Research on location-based services at UL:
(1) Partial Location Blinding
(2) Electronic Toll Pricing

Sjouke Mauw
University of Luxembourg
sjouke.mauw@uni.lu

(joint work with Xihui Chen, Gabriele Lenzini and Jun Pang)

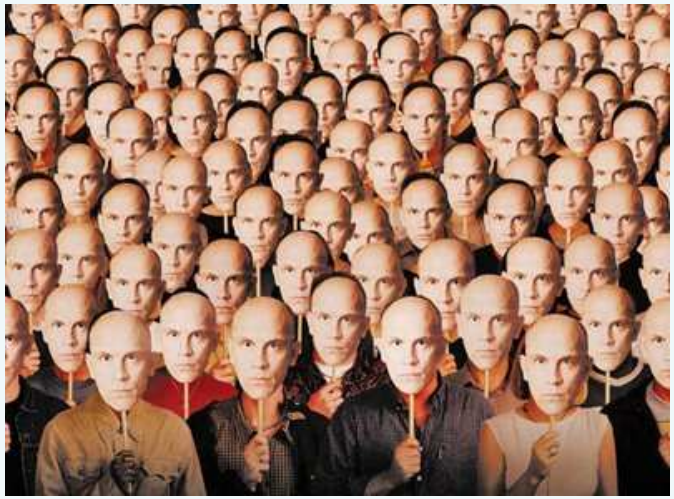
Main problem

Tension between conflicting security requirements:

- Location privacy
  Individuals can determine for themselves when, how, and to what extent location information about them is communicated to others.
- Location assurance
  The claimed location information of an individual corresponds to his actual location.

Location privacy: solution concepts

Hiding in the crowd.



Give inexact location.

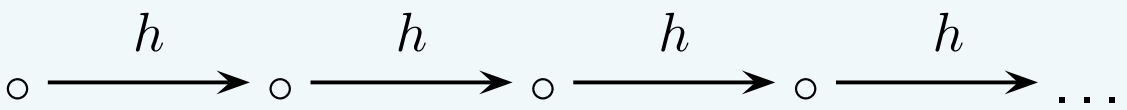
Usage scenarios

Actual solutions depend on the *usage scenarios*, e.g.

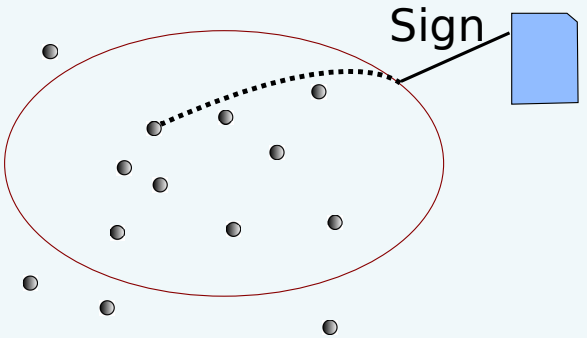
- E-tolling, Pay-as-you-drive (PAYD).
- Local services: Access control, location-based tariffing, location-based loyalty programs, etc.
- Recommend (nearest) business, events.
- Locate people on a map.
- Receive alerts.
- Advertising.
- …

Two specific solutions

1. ■ Usage: Local services
   - ■ Privacy concept: Inexact location
   - ■ Cryptographic primitive: Hash chains



2. ■ Usage: E-tolling
   - ■ Privacy concept: Hiding in the crowd
   - ■ Cryptographic primitive: Group signatures



1. Selective location blinding

Stakeholders:

- Client
  - Can determine own location using location device.
  - Wants to use several services at same location.
  - For each service lowest possible precision.
- Location verifier
  - Can verify and certify claimed location.
- Service provider
  - Offers service to client.
  - Needs to be sure about the client's location.
  - Required precision depends on the service.

Representing locations

A “location” is a list of natural numbers, e.g.

loc	= (latitude,	longitude,	time)
	= (98239723,	25201838,	1938749)

Control the precision:

uncertainty	latitude
0	98239723
1	98239720
2	98239700
⋮	⋮
7	90000000
8	00000000

A key chain for location x

- User creates key chain $K_n, K_{n-1}, \ldots, K_1, K_0$ for location parameter

$$x = x_{n-1} \cdots x_1 x_0$$

- Pack the consecutive digits of x:

K_0 is random initial key.

$$K_1 = h(K_0, x_0)$$
$$K_2 = h(K_1, x_1)$$
$$\vdots$$
$$K_n = h(K_{n-1}, x_{n-1})$$

- User sends x and K_0 to the location verifier.

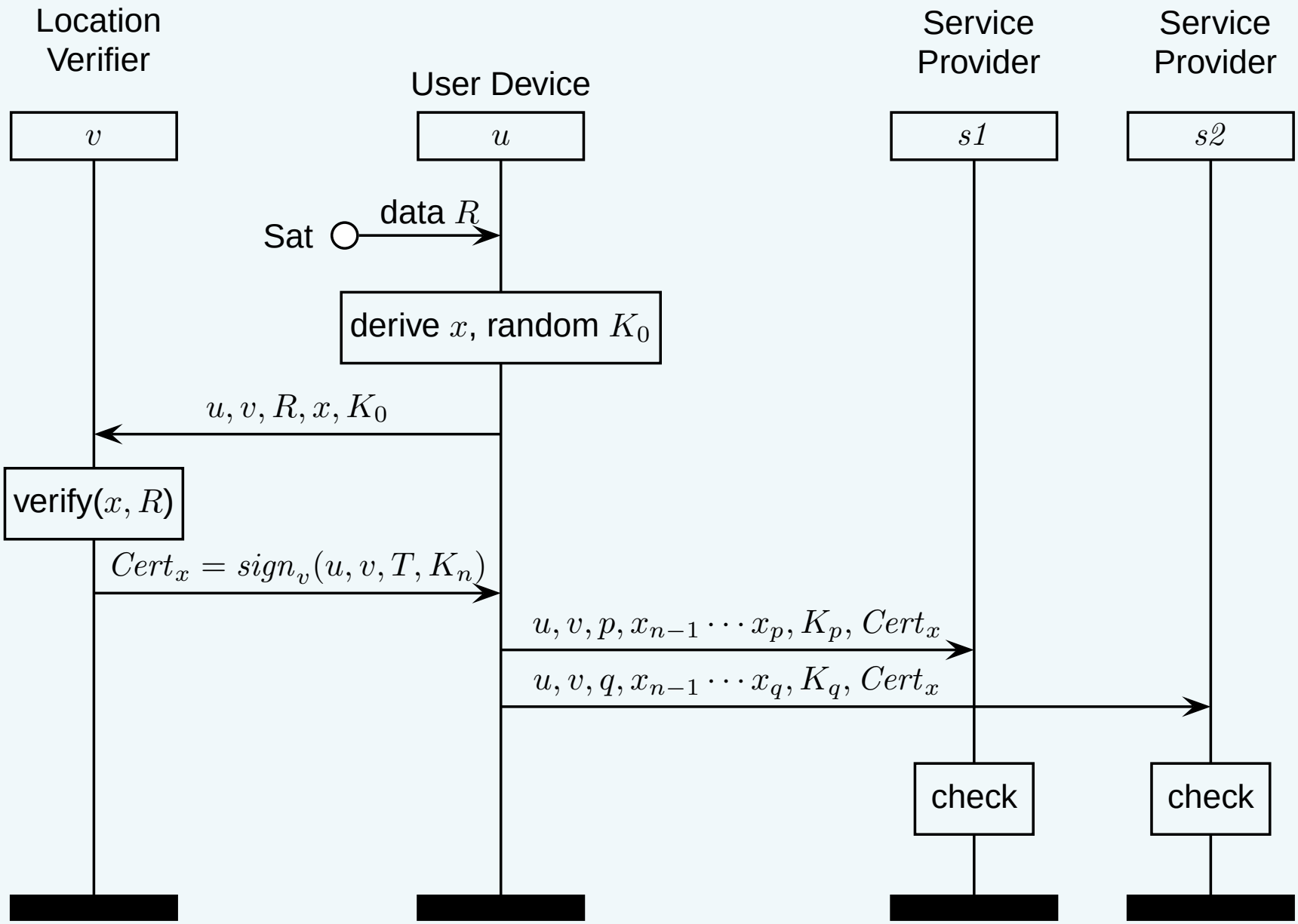
Using the key chain

- After verifying location x, the location verifier signs K_n: $sign_v(K_n)$.
- User selects uncertainty p for some service provider.
- User sends $x_{n-1} \cdots x_p$, K_p and $sign_v(K_n)$ to the service provider.
- The service provider partially reconstructs the hash chain:

$$K_{p+1} = h(K_p, x_p)$$
$$\vdots$$
$$K_n = h(K_{n-1}, x_{n-1})$$

- And the service provider verifies that the calculated K_n corresponds to the signed K_n.

Protocol


Location Verifier
User Device
Service Provider
Service Provider
v
u
$s1$
$s2$
Sat
data R
derive x, random K_0
u, v, R, x, K_0
verify(x, R)
$Cert_x = sign_v(u, v, T, K_n)$
$u, v, p, x_{n-1} \cdots x_p, K_p, Cert_x$
$u, v, q, x_{n-1} \cdots x_q, K_q, Cert_x$
check
check

2. Electronic Toll Pricing

Stakeholders:

- Client
  - Uses road.
  - Has trustworthy tamper-resistant location device.
  - Is motivated to not pay all toll fees.
  - Does not want the service provider to know his locations.
- Toll service provider.
  - Collects (anonymized) location data and charges the clients.
  - Curious to find out which location data links to which client.
- Authority
  - Trusted by all parties.
  - Offers PKI, resolves disputes, forms groups, etc.

Group signatures

- Group manager (= authority) and group members (= subset of the clients).
- Single group public key.
- One private signing key per member.
- A member can sign with his private key.
- Everybody can use the public key to verify that the signature was made by one of the group members.
- Nobody (except for the group manager) can determine which of the group members made the signature.

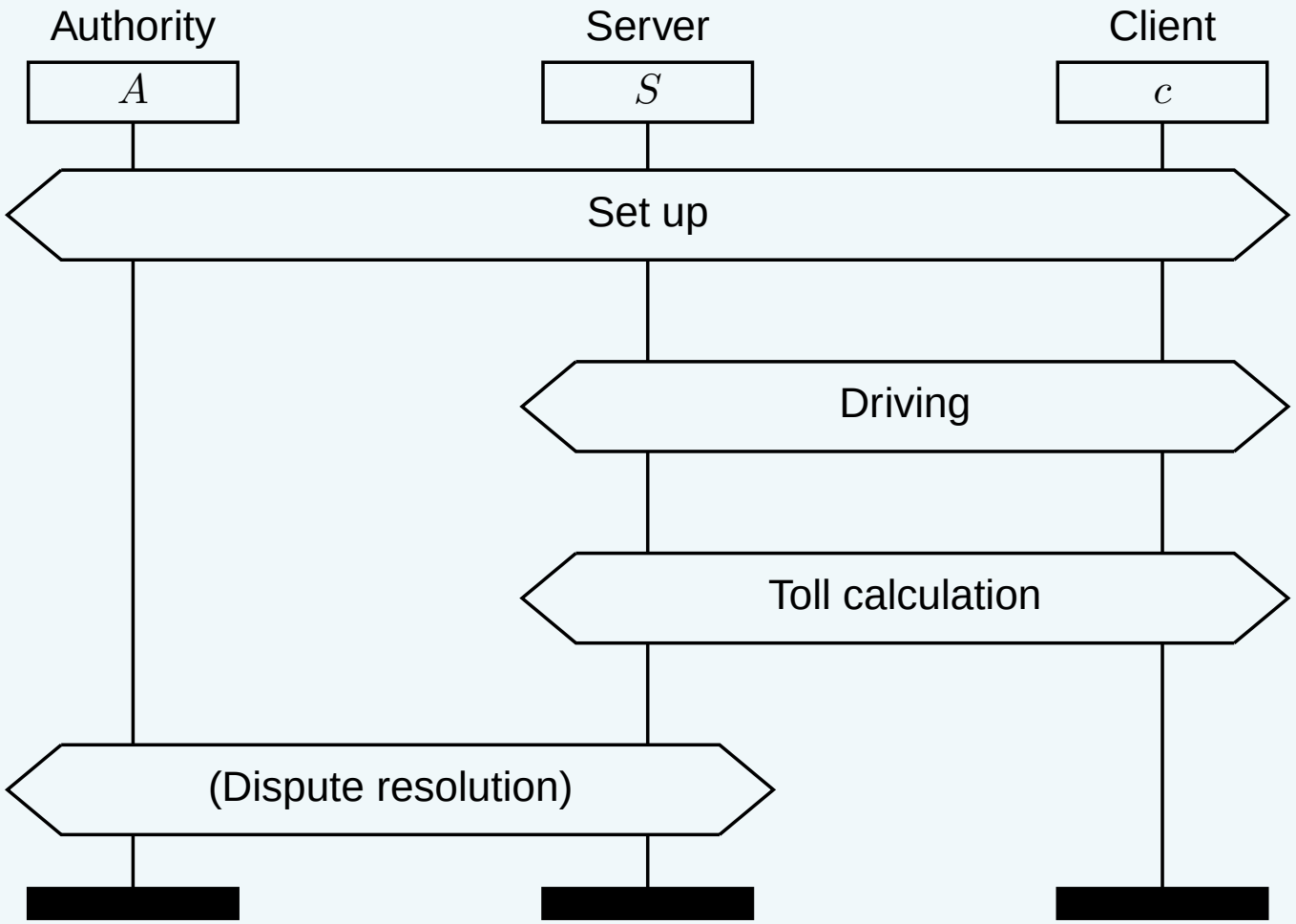
Requirements

Correctness An honest client pays for his own road usage and the server collects the right amount of toll.

Accountability If a malicious action that deviates from the specification of the system occurs, sufficient evidence can be gathered to identify its originator.

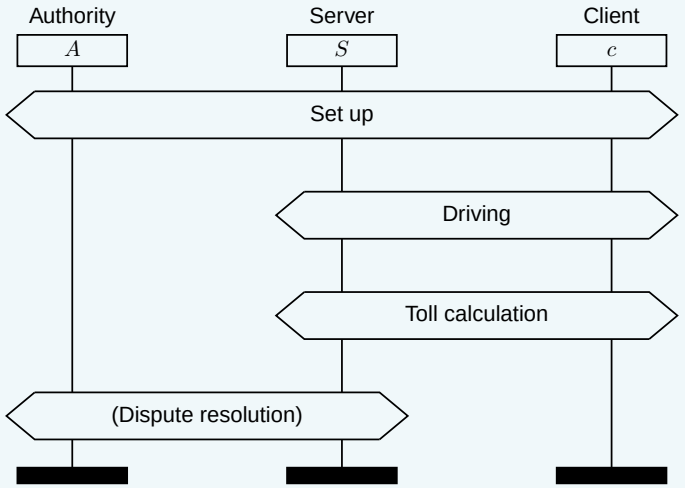
Unlinkability An intruder cannot link a given location record to its originator.

Phases


Authority
Server
Client
A
S
c
Set up
Driving
Toll calculation
(Dispute resolution)

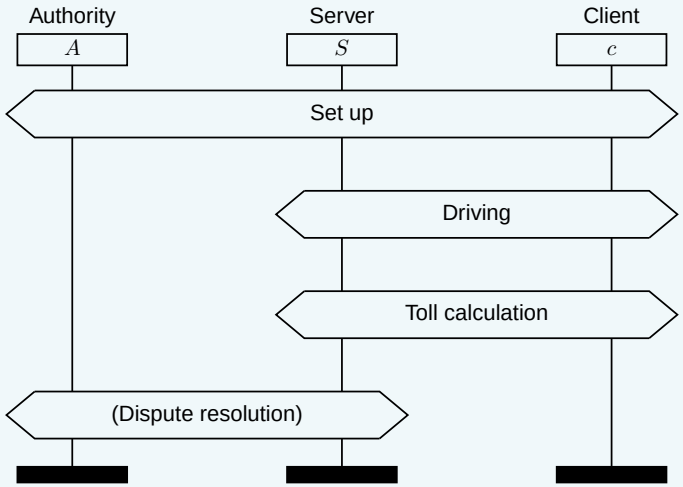
Phase 1: Set up

- Establish PKI.
- Authenticate parties.
- Set up groups.
- Establish group keys.



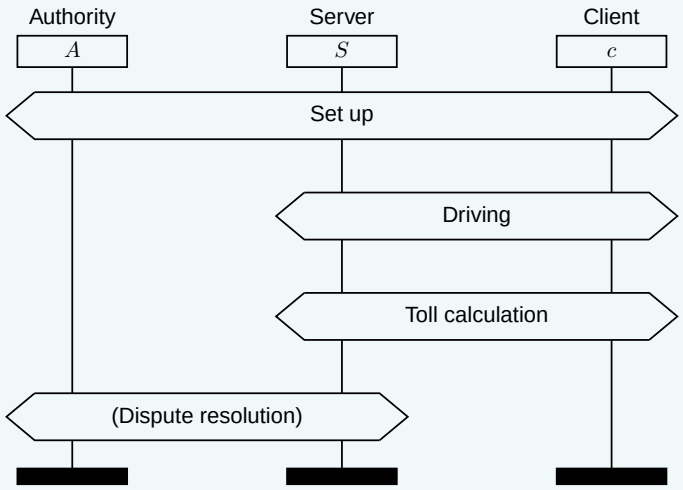
Phase 2: Driving

- While driving, a client produces location data.
- Client signs location data with his group private key.
- Client periodically sends signed location data over anonymous channel to server.



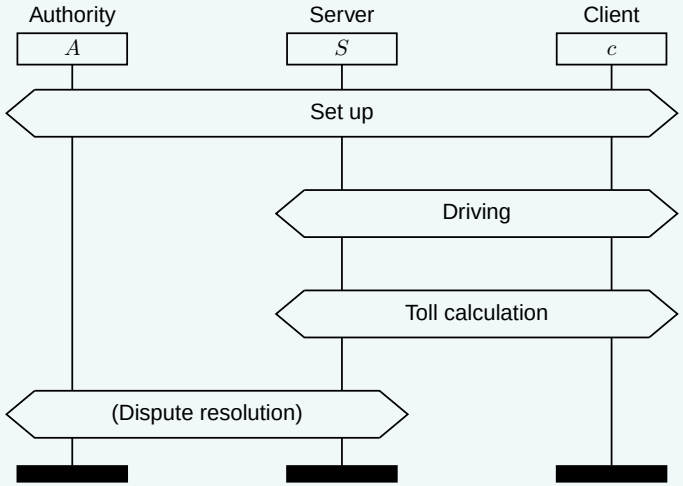
Phase 3: Toll calculation

- Server selects a group's location data. This data plus corresponding fees is sent to each group member.
- Client selects his location and fee data from the set.
- Client adds his fees and pays the sum to the server.
- Server adds all payments from the group members.
- If this equals the expected amount of toll for the whole group, this toll session ends correctly.
- If not, the server starts the dispute resolution phase.



Phase 4: Dispute resolution

- If conflict: Server sends all location data and payment information of a group to authority.
- Authority is the group manager and identifies which client signed which location data.
- Authority adds up the client's fees and compares it to the client's payment.
- Authority sends a (signed) list of due payments to the server.



Security analysis

The protocol satisfies the required properties:

Correctness An honest client pays for his own road usage and the server collects the right amount of toll.

Accountability If a malicious action that deviates from the specification of the system occurs, sufficient evidence can be gathered to identify its originator.

Unlinkability An intruder cannot link a given location record to its originator.

We used ProVerif to automatically verify unlinkability.

Conclusions

- Different usage scenarios give essentially different solutions. This is due to varying assumptions, intruder model, architecture, functional requirements.
- Side-channel attacks on these protocols are possible, e.g.
  - A certain “sum” of fees, can only be produced by a limited number of subsets of all location/fee records of a group.
- The simple hash chaining protocol seems the first to solve the problem with the given assumptions.
- The group signature protocol improves on existing protocols (VPriv, PrETP).