PROPS: towards a Privacy-Preserving Location Proof System

Sébastien Gambs
INRIA - Université de Rennes 1

(joint work with Marc-Olivier Killijian, Matthieu Roy and Moussa Traoré)

sgambs@irisa.fr

21 March 2013

Location proof system

Desiderata

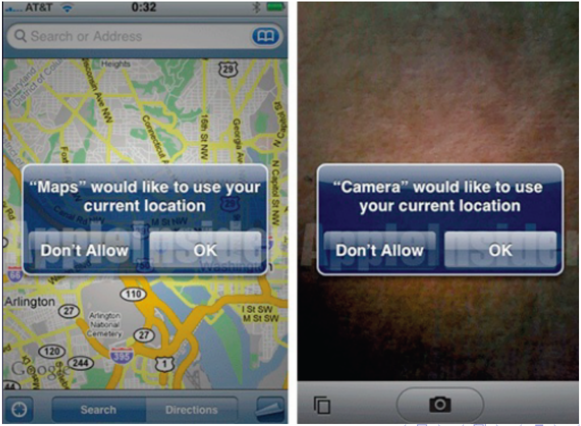
Ingredients

PROPS

Location proof system

Location-based services

- Personalize the service provided to the user according to his current location.



Example 1 : collaborative traffic monitoring

Example 2 : geosocial network

Verification of the position

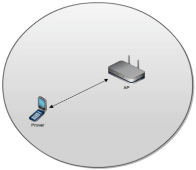
- For some applications, a user might be tempted to lie about his current position.
- Examples : position-based access control, geosocial network, real-time traffic map, discount tied to the visit of a particular shop, carpooling service, criminal investigation, local electronic election, . . .
- Challenge : to be able to verify the position claimed by an individual while respecting his privacy.
- Dual problem : to be able to compute its position for a device that has no geolocated capabilities.

Location proof system

- Architecture allowing a user to prove his position to another entity.
- Generally composed of two phases :
  1. Gathering phase (heart of the system) : the user (*prover*) interacts with one or several entities to acquire a proof of his location.
  2. Verification phase : the prover shows his proof to a verifier that can assess his validity.
- Two main families of approaches :
  1. Approach based on a trusted infrastructure.
  2. Collaborative approach.

Approach based on a trusted infrastructure

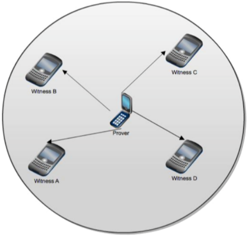
- Main idea : a user collects a location proof by proving his proximity with a trusted entity.



- Example of a trusted entity : dedicated access point.
- Proximity proven by a distance-bounding algorithm (*à la* Chaum and Brands) or by measuring the strength of the received signal (by WiFi or Bluetooth).
- Advantages : simple and efficient.
- Drawbacks : single point of failure, location leak, availability of a dedicated infrastructure.

Collaborative approach

- Main idea : a user collects a location proof by collaborating with neigbouring users that agree to act as *witnesses*.



- Existing protocols : APPLAUS, SLVPGP, Alibi.
- Advantages : cheap, scalable, independent of any infrastructure.

Security and privacy challenges of the collaborative approach

- Must be resistant to a collusion of malicious users.
- Must be resistant to localization attacks.
- Anonymity of the prover and the witnesses.
- Geo-privacy : protection of the location of a user with respect to an external observer.
- Location sovereignty : the prover can choose when he wishes to disclose his position and to which granularity.

Desiderata

Participants

Certification Authority (CA) : trusted third party registering new users.

Possible roles for a user :

- Prover : wishes to prove his position (current or past) to a verifier while preserving his privacy.
- Witness : is located in the vicinity of the prover and collaborates with him in order to generate a location proof.
- Verify : check the validity of a location proof shown by a prover.

Desiderata for a privacy-preserving location proof system (1/4)

- Completeness : a location proof generated in collaboration with honest witnesses while following the recipe of the protocol must always be accepted by an honest verifier.
- Soundness : impossibility for a prover to generate a proof for a location in which he has never been (*spatial soundness*) or for an arbitrary time (*temporal soundness*).
- Proof of ownership : only the legitimate owner of a proof must be able to convince a verifier of the validity of the proof.
- Implies the *non-transferability* property.

Desiderata for a privacy-preserving location proof system (2/4)

- Unforgeability : impossibility for a user (or a collusion of malicious users) to forge a fake proof for a location in which he has never been or for an identity that he does not own.
- Anonymity and unlinkability of the prover : the identity of the prover remains hidden both during the gathering and the verification phases.
- Impossibility to decide if two location proofs are linked to the same prover.

Desiderata for a privacy-preserving location proof system (3/4)

- Anonymity and unlinkability of the witnesses : a witness remains anonymous both during the gathering and verification phases.
- Impossibility to decide if two location proofs are linked to the same witness.
- Exception : we want to be able to detect if a witness has signed two shares of the same location proof.
- Location privacy for the witnesses : no need for a witness to reveal his exact position during the generation of a location proof (only a upper bound of his distance to the prover).
- Selective disclosure of the location : the prover can decide the granularity of the information revealed on his location.

Desiderata for a privacy-preserving location proof system (4/4)

Resistance to localization attacks :

- Distance fraud : a malicious prover manages to convince an honest witness that he is closer than in reality.
- Mafia fraud : a malicious user manages to convince an honest witness that an honest prover is further than in reality (*man-in-the-middle attack*).
- Terrorist fraud : collusion between several malicious users in order to fool an honest witness in generating a location proof for an absent user (*proxy attack*).
- Distance-hijacking fraud : after the proximity testing between an honest prover and an honest witness, a malicious user can assume the role of the prover.

Ingredients

Proximity testing

- Distance-bounding protocol : technique enabling an entity to convince another entity on an upper bound of the maximal distance between them.
- One of the only ways to counter relay attacks.
- Examples : Brands and Chaum 93, Bussart and Baga 04.
- Must be resistant to localization attacks.

Group signature

- Group signature : method to prove that someone belongs to a group by signing a message anonymously on behalf of the group.
- Concept invented in 1991 by Chaum and van Heyst.
- Example of application : verifiy that an individual belongs to a certain group that has the right to access a particular ressource but without learning the name of the individual.
- A group signature scheme possesses :
  - several private signature keys SK_i that can be used to sign a message on behalf of the group (such that it is impossible to trace back the signature to the index i of the private key).
  - a public verification key VK that can be used to verify a signature created with a private key from the group.
- Fundamental property : allow to authentify anonymously multiple times in an unlinkable manner.

Unique group signature (Franklin et Zhang 12)

- Additional property : two group signatures on the same message generated by the same user possess a large common component (*uniqueness*).
- Ensure the unlinkability unless a user tries to sign several times the same message.
- A detection algorithm taking as input two signatures on the same message returns *true* if these two signatures have been generated by the same user.

Commitment protocol

- Commitment phase : takes as input a value a as well as some auxiliary information aux (generally a random string) and outputs a commitment $comm(a)$ on this value.
- Opening phase : takes as input a commitment $comm(a)$ and some auxiliary information aux and outputs the value a associated to this commitment.

Desirable properties:

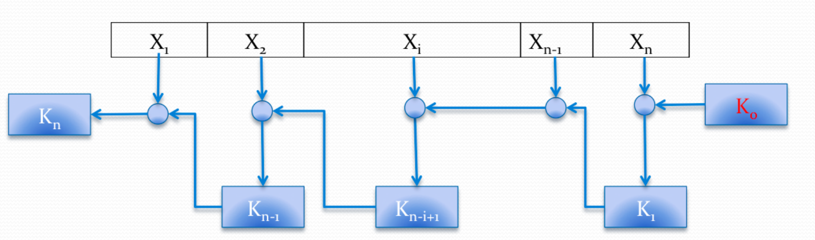
- Binding : there exists only one possible value a for the commitment $comm(a)$ (the adversary cannot open his commitment to several values of his choice).
- Hidding : the adversary does not learn any information on a from the commitment $comm(a)$.

Zero-knowledge proof

- Zero-knowledge proof : cryptographic protocol by which a prover can convince a verifier of the validity of a statement (for which he knows a proof) without having to reveal any other information that the veracity of this statement.
- Non-replicability : as the verifier will have learned nothing else than the veracity of the statement, he will not be able to act as a prover in front of another verifier.
- Example of application : the prover might be a individual that want to prove some property linked to its identity that is stored as an anonymous credential on a smartcard to a verifier that can be reader.

Selective disclosure of the location via hash chains

- Let $pos = X_1, \ldots, X_n$, be the representation of the position in which X_1 is the "coarsest" bit and X_n the more "precise" bit.
- Possible representation of the location as a hash chain : $K_i = h(K_{i-1} \oplus X_{n-i+1})$, for h a publicly known hash function and K_0 a random initial seed.



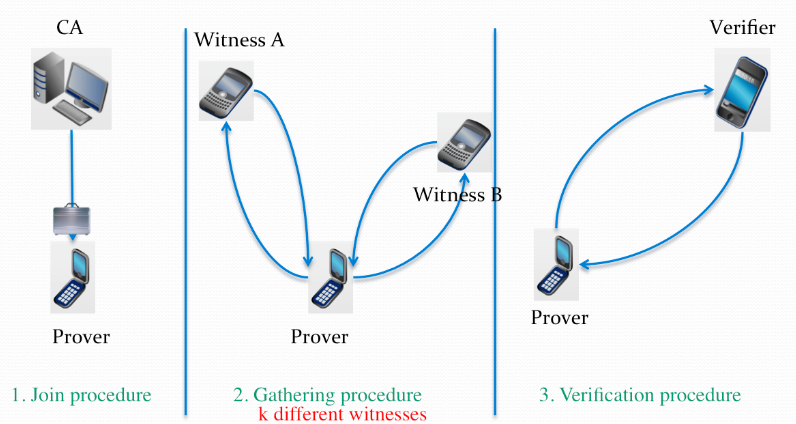
- Only K_n will be signed by the witness.

PROPS (PRivacy-preserving lOcation Proof System)

PROPS

- Collaborative privacy-preserving location proof system.
- The prover demonstrate his proximity with k different witnesses and collects the corresponding location shares.
- The location proof is composed of a combination of the k shares.
- Assumptions :
  - No central server storing the location proofs, each user "carries" with him his own proofs.
  - Availability of the proximity testing as a "black-box".

Overview of the protocol

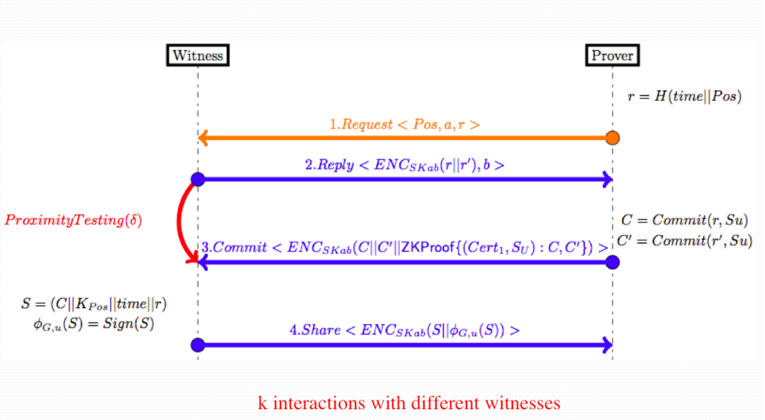


Registration phase

Upon his registration to the CA, a user receives :

- a private key S_U linked to his identity,
- a certificate on this private key $\sigma_{S_U,CA}$ signed by the CA,
- a private unique group signature key SKG_U.

Gathering phase



Gathering process (1/2)

The following algorithm is repeated in parallel with at least k different witnesses :

1. The prover sends his position *pos*, the current time *time* as well as a, his part of a Diffie-Hellmann key exchange protocol.
2. The witness verifies the plausibility of the position and the current time claimed by the prover and computes $r = h(time||pos)$.
3. The witness computes b, his part of a Diffie-Hellmann key exchange protocol as well as a session key SK_{ab} and a random string r'.
4. The witness starts a proximity testing with the prover and sends in parallel $\text{ENC}_{SK_{ab}}(r||r')$, the encryption of the message $r||r'$ under the session key SK_{ab}, as well as in clear b his part of the Diffie-Helmann.

Gathering process (2/2)

5. The prover computes two commitments, $C = \text{Commit}(r, S_U)$ and $C' = \text{Commit}(r', S_U)$, which corresponds to commitments on r et r' under the secret key of the user S_U.
6. The prover sends to the witness $\text{ENC}_{SK_{ab}}(C||C'||\text{ZKProof}\{(S_U, \sigma_{S_U,CA}) : C, C'\})$, which corresponds to the encryption under the session key SK_{ab} of C and C' concatenated with a zero-knowledge proof that these commitments have been generated with the same secret key S_U and that the prover possesses a valid signature $\sigma_{S_U,CA}$ du CA sur S_u.
7. If the witness accepts the zero-knowledge proof and the proximity testing succeeds then the witness agrees to sign the location via a group signature $S = (C||K_{pos}||time||r)$ and $\sigma_{G,U}(S)$.

Verification phase

In order to convince a verifier, the prover sends the following information

1. k shares of a location proof,
2. a zero-knowledge proof that he is the owner of the identity contained inside the commitment corresponding to the shares,
3. information about the location by choosing the granularity revealed through hash chains.

The verifier can then assess the validity of the knowledge proof and the fact that the k shares have been generated by different signers.

Security and privacy analysis of PROPS (1/3)

- Completeness and soundness : ensure by the proximity testing and the unique group signature that guarantees that the k shares of the proof come from different signers.
- Proof of ownership : guarantee by the knowledge proof performed during the verification that implies the possession of the private key S_U linked to this proof.
- Unforgeability : ensure by the uniqueness property of the unique group signature that implies that only a collusion of at least k malicious users can forge a fake location proof.

Security and privacy analysis of (2/3)

- Anonymity and unlinkability of the prover : ensure by the (unique) group signature, the zero-knowledge proofs and the absence of persistent identifier linking a location proof to a prover.
- Anonymity and unlinkability of the witnesses : ensure by the (unique) group signature and the absence of persistent identifier linking a location proof to a witness.
- Location privacy of witnesses : only an upper bound (a circle) is revealed by the proximity testing.

Security and privacy analysis of PROPS (3/3)

- Selective disclosure of location : guarantees by the coding of the location as a hash chain.
- Moreover, a user chooses when he wants to show his location proof (*sovereignty of the prover*)
- Resistance to localization attacks : ensured by the proximity testing.
- Possible additional property : revokable anonymity.

Comparison of approaches

Table I
COMPARISON OF APPROACHES

	Properties/Protocol	[5]	[3]	[2]	APPLAUS [6]	SLVPGP [4]	LINK[7]	[8]	PROPS
SECURITY	Correctness	✓	✓	✓	✓	✓	✓	✓	✓
	Ownership proof	✓	✓	✓	✓	✓	✓	✓	✓
	Unforgeability	✓	✓	✓	✓	✓	✓	✓	✓
	Robustness to distance fraud	✓	✓	✓		✓			✓
	Robustness to mafia fraud		✓			✓			✓
	Robustness to terrorist fraud					✓			✓
	Robustness to distance hijacking								✓
	No single point of failure	✓	✓	✓				✓	✓
	Collusion detection				✓				
	Proof share uniqueness								✓
PRIVACY	Prover anonimity and unlinkability (gathering phase)	✓	✓	✓	✓			✓	✓
	Prover anonimity and unlinkability (verification phase)								✓
	Witness anonymity and unlinkability (gathering phase)	✓			✓			✓	✓
	Witness anonymity and unlinkability (verification phase)	✓			✓	✓	✓		✓
	Witness location privacy	✓						✓	✓
	Confidentiality	✓				✓			✓
	Location sovereignty	✓							✓

Conclusion

Conclusion

- Proposition of an architecture for a privacy-preserving collaborative location proof system.
- A user carries his location proofs with him and chooses to whom and when he wants to show them and the granularity of the information revealed.
- Work in progress :
  - Choice of implementations for the cryptographic primitives.
  - Replacement of the black-box for the proximity testing by an explicit protocol.
  - Design of a secure multiparty computation version of the protocol involving a joint computation between witnesses rather than on pairwise interactions between the prover and each witness.
  - Selective disclosure of the time.

This is the end!

Thanks for your attention.
Questions?

Group signature : operations

- Registration of the user : the certification authority (CA) registers the user and assigns him a private signature key SKG_U.
- Signature of a message on behalf of a group : takes as input a message m and a private signature key SKG_U and produces as output a signature $\sigma_{G,U}(m)$ on this message.
- Vérification of a group signature : takes as input the verification key VKG (which is public and has been set up by the CA) as well as a message m and a group signature on this message $\sigma_{G,U}(m)$ and returns *accept* or *reject* as output.
- Anonymity revokation (optional operation) : takes as input a message m and a group signature $\sigma_{G,U}(m)$ and returns the identity U of the signer of this message.

Properties of a group signature scheme

- Completeness and soundness : a valid signature must always be verifiable while a fake signature should be able to pass the verification procedure (except with small probability).
- Unforgeability : only the members of the group should have the ability to produce a valid signature.
- Anonymity : from a message and its signature, it should be impossible to find the identity of the member who has signed the message.
- Unlinkability : from two different messages and their signatures, it should be impossible to determine if they have been issued by the same signer.
- Other properties : impossibility to generate a fake signature for a specific member of the group even if several members collude together.

Properties of a zero-knowledge proof

- Completeness : if the prover and verifier are honest then the prover must always be convinced at the end of the protocol.
- Soundness : if the statement is false, then no malicious prover should be able to convince an honest verifier of the veracity of the statement (except with negligible probability).
- Zero-knowledge : the verifier learns no other information than the veracity of a statement.
- The first two properties define the concept of interactive proofs while the last one is specific to zero-knowledge proofs.
- Remark : zero-knowledge proofs can be *non-interactives*.