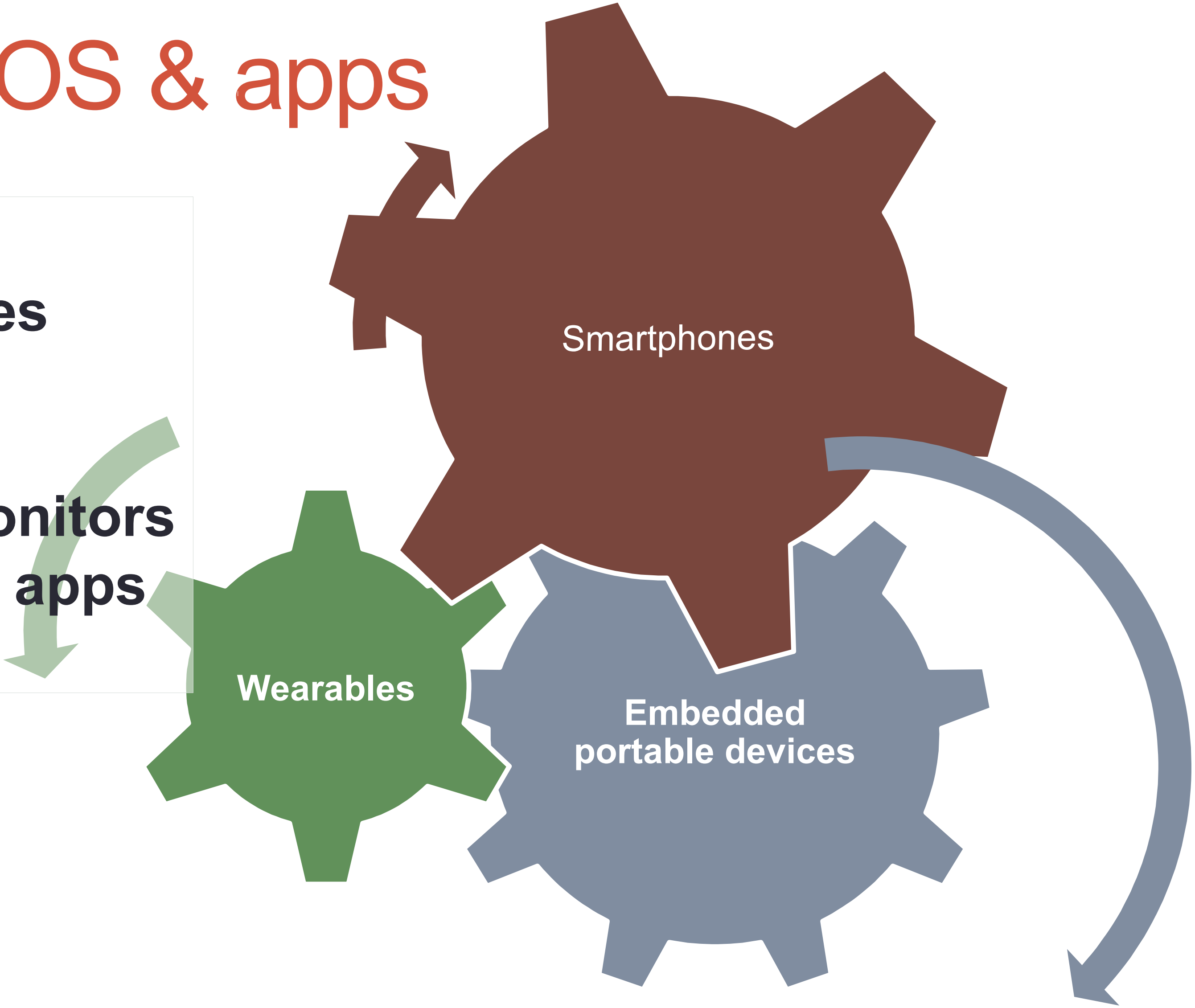
How private is your mobile health advisor? Free popular m-Health apps under review

Papageorgiou A., Strigkos M., Politou E., Alepis E., Solanas. A, Patsakis C.

Cryptacus: Workshop & MC meeting 2017

Android OS & apps

Usages:
Smart phones
Wearables
Smart cars
Smart TV Monitors
Smart home apps
and more…



How private is your mobile health advisor? Free popular m-Health apps under review

Problem statement

- Million of users today are sharing their **health data** using apps
- Many different publishers/developers from all over the world store & process users' data
- **Ground truth**: Users do **not** know who can trust and in most of the cases **blindly trust the most popular apps**

How private is your mobile health advisor? Free popular m-Health apps under review

Health data sensitivity

- **Health data** are considered to be sensitive data by all of the well-known regulations e.g. HIPAA, PIPEDA, GDPR etc.
- Health data can harm the reputation of a person and/or create financial costs.
- Anyone would expect that **at least the popular apps** would protect their users' health data

How private is your mobile health advisor? Free popular m-Health apps under review

Research questions

- **What data** are shared **with whom** (vendors, third parties)?
- Are these data transmitted securely?
- How do developers respond to bug reports?
- How well prepared are we for the General Data Privacy Regulation (**GDPR**)?

Our sample

20 apps for (i) pregnancy and baby growth, (ii) 'personal/family members' health agenda and symptoms assistants/checkers, (iii) blood pressure and diabetes support

- **Content in English**
- Minimum rating of **3.5/5 stars on Google Play**

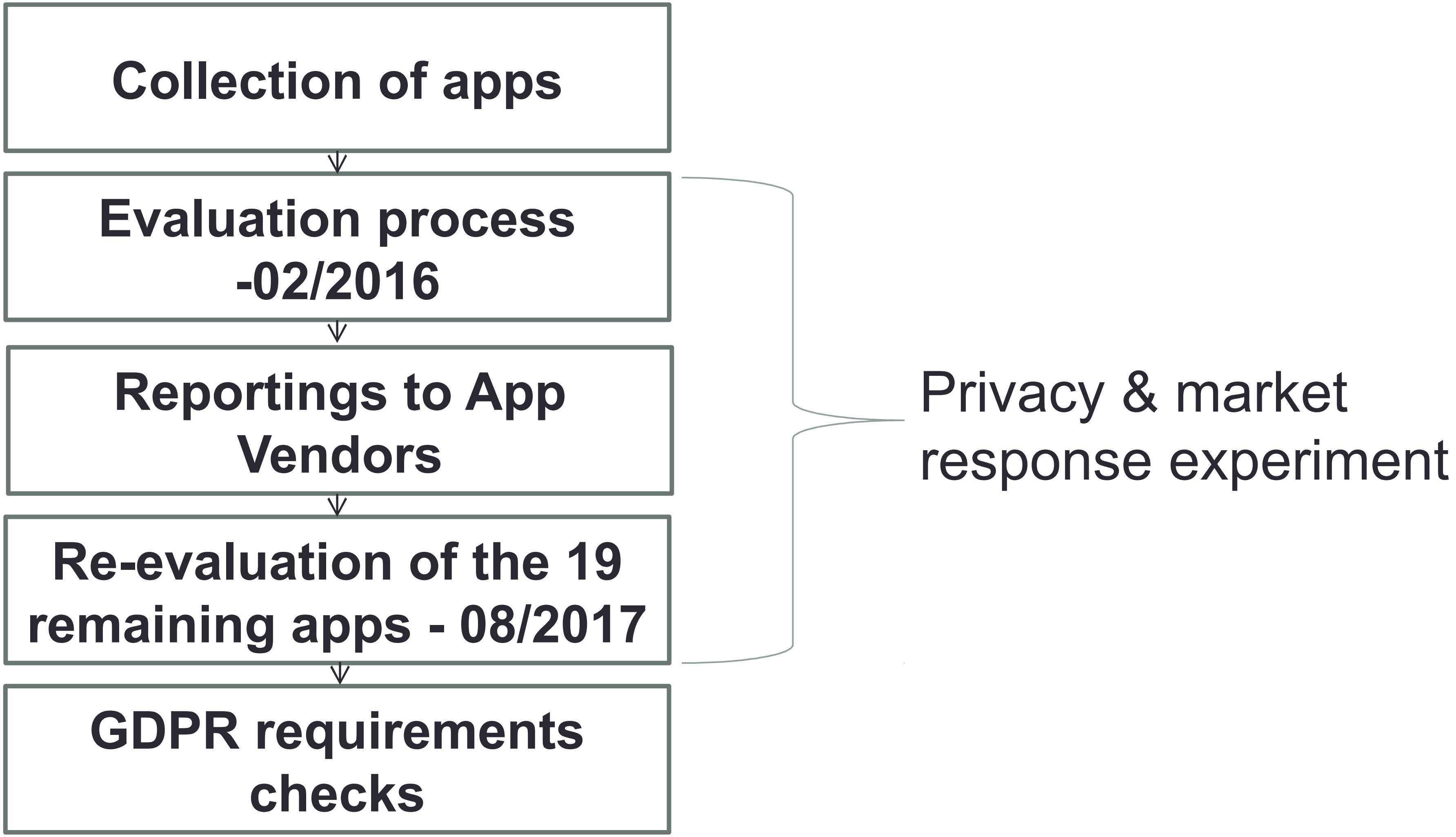
Downloads	#of apps
5.000.000 – 10.000.000	2
1.000.000 – 5.000.000	9
500.000 – 1.000.000	3
100.000 – 500.000	6

*Stats by Google Play up to **01/2016** when we started the first round of APK collection*

Steps of our methodology

- We carefully read the scope and objectives of each app and emulate a typical user's behavior
- Privacy policies inspection
- Dynamic analysis (web debugging tool)
- SSL/TLS assessment (ssllabs.com)
- Reporting and Re-evaluation
- Examination of critical GDPR functional and non-functional requirements

Market response analysis



Collection of apps

Evaluation process -02/2016

Reportings to App Vendors

Re-evaluation of the 19 remaining apps - 08/2017

GDPR requirements checks

Privacy & market response experiment

How private is your mobile health advisor? Free popular m-Health apps under review

Findings – Health data

- **80% (16/20) of apps** transmitted health data over the network – **20% (4/20)** stored them **locally**
  - **50% (8/16) of apps** shared health data at least with one third party entity – **75% (6/8)** of them over HTTP
  - **44% (7/16) of apps** that transmitted health data sent them **via GET requests** including the **health data at the URLs**

How private is your mobile health advisor? Free popular m-Health apps under review

Findings – The user’s multimedia

- **20% (4/20) of the apps** requested them
  - **50% (2/4) of those over HTTP**
  - **75% (3/4) of the apps** transmitted them to **third party storage**
  - **Static links**

Patsakis, C., Zigomitros, A., Papageorgiou, A., & Solanas, A. (2014). Privacy and security for multimedia content shared on OSNs: issues and countermeasures. *The Computer Journal*, *58*(4), 518-535.

Findings – The app’s multimedia

There is no need to be a psychic!

The unencrypted transmission of multimedia content can easily lead to the exposure of the scope of the app, or even the condition of the user instantly!

Findings – Location

- **35% (7/20) of the apps** transmitted users' geolocation information or the address
  - **49% (3/7) of those apps** sent the location **over HTTP**
  - **71% (5/7) of the apps** that transmitted users' location requested it with a **GET request**
  - **One app sent user's location** to **2** of its **3rd party ad services** at a rate of almost **one request per 3 seconds** over **HTTP** connections via **GET requests**

How private is your mobile health advisor? Free popular m-Health apps under review

Findings – Email address

- **15 apps** were found to transmit at least to one domain the user’s email address
  - **33% (5/15)** used HTTP
  - **60% (5/15)** of them sent it to a third party
  - **One of them** sent it an **unknown IP** couldn't be identified based on online resources.

Findings – Search queries

- **25% (5/20) of the apps** transmitted the **search queries of their users**
  - **Only one app over HTTPS!**
  - **80% (4/5) of the apps** sent the searches to third parties
  - **Two of the apps** sent the health related queries **to 16 different 3rd party domains**
  - **ALL** of the apps that found to transmit their users' search queries used **GET requests.**

How private is your mobile health advisor? Free popular m-Health apps under review

Findings – Chat

- We found **2 apps** containing chat functionalities
- Chat is the place where users discuss their health issues and occasionally ask questions or help
- **No encryption!**

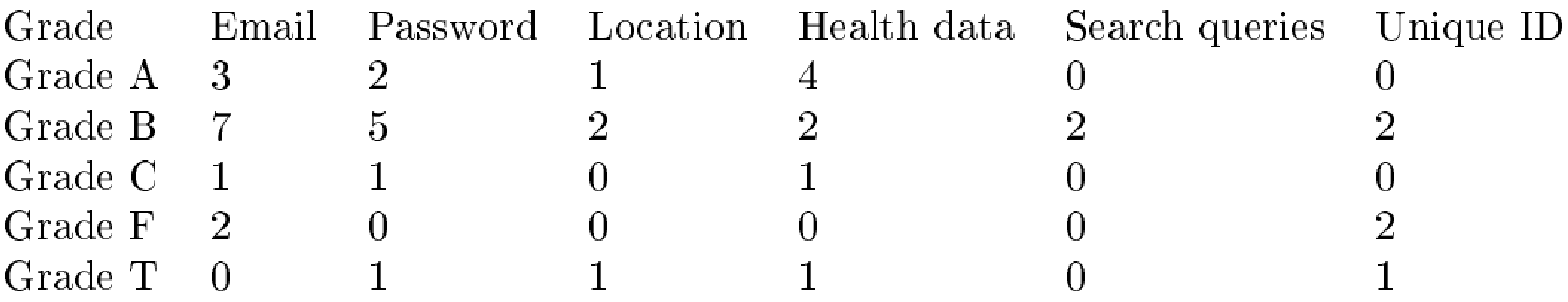
Hello, I have health issues, but at my job they don't know anything!

Don't worry nobody will find it here! I also have health issues. Let's talk!

How private is your mobile health advisor? Free popular m-Health apps under review

Findings – SSL/TLS

Number of HTTPS connections for each data category per SSL grade based on ssllabs.com results



Grade	Email	Password	Location	Health data	Search queries	Unique ID
Grade A	3	2	1	4	0	0
Grade B	7	5	2	2	2	2
Grade C	1	1	0	1	0	0
Grade F	2	0	0	0	0	2
Grade T	0	1	1	1	0	1

https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

Re-evaluation and market response

By the end of **July to August 2017** we ran a **re-evaluation process** using the updated versions of APKs

Meanwhile…

- Google notified by email the developers since the early 2017 to provide a valid privacy policy when they are requesting **sensitive permissions** or **user data** either their apps are at risk of removal from the Play Store on March 15

How private is your mobile health advisor? Free popular m-Health apps under review

Findings – Privacy Policy

(02/2016) Before our reportings

2/20 apps do not provided any link, **one app** provided a link to non-English content, **one app** provided a link to a 404 error page

(07/2017) After our reportings and Google's recommendations by email

Only one of the apps responded providing a link to a **valid Privacy policy** section

Major & Minor issues

Major

- **75%** had major issues
- **53% of them** fixed at least **one major** issue
- **27% of them** fixed all of the reported issues

Minor

- **60%** had minor issues
- **42% of them** fixed **at least one** minor issue
- **25% of them** fixed all of the reported issues

How private is your mobile health advisor? Free popular m-Health apps under review

GDPR readiness - 25th May 2018

Consent

- **Only one** apps is found to asks for user consent up front each time the user provides additional information

Right to withdraw consent

- **37% of the apps** provide a mechanism to user to withdraw its consent, and allow the erasure of any previously consented information

Right to data portability

- **37% of the apps** provide a mechanism to send, upon request, the personal data to another entity in a machine readable format

Transfer to third countries

- **42% of apps** notify their users in advance, even before their registration, that they are sharing data with third parties. **Only 21% of apps** in a functional manner (i.e. pop up with a checkbox)

How private is your mobile health advisor? Free popular m-Health apps under review

Conclusions

- Very **sensitive data** are managed by apps that are vulnerable to **simple sniffing attacks**
- Most of the detected vulnerabilities have **very simple solutions** that do not require much effort to fix, but **only few apps fixed them**
- **Users** can be **victims** of user profiling, blackmailing, stalking, defamation, and even identity theft for economical or reputation attacks

Open challenges

- App developers/publishers **seem to keep repeating** the same mistakes over every new software environment
- Will **GDPR** change this situation?
- **We are in the IoT era;** What about wearables? **Would you 'wear' such an app to your body?**

[How private is your mobile health advisor? Free popular m-Health apps under review](#)

References

[1] A. Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Pérez-Martínez, R. Di Pietro, D. N. Perrea, A. Martínez-Ballesté: Smart health: A context-aware health paradigm within smart cities. IEEE Communications Magazine 52(8): 74-81 (2014)

[2] “Home Page of EU GDPR,” http://www.eugdpr.org/

[3] T. Dehling, F. Gao, S. Schneider, and A. Sunyaev. Exploring the far side of mobile health: information security and privacy of mobile health apps on ios and android. JMIR mHealth and uHealth, 3(1):e8, 2015.

[4] S. Fahl, M. Harbach, T. Muders, L. Baumgärtner, B. Freisleben, and M. Smith. Why eve and mallory love android: An analysis of android ssl (in) security. In Proceedings of the 2012 ACM conference on Computer and communications security, pages 5061. ACM, 2012.

References

[5] K. Knorr and D. Aspinall. Security testing for android mhealth apps. In Software Testing, Verification and Validation Workshops (ICSTW), 2015 IEEE Eighth International Conference on, pages 1-8. IEEE, 2015.

[6] C. Patsakis, A. Zigomitros, and A. Solanas, “Analysis of privacy and security exposure in mobile dating applications,” in International Conference on Mobile, Secure and Programmable Networking. Springer, 2015, pp. 151–162.

[7] M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, “Analyzing android encrypted network traffic to identify user actions,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 1, pp. 114–125, 2016.

[8] P. de Hert and V. Papakonstantinou, “The new General Data Protection Regulation: Still a sound system for the protection of individuals?” Computer Law & Security Review, vol. 32, no. 2, pp. 179–194, 2016.

Thank you for your attention

Q&A

apapageorgiou@ieee.org