Human Factors in Big Data Privacy

Matthew Smith

Usable Security and Privacy Lab, Universität Bonn
Human Factors Group, Fraunhofer FKIE
If you are not paying
you are the product
In this talk: Two Big Domains

Mobile Computing

Social Networking
Many Interested Parties
The Hidden Privacy Threat of ... Flashlight Apps?

by Chris Brook

September 9, 2014, 1:17 pm

Free mobile apps a threat to privacy, study finds

PRIVACY VULNERABILITIES IN POPULAR ANDROID APPS DISCLOSED

12 Most Abused Android App Permissions
Privacy Threats (Social Media)

- Just in the last two years the number of photos uploaded to Facebook per month has risen from 2 billion to over 6 billion
- While one’s own media is uploaded consciously,
- the flood of media uploaded by others is so huge that it is almost impossible to stay aware of all media
- and most isn’t relevant anyway.

- We have a Big Data privacy problem
  - on the users side
  - not on the provider side.
Friendly Fire

- Microsoft’s Scott Charney offered a very good example during his Keynote speech at the RSA Conference 2012:

  If a friend takes a picture of me during a volleyball game, shares this picture with other friends and one of them uploads the picture to the web, my insurance company can find and use that picture against me.
This is happening

- There have been reports that insurance companies are looking for just such information which could raise premiums or even deny claims.¹
- The same is true for banks and credit rating companies.²


Data & Meta-Data
Privacy Threats & Metadata

1. Associate photo to person
   - Non-technical: person is recognizable on photo
   - Technical: image metadata contains link (name, unique identifier)

2. Photo contains objectionable content
   - Non-technical: image shows embarrassing actions or setting
   - Technical: image metadata contains objectionable entries like time, location, personal references
   - Metadata increasingly is automatically added and users may not be aware of embedded metadata.

Prof. Matthew Smith – Usable Security and Privacy – University of Bonn, Germany
Usable Security: An Emerging Research Field

Complexity is the worst enemy of security
  - Systems are getting ever more complex

We have the technology to make – almost – everything secure
  - We just don’t have the people to do it properly

We have two options:
  - Create more secure humans
  - Create more usable technology
Creating Awareness at Point of “Sharing”
Android Permissions

Brightest LED Flashlight Free
Version 1.0.8 can access

- modify or delete the contents of your USB storage

Camera/Microphone
- take pictures and videos

Wi-Fi connection information
- view Wi-Fi connections

Device ID & call information
- read phone status and identity

Other
- run at startup
- full network access
- modify system settings
- view network connections
- prevent phone from sleeping
- control flashlight
- change system display settings

Updates to Brightest LED Flashlight Free may automatically add additional capabilities within each group. Learn more
We have two options:

- Educate users about permission (good luck with that)
- Create a more intuitive way of communicating with users
Personal Warnings

Shazam – Musik
benötigt Zugriff auf

Ihr Standort
Diese App wird wissen wo Sie sich befinden und wohin Sie gehen.

Internet
Diese App kann mit dem Internet kommunizieren und somit Ihre privaten Daten hochladen oder Schadsoftware, wie z.B. Viren, herunterladen.

AKZEPTIEREN
Personal Warnings

Facebook
benötigt Zugriff auf

03.12.2014 13:30 - 03.12.2014 14:00
Berlin

Kontakte

Diese App kann alle Kontakte in Ihrem Adressbuch sehen und auch hinzufügen und Sie somit möglicherweise veranlassen unbekannte und kostenpflichtige Nummern anzurufen.

Sascha Fahl
+4915256807857
sascha.fahl@googlemail.com

Anrufe tätigen

Diese App kann beliebige Telefonnummern anrufen, unter anderem auch Premiumdienste, und dadurch Kosten verursachen.
User Study

- **Lab Study**
  - N=36, 12 female, 19-30 years old
- **Online Study**
  - N=332, 128 female, 18-64 years old
- Installed mockup app on personal device (lab) or Web-based Play Store mockup (online)
- Each participant was asked to choose between two apps in six categories
- One app requested more permissions than the other
  - having similar functionality, ratings, and visual appeal
“Omg, it can see my photos? I don't want that! *This scares me a bit...*”

“Now *I understand what this „phone status“ permission means*. I did not get that before. I'll be more careful in the future!”

“The new system is a lot better. I'd prefer to use it in the future because it helps me to *understand whether a permission might be necessary or not.*”
Chrome Meta-data Extension

- Visualize relevant meta-data
  - Browsing mode
    - Raise awareness
    - Useful for positive meta-data
  - Upload mode
    - Interrupt upload process
    - Visualize meta-data
    - Help remove/edit/encrypt meta-data
    - Enable users to make conscious choice

Quick indicator icons (size x2)
Uploading

Editing buttons

- i explain content
- edit content
- remove metatag

Continue upload

Photo.JPG 3264x2248 Pixel | image/jpeg | 1792 kByte

Location

EXIF
Lat: 45.97106
Lng: 8.97145

Click to edit this exif tag

Date & Time

GPS Date
2013:10:11 09:32:08

Date / Time

People

Name: Sebastian

Location

Sub-Location
Augusta Street

City 
Linden

Province/State
Wisconsin

Content Description

Caption
Grandma on a visit

Show all metadata

Continue upload
Continue upload; encrypt metadata

grandma-visit-08.jpg 1088x1672 Pixel | image/jpeg | 1704 kByte
Awareness Improvement

- Lab study with 43 attendees
  - 62.8% of the participants were female
  - 37.2% were male
  - Average age was 24

- How much does the new feature improved awareness about what is shared with their photos.
  - 4.5 on a 5 point likert scale (5 very much)
  - with 69% answering very much.

- Same question about control of what is shared,
  - 4.3
  - with 55% answering very much.
Staying on top of the big-data deluge

(what do others share about me?)
Privacy Threats (Social Media)

- Just in the last two years the number of photos uploaded to Facebook per month has risen from 2 billion to over 6 billion.
- While one’s own media is uploaded consciously,
- the flood of media uploaded by others is so huge that it is almost impossible to stay aware of all media
- and most isn’t relevant anyway.

- We have a Big Data privacy problem
  - on the users side
  - not on the provider side.
Users define private locations on a map or update their current location at the service using a LBS. Based on co-location checks of users' location and the location information of photos uploaded to the SNS via the service, the service notifies users who may be depicted in a photo based on respective locations.
Online Survey with 414 participants:

- “I am less upset if someone finds out where I have been than if that person gets to see private photos of myself.”
  - mean 3.0 (sd=1.7); 66.2 % agreed, 15.7 % neutral

- “I am less upset if my SNS knows where I have been than if my friends and strangers gets to see unwanted photos of myself.”
  - mean 3.3 (sd=1.8); 60.4 % agreed, 16.2 % neutral

- “If there is a privacy service that notifies me about unwanted photos in which I am depicted but needs to know where I have been, I would use it. I would tell it where I have been to get to see potential photos of myself.”
  - mean 3.7 (sd=1.8); 53.2 % agreed, 16.1 % neutral
Open Problems

- What goes on behind the (cloud) curtain?

- And how do we make that transparent & understandable?