A Curious Case of "Consent Button"

[... neither do I want to accept, nor decline ...]

Nurul Momen & Lothar Fritsch

Karlstad University

19 July, 2019.
HotPETs, KTH, Stockholm

I want to find an app to wash my hands ...

Image source: running faucet by Steve Johnson (CC-BY-2.0)

What happens next?

- Personal data access: a lot more than a user can observe.
- Partial identities can be extracted from privilege usage data.

Paper I. How much Privilege does an App Need? Investigating Resource Usage of Android Apps; N Momen, T Pulls, L Fritsch, and S Lindskog; In *Proceedings of the Fifteenth International Conference on Privacy, Security and Trust (PST), Calgary, Canada, August 28-30*, IEEE, 2017.
Paper II. Derived Partial Identities Generated from App Permissions; L Fritsch, and N Momen; In *Proceedings of the Open Identity Summit 2017; Lecture Notes in Informatics (LNI) 277, ISSN 1617-5468, ISBN 978-3-88579-671-8, October 05–06, 2017; Karlstad, Sweden.*, Gesellschaft für Informatik e.V., 2017.

Good and bad behavior of apps

1. Requirement types (price): what does it ask for & how much of the privilege is being used?
2. Legal requirements: does it comply with the regulations?
3. Crowd-sourced user feedback: what do other users think?

Let's judge an apps' behavior ...

ix. Fitbit: 20 (9/3/3/T) [Threat count, T=5]
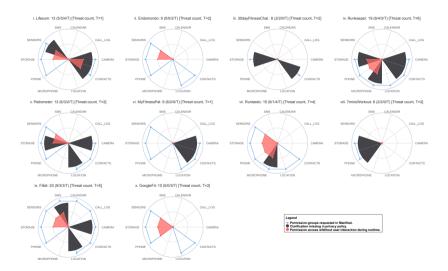
Legend
- Permission-groups requested in Manifest.
- Clarification missing in privacy policy.
- Permission access whithout user interaction during runtime.
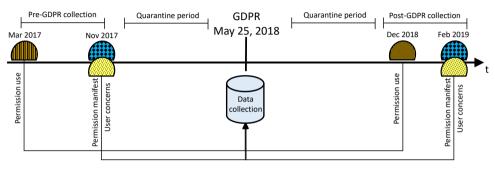
Let's compare with other apps ...

i. Lifesum: 13 (5/3/4/T) [Threat count, T=1]   ii. Endomondo: 9 (5/0/2/T) [Threat count, T=2]   iii. 30dayFitnessChal.: 6 (2/2/0/T) [Threat count, T=2]   iv. Runkeeper: 19 (6/4/3/T) [Threat count, T=6]

v. Pedometer: 13 (6/3/2/T) [Threat count, T=2]   vi. MyFitnessPal: 9 (6/2/0/T) [Threat count, T=1]   vii. Runtastic: 15 (6/1/4/T) [Threat count, T=4]   viii. 7minsWorkout: 6 (2/2/0/T) [Threat count, T=2]

ix. Fitbit: 20 (9/3/3/T) [Threat count, T=5]   x. GoogleFit: 10 (5/0/3/T) [Threat count, T=2]

Legend
- Permission-groups requested in Manifest.
- Clarification missing in privacy policy.
- Permission access without user interaction during runtime.

Paper III: A Multilateral Privacy Impact Analysis Method for Android Apps; M Hatamian, N Momen, L Fritsch, K Rannenberg; In *Proceedings of Annual Privacy Forum 2019*, Rome, Italy, page 87-106.
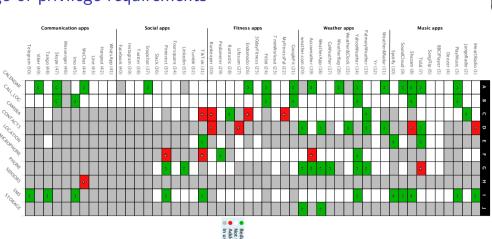
But, apps change requirements!

Overview of data collection periods.

Paper IV: Did app privacy improve after GDPR? N Momen, M Hatamian, L Fritsch; To appear in *IEEE Security Privacy Magazine 2019*.
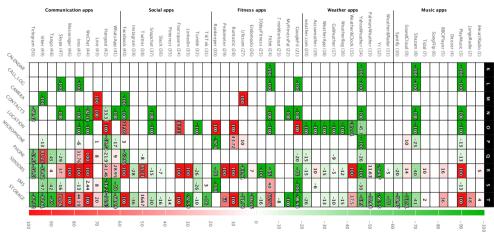
7 / 15

Change of privilege-requirements

Paper IV: Did app privacy improve after GDPR? N Momen, M Hatamian, L Fritsch; To appear in *IEEE Security Privacy Magazine 2019*.

Change of privilege usage pattern

Paper IV: Did app privacy improve after GDPR? N Momen, M Hatamian, L Fritsch; To appear in *IEEE Security Privacy Magazine 2019*.

Wait, wait … That's a lot to consider!

How can a user re-evaluate decisions taken earlier with ease?

Confused?

I don't know!

Confused?

I don't know!
So, maybe?

Accept **Maybe** **Decline**

Paper V: Partial Commitment–"Try Before You Buy" and "Buyer's Remorse" for Personal Data in Big Data Machine Learning; L Fritsch; *IFIP International Conference on Trust Management, page 3-11.*

Partial commitment

Consent with an expiry date.
Consent for a subset of data.
Consent for limited access.

Evaluation of privacy-preserving-performance.
Decision to continue or revoke access.
Intervenability.

Wrapping up ...

Problems:

- ▶ Leaving the *data-tap* open.
- ▶ Poor means for monitoring.
- ▶ Consent for eternity.

Looking ahead:

- ▶ Methods to determine privacy-impact assessment cues.
- ▶ Burdensome responsibility to assess the cues.
- ▶ Starting a discussion about *partial commitment*.

Questions & discussion

Contacts:
1. Nurul Momen, PhD Candidate, PriSec, Computer Science Dept. Karlstad University.
email: nurul.momen@kau.se
2. Lothar Fritsch, Associate Professor, PriSec, Computer Science Dept. Karlstad University.
email: lothar.fritsch@kau.se

References:
Paper I: How much Privilege does an App Need? Investigating Resource Usage of Android Apps; N Momen, T Pulls, L Fritsch, and S Lindskog; In *Proceedings of the Fifteenth International Conference on Privacy, Security and Trust (PST), Calgary, Canada, August 28-30*, IEEE, 2017.
Paper II: Derived Partial Identities Generated from App Permissions; L Fritsch, and N Momen; In *Proceedings of the Open Identity Summit 2017; Lecture Notes in Informatics (LNI) 277, ISSN 1617-5468, ISBN 978-3-88579-671-8, October 05–06, 2017; Karlstad, Sweden.*, Gesellschaft für Informatik e.V., 2017.
Paper III: A Multilateral Privacy Impact Analysis Method for Android Apps; M Hatamian, N Momen, L Fritsch, K Rannenberg; In *Proceedings of Annual Privacy Forum 2019*, Rome, Italy, page 87-106.
Paper IV: Did app privacy improve after GDPR? N Momen, M Hatamian, L Fritsch; To appear in *IEEE Security Privacy Magazine 2019.*
Paper V: Partial Commitment–"Try Before You Buy" and "Buyer's Remorse" for Personal Data in Big Data Machine Learning; L Fritsch; *IFIP International Conference on Trust Management, page 3-11.*