HOCHSCHULE
FÜR ANGEWANDTE
WISSENSCHAFTEN
MÜNCHEN

Mobile Security - an overview

Fakultät für Informatik und Mathematik
of Hochschule für Angewandte Wissenschaften München

Handout

geschrieben von

Felix Strobel, André Braunersreuther

betreut von

Prof. Dr. Gudrun Socher

June 2019

Contents

List of Figures

List of Tables

1 Introduction

1.1 Definition

IT-Security is a generic term for a lot of different topics. Mobile security is a particular part of security with the same concerns but with focus on mobile devices. The rising of mobile devices started with the first mobile phones and handhelds. With arriving the first touchscreen devices and a much higher usability the number of mobile devices rised to a smartphone-penetration of 66% in 2018. [1]
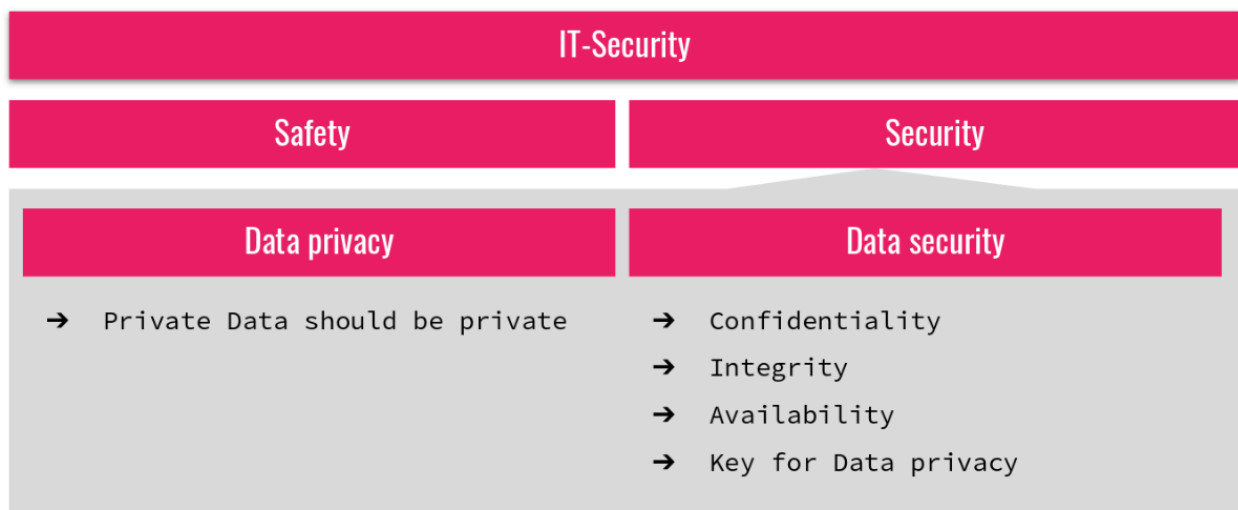

Figure 1.1: Parts of IT-Security

1.1.1 Safety

The main question in safety is: *Does my application what it is supposed to do?*.
So it is about functionality and often directly defined by customers or stakeholder. One strategy to avoid problems with safety topics are automated test. For example unit tests and integration test running by a continuous integration (CI).
But safety is not the focused topic.

1.1.2 Security

Security is about information and data. Like in Fig. 1.1 it can be split into privacy and security.

Privacy

Privacy' subject is to make sure that personal data like age, name or address are accessible only by people who are allowed.
Since GDPR came into force, it is not only a ideological question it is also a lawful question. And not fulfill this law can result in very high fines.
The goals, to keep private data private, can only get achieved with security.

Security

Security has three general targets.

Confidentiality is about making sure to restricted the access to a level where only people with the necessary privileges are allowed to see, change or delete these data.

Integrity makes sure that every unauthorized change can be detected and changes are verifiable.

Availability Means that the information should be always available to the user.

But there are also some more specific target. These does not fit in every use case.

Authenticity aims on reliability. It should be clear that a message comes from the specific sender.

Anonymity In some cases it should not be possible to connect a network package to a specific person.

In a lot of cases it is a trade of between these targets. In this case it should be clear why and what it means to not fulfill the target to 100%.

1.2 Motivation

Mobile devices get used for a lot of topics. Manage contact, doing phone calls and messaging are only the simplest examples. Nowadays the smartphone is used for nearly everything and became a personal assistant. That means a lot of personal data are stored on the device. Just to mention some of these data:

- Identities, for social media but also for credit/customer cards or online banking.

- Histories, like browser history or location history

- Payments

- Location

Implementing secure mobile applications can be more difficult than for a regular desktop environment because the user wants a simpler UI and an easy and fast access to their data. So it should be avoided to ask for long inputs or complicated authentication methods.

A further difference to the desktop environment is the mobility of these devices. Because of that an smartphone can easily get in the wrong hands. And the connectivity of these devices is higher since they support nearly every modern interface, which can be wired but in the most time is wireless. All these interfaces open a new attack vector, which can be used to get some data or control over the device.

But away from the technical background there are more reasons to secure a mobile application.

- The store provider check their apps for common bugs which can lead to secure gap

- Laws like *GDPR* force us to secure user data

- Corrupt data inside the app can destroy the user experience

- Loosing data can lead to reputational damage

- A exploited security issue can cost a lot of money

- Your own standards

2 Example

This example is about Google and Apple Pay. It explains how these two paying applications work and why it is done how it is done.
Before diving into the algorithm behind the paying methods, some terms should be explained.

Payment Networks are credit institutions which managing credit cards and the transfer from money. But also Paypal and VisaCheckout are payment Networks.

Token Service Provider are providing a very secure environment to map credit card information to individual token. [2]

Secure Enclave is the build in security chip in Apple devices. All keys are stored in here.

Secure Element is also apple specific and is paired with the Secure Enclave via hardware in the factory. It is located in the NFC-Chip to emulate the credit card.

Apple Pay and Google Pay are similar but different in detail. Both have four main steps.

1. Adding a card

2. Initiate

3. Authorize

4. Finish

2.1 Google Pay

Google Pay is using the process of tokenization [3] like a lot other mobile payment application and is standardized together with card issuer and token service provider (TSP).
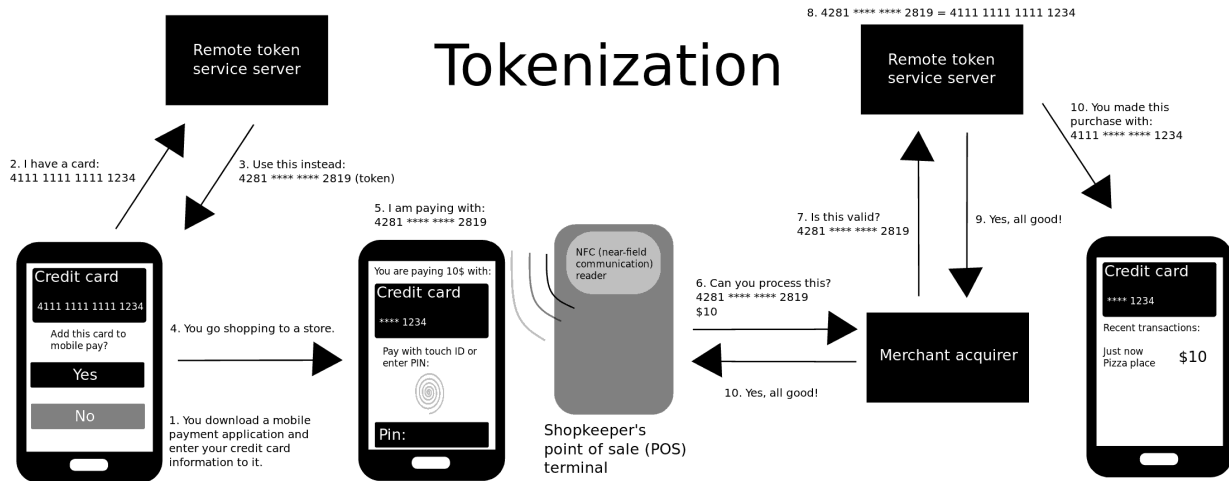

Figure 2.1: Mobile payment tokenization

2.1.1 Adding a card

After downloading the payment app (Fig. 2.1 Step 1) the user gives the card number. In the background the app ask for a token to represent the card. (Fig. 2.1 Step 2 and 3)
This token, provided from a TSP, is stored at the device and encrypted with a single or limited used key provided from the Payment Network.
This is an elegant way to not safe user data on the device. Security of the token is finally guaranteed by encryption. So this step applies two principles of security.

2.1.2 Initiate payment

The customers taps their device on a NFC Terminal (Fig. 2.1 Step 4). With this action the application start transmitting the token, a token expire date and the cryptogram (Fig. 2.1 Step 5). The cryptogram is generated by the token, timestamp and an Application Transaction Counter which is increased at every transaction and prevent the multiple use of one message.
This is a good example how appropriate protocols can be a secure way to communicate even if everybody could listen.

2.1.3 Authorize

The merchant receive the message from NFC terminal and sends all information including the price to his card network (Fig. 2.1 Step 6 and 7). The card network validates the cryptogram with help of TSP and matches the token to the real card number (Fig. 2.1 Step 8).
This step also fulfills one principle of security - validation.

2.1.4 Finish

Billing details get decrypted and the acquiring bank completes the transaction with customers bank Merchant and customer get information about validation (Fig. 2.1 Step 9 and 10).
All with appropriated protocols.

Bibliography

[1] https://www.publicismedia.de/wp-content/uploads/2017/10/2017-10-16-mobile-advertising-forecasts-2017-de.pdf - Visited on 01.07.2019

[2] https://blog.rsisecurity.com/what-is-a-token-service-provider/ - visitied on 29.05.2019

[3] https://developer.samsung.com/tech-insights/pay/tokenization - visited on 30.05.2019