Develop and Disseminate Hands-on Lab Materials of Privacy Concepts and Technologies to Educators

Na Li, Lin Li, Mengjun Xie and Bugrahan Yalvac

Presented by Dr. Na Li
Associated Professor
The Coordinator of Cybersecurity Concentration
Department of Computer Science
Prairie View A&M University

@CISSE 2023

NSF Award # 1712496

Developing Innovative Privacy Learning Modules to Engage Students in Cybersecurity Education

- Prairie View A&M University

Na Li (Principal Investigator)
Lin Li (Co-Principal Investigator)

- University of Tennessee at Chattanooga

Mengjun Xie (Co-Principal Investigator)

Li Yang (Former Co-Principal Investigator)

Evaluator: Bugrahan Yalvac (Texas A&M University, College Station)

Introduction

- Privacy definition -> different preferences
- Privacy v.s. Security -> not the same
- Privacy protection is needed (data breach incidents)
- More critical in the era of big data
- The lack of privacy educational materials
- Target younger generations -> hands-on based learning

Project Objectives

Develop privacy curriculum for undergraduate students and explore the best way to integrate privacy into cybersecurity education. Specifically, design and develop:

- self-contained privacy learning modules used not only for privacy course but also other related courses, such as Web Development, and Computer Network.
- effective hands-on labs for different learning modules
- designing and implementing labware to learn privacy related concepts

Topics of Privacy

- Data Privacy
- De-anonymization
- Relationship Privacy in Online Social Networks
- Image Privacy
- Location Privacy in Location Based Services (LBS)
- Web Tracking
- IoT Security & Privacy

Location Based Services (LBS)

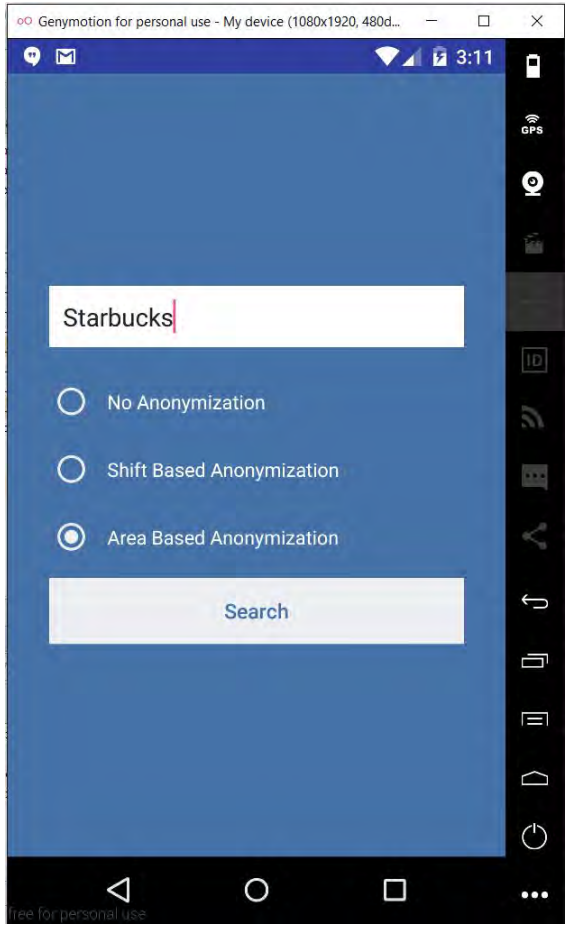
- Software services using location (geographical) data to control features (ref. wikipedia)
- Widely used in social networks, often accessible with mobile devices (e.g., Facebook, Foursquare, etc)
- Question: should a client always trust a LBS?

Anonymization Mechanisms in LBS

- Anonymization prevents from exposing user's exact location to LBS
- Mechanisms we implemented include
  - No Anonymization
  - Shift-based Anonymization
  - Area-based Anonymization

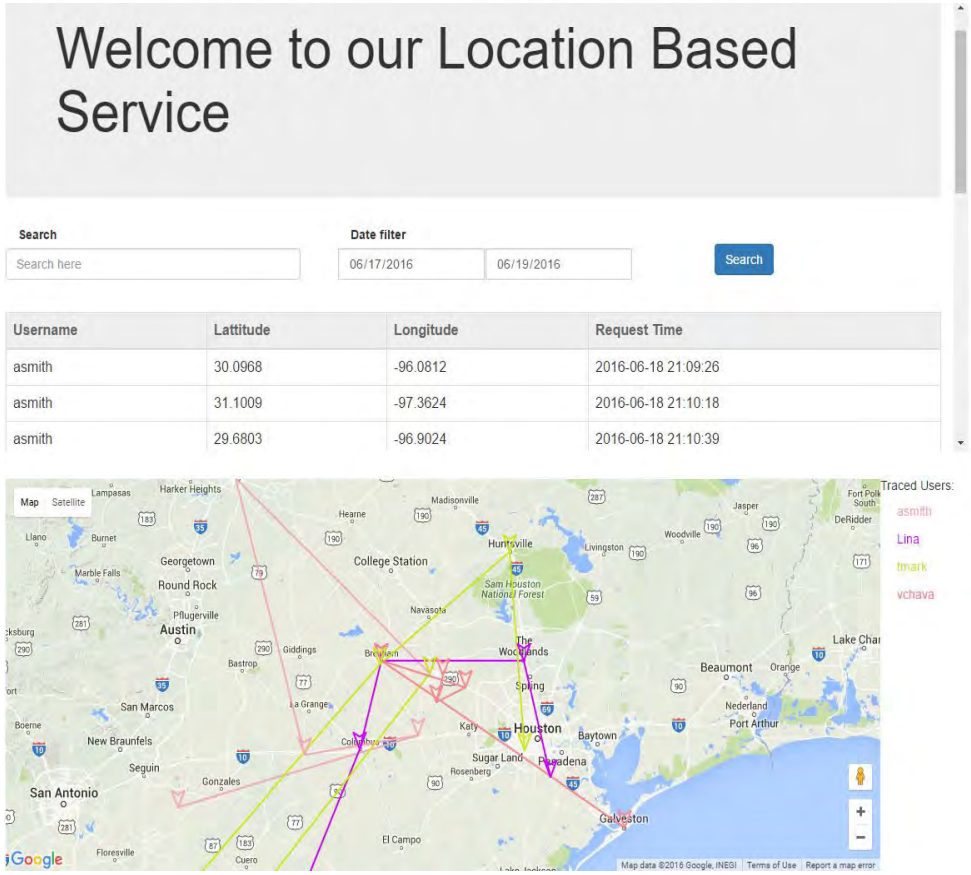
Privacy-aware LBS System

Three components: (i) Android Client, (ii) semi-honest LBS Server, (iii) trustable Analytic Server



Requests with user location info

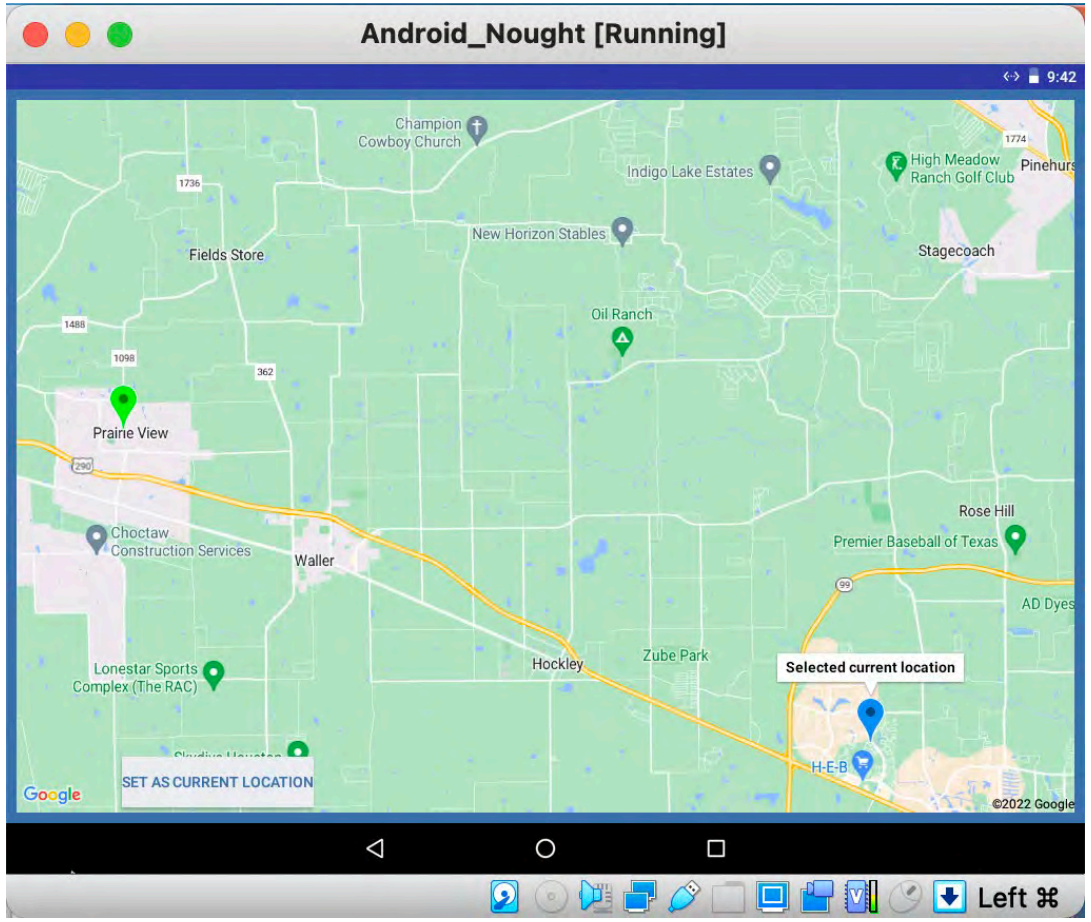
Responses with retrieved landmark location info

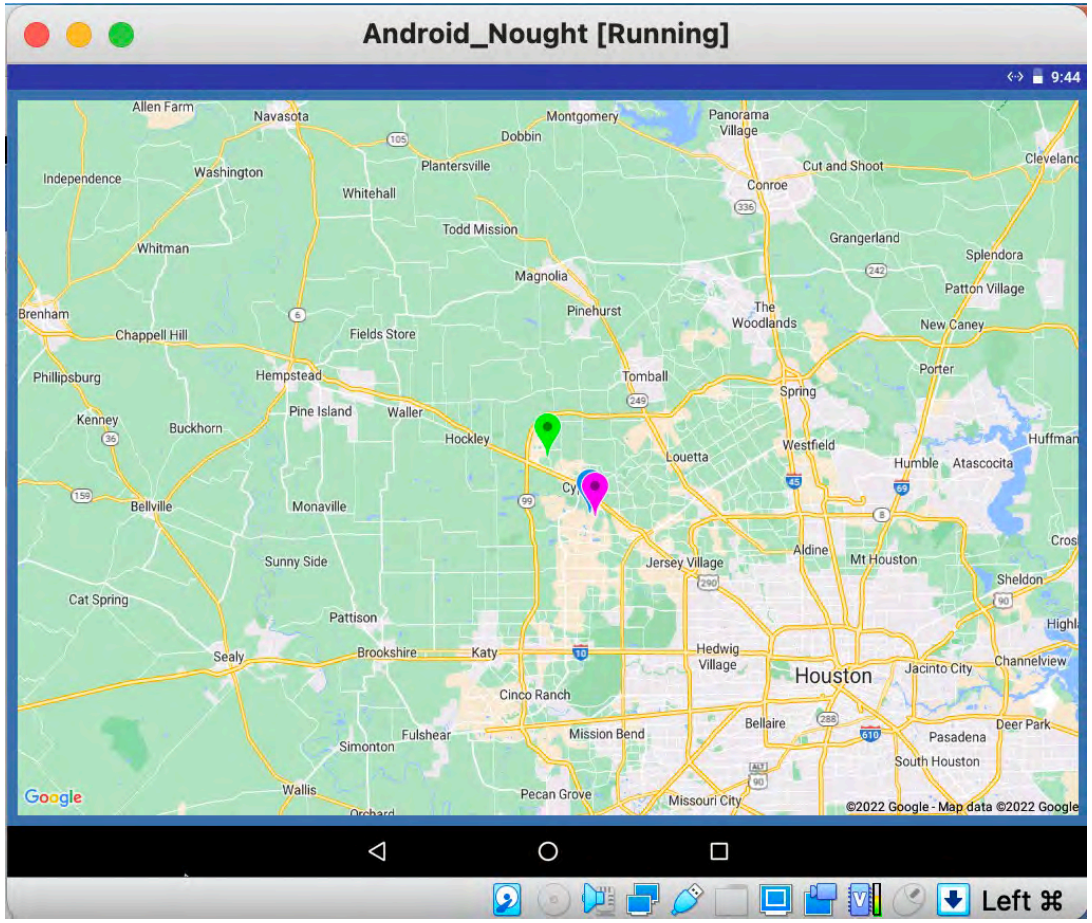


I. Android Client

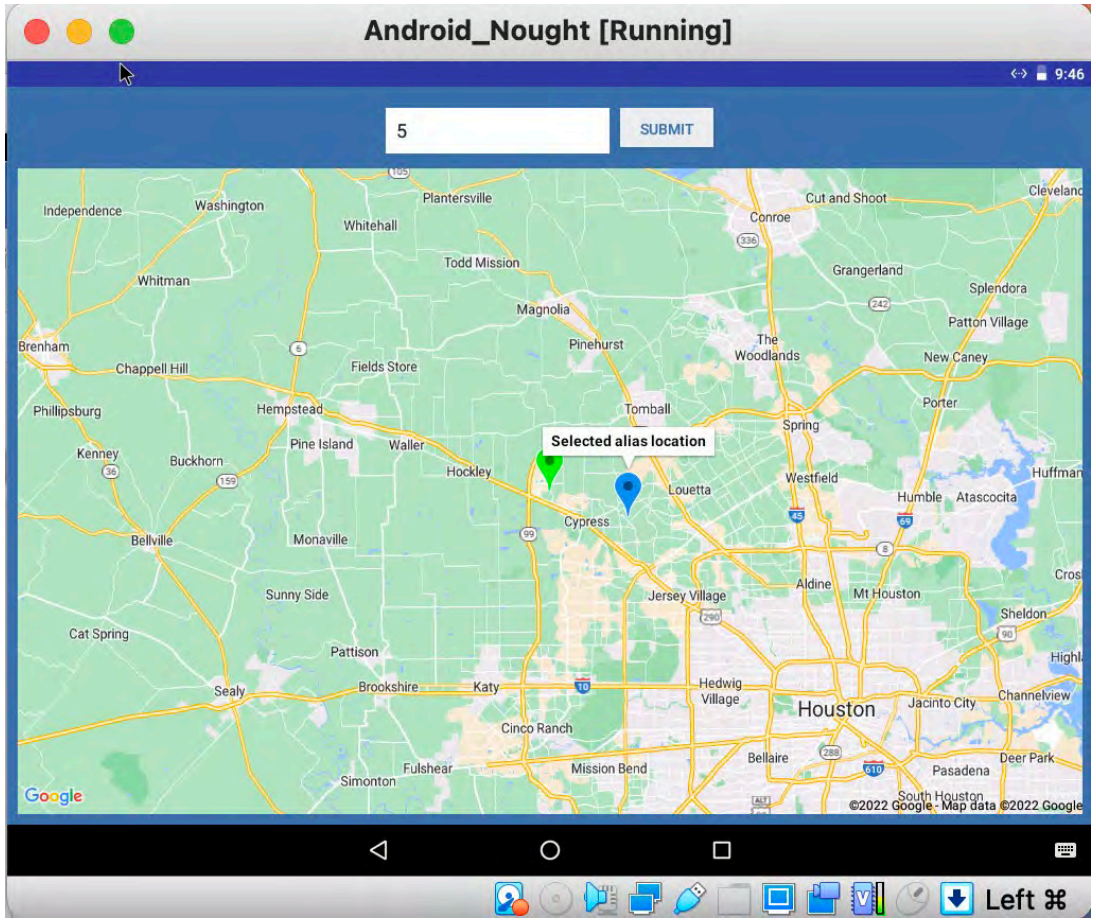
II. LBS Server

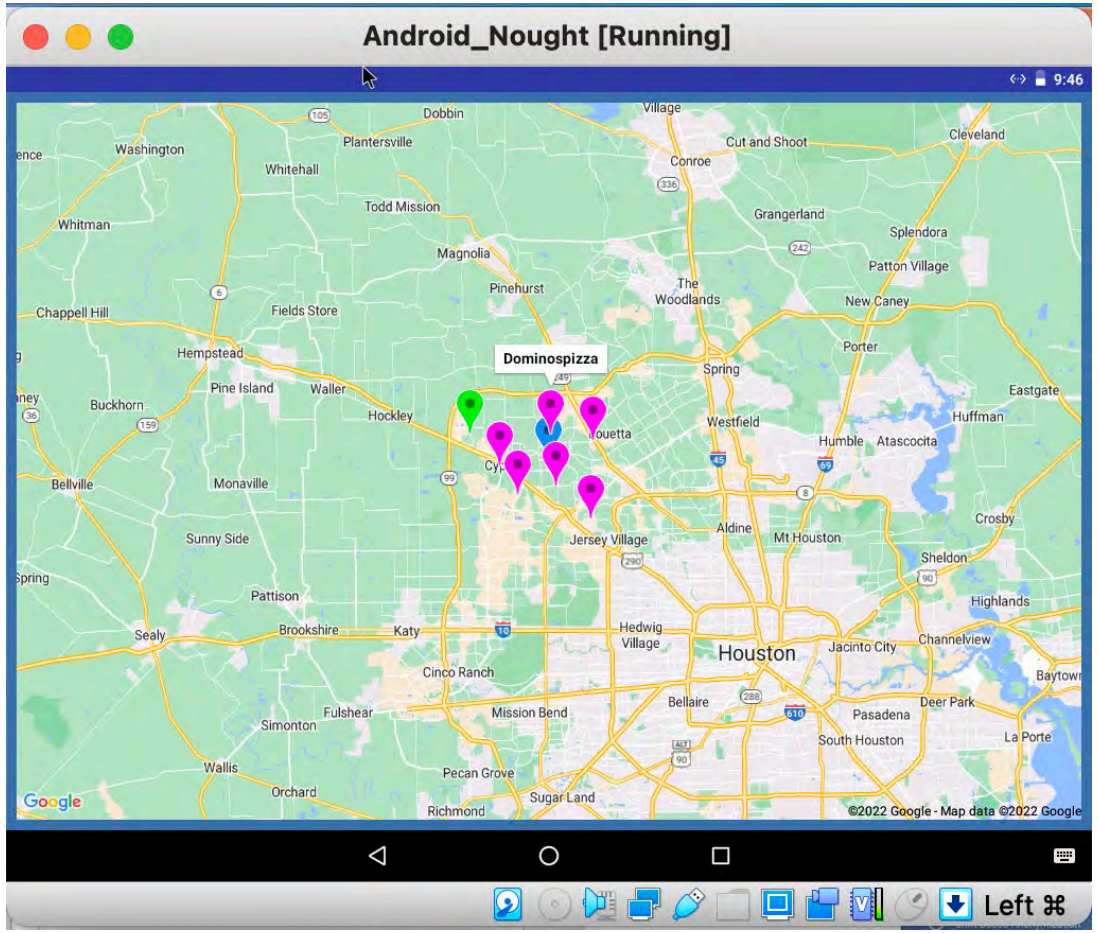
Shift-based Anonymization





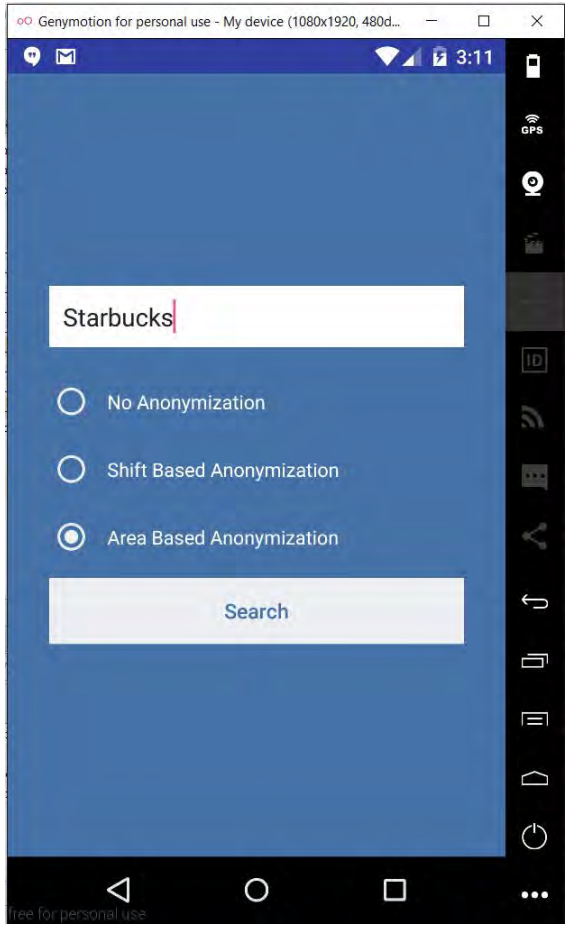
Area-based Anonymization





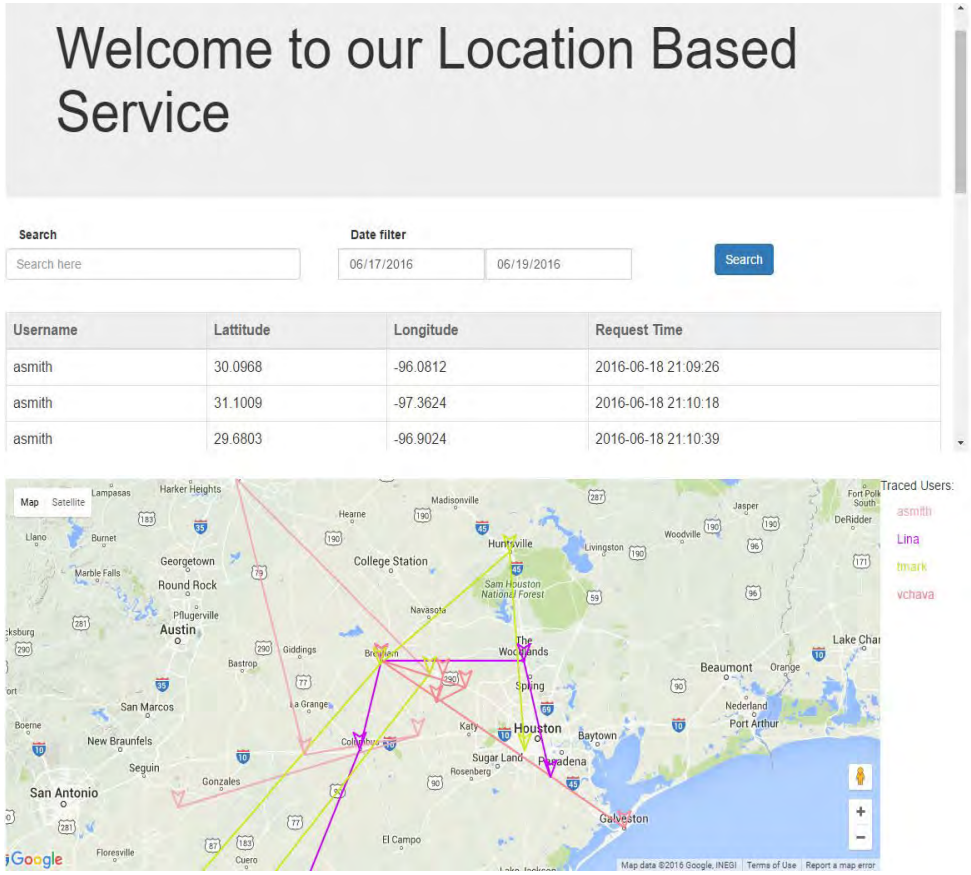
Privacy-aware LBS System

Three components: (i) Android Client, (ii) semi-honest LBS Server, (iii) trustable Analytic Server



Requests with user location info

Responses with retrieved landmark location info

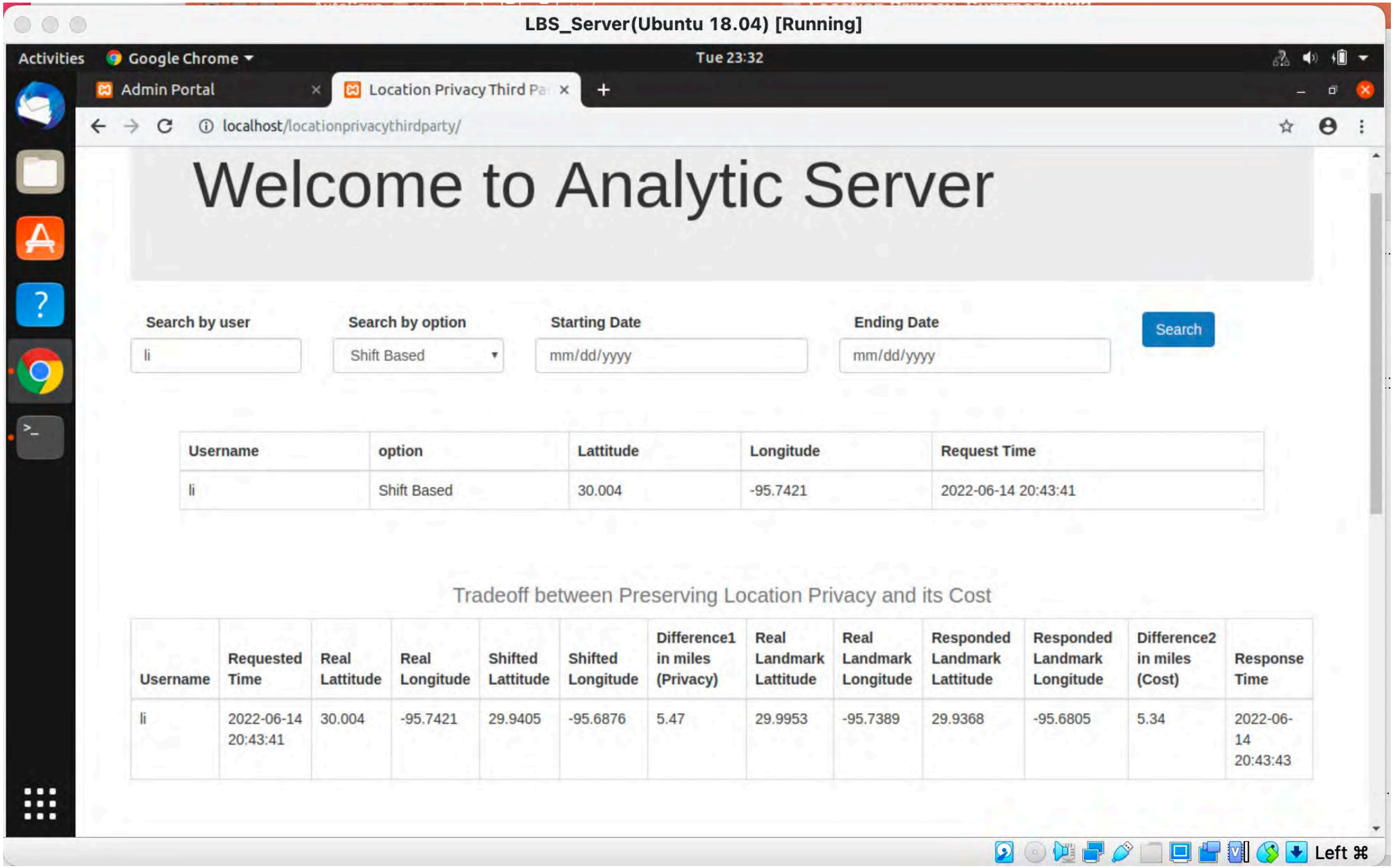


I. Android Client

II. LBS Server

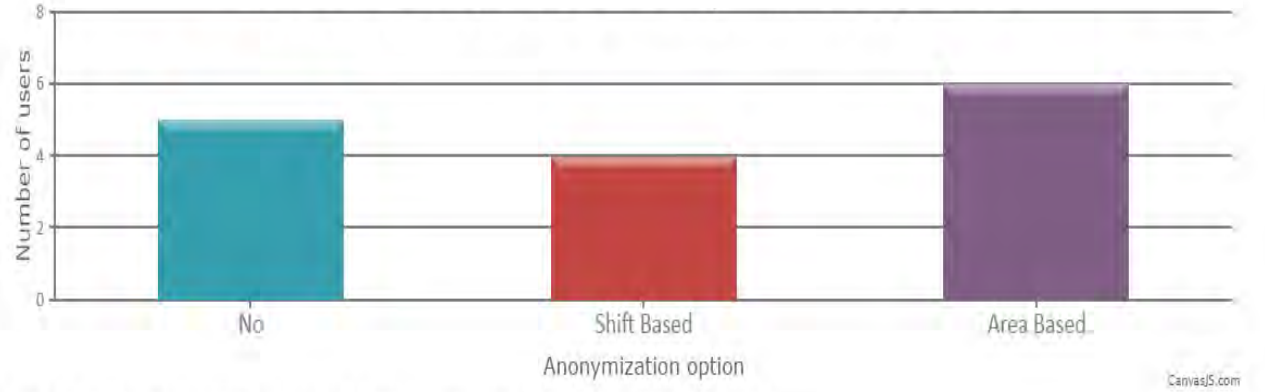
Tradeoff - Privacy Protection and Utility Cost

- Extreme case: disable location tracking on the phone, but no LBS!
- Utility definitions
  - different in different contexts
  - e.g., money or accuracy of inquired information


LBS_Server(Ubuntu 18.04) [Running]
Activities
Google Chrome
Tue 23:32
Admin Portal
Location Privacy Third Pa
localhost/locationprivacythirdparty/
Welcome to Analytic Server
Search by user
li
Search by option
Shift Based
Starting Date
mm/dd/yyyy
Ending Date
mm/dd/yyyy
Search
Username
option
Lattitude
Longitude
Request Time
li
Shift Based
30.004
-95.7421
2022-06-14 20:43:41
Tradeoff between Preserving Location Privacy and its Cost
Username
Requested Time
Real Lattitude
Real Longitude
Shifted Lattitude
Shifted Longitude
Difference1 in miles (Privacy)
Real Landmark Lattitude
Real Landmark Longitude
Responded Landmark Lattitude
Responded Landmark Longitude
Difference2 in miles (Cost)
Response Time
li
2022-06-14 20:43:41
30.004
-95.7421
29.9405
-95.6876
5.47
29.9953
-95.7389
29.9368
-95.6805
5.34
2022-06-14 20:43:43
Left ⌘

The Analytic Server

The distribution of user preferences on anonymization



Note: 0 refers to No anonymization, 1 refers to Shift based anonymization, 2 refers to Area Based anonymization

User preference changes over time

Note: 0 refers to No anonymization, 1 refers to Shift based anonymization, 2 refers to Area Based anonymization

Workshop

- Faculty virtual workshop in summer 2022
- 29 faculty from twenty institutions nationwide
- 10 Full Professors (34%), 8 Assistant Professors (28%), 6 Associate Professors (21%), 4 lecturers (14%), and 1 part-time instructor (3%)
- Customized Ubuntu VirtualBox images for the labs
- 25 participants completed both the pre and post workshop surveys
- A survey after each lab session

Awareness of the Topics

Survey responses to a 5-point scale

Never heard anything about the term	Only heard the term	Know only a few things about the term	Know some basic concepts of the term	Know the term's concepts and applications

Lab	Pre: μ (σ)	Post: μ (σ)
DP	4.08 (0.79)	4.84 (0.36)
RP	3.44 (1.06)	4.72 (0.79)
IP	3.32 (0.88)	4.56 (0.63)
DA	3.04 (1.25)	4.52 (0.81)
IoT	3.04 (1.25)	4.52 (0.81)
LP	3.44 (1.13)	4.56 (0.75)
WT	3.56 (1.09)	4.64 (0.55)

TABLE I

CHANGES IN PARTICIPANTS' AWARENESSES OF THE TOPICS

Interest in Teaching the Topics

Survey responses to a 5-point scale

Never heard anything about the term	Only heard the term	Know only a few things about the term	Know some basic concepts of the term	Know the term's concepts and applications

Lab	Pre: μ (σ)	Post: μ (σ)
DP	4.16 (0.96)	4.56 (0.69)
RP	3.72 (1.11)	4.04 (1.11)
IP	3.76 (0.99)	3.96 (1.14)
DA	3.72 (1.18)	4.04 (1.07)
IoT	4.24 (0.91)	4.48 (0.85)
LP	3.92 (0.97)	4.28 (0.91)
WT	4.12 (0.81)	4.36 (0.79)

TABLE II

CHANGES IN PARTICIPANTS' INTEREST IN TEACHING THE TOPICS

Responses to 7 Statements

(1) This lab increased my knowledge and skills in [session topic].
(2) I learned how to teach [session topic] more effectively.
(3) The session was well organized.
(4) The session objectives were stated clearly and met.
(5) The information provided and/or skills presented were relevant and useful.
(6) The presenter(s) provided adequate time for Q&A.
(7) The session materials provided were useful.

TABLE III
PARTICIPANTS' RESPONSES TO THE SEVEN STATEMENTS. THE # WITHIN THE PARENTHESIS REPRESENTS THE SURVEYS RETURNED

#	**DP** (22)	**RP** (22)	**IP** (19)	**DP** (20)	**IoT** (18)	**LP** (18)	**WT** (21)
1	5.27	5.61	5.42	5.35	5.67	5.33	5.43
2	5.14	5.3	5.11	5.05	5.44	5.11	5.24
3	5.41	5.70	5.58	5.40	5.72	5.50	5.29
4	5.45	5.57	5.63	5.35	5.72	5.72	5.19
5	5.55	5.65	5.58	5.30	5.67	5.61	5.38
6	4.95	5.70	5.74	5.60	5.50	5.67	5.48
7	5.36	5.65	5.53	5.40	5.67	5.44	5.43

on a 6-point Likert-Scale (1 = Strongly disagree, 2 = Disagree, 3 = Slightly disagree, 4 = Slightly Agree, 5 = Agree, 6 = Strongly Agree).

- Results show that almost all participants agreed that the sessions increased their knowledge and skills in the privacy technologies. They learned how to teach the topics effectively.
- Participants reported that the sessions were well organized, objectives were stated clearly and met, the information provided and/or skills presented were relevant and useful, presenter(s) provided adequate time for questions and answers, and the session materials were useful.

Conclusions

- Introduced the project (NSF IUSE **1712496**)
- One example of the lab – location privacy in LBSs
- Faculty workshop feedback

Publications from Project

- N. Li, L. Li, M. Xie, and B. Yalvac “Develop and Disseminate Hands-on Lab Materials of Privacy Concepts and Technologies to Educators” to appear in The Journal of The Colloquium for Information Systems Security Education, 2023
- J. Liu, L. Li, and N. Li, “Relationship Privacy Preservation in Photo Sharing”, Journal of Elsevier, 2023
- A. Sanchez, O. Ogunbowale, O. Adetola, and N. Li, “Hands-on Lab Development for Policy Violations in Voice Personal Assistants”, Journal for Computing Sciences in Colleges, 2023
- N. Li, “Privacy Attacks Against Relationship on OSNs,” Encyclopedia of Cryptography, Security and Privacy, edited by Sushil Jajodia, Pierangela Samarati and Moti Yung, Springer, 2021 (https://link.springer.com/referenceworkentry/10.1007/978-3-642-27739-9_1601-1)
- S. Shormin, L. Li and N. Li, “Facelock—A Labware for Teaching Photo Privacy in Online Social Networks through Face Recognition”, Journal for Computing Sciences in Colleges, 2020.

- Y. Liu, and N. Li, “Retrieving Hidden Friends: A Collusion Privacy Attack Against Online Friend Search Engine”, IEEE Transactions on Information Forensics & Security, 2019.
- **N. Li**, V. Chava, and L. Li "A Labware for Educating Location Privacy Protection in Location-based Services", Journal for Computing Sciences in Colleges, 2017.
- J. Liu, L. Li and **N. Li**, “Learning and Preserving Relationship Privacy in Photo Sharing” In the Proceeding of the 9th IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT2022), 2022.
- **N. Li**, R. Murugesan, L. Li, and H. Zheng, “IDEAL: An Interactive De Anonymization Learning System," In the Proceeding of the 44th IEEE Computer Society Signature Conference on Computers, Software, and Applications (COMPSAC), 2020.
- **N. Li**, L. Li, and Y. Liu, “FriPEL: Friendship Privacy Educational Labware”, In the Proceeding of the 4th International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2018) **(Best paper award).**
- Y. Liu and **N. Li**, "An Advanced Collusion Attack against User Friendship Privacy in OSNs" In the Proceeding of the 40th IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC 2016) (Symposium on Security, Privacy and Trust in Computing).