



#### Risk Assessment von Smartphone Apps im Unternehmenskontext

Majid Hatamian, Dr. Sebastian Pape, Prof. Dr. Kai Rannenberg



#### GFFT Technology Race IT-Security bei Thyssenkrupp

28. Juni 2018



### Background: Bring Your Own Device





### Effects of Bring Your Own Device



Source: www.dilbert.com, May 28, 2008

- Loss of Control
- Additional Risks
- Hard to counter
  - $\rightarrow$  Solution:
    - Educate Employees
  - Awareness Raising
  - Security Policies







M. Hatamian, <u>S. Pape</u>, K. Rannenberg

Source: Statista, June 2018



### VeraCode: Mobile Apps Top 10 Risks

#### A. Malicious Functionality

- Activity monitoring and data retrieval
- Unauthorized dialing, SMS, and payments
- Unauthorized network connectivity (exfiltration or command & control)
- UI Impersonation
- System modification (rootkit, APN proxy config)
- Logic or Time bomb
- B. Vulnerabilities
- Sensitive data leakage (inadvertent or side channel)
- Unsafe sensitive data storage
- Unsafe sensitive data transmission
- Hardcoded password/keys





# Privacy Risks of Smartphone App Usage

- Apps are useful and provide utility.
- APIs (e.g. geolocation API) as
  - ... enabler of utility.
  - … threat to user privacy.



- Negative examples: "Brightest Flashlight", Uber & Facebook
- Lack of risk transparency and "hidden" information flows lead to a bias in users' risk perceptions.
- Explicitness regarding consequences can help (Laughery et al. 1993).



# Current Privacy-Risk Communication

### Current privacy risk information is...

- ... static,
- ... coarse-grained & technical,
- ... timed inappropriately,
- … largely ignored,
- ... not supporting informed decision-making.

Eacebook Messenger	
Accept & download	
Your messages	
Edit your text messages (SMS or MMS), r	ead
text messages (MMS), receive text messa	ages
(SMS)	
Storage	
Modify or delete the contents of your USE	
storage	
System tools	
Change network connectivity, prevent pho	one
from sleeping	
Your location	
Approximate (network-based) location,	
precise (GPS) location	



## Corporates Smartphone Apps Risk Assessment (COSARA)

# Motivation

- Invasive apps access (ir)relevant resources without users' knowledge
- It is challenging for the corporates to protect their confidential data from threats

e.g. data leakage, malware

• Employees usually use a diverse number of apps on their smartphones/tablets that their actual behaviour is not clear/verified.



### Transparency tool: Android App Behaviour Analyser (A3)

- Analysing installed apps' behaviour
- Measuring the potential privacy risks
- Risk communication to the user

06/28/2018



#### A3 Architecture





#### A3: Screenshots

0 11 11 6 15 0 1 1	<b>  💐 🛜 🔏 4</b> 3%	17:16	<b>€ № ∧1</b> 35% <b>≧</b> 14:24	🔲 🔂 💦 🕺 📶 35% 🛓 14	24 <b>⊡ С₀ № № "1</b> 35% <b>≟</b> 14:25
			1 <u>11</u> 2		
Scan Options			List of suspicious apps	List of suspicious apps	Report
			Q Search Here	Q Search Here	
Scan Duration	Default (	•	Pinterest	Photo Editor Pro	Read external storage 08:12:34
Scan Interval	1 Seconds	*	7 permissions used	2 permissions used	No anomalous access at that time
Delete Older Scans	Default (	•	SayHi 9 permissions used	Pinterest REPORT 7 permissions Useu	Read external storage 08:12:35 No anomalous access at that time
WIFI only			Tinder	54x Read external storage	Read external storage
Networking, only when connected to a Wifi netwo	rk		8 permissions used	51x Write external storage	08:12:45 No anomalous access at that time
			Twitter 12 permissions used	36x Access to read the Clipboard	Read external storage 08:12:48
			AASAservice 2 permissions used	Allows an application to read the users contacts data	You can give an explanation to why you want to report these resources:
			Active applications 2 permissions used	<sup>6x</sup> App prevent the System to change in the sleepmode	Enter your explanation here
			Android system	5x Required to be able to access the camera device	CANCEL REPORT
			ANT Padia Sarvica		REFORT



### 2-Phase Experiment

#### Phase 1:

- Installation of popular Apps on A3 Samsung
- Monitored access to resources
- Over period of 5 days
- No Interation with device

Phase 2:

- Like phase 1, but:
- Made Accounts
- No further interaction



M. Hatamian, J. Serna, K. Rannenberg, and B. Igler. 2017. "FAIR: Fuzzy Alarming Index Rule for Privacy Analysis in Smartphone Apps", 14th International Conference on Trust and Privacy in Digital Business (TrustBus 2017), pp. 3-18



### Use Case Analysis by A3 (First Phase)

	Health & Fitness						Social Networks					Dating & Friends				
Permissions	S Health	Google Fit	Lifesum	Pedometer	Calorie Counter	Facebook	Twitter	Instagram	LinkedIn	Pinterest	ΓΟΛΟΟ	OkCupid	Tinder	Badoo	SayHi	
READ_EXTERNAL_STORAGE	594	10	2	5	6	35	16	427	3	14	21	8	14	50	5	
WRITE_EXTERNAL_STORAGE	594	10	2	5	6	35	16	427	3	14	21	8	14	50	5	
READ_PHONE_STATE	Ι	-	Ι	-	-	5	-	-	Ι	-	-	-	4	35	-	
ACCESS_WIFI_STATE	Ι	Ι	Ι	-	Ι	Ι	-	-	Ι	Ι	Ι	-	Ι	57	-	
ACCESS_FINE_LOCATION	Ι	130	-	-	7	Ι	-	-	Ι	Ι	Ι	-	Ι	395	-	
ACCESS_COARSE_LOCATION	Ι	Ι	-	-		Ι	-	-	Ι	Ι	Ι	-	Ι	5	2	
READ_CONTACTS	Ι	Ι	Ι		Ι	1	-	-	Ι	Ι	Ι	-	١	-	-	
WRITE_CONTACTS	Ι	Ι	Ι	Ι	Ι	Ι	—	Ι	Ι	Ι	Ι	-	١	Ι	-	
RECORD_AUDIO	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
CAMERA	-	-	—	—	-	-	-	-	-	—	-	-	-	-	-	
BODY_SENSORS	425	-	-	-	-	-	-	-	-	1	-	-	1	-	-	



### Use Case Analysis by A3 (Second Phase)

	Health & Fitness						Social Networks					Dating & Friends				
Permissions	S Health	Google Fit	Lifesum	Pedometer	Calorie Counter	Facebook	Twitter	Instagram	LinkedIn	Pinterest	LOVOO	OkCupid	Tinder	Badoo	SayHi	
READ_EXTERNAL_STORAGE	1067	18	44	1	43	1531	63	580	28	54	143	41	212	349	27	
WRITE_EXTERNAL_STORAGE	1067	18	42	1	43	1375	49	583	27	51	118	41	196	343	29	
READ_PHONE_STATE	Ι	Ι	Ι	Ι	-	4	Ι	Ι	Ι	Ι	Ι	Ι	4	176	_	
ACCESS_WIFI_STATE	Ι	Ι	Ι	Ι	I	39	-	-	Ι	Ι	Ι	Ι	Ι	170	_	
ACCESS_FINE_LOCATION	3	452	-	-	123	346	43	31	Ι	Ι	37	35	37	599	_	
ACCESS_COARSE_LOCATION	Ι	Ι	-	-	16	381	Ι	_	-	Ι	4	3	Ι	47	29	
READ_CONTACTS	-	Ι	-	-	2	5	14	-	6	6	-	-	-	1	_	
WRITE_CONTACTS	-	-	-	-	_	_	_	_	1	_	-	-	-	_	-	
RECORD_AUDIO	-	-	-	—	-	1	8	2	-	_	_	_	-	1	_	
CAMERA	4	-	4	_	4	15	16	27	_	5	-	_	-	10	8	
BODY_SENSORS	465	-	-	-	-	-	-	-	-	-	-	-	-	-	-	

Additional observation: most access was done when user was not using the phone



### Privacy Risk Scores (A3)





## Corporates Smartphone Apps Risk Assessment (COSARA)

## COSARA

... is a methodology to support corporates to ease and automate the process of creating black/white lists

... performs risk assessment to rank similar functionality apps based on their real behaviour.



## **COSARA:** Architecture





### Main benefits of COSARA

- Decision making about apps that are neither in black nor in white lists
- Help for Classification of apps into allowed or not allowed risk level, e.g. by ICT security departments
- Ranking similar functionality apps to infer which ones are aggressively accessing users' personal info
- Enabling employees to report invasive activities that they have observed from their installed apps
- Recording and monitoring the history of app's version changes



#### **Deutsche Telekom Chair of Mobile Business & Multilateral Security**

#### **Dr. Sebastian Pape**

Goethe University Frankfurt Theodor-W.-Adorno-Platz 4 60629 Frankfurt, Germany

Phone +49 (0)69 798 34668 Fax +49 (0)69 798 35004

E-Mail: sebastian.pape@m-chair.de WWW: <u>www.m-chair.de</u>

