FROM INSECURITY TO INSECURITY THOUGHT THE SECURITY

- **Media Data** incl. Advertisement and Profile images
- **Y2014:** Media data transferred as is **without protection** and hosted on Amazon Storage Service (AWS S3)
- **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



PureVPN iOS V.1.0.2

PureVPN ANDROID V.5.4.0



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

CYBERGHOST iOS V.6.4

CYBERGHOST ANDROID V.5.5.1.7



License information, 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

iOS vs. ANDROID: CINEMAGIA 3.9.3 vs. 5.0.9 – Sept 2016



- iOS – MITM with preinstalled cert
- Android – Mainly w/o protection

Account Info

Booking 'n' Purchases Info

Credentials Info

Device Info

Location 'n' Maps Info

Payment 'n' Transaction Info

Social Info

Account Info

Booking 'n' Purchases Info

Credentials Info

Device Information

Location 'n' Maps Info

Payment 'n' Transaction Info

Social Info

https://secure.librapay.ro

Companie: cinemagia.ro (Imedia Plus Group SA)

Suma de plata: 28.00 RON

Numar card

5

Data expirare

04 Aprilie 2018

Nume posesor card

Yury Chemerkin

Cod securitate (CVV)

(ultimele 3 cifre de pe verso) 123

☒ Activeaza optiunea plati rapide.
Prin selectarea acestei optiuni vei beneficia de serviciul Wallet LibraPay care iti va permite sa efectuezi ulterior plati introducand doar codul de securitate CVV al cardului folosit. Vei primi mai multe detalii pe email.

Prin accesarea butonului "Plateste" esti de acord cu termenii si conditiile LibraPay.



GHOST PROJECTS: MOBILE APPS ALIVE, BUT NO CHANGES SINCE MAY Y2014

ALTERGEO iOS 4.6 / Android 3.13

AlterGeo is Russian clone of Foursquare & Swarm; nothing is protected except browser log-in, but not an in-app login

Account Information: Account Details, GEO & Address Data

Contact Information: Profile, Social, GEO, Stream, Place Details, Media URLs

Analytics 'n' Ads Information: Device Data & Environment

Browser Information: Credentials IDs, Passwords, Tokens

Credentials Information: Credentials IDs, Passwords, Tokens

Location Info: Messages, GEO & Address Data, Place Details, Media Data

Loyalty Information: GEO & Address Data + Place Details

Media Information: Place Details

Social Information: Media Data, Stream, Place Details + GEO Data

Out of backup file (rest is in backup)

Account Information: Address Data

Contact Information: Media Data

Location Info: GEO & Address Data, Place Details, Media Data

WEIRD PROJECTS: WEATHER STREET STYLE 1.8.6 ANDROID ONLY



Weather style is app to show what people wear at the moment in different countries. Everything in plaintext

Account Information

- | Account & Media Data
- | Address Data, Account Settings

Credentials Information

- | Credentials IDs + Passwords
- | Activation IDs + Tokens

Device Information:

- | Device Details

Location 'n' Maps Information:

- | GEO Data, GEO Snapshots

Social Information:

- | Contact Profile, Media Data, Messages

Weather Information:

- | Weather Data





IHG & MARRIOTT APPS WHEN ENCRYPTION DOESN'T MATTER

Everything is MITMed with crafted / stolen / preinstalled certificate

Account, Analytics, Application Info, Booking, Credentials, Device Information, Financial Information, Location, Log, Loyalty, Media, Payment 'n' Transaction, Personal 'n' Private and Travel Information

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

Limited access by a time (no longer 180 days)

Booking 'n' Purchases Information: Orders & Reservation History



FLOW & IFTTT

ABSOLUTE POWER OVER YOUR ACCOUNTS 😊

IFTTT & Flow are two apps to automatize any kind of activities with social networks or IoT

In this research were found over 8K data items

- 30 unique data groups

- 105 unique data items

- 462 unique pairs of data group & data item

In each app Flow and IFTTT were found

- 15 unique data group out of all 30 = 50%

- 52 unique data items out of all 105 = 50%

- ~150 unique pairs of data group & data item out of all 462 = 30%

Everything is MITMed with crafted / stolen / preinstalled certificate

- Account, Analytics, Browser, Credentials, Device Info, Events, Location,

- Media, Message, News, Social, Storage Info, Tasks, Weather, Workflow

Data includes everything to direct access, such as credentials/tokens, and data itself from linked services, such as Dropbox or mobile device GEO/network lists



WECHAT

HOW TO FAIL BEING AWESOME

Many Chinese apps might be with a lack of protection or overloaded with own protocols, encryption of data and code

Awesome protected (many security fails fixed by now), encrypted, own protocol:

- Account Information: Account Settings 'n' Configs

- Address Book 'n' Contact Information: Contact Profile

- Application Information: Application Configs

- Location 'n' Maps Information: GEO Data

- Message Information: Media Data, vCard, Messages, Short Profile

But Location data is still out of protection

- Location 'n' Maps Information: Contact Media

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



FACEBOOK & MESSENGER. DUPLICATE DATA, PREVIEW AND LOCATION FAILS

Application Information

Log Data

Credentials (Passwords)

Credentials (App Passwords)

Transaction History

Contact Short Profile

Credentials (IDs)

Card Full Information

Card Short Information

Credentials (Tokens)

Browser Information

Preview

Message Information

GEO Data

GEO Snapshots

Generate app passwords

Manage app passwords

Your app passwords

testtsetsetset
7 June 2016

Test#1
8 March 2012

Generate app passwords

Generate App Passwords

Login Approvals won't always work when you try to access Apps that you log into using Facebook, such as Xbox, Skype etc.

Type the name of an App you want to approve and we'll automatically generate a password for it:

Hjfiyjiyfiyfi (EX: iPhone, Skype)

Generate

Cancel

Structure Sequence

https://m.facebook.com

settings

account

?refid=31

?password&refid=70

?password&ts=1604002&_rdr

password

change

?refid=70

settings

Overview Request Response Summary Chart Notes

Name	Value
fb_dtsg	AQGFtdaRN0Xu:AQFjx3NK3BuD
charset_test	€,€,€,€,€,€
old_password	test old
new_password	test new
confirm_password	
change_password	
save	Change Password

https://m.facebook.com/password/change/?refid=70

EMAIL APPS – MESSAGES MIGHT BE PROTECTED

N#7 - Non-standard protocol

N#6 - Pinned cert

N#4 - Intercept/MITM with preinstalled/crafted cert

N#2 – MITM on fly without preinstalled trusted cert

L#6 – out of backup file

L#0 – in backup

Gmail – N#4, L#0 Account data & media URLs, Settings + profile, Rest L#6

Yandex.Mail – Messages N#6, rest N#4, App Configs & Account settings – L#0, Rest L#6

MailTime – Message & Sender Info – N#7, Rest N#4 (iOS) or N#6 (Android), L#0

Mail.Ru – N#4, L#6 – Creds, Message Attachs & Sender Info, rest L#0

MyMail – N#4, L#6 – Creds, Message Attachs & Sender Info, rest L#0

YahooMail – N#4, L#6 – Creds, AddressBook & Media, Log & App Events

Newton Mail (prev. CloudMagic) – N#4, L#0 – Creds & Device Data, rest L#6

MS Outlook – Credentials – N#4, rest N#7, Attach & Sync Docs – L#6, rest L#0

Alto – N#4, Creds - Config, Analytics, Logs, Creds, Attachs – L#6, rest L#0

TAXI APPS – EVEN PAYMENTS MIGHT NOT BE PROTECTED

N#6 - Pinned cert

N#0 – No Protection

N#5 – same as N#4 but pinning inform about weird cert

L#6 – out of backup file

N#4 - Intercept/MITM with preinstalled/crafted cert

L#0 – in backup

Meridian – Social Account, Geo & Creds N#4, rest N#0, L#0

Taxi 777 – Device & Environment Analytics N#4, rest N#0, L#0

Fixtaxi (Aerotaxi) – N#0, L#0

Gett (Gettaxi) – N#4, L#0

CleverTaxi – N#4, L#0

CrisTaxi – Social Account, Geo & Creds N#4, rest N#0, L#0

YandexTaxi – Activation Code N#6, Creds, Geo & Address - N#5,
rest – Bank Card, Orders, Favorites N#4, L#0

WALLET APPS – PROTECT SYNC DATA ONLY

N#8 – Encrypted

L#8 – out of backup file

N#6 - Pinned cert

L#6 – out of backup file

N#4 - Intercept/MITM with preinstalled/crafted cert

L#0 – in backup

NS Wallet (any edition) – Device Data N#4, In-App iOS Payment N#6, Creds Sync Data L#8, rest L#0

EnPass – Creds Sync Data N#8, rest incl. Creds N#4, Creds Sync Data L#8, rest L#0

Dashlane – Creds Sync Data N#8, rest incl. Creds, app config, logs... N#4, Creds Sync Data L#8, rest L#0

LastPass – Creds Sync Data N#8, rest incl. Creds, app config, device info... N#4, Creds Sync Data L#8, rest L#0

Sticky Password – Creds Sync Data N#8, rest incl. Creds, License Details N#4, Creds Sync Data L#8, rest L#0

1Password – Creds Sync Data N#8, rest incl. Creds, app config, device info... N#4, Creds Sync Data L#8, rest L#0

MEDIA AND LOCATION LEAKS. NO PROTECTION

- AlterGeo
- Aviasales
- Booking.com
- Cris Taxi Bucuresti
- Evernote
- Fixtaxi (Aerotaxi)
- Foursquare
- Instagram
- Marriott
- Meridian Taxi
- momondo
- Plazius
- Skyscanner
- Taxi 777
- Velobike
- VK for iPad
- Weather Street Style
- WeChat
- Account Data
- Address Data
- Contact Media
- GEO Data
- GEO Snapshots
- Maps Data
- Media Data
- Messages (Comment on
- Personalization
- Place Details
- Tracked Data 'n' Favourites



SENSITIVE DATA. NO PROTECTION



- Aeroexpress
- AlterGeo
- Anywayanyday
- AppCompass
- Aviasales
- Booking.com
- British Airways
- Cinemagia
- Cris Taxi Bucuresti
- Evernote
- Facebook
- Messenger
- Fixtaxi (Aerotaxi)
- Flipboard
- Fly Delta
- Foursquare
- IHG
- Instagram
- KliChat
- Lookout
- Marriott
- Meridian Taxi
- Microsoft Office
- momondo
- OK Messages
- Pinterest
- Plazius
- Skyscanner
- Swarm
- Taxi 777
- Velobike
- VK
- Weather Street Style
- WeChat
- Account Details
- Account Settings 'n' Configs
- Address Data
- Application Configs
- Card Full Information
- Contact GEO, Media, Profile
- Credentials (IDs, Passwords, Tokens)
- Device Details, Environment
- Messages
- Orders & Reservation
- Passport Data (Short)
- Personalization
- Place Details
- Preview
- Stream
- Tracked Data 'n' Favourites
- Travel Details

UNTRUSTED PLACES



- Untrusted chargeable places.
 - When you connect your device to them you will see a notification you plugged to PC/Mac
 - Or lost devices
- Untrusted network places.
 - When you connect your device to them
 - You will see nothing
 - You will see a question about untrusted certificate. You accept or decline it
 - Someone make you to install trusted certificate

EXTRACTING LOCAL DATA. EXAMPLES

- Oxygen Forensic® Detective introduces offline maps and new physical approach for Samsung Android devices!
- The updated version offers a new physical method for Samsung Android OS devices via custom forensic recovery. This innovative approach allows to bypass screen lock and extract a full physical image of supported Samsung devices.
- <http://www.oxygen-forensic.com/en/events/news/666-oxygen-forensic-detective-introduces-offline-maps-and-new-physical-approach-for-samsung-android-devices>

Cannot Verify Server Identity

The identity of "outlook.office365.com" cannot be verified by Exchange. Review the certificate details to continue.

Cancel

Details

Continue

← Look here
Prepaid WiFi Network

CED Solutions, LLC

A Salute To Our Veterans

Checking for Mail...

Cannot Verify Server Identity

The identity of "lk.beeline.ru" cannot be verified by Safari. Review the certificate details to continue.

Cancel

Details

Continue

← Look here
Free WiFi Network

Идентифицируясь, вы принимаете условия
оферты

Поддержка

Cancel

Certificate

Trust



1.1.1.1

Issued by 1.1.1.1

Not Trusted

Expires 21/04/25 03:00:01

More Details

SUBJECT ALTERNATIVE NAME

Critical

No

URI

https://1.1.1.1

IP Address

1.1.1.1

Certificate

Details

SUBJECT NAME

US

Country

Organization

Cisco Systems Inc.

Organizational Unit

DeviceSSL
(WebAuth)

Common Name

1.1.1.1

ISSUER NAME

Country

US

Organization

Cisco Systems Inc.

Organizational Unit

DeviceSSL

Cancel

Certificate

Trust



outlook.com

Issued by Charles Proxy Cust...

Not Trusted

Expires 13/10/17 01:20:04

More Details

Organizational Unit

<http://charlesproxy.com/ssl>

Organization

XK72 Ltd

Locality

Auckland

State/Province

Auckland

Country

NZ



Certificate

Details

SUBJECT NAME

Country

US

State/Province

WA

Locality

Redmond

Organization

Microsoft Corporation

Organizational Unit

Microsoft Corporation

Common Name

outlook.com

ISSUER NAME

Common Name

Charles Proxy

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/>

DATA PROTECTION CONCEPTS (DPC)

There are known many of them, some were renamed but still 3:

Data-at-Rest (DAR)

Locally stored data on internet or external storage. Data might divide into several parts, full data, backup data, and containerized data

Data-in-Transit (DIT)

Data transmitted over Internet and local wireless network (as part of solid internet connection) and limited by it

Data-in-Use (DIU)

Referred to data operated in internal memory (not storage) and application code, like hardcoded values

IMPLEMENTATION OF DPC. DATA-AT-REST



VS



- No special tools for viewing various data types
 - No root to gain an access backup data
 - No root to gain an access to internal storage to the application data folder (works only for iOS older than 8.3) CVE-2015-1087
 - Root to gain an access to internal storage to the keychain folder
 - Root to gain an access to internal storage to the application data folder (iOS 8.3 and higher)
 - Root to gain an access to internal storage in general
- No special tools for viewing various data types
 - Root to gain an access to internal storage.
 - No root to gain an access to external storage, public folders or backup data
 - Unlocking locked bootloader wipes all data on several devices, e.g. HTC
 - Non-locked or unlocked bootloader might give an opportunity to root a device, grab data or install malicious application and de-root it back, e.g. Samsung, LG (details, news, <http://www.oxygen-forensic.com/en/events/news>)

IMPLEMENTATION OF DPC. DATA-IN-TRANSIT



VS



- OS-level proxy
- no app-level alternative tunnels

- App-level proxy is an alternative internet access

Do not require a root for cases, such as

- non-protected traffic,
- no SSL validation except centralized list of certificates
- MITM possible - fake/crafted/stolen SSL certificate installed as trusted

Require root for cases, such as

- SSL Pinning to bypass it automatically or manually
- Rest cases that directly impacts on app code and mixed with DIU

QUANTIFICATION SECURITY LEVELS. DAR



VS



Protection N/A or Jailbroken iOS

Non-Protected

Protection N/A, rooted, public folders, SD cards

Encoded data (zlib, bas64, etc.)

Encode Protected

Encoded data (zlib, bas64, etc.)

App Data access w/o jailbreak iOS <8.3

Weak Protected

Not Defined

Not Defined

Obesity Protected

Not Defined

Data available via sharing, such as iTunes

Medium Protected

Not Defined

Access limited by time, e.g. cache folders

Iterim Protected

Access limited by time, e.g. cache folders

Not Defined

Good Protected

Sandbox, root/unlocking not wipe data

Sandboxed data, jailbreak needs & wipe data

Strong Protected

Sandboxed data, root needs & wipe data

No public tools for a jailbreak is available

Extra Protected

No public tools for a jailbreak is available

Not Defined

Best Protected

Not Defined

QUANTIFICATION SECURITY LEVELS. DIT



VS



Protection N/A, Jailbroken, crafted certificate

Non-Protected

Protection N/A, rooted, crafted certificate

Encoded data (zlib, bas64, etc.)

Encode Protected

Encoded data (zlib, bas64, etc.)

Stolen or expired certificates

Weak Protected

Stolen or expired certificates

Not Defined

Obesity Protected

Not defined

Basic feature of SSL validation of certificates

Medium Protected

Basic feature of SSL validation of certificates

Not defined

Iterim Protected

App-level proxy/tunnel for internet

Not defined

Good Protected

Not defined

Not defined

Strong Protected

Not defined

System and/or user VPN

Extra Protected

System and/or user VPN

Not Defined

Best Protected

Not defined

LIST OF SOFTWARE RELATED TO SECURITY CHECKS

Non-Protected

File Viewers

Encode Protected

Online services & tools for calculations

Weak Protected

Obesity Protected

Medium Protected

Iterim Protected

Network Debug & Pentest

Good Protected

Debuggers, Disassemblers, Decompilers, activity tracers, and pentest frameworks

Strong Protected

Extra Protected

File & Device Access

Forensics & special pentest solutions

Best Protected

No tools

Free or paid
\$100-300 or less

Free or Paid
Home ~\$100
Enterprise \$300+

\$5-10k+,
lightweight -
\$100-1k

No tools, if no data available

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>

SOLUTIONS: DATA PROTECTION DBs

- We [as security experts] know what data is protected and not protected despite of it's locally stored, transferred or hardcoded
- Also, we know two simple things
 - not only users publish their data
 - developers can't protect data
- At the same time we're customers, right?
 - I'm as a customer prefer and have a right to know where devices shouldn't be connected to network or plugged PC/Mac.
 - Developers aren't going to tell me if they fail. Instead they're telling 'everything is OK but they're not responsible for anything'

SOLUTIONS: DATA PROTECTION DBs

- Goal is providing a solution that helps to keep ‘everyone’ informed about app security fails.
- *Everyone* means
 - app users as well as app developers
 - you don’t need to be expert to understand that how it affects you; you just know if it has required level of protected or not
 - but you have to get used that your application operates many data visible and not visible for you beyond the blueberry muffins over the weekend

PrivacyMeter



Vulnerabilities matter but exist over 40 years

Vulnerability is a defect/ flaw in design in dev's code or third party libraries

Lack of data protection is usually an insecurity by design and implementation fails

Even OWASP considers data protection as more important thing than vulnerabilities by now

Lack of data protection is described by 3 vulnerabilities

- | sensitive data leakage, storage, transmission CWE-200, CWE-312, CWE-319

PrivacyMeter gives answer about (at the moment)

- | list of apps and average values (Raw value, Environment value depend on OS)

- | list of app data items grouped by 'protection levels/categories'

- | data item protection level and explanation

- | examination of privacy policy in regards to gained app results

Results are available on the web-site <http://www.privacymeter.online/> see booklets (!)

Download the Autumn Report <http://www.privacymeter.online/reports> see booklets (!)

APPS FINDINGS. OVERALL RESULTS

Business

Communication

Entertainment

Finance

Food & Drink

Lifestyle

Photo & Video

Music

Navigation

News & Magazines

Productivity

Shopping

Social Networking

Tools & Utilities

Transportation

Travel & Local

Weather

250 apps = 135 iOS apps + 115 Android apps

8124 data items = 4287 (iOS) + 3837 (Android)

20+ application groups (17 unique groups)

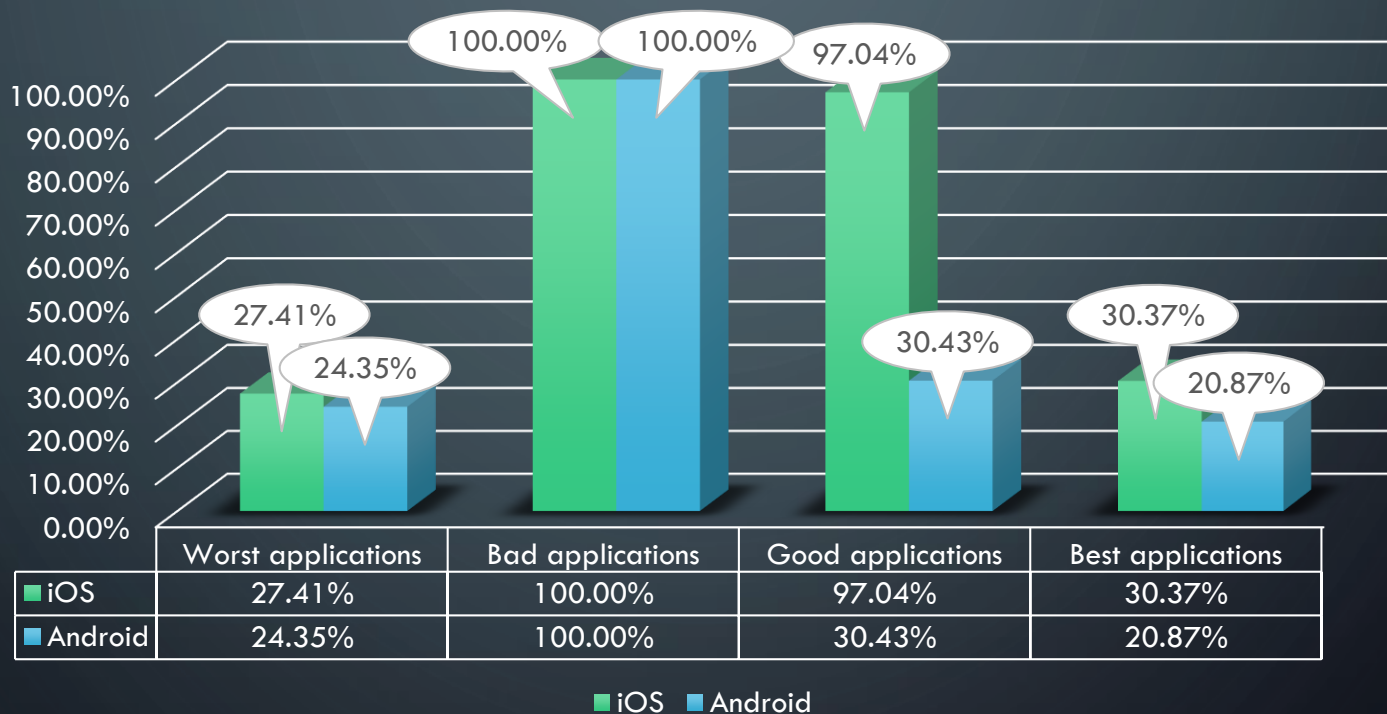
30 data groups & 105 data items over 8K data items

462 unique pairs of data group & data item

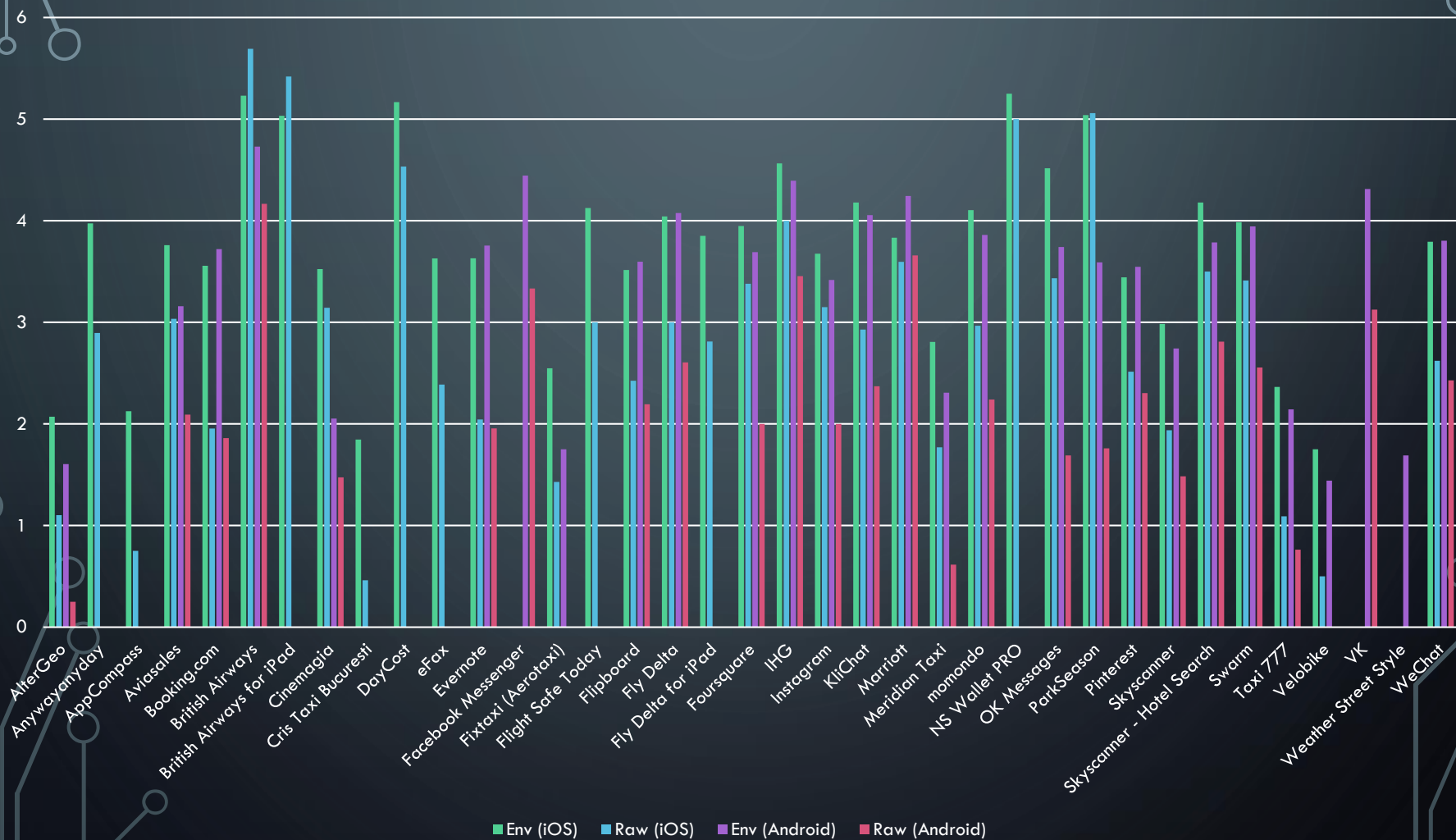
DATA GROUPS' AVERAGE PROTECTION LEVEL. iOS VS. ANDROID



QUANTITY OF APPS PER EACH GROUP



WORST PROTECTED ITEMS OVER APPS

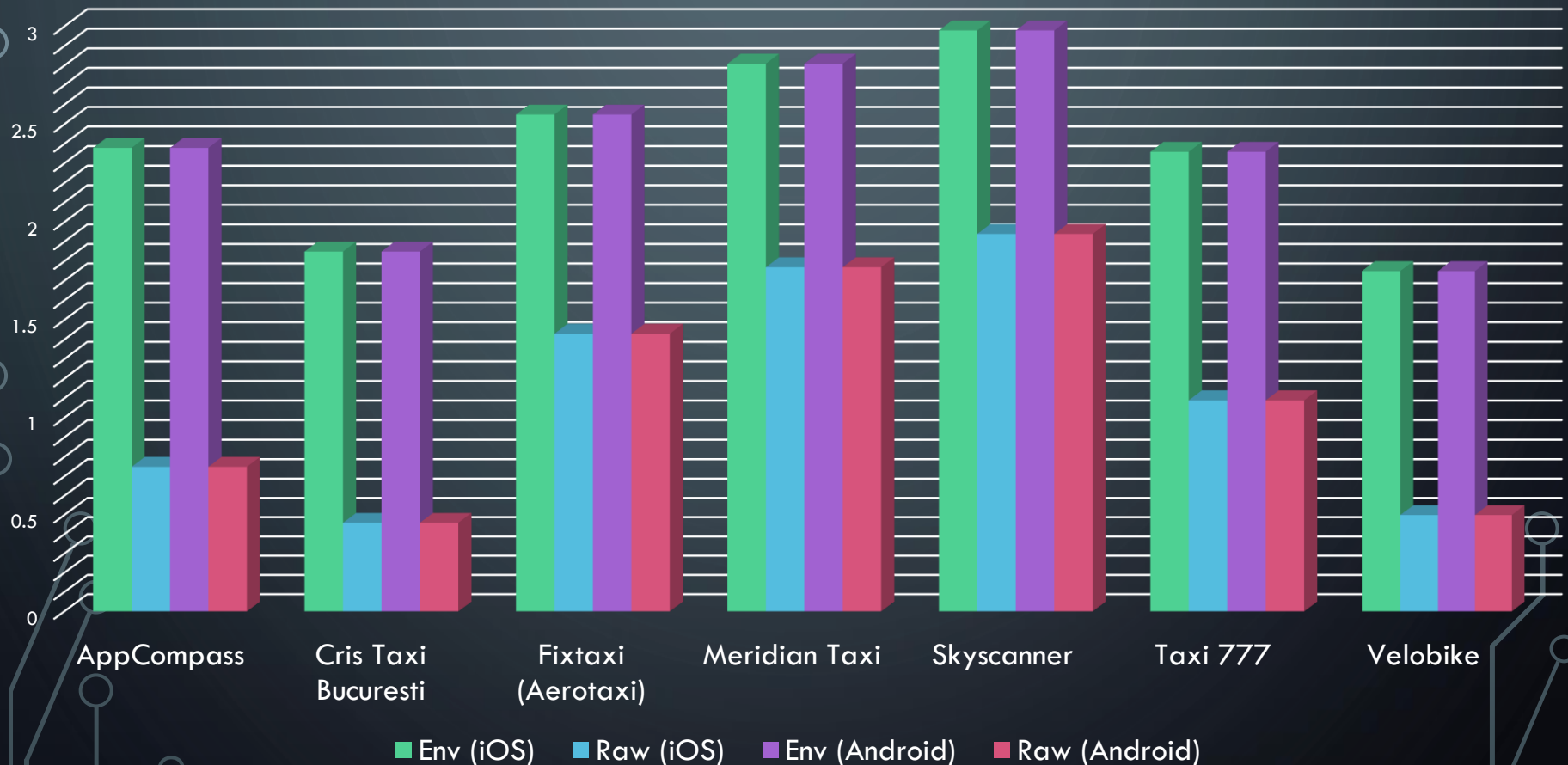


WORST PROTECTED ITEMS OVER APPS

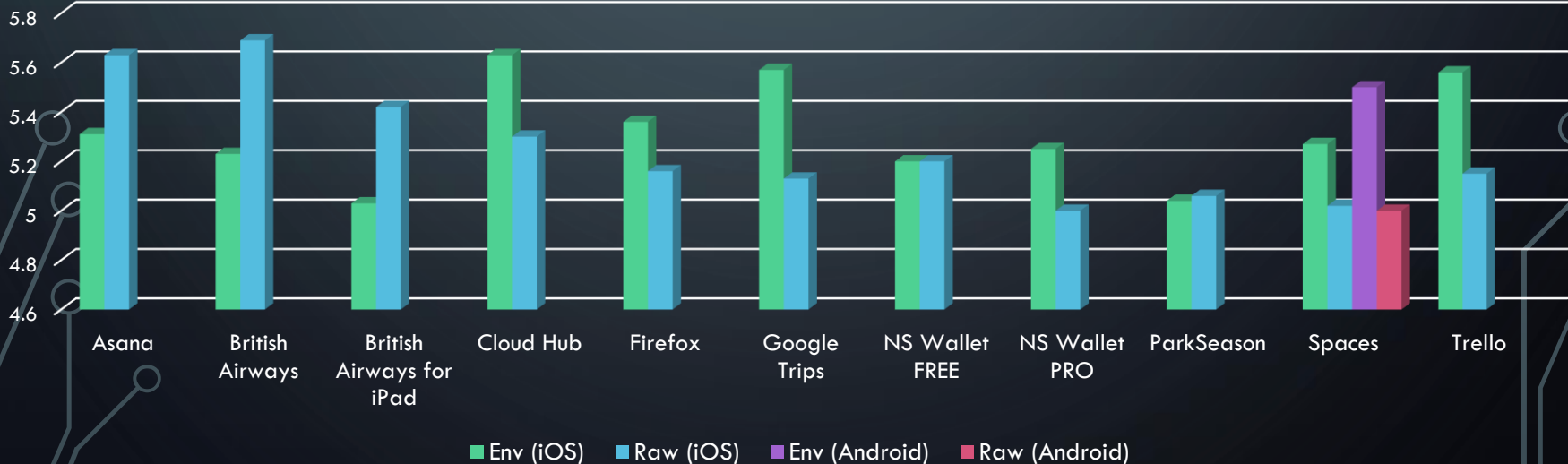
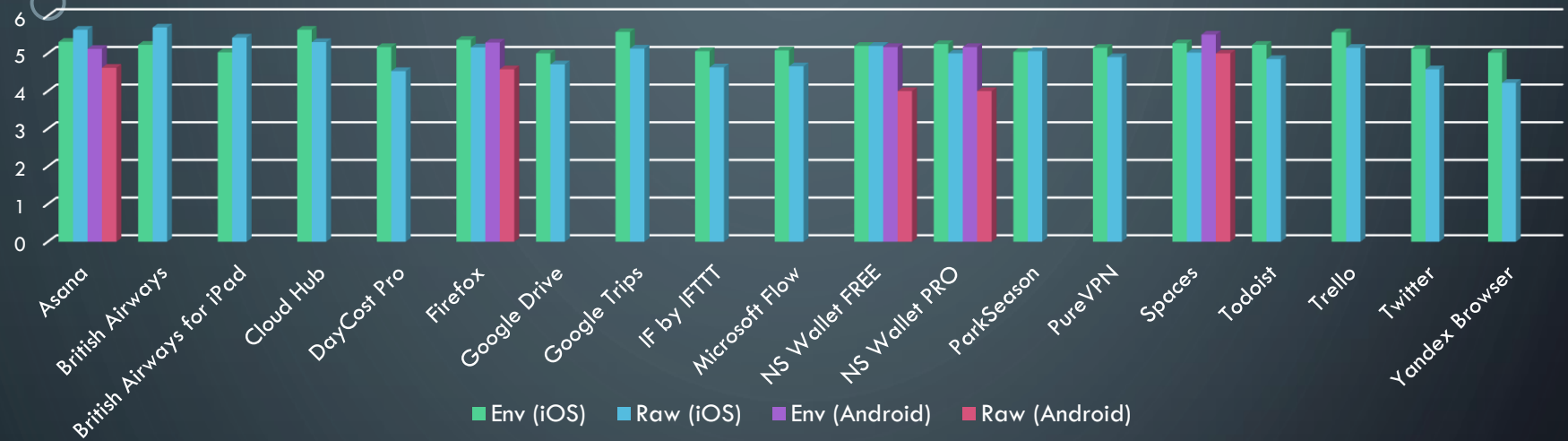
Many of applications reveal something in plaintext 8 groups, 16 data items, 30 pairs of group + data items

- 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

WORST iOS AND ANDROID APPLICATIONS



GOOD iOS & ANDROID APPS



GONNA MAKE THEM A POLL

GEEKS LOVE POLLS



<http://goo.gl/9WF2dC>



<http://goo.gl/CT4nTT>



RISKWARE BETRAYER. TWO POLLS

[YURY CHEMERKIN]



- MULTISKILLED SECURITY EXPERT
- EXPERIENCED IN :
 - REVERSE ENGINEERING & AV, DEVELOPMENT (PAST)
 - MOBILE SECURITY, & CLOUD SECURITY
 - IAM, COMPLIANCE, FORENSICS
 - PARTICIPATION & SPEAKING AT MANY SECURITY CONFERENCES



RISKWARE BETRAYER

WHO IS THE BIGGEST ONE?



YURY CHERMERKIN

SEND A MAIL TO: YURY.S@CHEMERKIN.COM

HOW TO CONTACT ME ?



ADD ME IN LINKEDIN:

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