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

RWTH AACHEN UNIVERSITY

Solutions for Assignment 1

Date for exercise session : 17.11.2016

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/

Solution

Relevant functionality of WhatsApp: Whatsapp uses a "store and forward" mechanism for exchanging messages between users. There were no / not many cases of **information disclosure** via communication of messages between client and server reported, so we can assume that exchange of messages between Whatsapp client and server was secure enough to guard against unintended disclosure of information, such as passwords, PINs and such. In addition, all stored messages where deleted after 30 days. Whatsapp uses the Signal protocol to implement the end-to-end encryption. For the Signal protocol the messages are stored in an encrypted format to which only the communication participants have the keys, but not the service provider.

Motivation from a security perspective: The introduction of end-to-end encryption only adds protection against one security threat: unintended disclosure of information via the server on which the messages are stored. Implementing the Signal protocol guards against Whatsapp unauthorised access to the

message storage (e.g. by insiders) and against being forced to disclose the contents of past, present and future encrypted messages. The main disclosure threat in regards to the message storage comes from state actors, as they can demand access to the server via legal means such as court orders. By introducing end-to-end encryption Facebook is able to plausibly deny access to the messages, as it does not have access to the keys. However, state actors can still use legal means to access the contents of the clients used for Whatsapp, e.g. via the smart phones used.

Motivation from a privacy perspective: A very similar reasoning applies to the privacy perspective, as information disclosure is also a privacy threat. Guarding against information disclosure threats from state actors, enables Whatsapp to provide privacy guarantees which go beyond the privacy which offline forms of communication such as letters offer in many countries. Keep in mind that the secrecy of letters can be legally undermined in most countries by intelligence agencies. In addition, having plausible deniability regarding the keys to access the messages and thus the contents of the messages, allows Whatsapp to deny requests from any kind of state actor world wide, as not just Western countries have demanded access to Whatsapp messages.

Other motivation: Competition in a business sense. Several other messaging platforms introduced some sort of additional security measure, including end-to-end encryption, so it is reasonable to expect that WhatsApp was worried about users switching to other providers. Another motivation might have been to remove one of the main fears of WhatsApp users when WhatsApp was bought by Facebook. Many users were afraid of Facebook having access to their WhatsApp messages, and by implementing full end-to-end encryption Facebook does not have that possibility.

Which motivation was more important? Non-state actors don't have a lot of opportunities to threaten the security of the message storage, beyond trying to gain unauthorised access to the storage. However, state actors can bypass security protection via legal means, e.g. by using court orders or by using their state monopoly on power e.g. via sending the police collect smartphones from potential suspects. In these situations, security is no longer the important consideration for the users who communicated, but privacy. Therefore the argument can be made that from the perspective of the service operator, protecting the privacy of the user from unintended disclosure is the main motivation for the move by WhatsApp to add end-to-end encryption.

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 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.

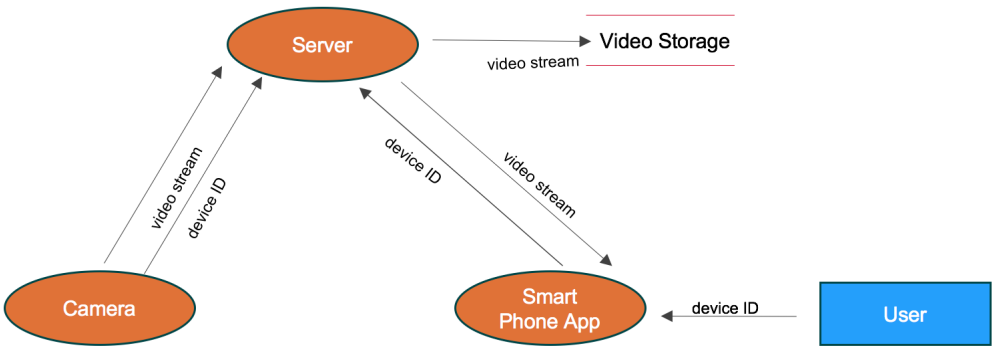

Figure 1: **Solution for (A)** DFD Diagram for the IoT video camera use case.

Solution

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

The data flow between the smartphone app and the server: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Non-Compliance (see below).

The data storage for the server side video storage: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Non-Compliance (see below).

The user of the smart phone app: Linkability, Identifiability, Content unawareness.

The system as a whole (smart phone app and the server): Non-compliance always applies to the whole system. It is the only threat which applies to the whole system.

(C)

The data flow between the smartphone app and the server

Linkability Yes. Different data flows of the same user (i.e. at different times or from different devices) can be linked via the device ID. Attack description: An identity thief who sees a camera from this manufacturer can try to intercept the WiFi traffic to obtain the deviceID. Then the thief can follow the user to his place of work, and WiFi traffic of the app to the same user via the deviceID.

Identifiability Yes. The stream as such contains nothing which points to the real-world identity of the user. However, there is a chance that the video stream contains images which help in identification. For instance, the camera might be pointing at the parking lot in front of the house of the user. From the license plate, an attacker can try to infer the identity of at least one person in the household of the user.

Non-repudiation No. Unless the video stream contains images adding in re-identification, non-repudiation is not a threat. For instance a video camera pointed at the garden of a user in winter, will probably not show anything unique to the user, so the user can claim that it is not his garden. However, the user can not deny using the video camera.

Detectability Yes. It is possible to determine that the user is using a video camera from the manufacturer. A man-in-the-middle attacker can use this to decide to capture the video stream.

Disclosure of information Yes. As no further protection of the video stream is specified, an attacker can see everything the camera is seeing. See above the example with the license plate.

The data storage for the server side video storage

Linkability Yes, if the deviceID is saved together with a video, all videos of a device can be linked. An attacker can use this to collect a backlog of videos from a single camera (e.g. 1 year back) and learn something about whatever the camera is monitoring.

Identifiability No, unless a video shows something leading to the real world identity of the user.

Non-repudiation No, unless a video shows something leading to the real world identity of the user.

Detectability No, unless a video shows something leading to the real world identity of the user.

Disclosure of information No, unless a video shows something leading to the real world identity of the user.

Alternatively, it is possible to argue that all of these threats apply to the use case, if the attacker has access to a database of pictures of persons. Pictures stored on social networks such as Facebook could be used for such a purposed. This would allow an attacker to use facial recognition to link videos to personal information. Under the assumption that an attacker has access to this, the privacy threats of identifiability, non-repudiation, detectability and disclosure of information are highly relevant.

The user of the smart phone app

Linkability Yes, every time the same device ID is used, the same user or another user of the camera is using the smart phone app.

Identifiability No, the user credentials do not link back to the real world identity.

Content Unawareness Yes. This depends on the EULA, which was not described in the use case. However, a tech savy should be able to understand that the video is saved on the server. In addition, if the company does not disclose other details of their operation, the user has no awareness of how his content is used / protected. E.g. he is not aware of the fact that zero encryption is used in the system.

The system as a whole (smart phone app and the server)

Policy and consent Non-compliance No EULA is described. If there would indeed not be an EULA, then the threat of non-compliance of the whole system is given. For this specific system, the EULA should also explain that there is no encryption used. If that is not mentioned, there is very likely breach of general laws, as there is a reasonable expectation of the user, that the video stream is protected from disclosure to unauthorised access.

(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.

Sketches of different possible approaches to add more privacy:

- Add SSL between smartphone app and server and between camera and server. Addresses leaking of sensitive information, in particular deviceID and video stream through the data flows. This addresses all privacy threats with regards to the data flow between the smartphone app and the server, except for detectability. With a high chance, any such data flow will have to use the DNS to connect to the server, so it is possible to determine when the app makes a connection to the server, and therefore it can be concluded that the user has a video camera by the manufactured and therefore has videos in the video storage.
- Save hash of deviceID on server instead of deviceID. Better protection when data gets stolen. If a cryptographic hash is used, then no linkability between different videos from the same camera is possible unless a hash collision occurs.
- Setup system where app and camera talk directly to each other, and only the discovery process is facilitated by the server. Similar to the way that the Signal protocol allows end-to-end encryption of messages with intermediate storage on the server, this might also be interesting for the video storage. However, preprocessing of the videos for time lapse and such, then needs to happen on the camera or the smartphone app. This

addresses all currently identified privacy threats, except for unawareness and non-compliance.

- Change the user interface of the app, to explain which data is sent where and how it is processed, e.g. on the server. This addresses the unawareness of the user.
- Add an end user license agreement (EULA) to specify how the user data is processed. The EULA has to be compliant to local law, e.g. of the county in which the server is hosted. This addresses the non-compliance of the whole system.

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

Solution

How would you argue for or against applying the LINDDUN privacy threat analysis framework to this example?
LINDDUN is not a good fit for this use case, as almost no details about the system as a whole and about its components are known. The only issue known from the use case, is that too many permissions were requested in regards to the Google profile of the user. However, it is not clear if all of the data from the Google profile was collected, and if and where this data flow was collected.

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?

Linkability Different Pokemon Go users with the same Google Profile can be linked. If an attacker gains access to the list of Google profile IDs, he can link these users to their profiles on other services using Google accounts.

Identifiability Google enforces providing real names, so there is a high chance of identifying a user from his Google account, even if only basic account information is accessed.

Content Unawareness The users where not aware of how much information the Pokemon Go operater got about them. Pokemon Go could have gained access to their pictures on Picassa, which is not implied by signing up for a simple video game.

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?
These threats applies to data generated by using a system or sharing data with a system, however it does not apply as such to the user. In order to prove something about the user without the rest of the system, the view of the user on e.g. the smartphone or laptop would have to be filmed which goes beyond the capabilities of the system which is being analysed. Non-compliance is a threat caused by the operators of the system and not by its users.

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?

Solution

Your solution is private. You can see this as another exercise: try not to talk to anybody about what you learned from this exercise.