CS-523 SecretStroll Report

Author 1, Author 2

Abstract—**Please report your design, implementation details, and findings of the second project in this report.**
You can add references if necessary [1].
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

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] J. Doe, "Example title," *Example conference*, 01 1987.