Lecture "Privacy Enhancing Technologies for Data Science (PETs4DS)
Winter Semester 2016/17
Informatik 5, Lehrstuhl Prof. Decker

RWTH AACHEN UNIVERSITY

Assignment 1

Date for exercise session : 17.11.2016

Information:

1. Participants are encouraged to present their solutions for the exercises.
2. In addition, solutions to the exercises will be presented at the exercise session and published in L2P.
3. Working on the exercises in groups is welcome.
4. The assignments of this lecture series are not graded.
5. Instead, participation in the exams depends on passing the presence exercise in January.

Exercise 1: security versus privacy

In April 2016, WhatsApp introduced full end-to-end encryption for messages sent between users of WhatsApp. WhatsApp has around 1 billion active users.
How would you motivate this move from these perspectives:

- security
- privacy

Which of these perspectives was the more important factor for adding end-to-end encryption in your opinion?

You can find more non-technical background on the encryption used by Whatsapp here:
https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/

Exercise 2: LINDDUN privacy threat analysis

(A) Make a data flow diagram based on the following simplified description of an Internet of Things device:

- The device is an IP-connected security camera.
- Whenever the camera is switched on, after the initial setup, it connects via WiFi to the server of the company who manufactured the camera.
- You can assume that the user already configured how the camera should access the Internet via his WiFi network. For that reason, you do not have to add any entities to the DFD relating to this.
- The camera then sends the server its device ID, and starts sending a video stream to the server.
- The server stores the video feed, in order to allow the user to view time lapse footage from the camera. This allows for instance, to quickly check if anything happened during the full night.
- In order to gain access to the camera, the user starts the smartphone app from the same manufacturer, and enters the device ID (which is printed on the side of the camera).
- The smartphone app then connects to the server of the manufacturer. It sends the device ID to the server, and the server forwards the video stream from the camera to the app.

(B) List all the potential privacy threat categories which apply to the following entities.

- The data flow between the smartphone app and the server.
- The data storage for the server side video storage.
- The user of the smart phone app.
- The system as a whole (smart phone app and the server).

(C) For each of these potential privacy threats, describe (verb ?) the following:

- does the privacy threat apply to the specific DFD element ?
- if yes, provide a short description of an attack using that privacy threat.
- If you need help, regarding the formulation of the attacks, you can take a look at the privacy threat tree catalog in LINDDUN_catalog_v2.pdf

(D) How would you change the system to address the identified privacy threats? List your changes to the system and explain how these changes address the privacy threats.

Exercise 3: applicability of privacy threat analysis

The popular mobile game Pokemon Go was released in the summer of 2016.
In the very first version, the game only allowed users to log in with an account from pokemon.com or with an existing Google account. The pokemon.com site was overloaded from the popularity of the game, therefore many users logged in with their Google account.
The game then requested access to the full user account without explaining this to users. In the second version, this was changed, so the game only requested access to the basic Google account information, such as the Google user ID and email address.

- How would you argue for or against applying the LINDDUN privacy threat analysis framework to this example?
- Can you formulate a potential attack against the user of the first version of Pokemon Go in relation to the threats of linkability, identifiability and unawareness?
- Why does the LINDDUN framework specify that non-repudiation, detectability, disclosure and non-compliance do not apply to users and other external entities of a system?

More background can be found here: http://www.polygon.com/2016/7/11/12151442/pokemon-go-security-risk-data-information-ios-android

Exercise 4: thought experiment about privacy levels

[This is an optional task, and your solution should stay private.]
Think about a situation in which you or somebody you know from your family or friends experienced disclosure of private information or had some other issue in relation to privacy. Now consider changing any or all details of the story in order to tell it to different audiences. How would you change it for the following audiences:

- dinner with one or both of your parents
- banter in a pub on a night out with friends
- as an example in this lecture
- on public radio

Is there an audience to which you would prefer not telling the story at all?