CS-523 SecretStroll Report

Wicky Simon, Nunes Silva Daniel Filipe

***Abstract*—Please report your design, implementation details, and findings of the second project in this report.**
THE REPORT SHOULD NOT EXCEED 5 PAGES.

I. Introduction

Provide a brief introduction about the aim of the project, and your road-map about the design/implementation for each sub-part.

II. Attribute-based credential

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

A. Test

How did you test the system? You need to test the correct path and at least two failure paths.

B. 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

We evaluate the privacy risks using simulated data of two hundred users who made use of the application hundred times each in average over twenty days. We assume that no mechanism to hide any kind of data is used, i.e. data is sent in cleartext inside standard IP packets. Any malicious adversary could hack the application servers or sniff the network between a user and the server in order to retrieve similar datasets which include IP addresses, locations, query types, timestamps and responses. According to [1], the IP address or a set or IP addresses are relevant attributes because they can be linked to a given user since they are persistent for a certain duration. Moreover, combining IP addresses with location and time data makes sense since users often keep their habits that they may share with very few people [2], i.e. they may work during the day at their office, be back home in the evening and do an activity at some specific location. Therefore, we deduce that this implementation leak senstive informations about the users. As a proof of concept for breaching users privacy, we try to infer work and home locations of users as well as habits in their activities.

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?

References

[1] A. V. W. R. R. R. M. L. Vikas Mishra, Pierre Laperdrix, "Don't count me out: On the relevance of ip addresses in the tracking ecosystem," *HAL*, 01 2020.

[2] K. P. Philippe Golle, *On the Anonymity of Home/Work Location Pairs*, 2009.