SureThing

Privacy Protection

João Costa
MSc Information Systems and Computer Engineering
January 10th , 2020

inesc-id.pt

inesc id lisboa 20 YEARS
DEFINING TECHNOLOGY

Agenda

- Introduction to Location-Based Services
- Related Work
- Solution Architecture
- Evaluation Methodology

Location-based services

- **Location-based services** (LBS) use real-time geo-data from a mobile device or smartphone to provide information, entertainment or security.
- **Location proof system**
- The **location proof** contains a prover identifier and location, witness identifier and location, a signature from CA for authenticity of data, and a token (i.e., random number and/or timestamp) to ensure freshness.

Privacy concerns

- The **collection** of personal information.
- **Unauthorized** secondary use of personal information.
- **Improper** access to personal information.
- **Errors** in storing personal information

Objectives

- Prover anonymity & unlinkability
- Prover location privacy
- Witness anonymity & unlinkability
- Witness location privacy

Privacy-preserving metrics

- K-anonymity
- L-diversity
- T-closeness

Privacy-preserving mechanisms

- Dummy location
- Cloaking
- Mix zones

Differential Privacy & Geo-Indistinguishability

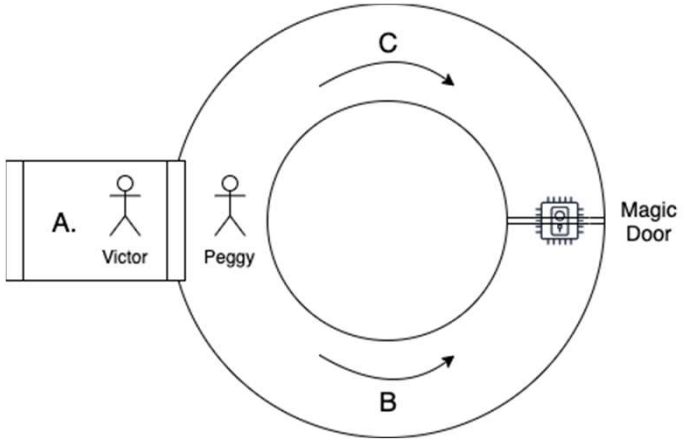
- **Differential Privacy** mechanism quantifies the maximum possible information gain by the attacker, which can reduce the risk of the privacy being compromised.
- The private information is limited and quantified by a **privacy loss parameter**, usually designated epsilon ε.
- **Geo-Indistinguishability** guarantees that any two locations within a given radius around the user are statistically indistinguishable.

Zero-Knowledge Proof

- A **Zero-Knowledge Proof** (ZKP) is a method by which one party (the prover) can prove to another party (the verifier) that they know a value *x*, without conveying any information apart from the fact that they know the value *x*.
- **Completeness**
- **Soundness**
- **Zero-knowledge**

Zero-Knowledge Proof

- A **Zero-Knowledge Proof** (ZKP) is a method by which one party (the prover) can prove to another party (the verifier) that they know a value *x*, without conveying any information apart from the fact that they know the value *x*.
- **Completeness**
- **Soundness**
- **Zero-knowledge**

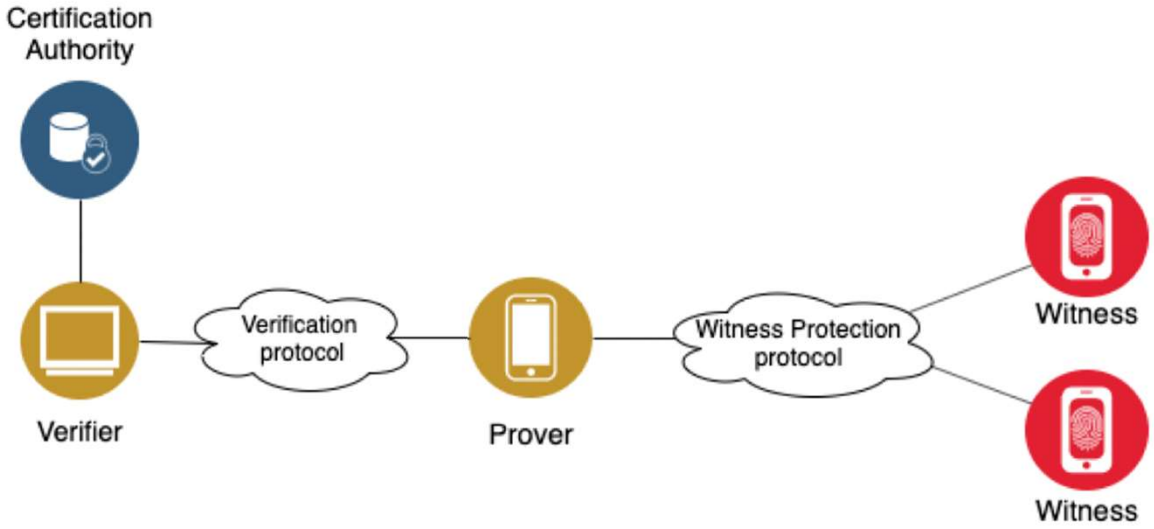


Solution Architecture

Attacker Model

- **Attacker A:** malicious prover/witness attempts to gain information of identity and location of the witness/prover.
- **Attacker B:** malicious verifier attempts to obtain more information of prover's identity and location and impersonate to another verifier.
- **Attacker C:** local eavesdropper attempts to intercept the communication between the users to gain information about the user's identity and location, or to manipulate the information.

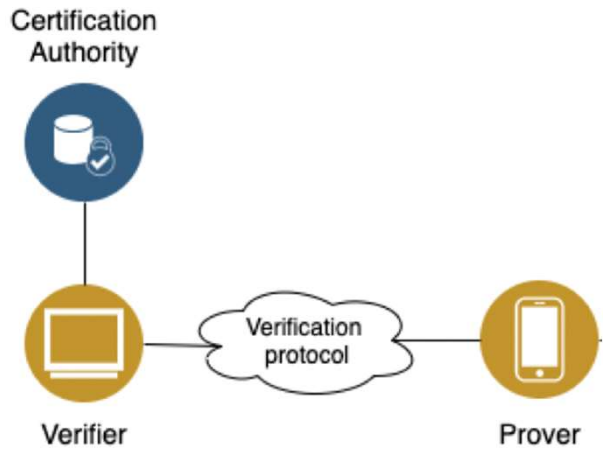
Overview


Certification Authority
Verifier
Verification protocol
Prover
Witness Protection protocol
Witness
Witness

Location Proof Collecting Phase

- **Witness Protection Protocol** protects the location of the Witnesses.
- This protocol uses **Clustering Geo-Indistinguishability** mechanism.

Location Proof Verification Phase



- **Verification Protocol** protects the identity of the Prover.
- This protocol uses **Zero-Knowledge Proofs** mechanism.

Evaluation Scenario

A real building standing in a shopping center where a loyalty application is deployed to reward frequent visitors.

- Level of privacy
- Tradeoff between privacy and accuracy
- Performance of the protocols
- Effectiveness of the system defense

Conclusion

- This system will protect the Witnesses location privacy by sending their obfuscated location to the Prover instead of the real location.
- It will protect against Witness identity by assigning pseudonyms in the registration of users with a Certificate Authority.
- This system will protect the Prover identity privacy by using zero-knowledge proofs, which allows a user to prove his location without revealing his identity.


inesc id
lisboa
20
YEARS
DEFINING TECHNOLOGY
Thank you!
Privacy Protection
SureThing