***Abstract*—In this project, we want to create a privacy-preserving app that returns Points of Interest (POI) near the user's location. Since users need to have a subscription to access our application, we want to implement an authentication method based using zero-knowledge proofs. We then evaluate the risks caused by the fact of sending the users IP address. Finally, we evaluate the threats one privacy due to the meta-datas that are still sent. We see what information can be extracted from them.**

Please report your design, implementation details, and findings of the second project in this report.
You can add references if necessary.
THE REPORT SHOULD NOT EXCEED 5 PAGES.

I. Introduction

Most recent location-based application opt for a free-to-use business model. They let the user use their services without any form of paid subscription. However, these types of application will frequently ask to login or create an account. The application can then build a marketing profile of the user by linking the different locations he goes to. One can recover the job, the house, the centres of interest... These information are valuable and we don't know what the application does with it.
In this project, we will code a location-based application that, based on the user's location, returns nearby points of interest. We want to avoid infringements on privacy like described earlier. In order to do so, the user should never have to login to the application, but he will have to prove that he has a subscription by using a zero-knowledge proof.

We start by designing an anonymous authentication mechanism using attribute-based credentials. We inspire ourselves from the signature scheme described in this paper[1], we consider that the messages to sign correspond to the POIs the user wants to see. However, we want to make our protocol non interactive and therefore, we use the Fiat-Shamir heuristic to sign our messages.
In a second part, we evaluate the privacy risks on the user and try to propose a defense.
Finally, we conduct a fingerprinting attack on the application to see what information an adversary can recover and we discuss how to improve our application to avoid such attacks.

II. Attribute-based credential

A. Details

In the algorithm, a Server object has access to an issuer object which can generate new parameters (secret and public), but also proceed requests from the Clients. Clients can communicate with an AnonCredential object which takes the user data to create valid signatures using the Fiat-Shamir heuristic. A sample run of the algorithm is described below :

Explain how you mapped the system to the attribute based credential. How did you use the Fiat-Shamir heuristic?

Algorithm 1 Sample run of the algorithm

1: The Server asks an issuer to generate a new public key and a secret key.
2: A Client wants to register. He creates an object AnonCredential who will create a registration request.
3: The AnonCredential creates a zero-knowledge proof based on the Fiat-Shamir heurisitc. The message to sign are the user attributes.
4: The Server receives the registration request. He asks an issuer to verify the correctness of the request and to send back credentials.
5: The Client asks the AnonCredential to proceed the received information.
6: The Client asks the AnonCredential to create a Signature object which can then be sent to the Server.
7: The Signature object is created using the Fiat-Shamir heuristic.
8: The Client can now have access to the application without having to reveal his credentials, but by presenting his Signature object.

B. Test

Tests : Provide a fake signature or
How did you test the system? You need to test the correct path and at least two failure paths.

C. Evaluation

Evaluate your ABC: report communication and computation stats (mean and standard deviation). Report statistic on key generation, issuance, signing, and verification.

III. (De)Anonymization of User Trajectories

A. Privacy Evaluation

Provide a privacy analysis of the dataset. You should explicitly state your assumptions, adversary models, methods, and findings.

B. Defences

Propose a defence that users of the service could deploy to protect their privacy. You should state your assumptions, adversary models, and provide an experimental evaluation of your defences using the datasets and the grid specification. You should also discuss the privacy-utility trade-offs of your defence.

IV. Cell Fingerprinting via Network Traffic Analysis

A. Implementation details

Provide a description of your implementation here. You should provide details on your data collection methods, feature extraction, and classifier training.

B. Evaluation

Provide an evaluation of your classifier here – the metrics after 10-fold cross validation.

C. Discussion and Countermeasures

Comment on your findings here. How well did your classifier perform? What factors could influence its performance? Are there countermeasures against this kind of attack?

V. Conclusion and learning outcome

This project was the occasion for us to put in practice the notions of our course. We discovered that if ideas like zero-knowledge proofs are easy enough to understand, they can be complicated to put in place.
This project also raised awareness on how metadatas can be used to retrieve valuable information, and how complicated it can be to create a zero-knowledge application.

References

[1] D. Pointcheval and O. Sanders, "Short Randomizable Signatures," vol. 9610, pp. 111–126, 2016, series Title: Lecture Notes in Computer Science. [Online]. Available: http://link.springer.com/10.1007/978-3-319-29485-8_7