Access Control and Privacy in Location-aware Services for Mobile Organizations

Thaier Hayajneh

University of Pittsburgh

TeleNet@Pitt

Outline

- Mobile organization and requirements
- Goals and Contributions of this paper
- Definitions
- General Architecture
- Access control mechanisms
- Privacy
- Conclusions and Future Work

TeleNet@Pitt

Mobile Organizations

- Mobile Organizations: community of individuals that, because of the role they have, need to access common information resources through location-based services.
- Examples:
  - *enterprises operating on field,*
  - *healthcare organizations*
  - *military and civilian coalitions*
- In these organizations the mobile members are characterized not only by an identity but also by a *role*.
- Example: an organization that management a national park in which LBS are used to support the mobile personnel as well the visitors of the park. Individuals have different roles, say rangers, scientists, employees and tourists. Equipped with location-aware mobile terminals with which they invoke LBS, such as map services.

System Requirements

- LBS are requested based on the roles of individuals. services ranger different from tourists. Requires development of an *access control mechanism*
- The accessibility of services may depend also on the position of the user. Extent classical ACM to consider Mobility.
- Privacy concerns are also very relevant because of the capability of the technologies to collect, store and disclose the location of individuals. (Location Privacy) (Identity + Location)

Goals of this Paper

- To propose a comprehensive approach. An architecture for a privacy-preserving access control system for mobile organizations.
- The system:
  - filters the requests for service sent by the user,
  - determines whether the request can be accepted based on the role and position of the user
  - forwards an anonymous request together with a perturbed location to the application server which implements the requested service.
- The architecture is based on GEO-RBAC with the concept of *spatial role*.

Contributions of this Paper

1) Definition of the semantics of the access control function. enhance the model of spatial role, *R & NR* role.
2) Definition of an event-based architectural framework for the access control system.
3) Definition of a privacy strategy which enables the user to dynamically control which location data are transmitted, according also to the organizational privacy rules.

The Position Model

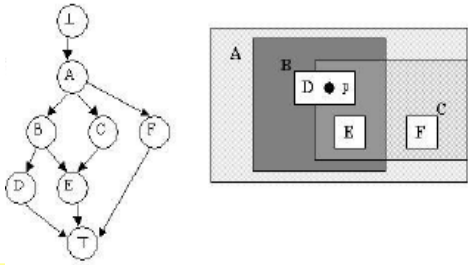
- The position model describes the position of the user.
- The *real position* corresponds to the position of the user on Earth acquired through some positioning technology
- The *logical position* supports a representation of positions that is almost independent from the underlying positioning technology.
- Logical positions are crucial in supporting advanced LBS

Spatial Role

- A spatial role describes a spatially bounded function for a user, or set of users.
- A role has a *role name* and a *role extent*.
- *ParkRanger*(*Yellowstone*)
- Each role is assigned a set of *permissions*.
- The model distinguishes between *role instances* and *role schemas*.

Spatial Roles Hierarchy

- MaxRole has assigned the union of all permissions.
- MinRole represents the minimum set of privileges available to all roles, possibly empty.
- $A(s0) \leq B(s1)$



TeleNet@Pitt

Access Control Function

- Determines whether a given permission/ service, can be granted to a user in position *p*.
- for a session role to be enabled, the user should be located within the space of the role extent
- Hence, as users are mobile, the set of enabled roles within a session changes in time.

TeleNet@Pitt

R-roles and NR-roles

Algorithm 1 *Given a session ss of user u, consider a set S of session roles in ss consisting of R-roles and NR-roles . Assign $ER = \emptyset$. Then for each role $r \in S$ do:*

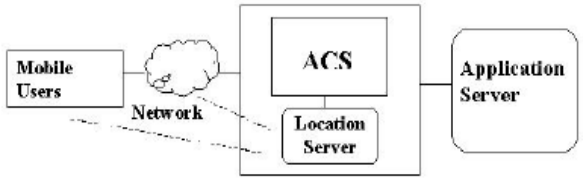
1. *Determine the real position rp of user u;*
2. *Compute the logical position lp, based on the role schema of r;*
3. *Determine whether lp is contained in the extent of r. If it is the case, then r is enabled and added to the set ER if not already present;*
4. *If the role r is not enabled but it is a* R-role, *determine whether one or more ancestor roles exist at the maximum distance specified by the* replacement *property which can be enabled. If it is the case, the roles are added to the set ER;*
5. *Add to the set ER the ancestors of its member roles.*

Extended roles in GEO-RBAC

- *dist* (distance) of the role indicating the maximum distance which is allowed for an ancestor to replace the role.
- The role schema is thus extended with the *dist* attribute which defines whether a role is a R-role or a NR-role.
  - **Definition 1 (Extended Role schema)**
- The structure of the role instance is thus extended with an attribute labeled *dist*
  - **Definition 2 (Extended Role Instance)**

General Architecture

- A set of *mobile users* equipped with mobile terminals and connected to a wireless network.
- *Application Server* providing a set of location aware information services
- *Access Control System* (ACS). It is a trusted component filtering the users' requests and protecting location privacy.



Access Control Mechanism

- *User-driven*
  - the status of roles is computed exclusively upon user request.
- *Event-driven*
  - The status of roles is autonomously checked by an agent tracking the position of the user connected to the LBS system.
- Access Control Mechanism components:
  - The *Policy DB* is a data base storing the security policies
  - The *Session DB* records the *status* of sessions.
  - An agent called *Role Tracker*.
  - *Event Manager* updates the status of sessions in *Session DB* and notifies the event to the corresponding terminal.

Privacy Preserving Access Strategy

- A user requiring a service transmits to the system, the service identifier, identity and position.
- location data are perturbed before being transmitted to the Application Server. Cloak the location by decreasing the spatial granularity of position, that is the detail of its geometric representation to obtain thus an uncertain position
- Have not addressed the issue of user anonymity. To ensure anonymity the removal of the user identity is not a sufficient condition, since the location can be linked with external data and thus reveal the identity of the user.

Conclusions & Future Work

- Integration of spatially-aware access control policies and location privacy methods for users that require location-based services
- Introduction of this concept in LBS opens the way to the development of a new category of services, they called it *role-tracking*.
- Plan to develop a distributed architecture for the access control functions and to provide support for k-anonymity.
- Plan to address issues related to frequently and rapidly moving users, that is, users that move while executing sessions with the system.

Thank You

Questions?

TeleNet@Pitt