black hat ASIA 2015

(In)Security of Mobile Banking ...and of Other Mobile Apps

Eric Filiol & Paul Irolla
ESIEA
Operational Cryptology and Virology Lab

esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

(C+V)°
Black Info Ops
We think dark to bring light

I am so sorry not to be here with you but a family member of
mine is extremely ill in hospital and his days are numbered.
I had to be with my family in these circumstances

Please feel to contact me for further technical details about this talk

Agenda

- Introduction & Background: The OpenDAVFI Project
- Our Analysis Tools
- The Paradigm of Insecurity: the Facebook App
- Analysis of Banking Apps
  - — The Protocol & a Few Statistics
  - — Case Studies: JP Morgan Access, BNP Paribas, Sberbank, Bradesco, Bank of China…
  - — Banking Apps Security Comparison: Western World versus Asian World
- Conclusion & Future Work

Introduction & Background

The Open DAVFI Project

Tools and Analysis

The OpenDAVFI Project

- Open and free fork of two-year project DAVFI to develop a sovereign and trusted AV (Android, Linux, Windows) by ESIEA/(C + V)^{o} Lab
  - Release scheduled in 2015 (administrative stuff pending)
- Funded partly by the French Government (6 millions euros with 0.35 % of funding)

Androïd (Open)DAVFI

- One of the key features is that all apps available on a secure market is fully analyzed (static & dynamic analysis including a reversing step).
- Whenever safe AND compliant to our security policy (see further), the app is certified & signed before made available on the secure market.

Our Trust Policy

- Legit apps can be malevolent when it comes to targeted marketing and user tracking capabilities.
- A few apps contains severe vulnerabilities.
- The “malware” definition needs to be extended.
- An app is trustworthy according to our Trust Policy if and only if:
  - It does not contain hidden functionalities.
  - User information collection must be motivated by explicit functionalities.
  - Web communications involving personal user informations must be encrypted.
  - The app does not contain known vulnerabilities.

Why Bank Apps?

- Progressively, banks are forcing users to move towards mobile banking.
- Because our money is a serious business.
- Our privacy and data confidentiality is an even more critical issue!
- So, we expect them to be at the edge of security and confidentiality and to take care of our core interests.
- Most banks have been contacted to provide (for free) all technical details. Up to now, only a very few have answered.
- A few (BNP Paribas, CA) are currently correcting part of the problems reported.

Our Analysis Tools

The Approach

- Based on advanced and innovative data-mining techniques
- The tools we have developped:
  - Egide: advanced static analysis and malware detection tool
  - Panoptes: advanced dynamic analysis tool (network communications analysis at runtime)
  - Tarentula: web crawling tool to collect apps
- These tools are non public at the present time

Static Analysis - Egide

- A program that reverses apps and generates a report which is a map and a guide in the source code
- Tasks: reverses to smali/java, detects risky behaviors/methods/sources/sinks, computes the control flow graph through entry point methods, computes statistics on group of apps, computes similarities between an app and a group of apps
- Generates a neural network and trains it on an app database, generates reports and graphs...
- Demos and examples of reports

Dynamic Analysis - Panoptes

- Task: reveals communications between an app and the Internet.
- Opens a fake access point and listens to HTTP/HTTPS/POP/IMAP communications
- Generates a tree of communication information
- Required material list :
  - Wifi card with Master mode available
  - Ethernet connection available
  - Rooted Android phone

Dynamic Analysis - Panoptes

Bypassing SSL Encryption with Panoptes

- A fake Certification Authority is installed in the phone.
- SSL/TLS requests are intercepted, terminated and a new one is initiated to the original destination address.
- The server response is copied, embedded in a SSL layer and signed with our fake Certification Authority

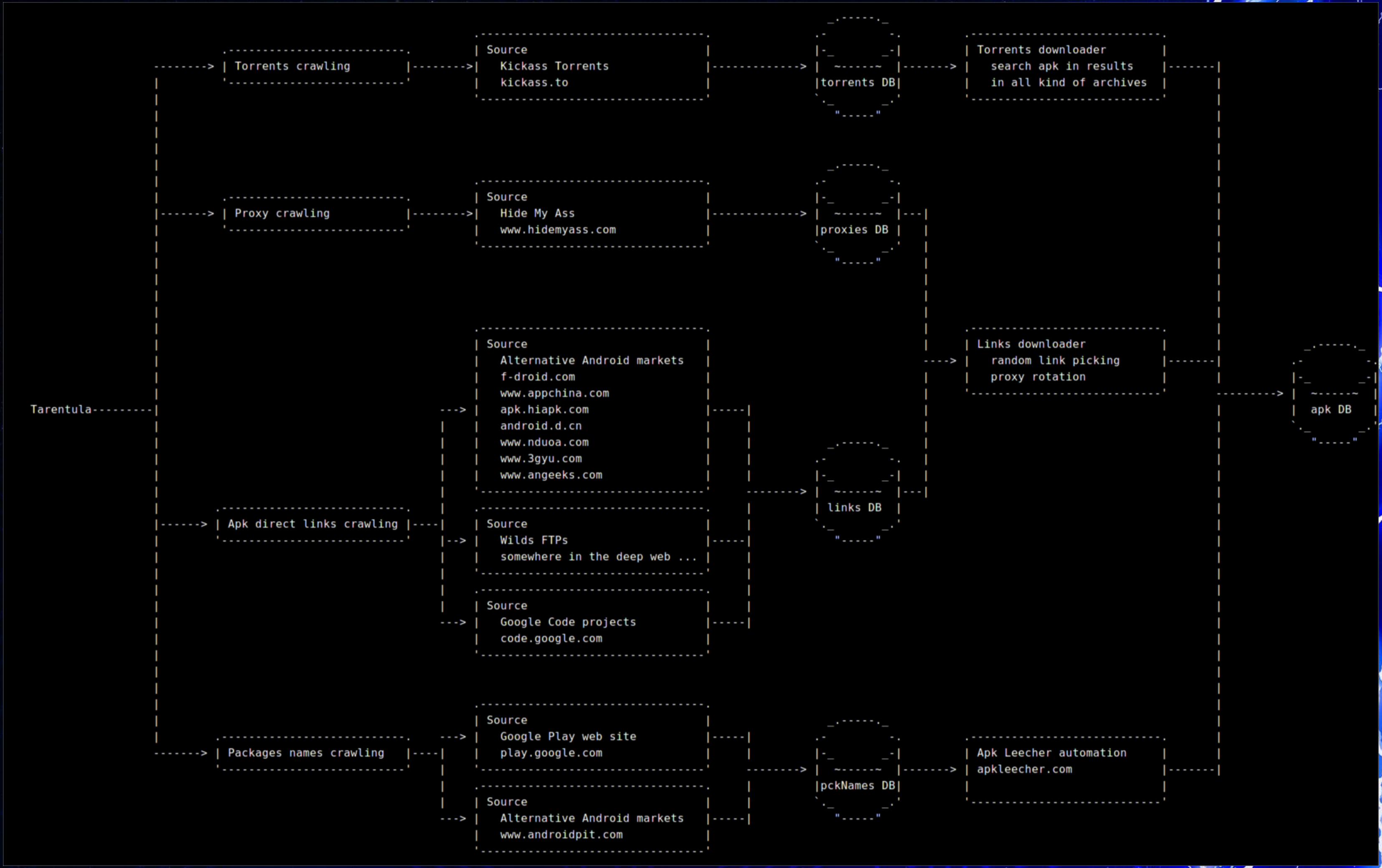
The Issue: Extending the APK DB

- Database of classified applications is the sinews of antiviral war
- A subject rarely explained or detailed in security papers
- A sophisticated data mining algorithm is useless with a poor database.
- So how to populate a database for training machine learning algorithms?
- How do the others make it?

The Issue: Extending the APK DB (2)

- Several universities gather malware and propose to share them
  - http://www.malgenomeproject.org/
  - http://user.informatik.uni-goettingen.de/~darp/drebin/
- A few websites share Android malware
  - http://virusshare.com/
  - http://contagiodump.blogspot.fr/
- It is a good starting point but not enough.

Tarentula Structure



```
                                                                                                                     _.------._
                                                                 .----------------------------------.              .-          -.        .-----------------------------.
                            .---------------------------.        | Source                           |             |-_          _-|       | Torrents downloader         |
                  --------> | Torrents crawling         |-------->|   Kickass Torrents               |------------> |   ~------~   |-------> |   search apk in results     |-------|
                  |         '---------------------------'        |   kickass.to                     |             |torrents DB|          |   in all kind of archives   |       |
                  |                                              '----------------------------------'              '-.        .-'        '-----------------------------'       |
                  |                                                                                                  "-----"                                                   |
                  |                                                                                                                                                            |
                  |                                                                                                                                                            |
                  |                                                                                                                                                            |
                  |                                                                                                  _.------._                                                |
                  |                                              .----------------------------------.              .-          -.                                              |
                  |         .---------------------------.        | Source                           |             |-_          _-|                                             |
                  |-------> | Proxy crawling            |-------->|   Hide My Ass                    |------------> |   ~------~   |---|                                         |
                  |         '---------------------------'        |   www.hidemyass.com              |             |proxies DB  |   |                                         |
                  |                                              '----------------------------------'              '-.        .-'    |                                         |
                  |                                                                                                  "-----"         |                                         |
                  |                                                                                                                  |                                         |
                  |                                                                                                                  |                                         |
                  |                                                                                                                  |                                         |
                  |                                              .----------------------------------.                                |   .-----------------------------.       |
                  |                                              | Source                           |                                |   | Links downloader            |       |         _.-----._
                  |                                              |   Alternative Android markets    |                                |---->|   random link picking       |-------|       .-         -.
                  |                                              |   f-droid.com                    |                                |   |   proxy rotation            |       |      |-_         _-|
                  |                                              |   www.appchina.com               |                                |   '-----------------------------'       |--------->  |  ~-------~  |
Tarentula---------|                                          --->|   apk.hiapk.com                  |----|                           |                                         |      |   apk DB    |
                  |                                         |    |   android.d.cn                   |    |                           |                                         |       '-.       .-'
                  |                                         |    |   www.nduoa.com                  |    |                           |                                         |         "-----"
                  |                                         |    |   www.3gyu.com                   |    |         _.------._        |                                         |
                  |                                         |    |   www.angeeks.com                |    |        .-          -.     |                                         |
                  |                                         |    '----------------------------------'    |       |-_          _-|    |                                         |
                  |                                         |                                            |-----> |   ~------~   |----|                                         |
                  |        .----------------------------.   |    .----------------------------------.    |       |  links DB    |                                              |
                  |------> | Apk direct links crawling  |----|    | Source                           |    |        '-.        .-'                                              |
                  |        '----------------------------'   |--->|   Wilds FTPs                     |----|          "-----"                                                  |
                  |                                         |    |   somewhere in the deep web ...  |    |                                                                   |
                  |                                         |    '----------------------------------'    |                                                                   |
                  |                                         |    .----------------------------------.    |                                                                   |
                  |                                         |    | Source                           |    |                                                                   |
                  |                                          --->|   Google Code projects           |----|                                                                   |
                  |                                              |   code.google.com                |                                                                        |
                  |                                              '----------------------------------'                                                                        |
                  |                                                                                                                                                            |
                  |                                                                                                                                                            |
                  |                                              .----------------------------------.                                                                        |
                  |                                              | Source                           |                 _.------._                                             |
                  |        .---------------------------.     --->|   Google Play web site           |----|           .-          -.         .-----------------------------.       |
                  -------> | Packages names crawling   |----|    |   play.google.com                |    |          |-_          _-|        | Apk Leecher automation      |       |
                           '---------------------------'    |    '----------------------------------'    |--------> |   ~------~   |------> | apkleecher.com              |-------|
                                                            |    .----------------------------------.    |          |pckNames DB|           |                             |
                                                            |    | Source                           |    |           '-.        .-'       '-----------------------------'
                                                             --->|   Alternative Android markets    |----|             "-----"
                                                                 |   www.androidpit.com             |
                                                                 '----------------------------------'
```

Appetizer - The Paradigm of Insecurity: the Facebook App

Facebook App

- Facebook collects information submitted by users (some sort of voluntary STASI)
- But what about information the app sends without the user knowledge?
- And what personal information are stored on the phone without users' awareness?
- Reminder: you can access any data on the phone by physical access in less a minute (video)

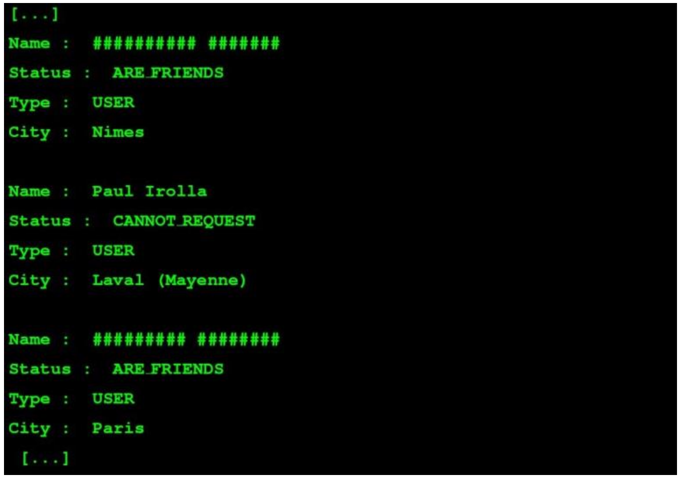
Facebook Insecurity

- After a connection to the Facebook account and some basic navigation, get all data created locally:

  *adb shell su -c 'cat /data/data/com.facebook.katana/**/*' > facebook-data.dump*

- Time to parse this thing !

  /"displayName":"([^"]?)"ng.*?"friendshipStatus":"([^"]*?)".*?"contactType":"([^"]*?)".*?"cityName":"([^"]*?)"/*



```
[...]
Name :  ########## #######
Status :  ARE_FRIENDS
Type :  USER
City :  Nimes

Name :  Paul Irolla
Status :  CANNOT_REQUEST
Type :  USER
City :  Laval (Mayenne)

Name :  ######### ########
Status :  ARE_FRIENDS
Type :  USER
City :  Paris
 [...]
```

Facebook Insecurity (2)

Other data that are unconsciously collected and stored on your smartphone :

- Private messages
- Private photos
- Private wall content
- Many other private and non private data…

Facebook: Network Analysis

- FB typical one-kilometer POST request (demo: Panoptes graph).
- Reverse procedure:
  - — Unescape url codes recursively
  - — Parse the output string as a JSON object
  - — Until the data super-structure is entirely reversed
    - Try to parse each string in the JSON object as a JSON object
    - Try to decode each strings which seems to be in a base64 format, then
      - — Try to unzip the result with gzip if the magic number is ’1F8B’, and finally
      - — Read the result string with a WINDOWS minidump reader like WinDBG (no joke)

FB Needs to Know You Better!

- Bootloader used
- Device model/manufacturer/serial/hardware/ROM
- CPU model/architecture/version + Kernel version
- Screen settings
- List of system applications
- All environnement variables
- Open file descriptors count
- Software and hardware file descriptors limit
- Locations settings + Developper settings + Lockpattern settings

  LOCK PATTERN ENABLED=1

  LOCK PATTERN SIZE=3

  LOCK PATTERN VISIBLE=1

FB Needs to Know You Better! (2)

- Application settings
- **Security settings**
- Sound used for alarm alert
- Spell checker settings + Screensaver settings
- Notification settings - including used sound
- Battery settings - including current energy level
- Sounds/music settings + Camera settings + Wifi connection settings
- Sdcard and memory size/free space/used space
- ++ Usual user tracking info (timestamp for each user action)

connection = WIFI

connection class = POOR

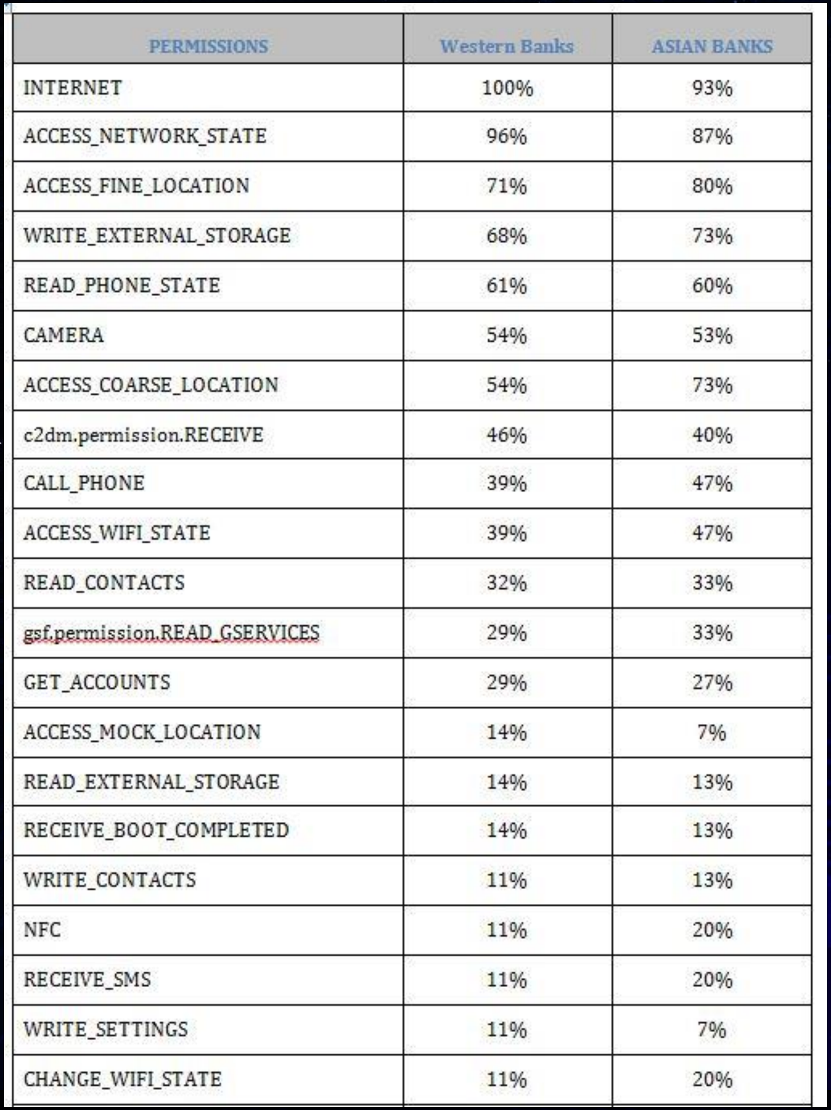
network extra info = Panoptes-AP

The Analysis of Banking Apps

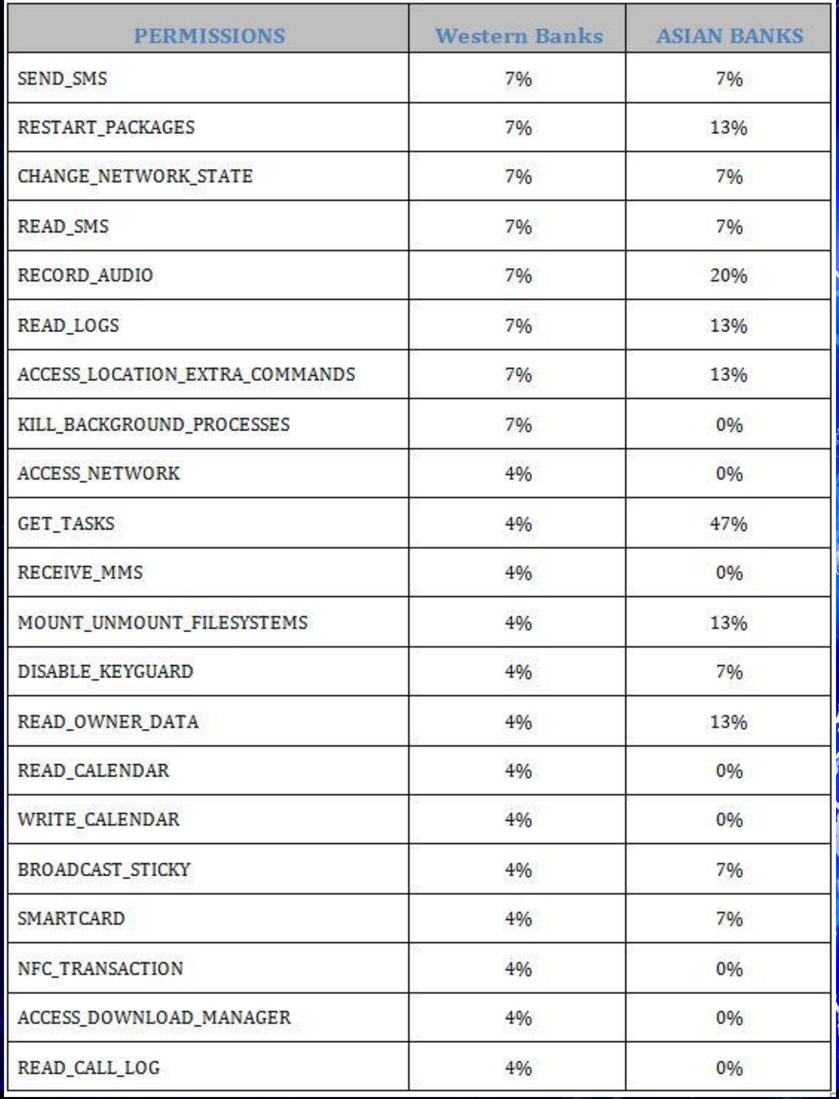
The Bank Apps Analyzed (up to now)

- BNP Paribas (France)
- LCL (France)
- Crédit Agricole (France)
- Sofinco (France)
- Société Générale (France)
- BforBank (France)
- Finaref (France)
- Bradesco (Brazil)
- BMCE (Morocco)
- Barclay (UK)
- UBS (Switzerland) - JP Morgan (USA)
- Wells Fargo (USA) - Bank of America (USA)
- Burke and Herbert (USA)
- PNC Financial Service (USA)
- Commerzbank (Germany)
- Deutsche Bank AG (Germany)
- HSBC (UK) - Santander Group (Spain)
- Sberbank (Russia) - Hapoalim Bank (Israel)
- Shahr Bank (Iran)
- VTB (Russia)
- LandKredit (Norway)
- Nordea Mobilbank (Norway)
- Oversea-Chinese Banking Corporation (Singapore)
- DBS Bank (Singapore)
- United Overseas Bank (Singapore)
- Bank of China (Hong Kong)
- Bank Negara (Indonesia)
- Commonwealth Bank of Australia
- National Australia Bank Limited
- Bank of Communications (China)
- Mitsubishi UFJ Financial Group (Japan)
- Advanced Bank Of Asia (Cambodia)
- Public Bank Berhad (Cambodia)
- Bangkok Bank (Thailand)
- State Bank of Mongolia
- HanaNBank (Korea)
- Agricultural Bank of China (China)
- Industrial Bank of Korea (Korea)
- Mizohobank (Japan)
- State Bank of India (India)

A Few Statistics - Permissions

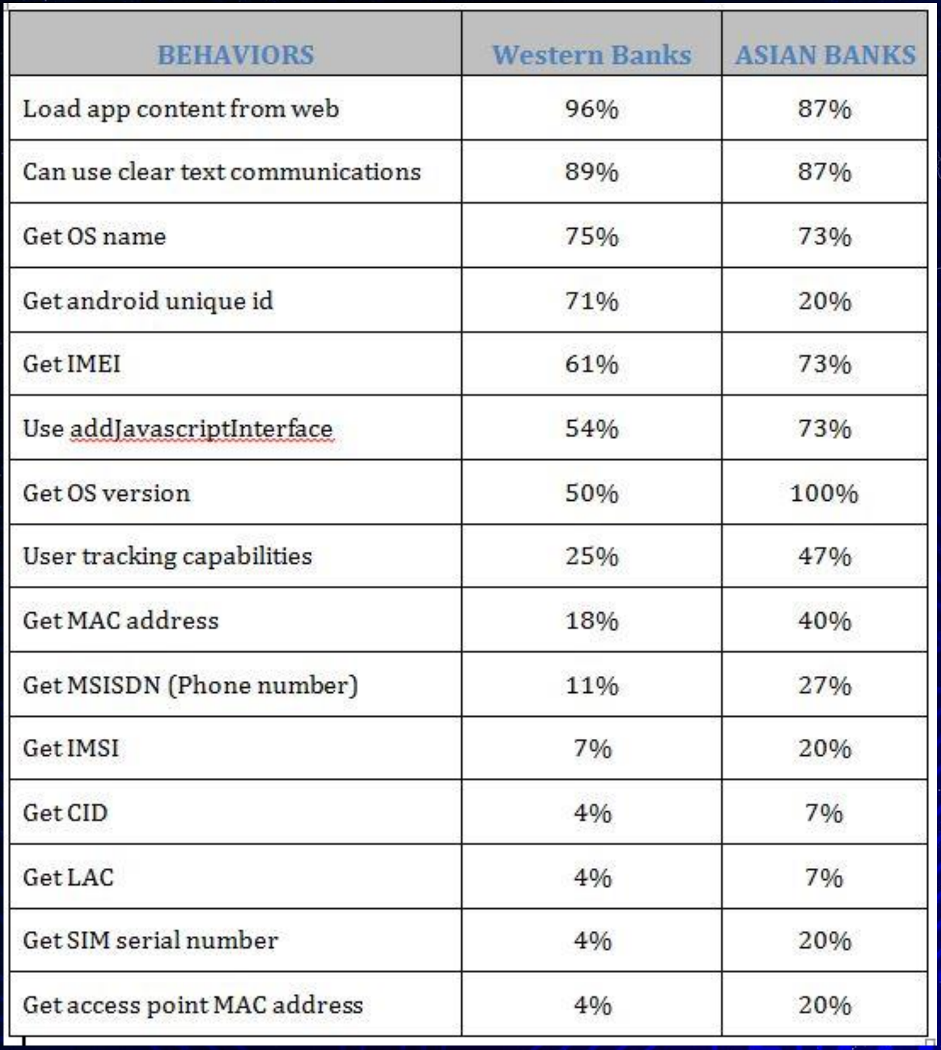


PERMISSIONS	Western Banks	ASIAN BANKS
INTERNET	100%	93%
ACCESS_NETWORK_STATE	96%	87%
ACCESS_FINE_LOCATION	71%	80%
WRITE_EXTERNAL_STORAGE	68%	73%
READ_PHONE_STATE	61%	60%
CAMERA	54%	53%
ACCESS_COARSE_LOCATION	54%	73%
c2dm.permission.RECEIVE	46%	40%
CALL_PHONE	39%	47%
ACCESS_WIFI_STATE	39%	47%
READ_CONTACTS	32%	33%
gsf.permission.READ_GSERVICES	29%	33%
GET_ACCOUNTS	29%	27%
ACCESS_MOCK_LOCATION	14%	7%
READ_EXTERNAL_STORAGE	14%	13%
RECEIVE_BOOT_COMPLETED	14%	13%
WRITE_CONTACTS	11%	13%
NFC	11%	20%
RECEIVE_SMS	11%	20%
WRITE_SETTINGS	11%	7%
CHANGE_WIFI_STATE	11%	20%



PERMISSIONS	Western Banks	ASIAN BANKS
SEND_SMS	7%	7%
RESTART_PACKAGES	7%	13%
CHANGE_NETWORK_STATE	7%	7%
READ_SMS	7%	7%
RECORD_AUDIO	7%	20%
READ_LOGS	7%	13%
ACCESS_LOCATION_EXTRA_COMMANDS	7%	13%
KILL_BACKGROUND_PROCESSES	7%	0%
ACCESS_NETWORK	4%	0%
GET_TASKS	4%	47%
RECEIVE_MMS	4%	0%
MOUNT_UNMOUNT_FILESYSTEMS	4%	13%
DISABLE_KEYGUARD	4%	7%
READ_OWNER_DATA	4%	13%
READ_CALENDAR	4%	0%
WRITE_CALENDAR	4%	0%
BROADCAST_STICKY	4%	7%
SMARTCARD	4%	7%
NFC_TRANSACTION	4%	0%
ACCESS_DOWNLOAD_MANAGER	4%	0%
READ_CALL_LOG	4%	0%

A Few Statistics - Behaviors



BEHAVIORS	Western Banks	ASIAN BANKS
Load app content from web	96%	87%
Can use clear text communications	89%	87%
Get OS name	75%	73%
Get android unique id	71%	20%
Get IMEI	61%	73%
Use addJavascriptInterface	54%	73%
Get OS version	50%	100%
User tracking capabilities	25%	47%
Get MAC address	18%	40%
Get MSISDN (Phone number)	11%	27%
Get IMSI	7%	20%
Get CID	4%	7%
Get LAC	4%	7%
Get SIM serial number	4%	20%
Get access point MAC address	4%	20%

Appraising of Asian Mobile Banking Security Assessment

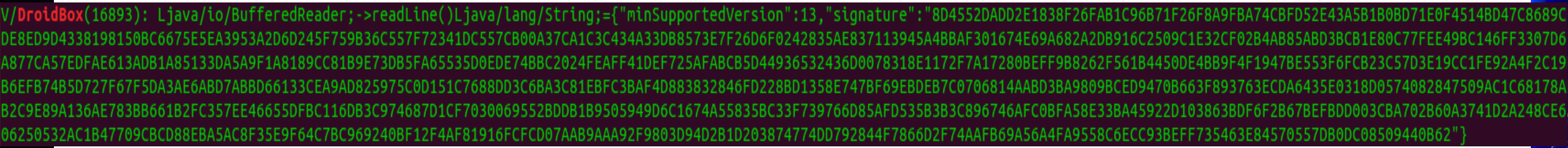
- Overall security awareness of Asian banks seems superior to what we have observed for European/American continents
- In particular, the use of custom obfuscation, security routines on the native layer (c libs.), custom trusted SSL root CA… is prevalent and shows a significative care for security
- Therefore the analysis was much harder than what we have performed for Western Banks apps
- But there is always some black sheeps in the flock…

Technical Summary Asian Bank Apps

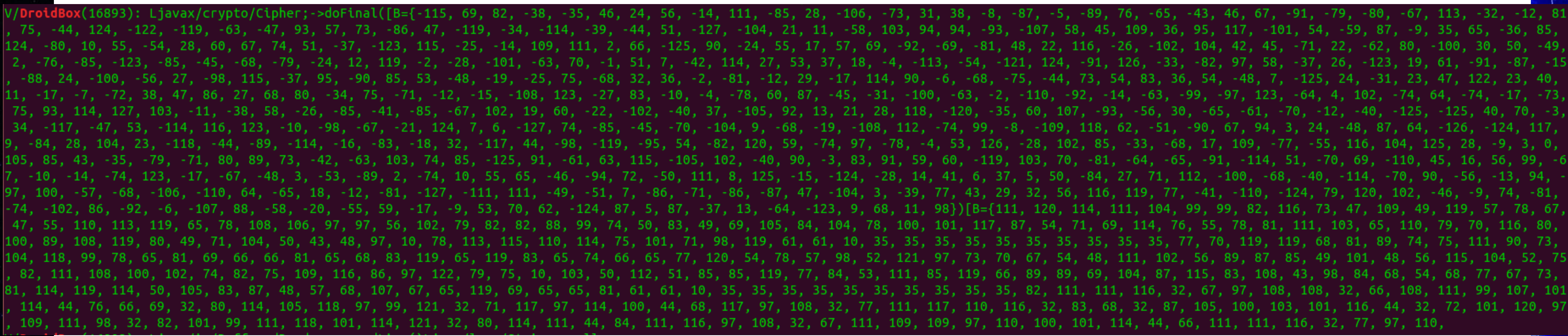
Banking application	Vulnerability found	Plaintext communications during runtime	Fake root CA countermeasure	User tracking capabilities	Strong use of crypto/obfuscation
Oversea-Chinese Banking Corporation	No	No	Yes	Yes	Yes
DBS Bank	Potential	Yes	Yes	Yes	No
United Overseas Bank	No	No	Yes	No	Yes
Bank of China	Yes	Yes	No	Yes	No
Bank Negara Indonesia	No	No	No	No	No
Commonwealth Bank of Australia	No	No	Yes	Yes	No
National Australia Bank Limited	Yes	Yes (But harmless)	No	Yes	No
Bank of Communications	No	No	Yes	No	No
Mitsubishi UFJ Financial Group	No	Yes	Partially	Yes	No
Advanced Bank Of Asia	No	No	Yes	No	No
Public Bank Berhad	N/A	N/A	N/A	No	N/A
Bangkok Bank	No	No	Yes	No	Yes
State Bank of Mongolia	Yes	No	No	No	No
Vnechtorgbank	No	No	No	No	No
Industrial Bank of Korea	N/A	N/A	N/A	No	N/A

Case Study – JP Morgan Access

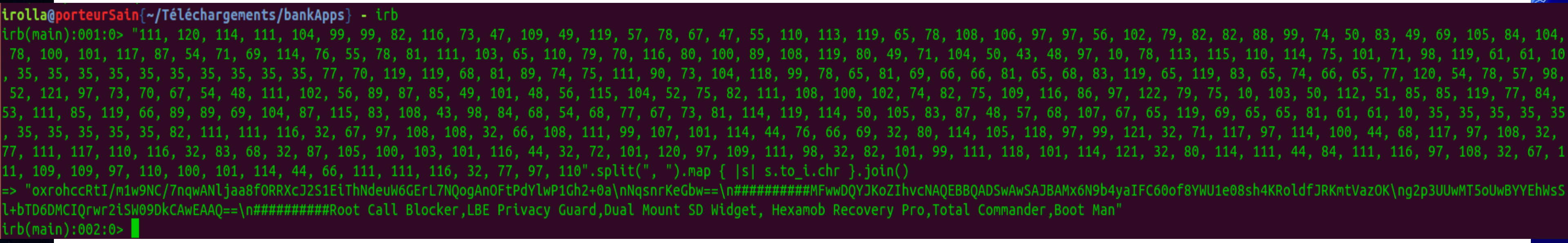
Demos



```
V/DroidBox(16893): Ljava/io/BufferedReader;->readLine()Ljava/lang/String;={"minSupportedVersion":13,"signature":"8D4552DADD2E1838F26FAB1C96B71F26F8A9FBA74CBFD52E43A5B1B0BD71E0F4514BD47C8689C
DE8ED9D4338198150BC6675E5EA3953A2D6D245F759B36C557F72341DC557CB00A37CA1C3C434A33DB8573E7F26D6F0242835AE837113945A4BBAF301674E69A682A2DB916C2509C1E32CF02B4AB85ABD3BCB1E80C77FEE49BC146FF3307D6
A877CA57EDFAE613ADB1A85133DA5A9F1A8189CC81B9E73DB5FA65535D0EDE74BBC2024FEAFF41DEF725AFABCB5D44936532436D0078318E1172F7A17280BEFF9B8262F561B4450DE4BB9F4F1947BE553F6FCB23C57D3E19CC1FE92A4F2C19
B6EFB74B5D727F67F5DA3AE6ABD7ABBD66133CEA9AD825975C0D151C7688DD3C6BA3C81EBFC3BAF4D883832846FD228BD1358E747BF69EBDEB7C0706814AABD3BA9809BCED9470B663F893763ECDA6435E0318D0574082847509AC1C68178A
B2C9E89A136AE783BB661B2FC357EE46655DFBC116DB3C974687D1CF7030069552BDDB1B9505949D6C1674A55835BC33F739766D85AFD535B3B3C896746AFC0BFA58E33BA45922D103863BDF6F2B67BEFBDD003CBA702B60A3741D2A248CE6
06250532AC1B47709CBCD88EBA5AC8F35E9F64C7BC969240BF12F4AF81916FCFCD07AAB9AAA92F9803D94D2B1D203874774DD792844F7866D2F74AAFB69A56A4FA9558C6ECC93BEFF735463E84570557DB0DC08509440B62"}
```



```
V/DroidBox(16893): Ljavax/crypto/Cipher;->doFinal([B={-115, 69, 82, -38, -35, 46, 24, 56, -14, 111, -85, 28, -106, -73, 31, 38, -8, -87, -5, -89, 76, -65, -43, 46, 67, -91, -79, -80, -67, 113, -32, -12, 81
, 75, -44, 124, -122, -119, -63, -47, 93, 57, 73, -86, 47, -119, -34, -114, -39, -44, 51, -127, -104, 21, 11, -58, 103, 94, 94, -93, -107, 58, 45, 109, 36, 95, 117, -101, 54, -59, 87, -9, 35, 65, -36, 85,
124, -80, 10, 55, -54, 28, 60, 67, 74, 51, -37, -123, 115, -25, -14, 109, 111, 2, 66, -125, 90, -24, 55, 17, 57, 69, -92, -69, -81, 48, 22, 116, -26, -102, 104, 42, 45, -71, 22, -62, 80, -100, 30, 50, -49,
 2, -76, -85, -123, -85, -45, -68, -79, -24, 12, 119, -2, -28, -101, -63, 70, -1, 51, 7, -42, 114, 27, 53, 37, 18, -4, -113, -54, -121, 124, -91, 126, -33, -82, 97, 58, -37, 26, -123, 19, 61, -91, -87, -15
, -88, 24, -100, -56, 27, -98, 115, -37, 95, -90, 85, 53, -48, -19, -25, 75, -68, 32, 36, -2, -81, -12, 29, -17, 114, 90, -6, -68, -75, -44, 73, 54, 83, 36, 54, -48, 7, -125, 24, -31, 23, 47, 122, 23, 40,
11, -17, -7, -72, 38, 47, 86, 27, 68, 80, -34, 75, -71, -12, -15, -108, 123, -27, 83, -10, -4, -78, 60, 87, -45, -31, -100, -63, -2, -110, -92, -14, -63, -99, -97, 123, -64, 4, 102, -74, 64, -74, -17, -73,
 75, 93, 114, 127, 103, -11, -38, 58, -26, -85, -41, -85, -67, 102, 19, 60, -22, -102, -40, 37, -105, 92, 13, 21, 28, 118, -120, -35, 60, 107, -93, -56, 30, -65, -61, -70, -12, -40, -125, -125, 40, 70, -3,
 34, -117, -47, 53, -114, 116, 123, -10, -98, -67, -21, 124, 7, 6, -127, 74, -85, -45, -70, -104, 9, -68, -19, -108, 112, -74, 99, -8, -109, 118, 62, -51, -90, 67, 94, 3, 24, -48, 87, 64, -126, -124, 117,
9, -84, 28, 104, 23, -118, -44, -89, -114, -16, -83, -18, 32, -117, 44, -98, -119, -95, 54, -82, 120, 59, -74, 97, -78, -4, 53, 126, -28, 102, 85, -33, -68, 17, 109, -77, -55, 116, 104, 125, 28, -9, 3, 0,
105, 85, 43, -35, -79, -71, 80, 89, 73, -42, -63, 103, 74, 85, -125, 91, -61, 63, 115, -105, 102, -40, 90, -3, 83, 91, 59, 60, -119, 103, 70, -81, -64, -65, -91, -114, 51, -70, 69, -110, 45, 16, 56, 99, -6
7, -10, -14, -74, 123, -17, -67, -48, 3, -53, -89, 2, -74, 10, 55, 65, -46, -94, 72, -50, 111, 8, 125, -15, -124, -28, 14, 41, 6, 37, 5, 50, -84, 27, 71, 112, -100, -68, -40, -114, -70, 90, -56, -13, 94, -
97, 100, -57, -68, -106, -110, 64, -65, 18, -12, -81, -127, -111, 111, -49, -51, 7, -86, -71, -86, -87, 47, -104, 3, -39, 77, 43, 29, 32, 56, 116, 119, 77, -41, -110, -124, 79, 120, 102, -46, -9, 74, -81,
-74, -102, 86, -92, -6, -107, 88, -58, -20, -55, 59, -17, -9, 53, 70, 62, -124, 87, 5, 87, -37, 13, -64, -123, 9, 68, 11, 98})[B={111, 120, 114, 111, 104, 99, 99, 82, 116, 73, 47, 109, 49, 119, 57, 78, 67,
 47, 55, 110, 113, 119, 65, 78, 108, 106, 97, 97, 56, 102, 79, 82, 82, 88, 99, 74, 50, 83, 49, 69, 105, 84, 104, 78, 100, 101, 117, 87, 54, 71, 69, 114, 76, 55, 78, 81, 111, 103, 65, 110, 79, 70, 116, 80,
100, 89, 108, 119, 80, 49, 71, 104, 50, 43, 48, 97, 10, 78, 113, 115, 110, 114, 75, 101, 71, 98, 119, 61, 61, 10, 35, 35, 35, 35, 35, 35, 35, 35, 35, 35, 77, 70, 119, 119, 68, 81, 89, 74, 75, 111, 90, 73,
104, 118, 99, 78, 65, 81, 69, 66, 66, 81, 65, 68, 83, 119, 65, 119, 83, 65, 74, 66, 65, 77, 120, 54, 78, 57, 98, 52, 121, 97, 73, 70, 67, 54, 48, 111, 102, 56, 89, 87, 85, 49, 101, 48, 56, 115, 104, 52, 75
, 82, 111, 108, 100, 102, 74, 82, 75, 109, 116, 86, 97, 122, 79, 75, 10, 103, 50, 112, 51, 85, 85, 119, 77, 84, 53, 111, 85, 119, 66, 89, 89, 69, 104, 87, 115, 83, 108, 43, 98, 84, 68, 54, 68, 77, 67, 73,
81, 114, 119, 114, 50, 105, 83, 87, 48, 57, 68, 107, 67, 65, 119, 69, 65, 65, 81, 61, 61, 10, 35, 35, 35, 35, 35, 35, 35, 35, 35, 35, 82, 111, 111, 116, 32, 67, 97, 108, 108, 32, 66, 108, 111, 99, 107, 101
, 114, 44, 76, 66, 69, 32, 80, 114, 105, 118, 97, 99, 121, 32, 71, 117, 97, 114, 100, 44, 68, 117, 97, 108, 32, 77, 111, 117, 110, 116, 32, 83, 68, 32, 87, 105, 100, 103, 101, 116, 44, 32, 72, 101, 120, 97
, 109, 111, 98, 32, 82, 101, 99, 111, 118, 101, 114, 121, 32, 80, 114, 111, 44, 84, 111, 116, 97, 108, 32, 67, 111, 109, 109, 97, 110, 100, 101, 114, 44, 66, 111, 111, 116, 32, 77, 97, 110,
```



```
irolla@porteurSain{~/Téléchargements/bankApps} - irb
irb(main):001:0> "111, 120, 114, 111, 104, 99, 99, 82, 116, 73, 47, 109, 49, 119, 57, 78, 67, 47, 55, 110, 113, 119, 65, 78, 108, 106, 97, 97, 56, 102, 79, 82, 82, 88, 99, 74, 50, 83, 49, 69, 105, 84, 104,
 78, 100, 101, 117, 87, 54, 71, 69, 114, 76, 55, 78, 81, 111, 103, 65, 110, 79, 70, 116, 80, 100, 89, 108, 119, 80, 49, 71, 104, 50, 43, 48, 97, 10, 78, 113, 115, 110, 114, 75, 101, 71, 98, 119, 61, 61, 10
, 35, 35, 35, 35, 35, 35, 35, 35, 35, 35, 77, 70, 119, 119, 68, 81, 89, 74, 75, 111, 90, 73, 104, 118, 99, 78, 65, 81, 69, 66, 66, 81, 65, 68, 83, 119, 65, 119, 83, 65, 74, 66, 65, 77, 120, 54, 78, 57, 98,
 52, 121, 97, 73, 70, 67, 54, 48, 111, 102, 56, 89, 87, 85, 49, 101, 48, 56, 115, 104, 52, 75, 82, 111, 108, 100, 102, 74, 82, 75, 109, 116, 86, 97, 122, 79, 75, 10, 103, 50, 112, 51, 85, 85, 119, 77, 84,
53, 111, 85, 119, 66, 89, 89, 69, 104, 87, 115, 83, 108, 43, 98, 84, 68, 54, 68, 77, 67, 73, 81, 114, 119, 114, 50, 105, 83, 87, 48, 57, 68, 107, 67, 65, 119, 69, 65, 65, 81, 61, 61, 10, 35, 35, 35, 35, 35
, 35, 35, 35, 35, 35, 82, 111, 111, 116, 32, 67, 97, 108, 108, 32, 66, 108, 111, 99, 107, 101, 114, 44, 76, 66, 69, 32, 80, 114, 105, 118, 97, 99, 121, 32, 71, 117, 97, 114, 100, 44, 68, 117, 97, 108, 32,
77, 111, 117, 110, 116, 32, 83, 68, 32, 87, 105, 100, 103, 101, 116, 44, 32, 72, 101, 120, 97, 109, 111, 98, 32, 82, 101, 99, 111, 118, 101, 114, 121, 32, 80, 114, 111, 44, 84, 111, 116, 97, 108, 32, 67, 1
11, 109, 109, 97, 110, 100, 101, 114, 44, 66, 111, 111, 116, 32, 77, 97, 110".split(", ").map { |s| s.to_i.chr }.join()
=> "oxrohccRtI/m1w9NC/7nqwANljaa8fORRXcJ2S1EiThNdeuW6GErL7NQogAnOFtPdYlwP1Gh2+0a\nNqsnrKeGbw==\n##########MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMx6N9b4yaIFC60of8YWU1e08sh4KRoldfJRKmtVazOK\ng2p3UUwMT5oUwBYYEhWsS
l+bTD6DMCIQrwr2iSW09DkCAwEAAQ==\n##########Root Call Blocker,LBE Privacy Guard,Dual Mount SD Widget, Hexamob Recovery Pro,Total Commander,Boot Man"
irb(main):002:0>
```

Case Study – JP Morgan Access (2)

*”oxrohccRtI/m1w9NC/7nqwANljaa8fORRXcJ2S1EiThNdeuW6GEr
L7NQogAnOFtPdYlwP1Gh2+0aNqsnrKeGbw==
###########
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMx6N9b4yaIFC60o
f8YWU1e08sh4KRoldfJRKmtVazOKg2p3UUwMT5oUwBYYEhWsSl
+bTD6DMCIQrwr2iSW09DkCAwEAAQ==
###########*

*Root Call Blocker,LBE Privacy Guard,Dual Mount SDWidget,
Hexamob Recovery Pro,Total Commander,Boot Man”*

Case Study – JP Morgan Access (3)

```
String[] arrayOfString = str2.split(”##########”);
…
RootTools.log(”Executing sh Commands : ” +
arrayOfString5[0] + arrayOfString5[1]);
…
List localList = runcmd(arrayOfString6);
```

Case Study – JP Morgan Access (4)

- Dynamic Analysis :
  - An encrypted string is received
  - APK Instrumentation reveals it contains signatures and lists of strings.
- Static Analysis reveals some strings are sent directly into a shell.
- Well, that's a remote shell, isn't it?
- Technical details sent to the bank in December 2014. No News since. The vulnerability is still active. Nothing has been corrected yet 👎😠

Case Study – BNP Paribas

- Dynamic analysis failed!
- Static analysis reveals that *addJavascriptInterface* loads plaintext javascript.
- That means MITM attackers can gain a reverse shell on vulnerable phones (nearly 75 % of the present smartphones)
- Demo
- Three months later, the bank has corrected nothing. The vulnerability is still exploitable

Case Study - Sberbank

```
wifinetworks=001122334400:-45,0060B3E268C8:-66,4018B1CF2655:-77,4018B1CF2255:-
77,4018B1CF6455:-79,C8D3A352B1B0:-78,4018B1CF6
515:-83,586D8F747EC7:-85,4018B1CF2654:-76,4018B1CF2254:-83,4018B1CF6454:-
84,4018B1CF6514:-88,4018B1CF23D4:-90,4018B1CF23D5:-83,4018B1CF63D4:-
92,D8C7C8138A92:-90
```

- 001122334400 is the MAC address of our wifi access point used for interception
- So the app sends MAC addresses and signal strength in plaintext to the surrounding wifi networks

Case Study – Sberbank (2)

- Dynamic analysis reveals that all surrondings wifi networks info are sent in plaintext to yandex servers.
- Static analysis reveals that it is used for fine indoor geolocation.
- In fact, Google maps services (installed on every Android phones) does it too
- That is basically world wifi networks mapping
- *”Hello Google, someone stole my wifi router, can you send me its coordinates please ?”*
- Demos

Case Study - Bradesco

- Dynamic analysis reveals that a private key for accessing bank services is received in plaintext.
- The embedded *Jquery* JavaScript lib contains vulnerabilities
- Demo

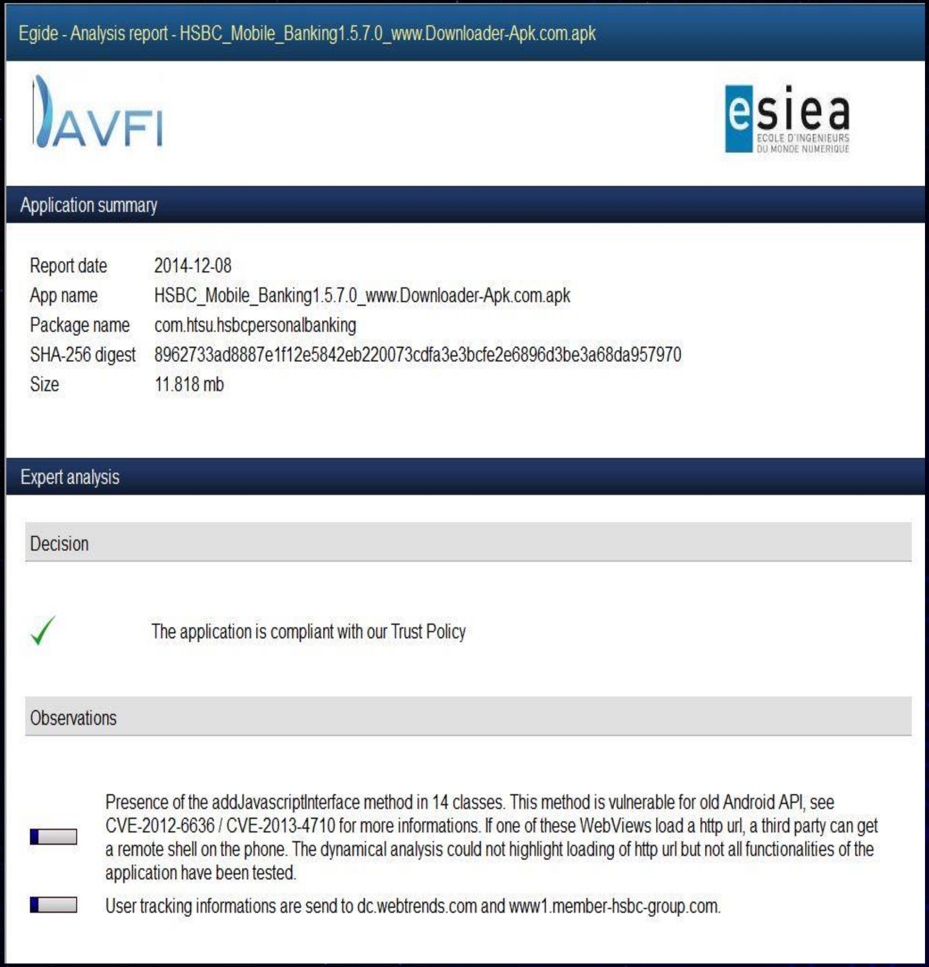
Bank of China (Hong Kong)

- The application can check for available updates
- A link on the official market is sent whenever a new update is available
- Then the app downloads and installs the file
- Moreover other navigation links (loaded by the app) are received
- Security issue: this process is done entirely in http
- Demo with Panoptes graph

Bank of China (Hong Kong) (2)

- Potential risks with a MitM attack:
  - — Installation of an arbitrary app by social engineering
  - — Loading of arbitrary web pages
  - — Exploiting the confidence of using a bank app, social engineering could be devastating
- Demos with Panoptes graph

One more for the Road



Egide - Analysis report - HSBC_Mobile_Banking1.5.7.0_www.Downloader-Apk.com.apk

Application summary

Report date	2014-12-08
App name	HSBC_Mobile_Banking1.5.7.0_www.Downloader-Apk.com.apk
Package name	com.htsu.hsbcpersonalbanking
SHA-256 digest	8962733ad8887e1f12e5842eb220073cdfa3e3bcfe2e6896d3be3a68da957970
Size	11.818 mb

Expert analysis

Decision

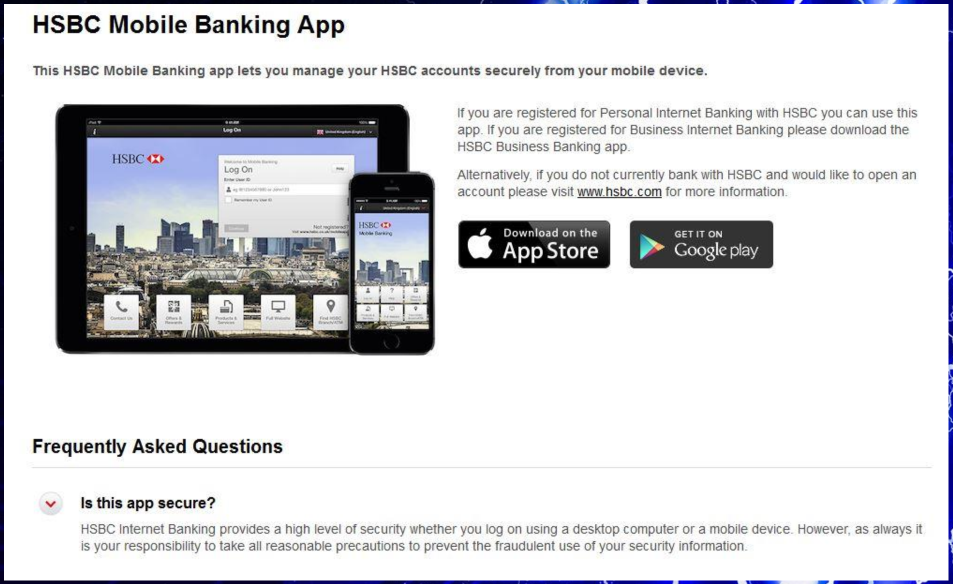
✓ The application is compliant with our Trust Policy

Observations

▬ Presence of the addJavascriptInterface method in 14 classes. This method is vulnerable for old Android API, see CVE-2012-6636 / CVE-2013-4710 for more informations. If one of these WebViews load a http url, a third party can get a remote shell on the phone. The dynamical analysis could not highlight loading of http url but not all functionalities of the application have been tested.

▬ User tracking informations are send to dc.webtrends.com and www1.member-hsbc-group.com.

The answer to our contact attempt: a link
To the HSBC page below



HSBC Mobile Banking App

This HSBC Mobile Banking app lets you manage your HSBC accounts securely from your mobile device.

If you are registered for Personal Internet Banking with HSBC you can use this app. If you are registered for Business Internet Banking please download the HSBC Business Banking app.

Alternatively, if you do not currently bank with HSBC and would like to open an account please visit www.hsbc.com for more information.

Frequently Asked Questions

Is this app secure?

HSBC Internet Banking provides a high level of security whether you log on using a desktop computer or a mobile device. However, as always it is your responsibility to take all reasonable precautions to prevent the fraudulent use of your security information.

Conclusion & Future Works

Future Work

- We intend to cover all banking apps throughout the world.
- Other kind of apps will be analyzed (games, email clients, security tools...)
- Develop our tools further with advanced mathematics (Ph D started in January 2015)
- Publish the {Egide, Panoptes} reports once security issues will be corrected by banks
- Verification analysis will be performed to check whether the users' privacy issues have been solved as well.

Conclusion

- Mobile (Banking) apps are far from being totally clean. Beyond a few cases of vulnerabilities, users' privacy is not the priority of developpers or outsourcers (here banks)!
  - — Difference of awareness and security vision however between Asia and Western world
- There is a strong need for pressure on app developpers to take care of users' privacy.
- The bank apps market is not mature and has developped too quickly. Functionalities take precedence over security and users' fundamental rights for privacy and data confidentiality.
- It is very difficult to identify a visible contact point to report security issues

Conclusion (2)

- All the tested apps are on the Google Play!
- This means that Google does not perform apps’ security analysis at all! It does not care about users’ privacy either (but we all already know that)
- Google has the power to force developers to do a better job
- Choose open source apps (when available, for banks, well it is pure Utopia)
- Prefer local/national banks instead of international banks

Many thanks for your attention

Questions & Answers

Contact: {filiol, irolla}@esiea.fr

esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

(C+V)°
Black Info Ops
We think dark to bring light