Secure Multi-Party Computation: formalization of privacy in Location Based Mobile Services (LBMS)

IFIP Summer School 2011

7-9-2011

luigi grillo

grillo@dmi.unict.it

University of Catania

Outline

- LBMS definition
- Privacy and Security context
- Case of Study: Vpriv protocol
- The VPriv enhancement proposal
- Conclusion & Future work

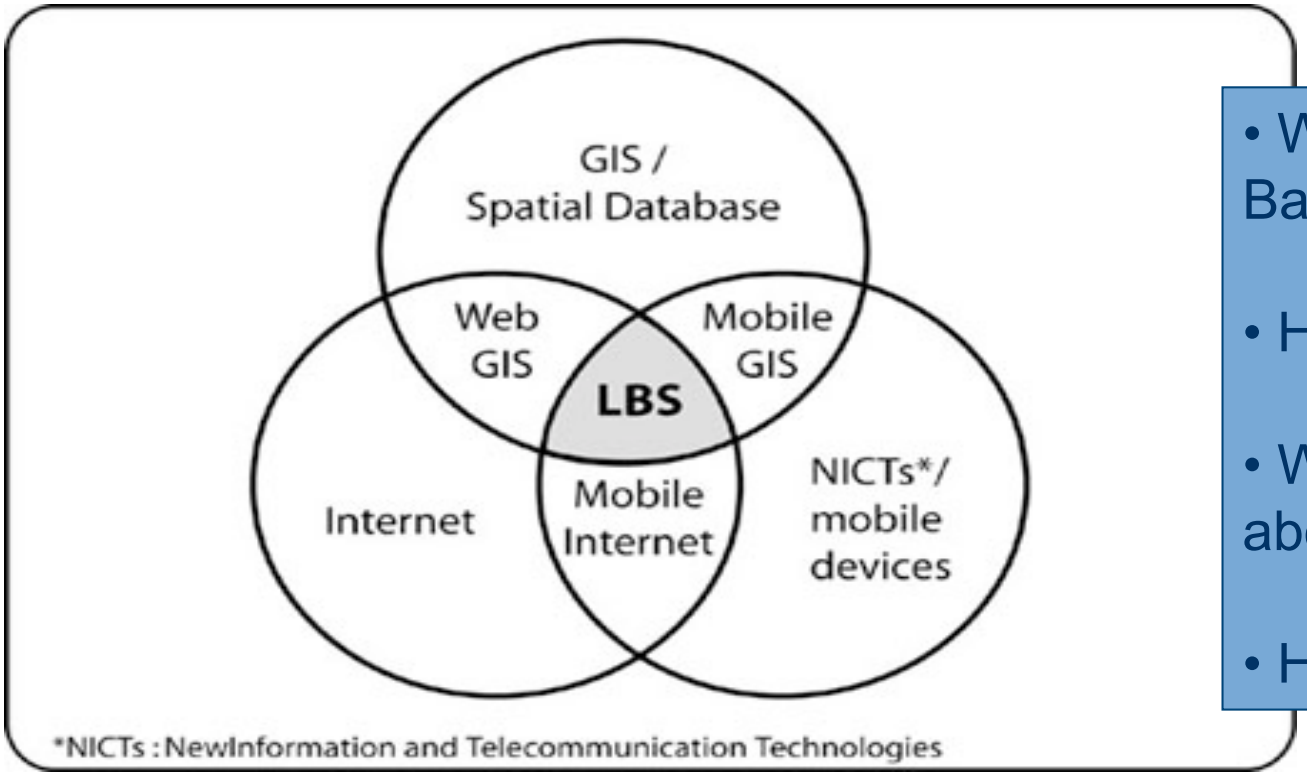
Location based Services definition

Applications that rely on
the location coordinates of the users,
to provide services

Location based Mobile Services definition(*)

DEF 1. LBMS's are information services accessible with mobile devices through the mobile network and utilizing the ability to make use of the location of the mobile device. (Virrantaus et al. 2001)

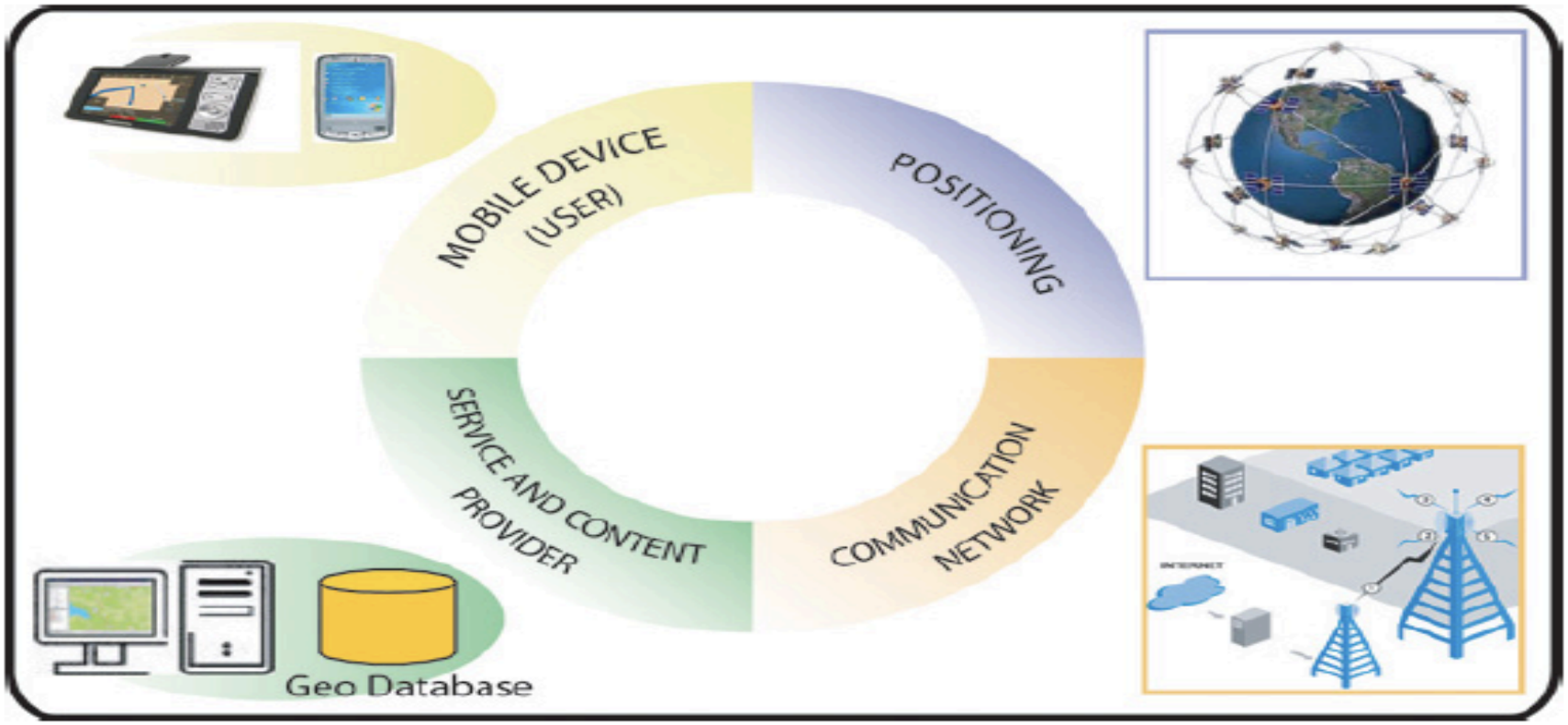
DEF 2. A wireless-IP service that uses geographic information to serve a mobile user. Any application service that exploits the position of a mobile terminal. (Open Geospatial Consortium 2005)



- What are Location Based Services?
- How is it useful?
- What is special about it?
- How does it work?

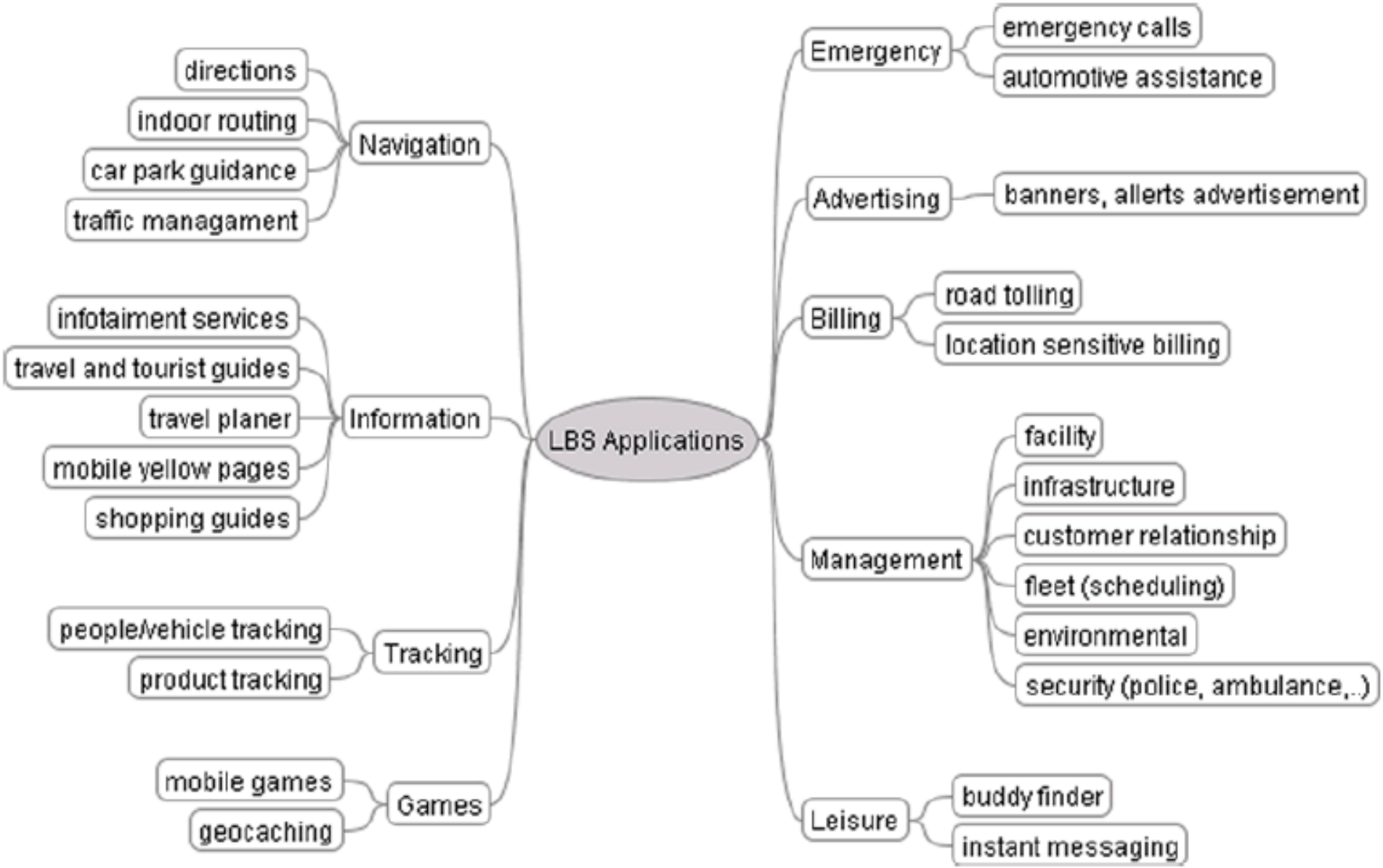
(*) Foundations of Location Based Services Lesson 1 CartouCHe1 - Lecture Notes on LBS, V. 1.0 Stefan Steiniger, Moritz Neun and Alistair Edwardes2

LBMS Components



Mobile Applications are tremendously increasing the requests of services based on user location information.

LBMS Categories



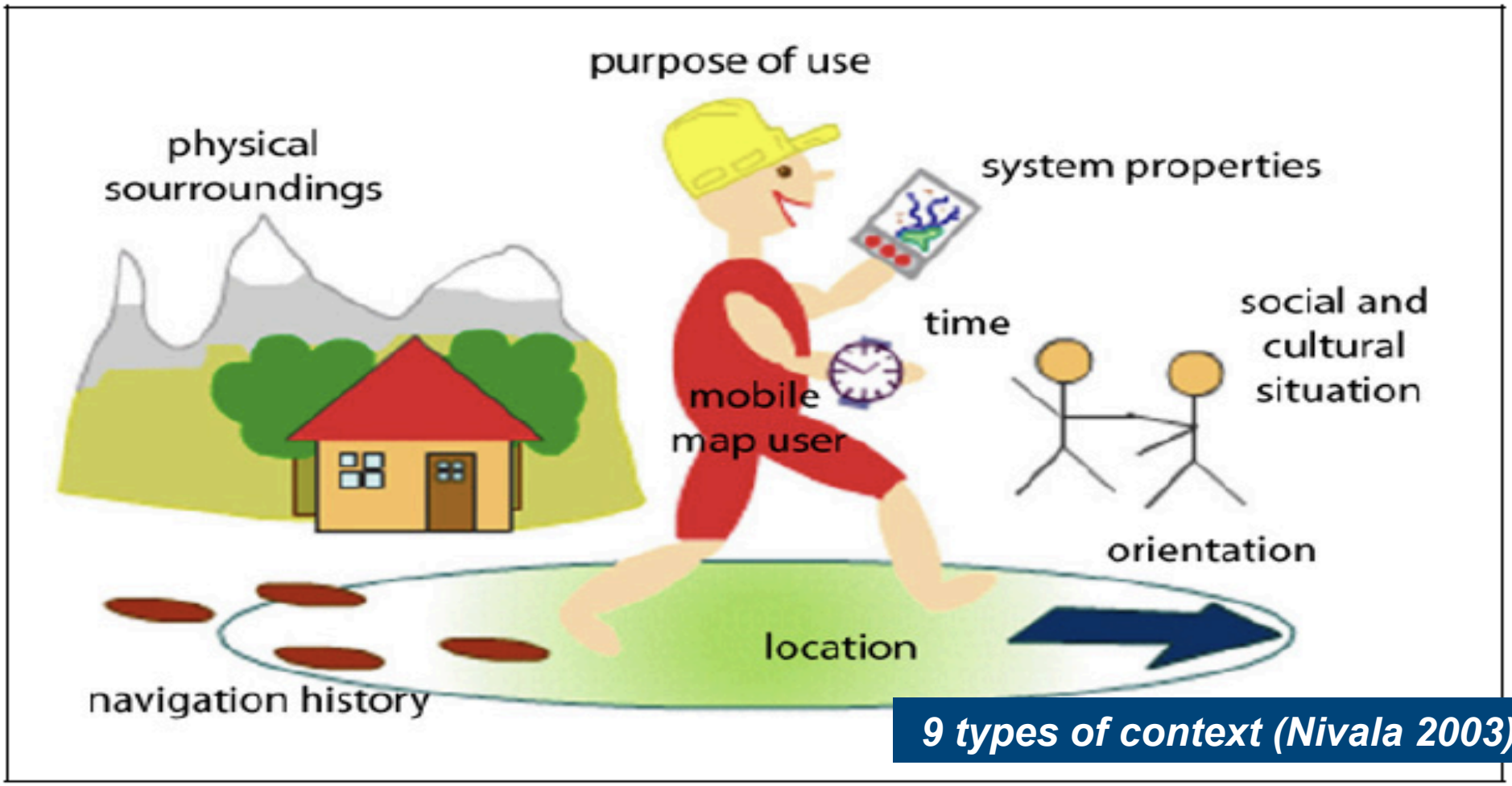
LBMS: **common characteristics**

- require users authenticity
- deal with sensible user information
- impact big number of users
- simple mat. operations are involved

Mobile Applications are tremendously increasing the requests of services based on user location information

What's special about it?

LBMS are **aware of the context** (location, time and task): ***ubiquitous computing***.



9 types of context (Nivala 2003)

LBMS: some key examples

Antikainen H., J. Rusanen, S. Vartiainen, M. Myllyaho, J. Karvonen, M. Oivo, J. Similä ja K. Laine (2006). **Location-based Services as a Tool for Developing Tourism in Marginal Regions**. Nordia Geographical Publications 35:2, 39-50. NGP Yearbook 2006. Theme Issue on Northern nature and Human Activities.

Sarin Kizhakkepurayil, Oh Jeon-Yeoul and Young Lee. **Mobile Application for Healthcare System - Location Based**. Innovations and Advances in Computer Sciences and Engineering 2010, 297-302, DOI: 10.1007/978-90-481-3658-2_51

Andrew J. Blumberg, Hari Balakrishnan and Raluca Popa. **VPriv: Protecting privacy in location-based vehicular services**. 18th Usenix Security Conference, 2009.

...key points

- Smarthphones, with their ability to manage the user localization, have been the first real **ubiquitous computing** platform.

- Special focus on Location Mobile Services for **human** and **social development**, particularly for the developing countries.

- LBMS play a central role with intrinsic privacy issues

Outline

- LBMS definition
- Privacy and Security context
- Case of Study: Vpriv protocol
- The VPriv enhancement proposal
- Conclusion & Future work

Three basic concepts

1. Privacy is "*the claim of individuals [..] to determine for themselves when, how, and to what extent information about them is communicated to others*", A.F. Westin

2. ”*[..] neither the law nor people's intuition is keeping up with the pace of technological change; this is a classic example of where the transition from inexpensive (a policeman follows your car) to free (the police mine the location database) will cause a dramatic change in the* ***possibilities for abuse***”, Andrew J. Blumberg

3. *The concept of privacy in computing is influenced by different research fields: legislative, social psychology and computer science. It changes with the time/spatial context*.

Privacy & Security context



Application Service Provider

The challange is:
Proving the user Location
Without compromising Privacy



LBMS Application

Protecting privacy does not necessarily mean an implementation of security.

Proving Location

Definitions

Location Proof

An electronic form of document that certifies someone's presence at a certain **location** at some point in **time**

Location Proof architecture

A mechanism with which mobile users can obtain **location proof**s from **proof issuers** and with which applications can verify the **validity** of these proofs

Architecture Design Requirements

1. **Scalability**
2. **Application-Agnostic Location Proofs**
3. **Proactive Location Proofs**
4. **User Anonymity**
5. **Location Privacy**
6. **No Dedicated Hardware**

Wanying Luo&Urs Hengartner 2010 – University of Waterloo

Guaranteeing Privacy

Which approach to the problem?

Heuristic Approach 1

1. *Build a protocol*
2. *Try to break the protocol/ Intuitive analysis*
3. *Fix break*
4. *Return to 2*

Heuristic Approach 2

1. *Design protocol*
2. *Provide a list of attacks that cannot be carried out on the protocol*
3. *Reason that the list is complete*

A rigorous approach

- Provide an exact problem definition
  - Adversarial power definition
  - Network model
  - Meaning of security
- Formal Prove that the protocol is secure

Rigorous approach

- Provide an exact problem definition
  - Threat Model definition
  - Network model
  - Meaning of security
- Prove that the protocol is secure



LBMS Application



Application Service Provider

- **Dishonest Users**
- **Malicious intruders**
- **Curious APs and Applications**
- **Malicious Applications**
- **Active and passive eavesdroppers**

Further threat: Wormwhole attack,Weak identities

Which approach?

Conjecture

LBMS are an instance of a Secure Multi-party Computation

Secure Multi-party Computation

- A set of parties with private inputs wish to compute some joint function of their inputs.
- Parties wish to preserve some security properties. E.g., privacy and correctness.
  - Example: secure election protocol
- Security must be preserved in the face of adversarial behavior by some of the participants, or by an external party.

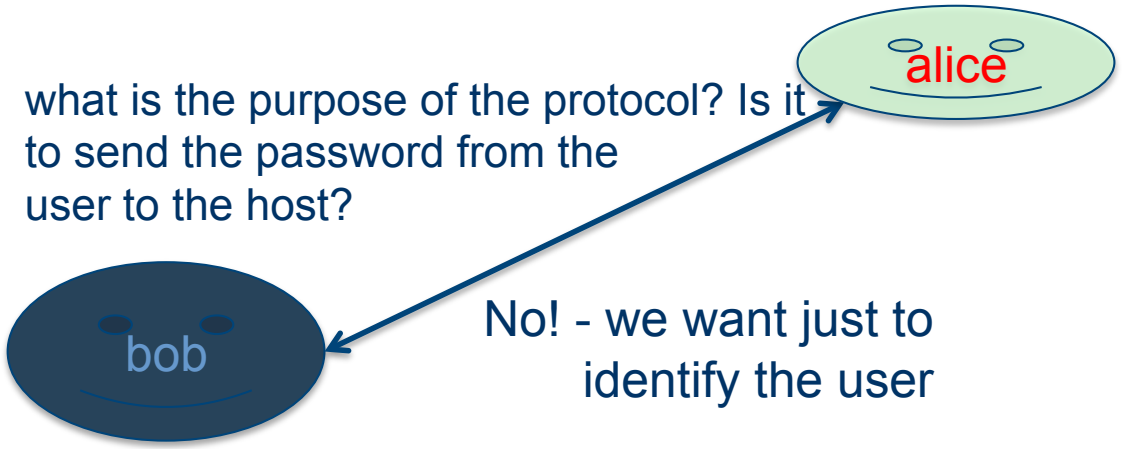
Examples.

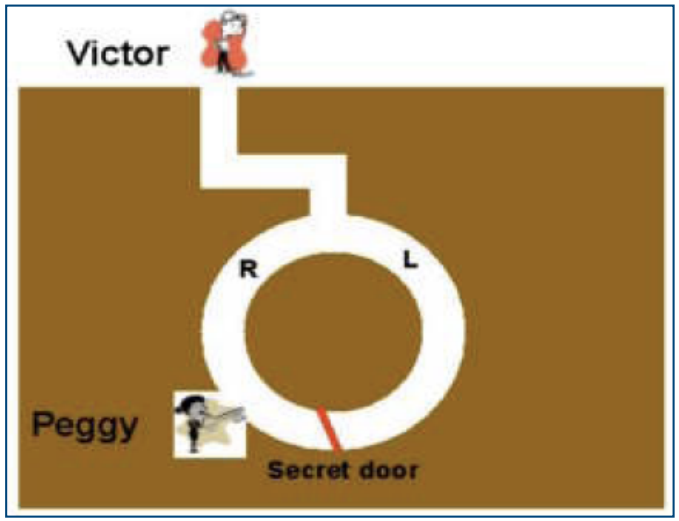
- Privacy Information Retrieval
- Yao Millionaires Problem
- Privacy-preserving data mining
- **Privacy Preserving Geometric Computation**

zero-knowledge protocols

- a protocol is zero-knowledge if it communicates exactly the knowledge that was intended, and no (zero) extra knowledge. (first introduced by Goldwasser, Micali, Rackoff)

EX: user identification protocol





The only thing the host needs to know here is 1 bit of information, namely whether the statement "I know the secret corresponding to user name xxx" is true or not. The real purpose of the protocol is to communicate this piece of knowledge to the host

The approach

Conjecture

LBMS are an instance of a Secure Multi-party Computation

Similarities example
PrivacyPreserving Geometric Computation - Range Searching

Alice has a private range (represented by either a hyper-rectangular shape or by spherical shape), and Bob has N private points. Alice and Bob want to jointly find out the number of points in Alice's range; however, neither of them is willing to disclose their data to the other party

M.J. Atallah and W.Du. Secure multi-party computational geometry. In WADS2001: Seventh International Workshop on Algorithms and Data Structures, pages 165-179, Providence, Rhode Island, USA, August 8-10 2001.

Objective (research question):

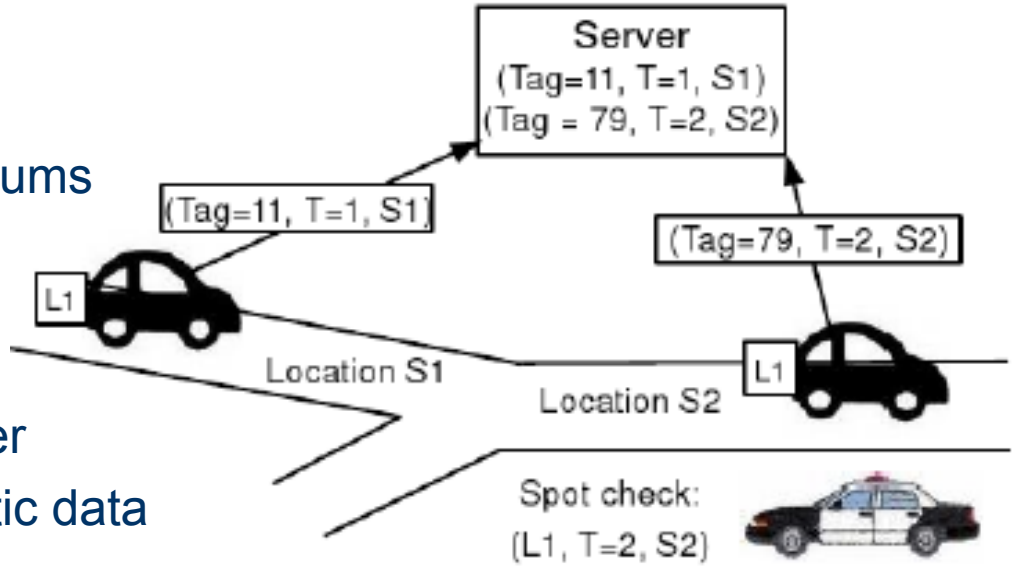
Formalization of LBMA in term of Secure Multi-party Computation to apply formal correctness verification methods.

Outline

- LBMS definition
- Privacy and Security context
- Case of Study: Vpriv protocol
- The VPriv enhancement proposal
- Conclusion & Future work

Vpriv General Description

- Model: a protocol that preserve privacy for three spicific functionality:
  - Usage-based tolls
  - Automated speeding tickets
  - “Pay-as-you-go” insurance premiums
- Treath Model
  - The driver attempts to cheat
  - The driver turns off the trasponder
  - The transponder uploads synthetic data
  - Transponder spoofing
  - The server guesses the path of the car
  - The server attempts to cheat during the function computation protocol
  - intermediate router synthesizes false packets



http://cartel.csail.mit.edu/#vpriv

Vpriv

- Partcipants:

  n vehicle users, 1 service provider

- Protocol overview

For each period Pj there are three phases

1. Registration phase

Commitments between the users and the service provider to exchange the random tags set V generated by each user $[M]_d$.

2. Driving phase

Each user chose a tag from his set V and send it in clear to the service provider whom collect all the tags of all users in a DB containing tuple (v,l,t).

3. Reconciliation phase

A protocol is started to compute and settle the payable debts.

Vpriv protocol details

- Phase 1: registration phase

$$\mathcal{V} \rightarrow \mathcal{S}: \; r^i = \left(id, i, [k^i]_{dk^i}, [f_{k^i}(v_1)]_{dv_1^i}, \ldots, [f_{k^i}(v_n)]_{dv_n^i} \right)$$

(V=*vehicle;* S=*service provider; i round number ε [1;s]*)

Vehicle: 1) generate fresh random tags, 2) generate fresh key 3) register **commitments** to their encrypted version with the service provider



Vpriv protocol details

- Phase 2: driving phase

V -> S: (v)

Each vehicle emits its tags $v_1, \ldots v_m$ in random order along its route.

The server build DB (v,l,t)

Vpriv protocol details

- Phase 3: reconciliation phase

$$\mathcal{S} \rightarrow \mathcal{V} : W = \left[(w_1, c_1), \ldots, (w_m, c_m)\right]$$
$$\mathcal{V} \rightarrow \mathcal{S} : id, C$$

For each round *i:*



$$\mathcal{V} \rightarrow \mathcal{S} : id, U^i = \left[\left(f_{k^i}(w_{\sigma^i(1)}), [c_{\sigma^i(1)}]_{dc_1^i}\right), \ldots, \left(f_{k^i}(w_{\sigma^i(m)}), [c_{\sigma^i(m)}]_{dc_m^i}\right)\right]$$
$$\mathcal{S} \rightarrow \mathcal{V} : b^i$$
$$\mathcal{V} \rightarrow \mathcal{S} : \begin{cases} id, dk^i, dc_1^i, \ldots, dc_m^i & \text{if } b^i = 0 \\ id, dv_1^i, \ldots, dv_n^i, D^i & \text{if } b^i = 1 \end{cases}$$

Vpriv protocol criticality

a) The user could send tags which are dierent than the ones committed during the registration phase;

b) The user could modify the time and/or the location of the tuples while driving;

c) The user could fail to send a tuple.

Protocol limitation: Spot Check

An enforcement device secretly collects identifying data (ex taking the license plate) buiding a DB of tuples (id,v,l,t). Before the reconciliation the server challanges the client with

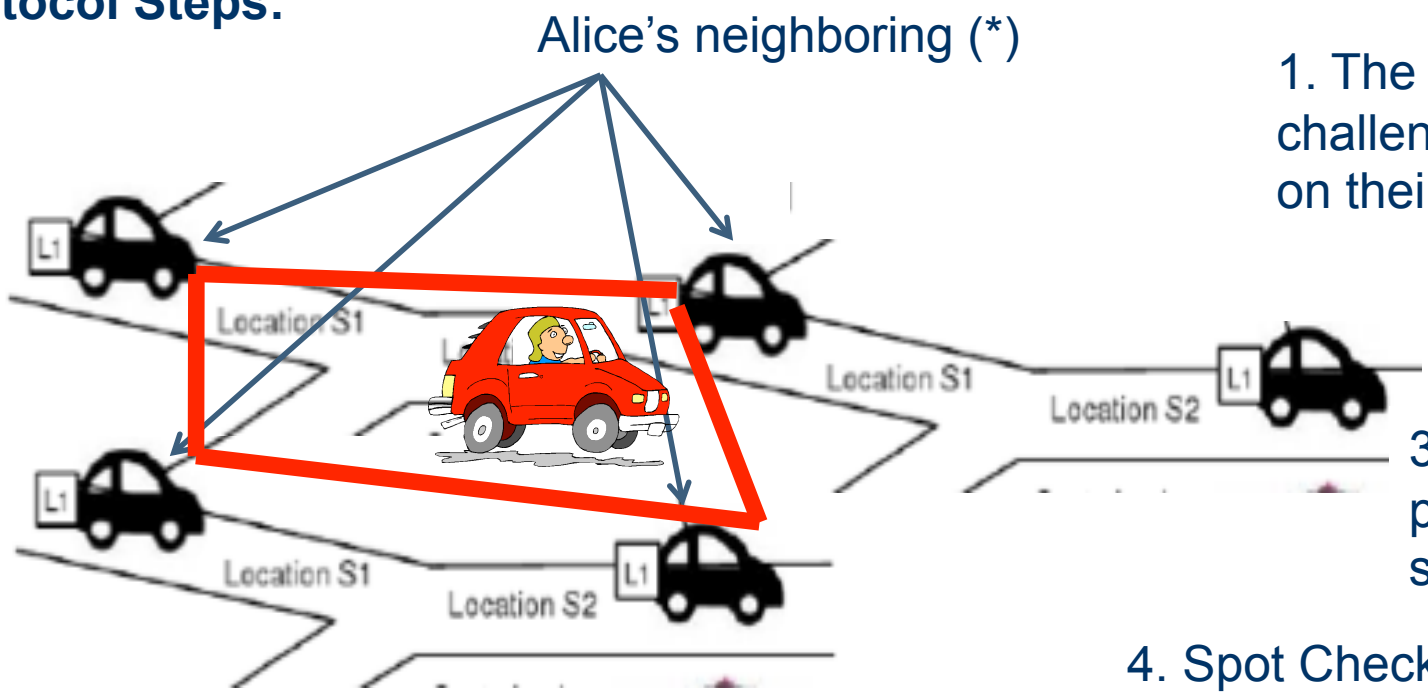
(l,t) | (id,v,l,t) belong to DB

Outline

- LBMS definition
- Privacy and Security context
- Case of Study: Vpriv protocol
- The VPriv enhancement proposal
- Conclusion & Future work

VPriv enhancement proposal

Protocol Steps:



1. The server randomly challenges a set of users on their location. (*)

2. The polygon P is defined

3. Point-inclusion problem resolution starts (**)

4. Spot Check: the ask to the user to move to a known position

*(**) **Point-inclusion problem**. "Alice has a private point z, and Bob has a private polygon P. They want to nd out whether the point is inside the polygon or not. Alice does not want Bob or anybody else to know any information about the point, and likewise, Bob does not want anybody else to know any information about the polygon. Furthermore, Alice and Bob can only learn whether the point is inside or outside of the polygon, nobody is allowed to learn the relative position between the point and the polygon."*

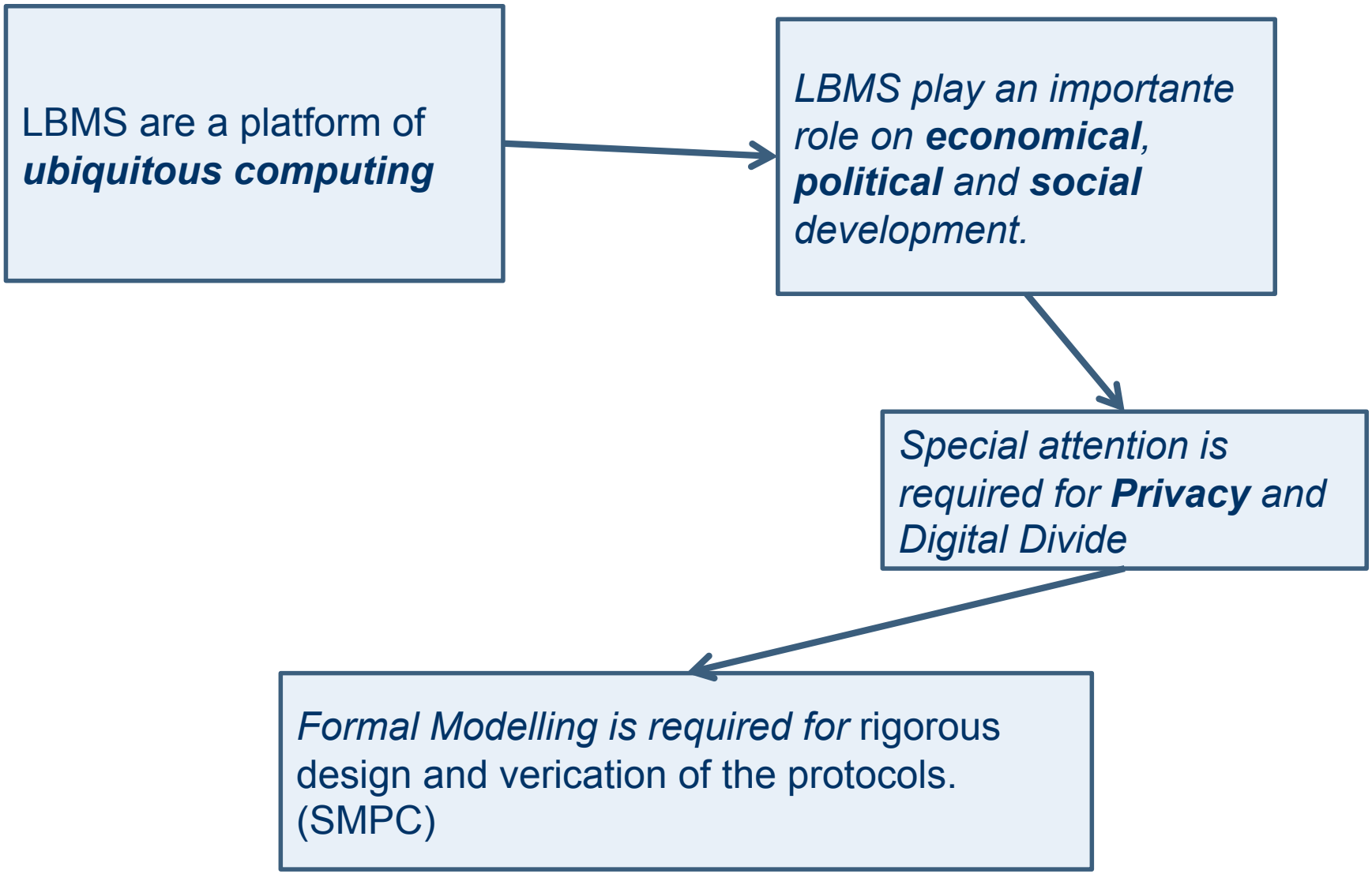
(*) . M.Graham, D. Gray. ProVer: A Secure System for the Provision of Veried Location Information. Mobile Computing, Applications and Services Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2010, Volume 35, Part9.

Conclusion

- **The LBMS outline has been defined**
  - first real *ubiquitous computing* platform
  - play an important role in human and social development

- **LBMS privacy & security requirements have been formalized**
  - VPriv protocol criticity have been arised
  - Enhancement has been proposed in terms of **SMPC**

Conclusion


LBMS are a platform of ***ubiquitous computing***
*LBMS play an importante role on **economical**, **political** and **social** development.*
*Special attention is required for **Privacy** and Digital Divide*
Formal Modelling is required for rigorous design and verication of the protocols. (SMPC)

Future work

- Implementation of the proposed protocol
- Formal Analisis of the protocol (pi-calculus/ Proverif ?)
- Deeper investigation on SMPC paradigm

Thank you!