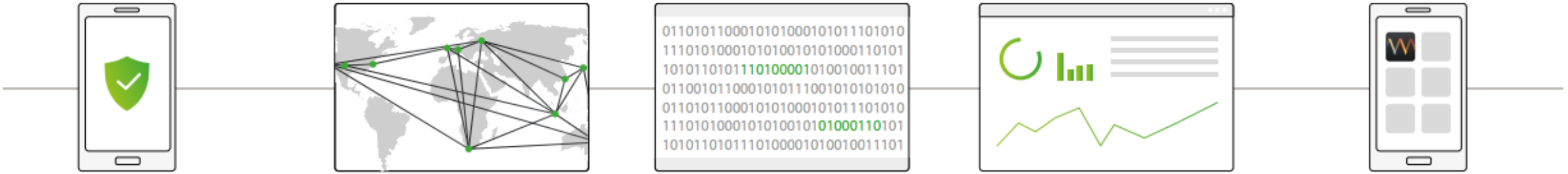
Mobile Security Threats

ZDENĚK LETKO
zdenek.letko@wandera.com
Software Engineer
Wandera CZ s.r.o.

wandera

Wandera – How It Works



Wandera
Mobile App

Understand mobile data usage with the end user device app

Wandera
Cloud Gateway

Unrivaled data visibility with our in-line gateway

SmartWire
Cloud Intelligence

Machine learning data analysis and app content inspection

RADAR
Management Portal

Powerful controls and easy management informed by real-time reports

Wandera
EMM Connect

Simple integration from Wandera to EMM/MDM, facilitates large-scale deployment

- Threats Detection
- Compliance
- Data Cost Management

wandera

Sensitive Information

- API keys
- Session IDs
- Encryption keys
- Authentication tokens
- Passwords
- Credit card numbers
- Personal Identifiable Information (PII)
- Location
- ...

Taxonomy of Mobile Threats

- OWASP – Open Web Application Security Project (Mobile Security Project)
  https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- Zimperium
  (Modern Mobile Threat Landscape - Network and Host)
  https://www.zimperium.com/download-whitepaper
- Wandera
  https://www.wandera.com/mobile-threat-vectors-explained/
- Avast
- Appthority
- McAfee
- …

wandera

M1 – Improper Platform Usage

- Misuse of a security tool that is part of the operating system
- Examples
  - (iOS) Use local storage instead of Keychain to store security significant data
- Advices
  - Invest your time to study API and frameworks
  - Do not assume anything (e.g., certain functionality)

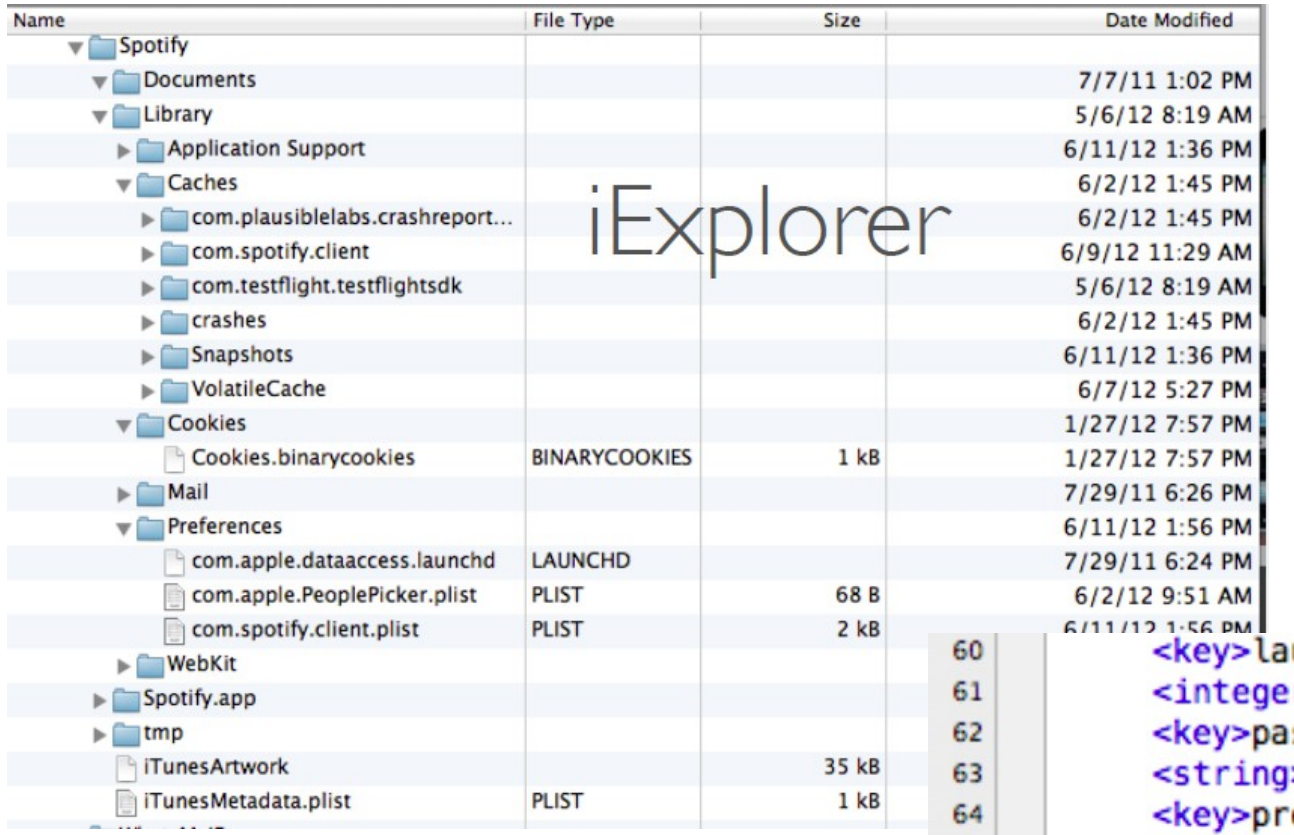
M1 – Improper Platform Usage

- Resources
  - Introduction to Secure Coding Style (Apple)
  - Security Overview (Apple)
  - Tutorial: Understanding Android's Security Framework (Android)
  - Windows UWP Security

M2 – Insecure Data Storage

- Insecure data storage and unintended data leakage
  (SQL databases, log files, binary data stores, cookie stores, cloud synced, ...)
- Examples
  - Application storage
  - Copy&paste buffer caching
  - URL caching
- Advices
  - Be aware of caches
  - Track where your data are stored

M2 – Insecure Data Storage



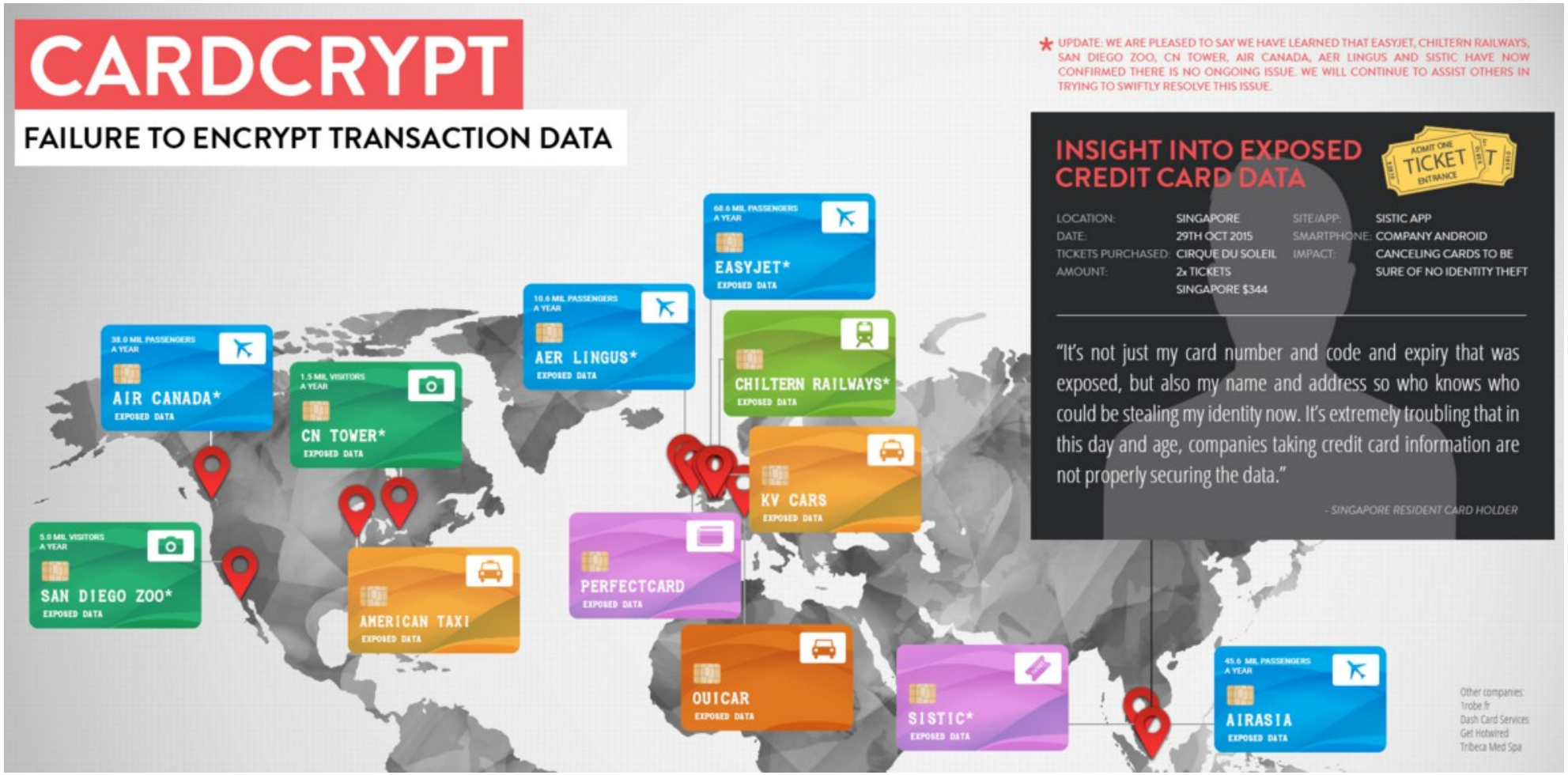

```
60      <key>launchCount</key>
61      <integer>92</integer>
62      <key>password</key>
63      <string>4e6e1e6144431fcde96a0657729d66b5b1f48df9</string>
64      <key>proVersion</key>
65      <true/>
66      <key>ratePopupShowed</key>
67      <true/>
68      <key>username</key>
```

wandera

M3 – Insecure Communication

- Moving data from A to B insecurely
  (TCP/IP, TLS, WiFi, Bluetooth, NFC, GSM, 3G, SMS, …)
- Examples
  - Use of non-secured channels
  - Lack of certificate inspection (SSL, TLS)
  - Weak handshake negotiation
- Advices
  - Transport sensitive data securely – always!
  - Track where data goes and how

M3 – Insecure Communication



wandera

M3 – Insecure Communication

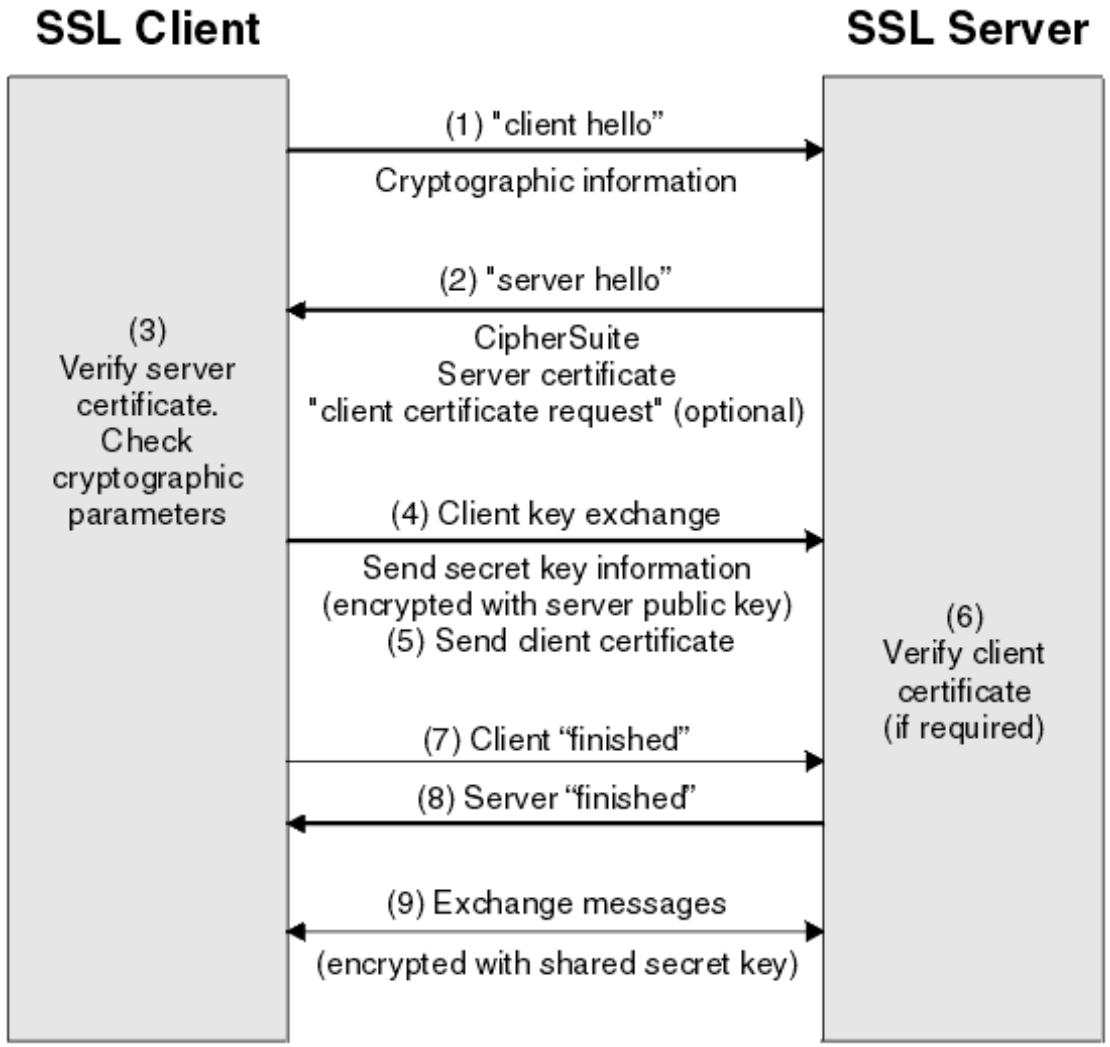
- CardCrypt regex:

```
^(?:4[0-9]{12}(?:[0-9]{3})?          # Visa
|  5[1-5][0-9]{14}                   # MasterCard
|  3[47][0-9]{13}                    # American Express
|  3(?:0[0-5]|[68][0-9])[0-9]{11}    # Diners Club
|  6(?:011|5[0-9]{2})[0-9]{12}       # Discover
|  (?:2131|1800|35\d{3})\d{11}       # JCB)$
```

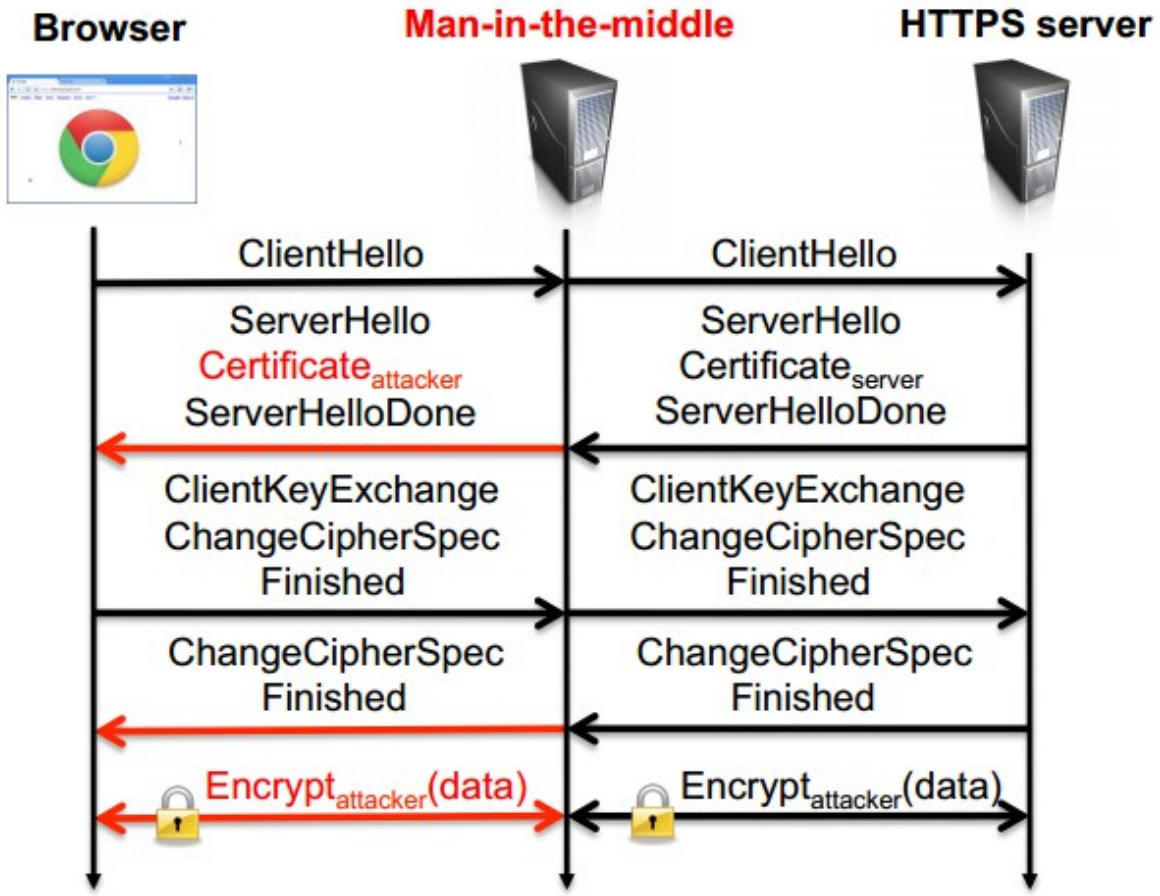
- URL:
  http://services.XXXXXXX.com/mci/start;jsessionid=0000MGP0s4IfmahBnFIOEXYnYa_:acsaywg00017mciprd1f2CloneId?_flowExecutionKey=_c560FB507-C2B0-26A9-08EB-7482E4BD0734_kA0E60EBA-A1C8-37BF-F699-E947E4BF171D

- POST message:
  _flowExecutionKey#_c560FB507-C2B0-26A9-08EB-7482E4BD0734_kA0E60EBA-A1C8-37BF-F699-E947E4BF171D#creditCard.type#AX#creditCard.form_of_payment#**3790XXXXXXXXXXX**#creditCard.expiry.month#07#creditCard.expiry.year#2019#creditCard.nameOnCard#Melissa#XXXXXXX#_eventId_continue#Continue

M3 – Insecure Communication



M3 – Insecure Communication



M4 – Insecure Authentication

- Weaknesses in session management, user identification, device enrollment, …
- Examples
  - Trivially Guessed Identifiers
  - Private Data Used As Identity
  - Anonymous Service Endpoints
  - Client only logout
- Advices
  - Bother who is on the other side
  - Implement session timeouts

M5 – Insufficient Cryptography

- Cryptography was attempted but it wasn't done correctly :-)
- Examples
  - Small or poor keys (predictable randomness)
  - Easily forged integrity checks
  - Wrong type of crypto (symmetric when asymmetric is more appropriate)
- Advices
  -

An empirical study of cryptographic misuse in android applications

M6 – Insecure Authorization

- Any failures in authorization
- Examples
  - Authentication instead of authorization
  - Client-based authorization decisions
  - Forced browsing
- Advices
  - Always check permissions

M7 – Client Code Quality

- Code-level implementation problems in the mobile client (language dependent)
- Examples
  - Buffer overflow in C
  - Format string vulnerability
  - …
- Advices
  - Keep high code quality (reviews, testing, static analysis)

M8 – Code Tampering

- Modifications to the application package (code or resources)
- Examples
  - Malware payloads
  - Short-circuited in-application purchase
  - Steal credentials or data
- Advices
  - Package/code region checksum
  - Complicate static analysis (misleading code)
  - Complicate dynamic analysis (detect jailbroken/rooted device)

M9 – Reverse Engineering

- Analysis of the app to determine its source code, libraries, algorithms, and other assets
- Examples
  - (Android) apk is an archive containing assets and classes.dex
    Dex to Jar converter + Java decompiler ;-)
- Advices
  - Avoid security through obscurity
  - Obfuscate your code
  - Place important logic on the server side if possible

M10 – Extraneous Functionality

- Extra security security controls that are not intended to be released
- Examples
  - Plaintext password in comments or assets
  - Disabled (two-factor) authentication from testing process
  - Existing (hidden) backdoor functionality
- Advices
  - Avoid security through obscurity
  - Set up process to avoid human errors

Wrap up

- Security is a complex task
- Understand what you are doing
- Employ best practices and available tools
- Set up processes to minimize possibility of human errors
- Design security with respect to possible attack