# Network and Computer Security

## Alameda

## Group 28

# Spy Kid


95145 Eva Verboom

95383 Felipe Gorostiaga

97144 Pedro Mendes


October 23, 2019

# Contents

# 1 The Problem

During this project we will be working on the development of a secure child locator. As a guardian, one might want to track their children to ensure that they aren't straying too far from where they are supposed to be and in case something is wrong, to find them. Of course, this is very sensitive information, because you do not want malicious actors to be able to track your children and misuse the information in any way. Therefore, accessing the information should only be possible for authorised guardian and secure communication of the child's location is required as well as secure storage on remote servers. We will tackle the security issues in the same order, first we will ensure that the application only allows authorised users to access the information they are allowed to access and then we will work on secure communication protocols. When this is ensured, we will direct our focus on the servers where the data is stored, assuming that the server is "honest but curious".

## 1.1 Requirements

The security requirements needed to solve this problem are then:

- The system must maintain the confidentially of all data that is classified as confidential;
- The system must identify users in a reliable way;
- The system must only show data to users if they are authorised to access that particular data;
- The system must not allow anyone to fake localisation data;
- The system must add time-stamps to the location broadcasted by the child's device;
- The system must use secure communication channels to exchange data between the server and the clients.

## 1.2 Trust Assumptions

There are three groups of actors to be distinguished here: the children, the guardians and the external servers. Both children and guardians shall be fully trusted by the system (though only after authentication) and the external servers shall be partially trusted. All other actors that can in some way have access to the data are untrusted parties.

# 2 Proposed Solution

## 2.1 Deployment

The system will consist of 3 moving parts:

- A centralised server (may or may not be a distributed system);
- Multiple guardian clients;
- Multiple child clients.

A graphical representation of the machines and the way they are interconnected is shown in Figure 1.

To achieve secure communication from the child and guardian clients both will require appropriate methods of authentication.

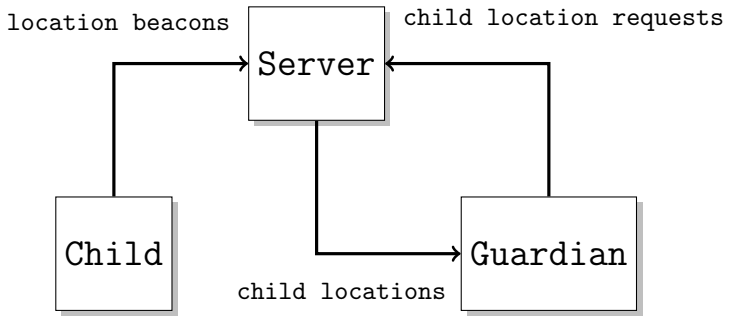


Figure 1: Diagram of the System

## 2.2 Secure channels

The guardian will have to establish a public and private key pair with the server to ensure confidentiality and a local only password to use the app (maybe also making use of fingerprint scanning).

The child and guardian clients need to agree on a private key that only they know, to encrypt every piece of data they send to the server. In order for the agreement of the keys to not be intercepted this agreement has to be made physically, through the scanning of a QR code or other similar method.

Afterwards the child client also establishes a secure channel with the server using the same method the guardian client uses.

## 2.3 Secure Protocols

Effectively the entities that will interact in the system are only the child and guardian clients, the server will only serve safe remote storage for the data. By using public private key pairs for communication with the server we ensure authenticity and by using private key encryption for the data we ensure confidentiality and integrity of the data, meaning the server can never read the sensitive data sent to it.

The other task of the server is to pair guardians with their children making sure that no guardian can ever request and get data from a child other than their own, despite the fact that they would need to know that child's symmetric key to decrypt the data.

# 3 Plan

## 3.1 Project Versions

### 3.1.1 Minimum Viable Product (MVP)

The MVP of our product should consist of the following:

- Guardian accounts which can be authenticated by the server;
- Guardians should be able to create accounts for their children;
- Child clients should be able to localise themselves outdoors;
- A central server that communicates with all clients and authorises guardians to view the tracking data of their children;
- Secure channels for data communication between the server and all clients, using library protocols.

#### 3.1.2 Intermediate

The intermediate version of our product should include:

- Child clients should also be able to locate themselves indoors;
- Child clients should be able to send alerts, when they press an SOS button or go out of safe zones;
- Guardians should know when a child broadcasted a certain location;
- Guardian clients should be able to receive alerts send by the child and when the child did not broadcast for a certain period of time.
- Allow multiple guardians.

#### 3.1.3 Full Feature Release

Finally, the full feature release will extend the product with:

- Login as a user should be done using two-factor authentication;
- Data should be send and stored encrypted, such that only guardians are able to track the child and the server is unable to know the location;
- Provide history of the child's location.

### 3.2 Effort Commitments

The table below describes the activities each member of the team commits to during the project. This division of tasks is general and all team members also commit to helping each other where needed. Changes to the schedule during the project are likely, though every team members holds responsibility for his/her own subjects.

| Week | Eva | Felipe | Pedro |
|---|---|---|---|
| 28/10—3/11 | Basic non secure child client | Basic non secure guardian client | Basic non secure server |
| 4/11—10/11 | Basic secure child client and testing | Basic secure guardian client and testing | Basic secure server and testing |
| 11/11—17/11 | Intermediate child client | Intermediate guardian client | Intermediate secure server |
| 18/11—24/11 | Test intermediate child client | Test intermediate guardian client | Test intermediate secure server |
| 25/11—1/12 | Advanced child client and general outlines report | Advanced guardian client | Advanced server |
| 2/12—8/12 | Testing final product | Testing final product | Testing final product |
| 9/12—15/12 | Finishing report | Finishing report | Finishing report |

## 4 References

The main technology for developing the applications will be the android studio and the built in Java encryption libraries (which have been tested at the time of writing this proposal).

For the server we intend to use Postgres as the database and Rust as the programming language due to being a memory safe and high performing language (which have also been installed and tested to work).