Telcordia | the elements of success

As presented at NIKSUN WWSMC
July 25-27, 2011 | www.niksun.com

Security Issues with a Situational Awareness Service

Emerging Mobile Technologies Group
Telcordia Applied Research

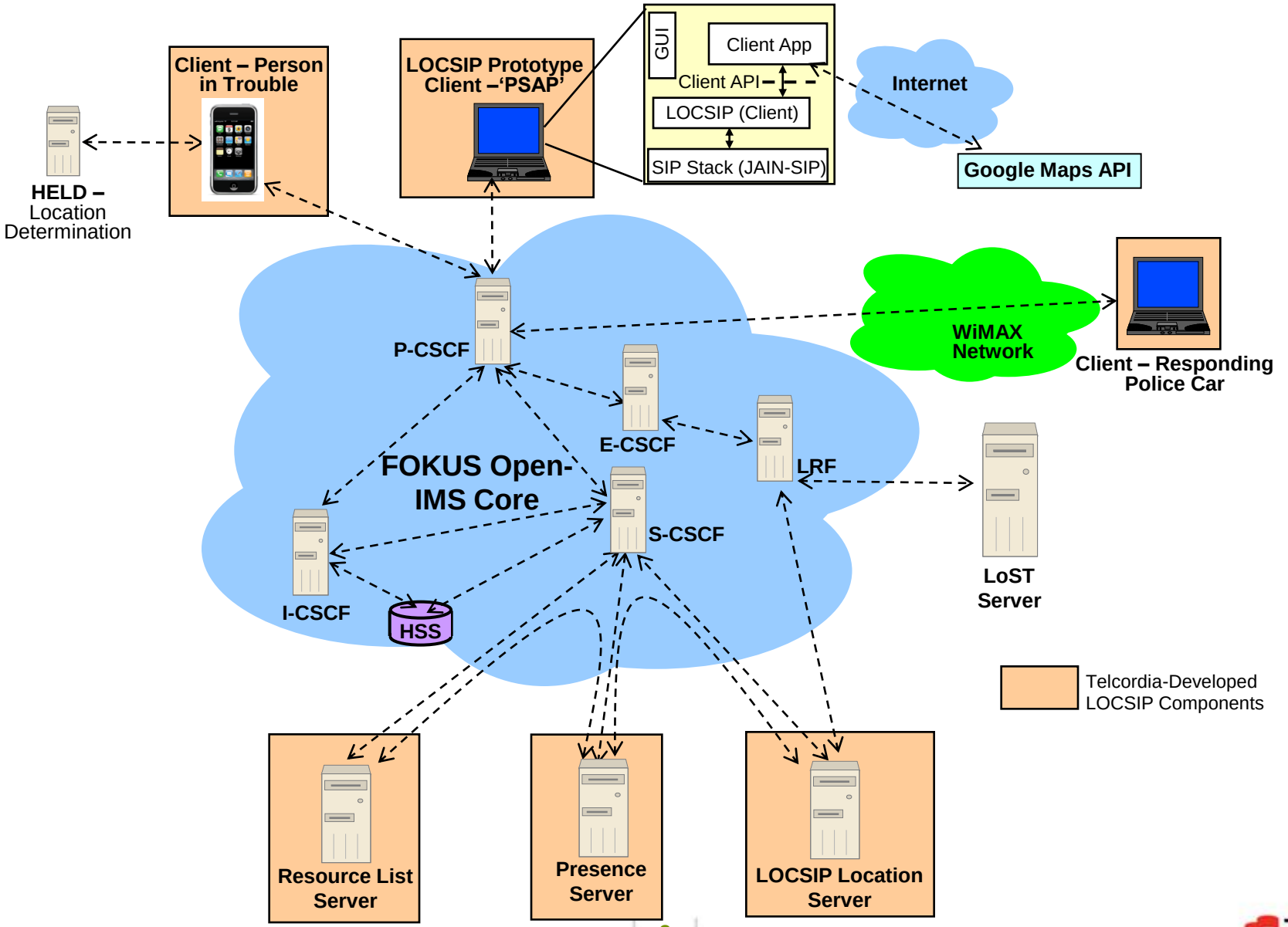
Phiroz Madon pmadon@telcordia.com 732-758-2856
Mike Loushine mloushin@telcordia.com 732-758-5358

July 26th, 2011

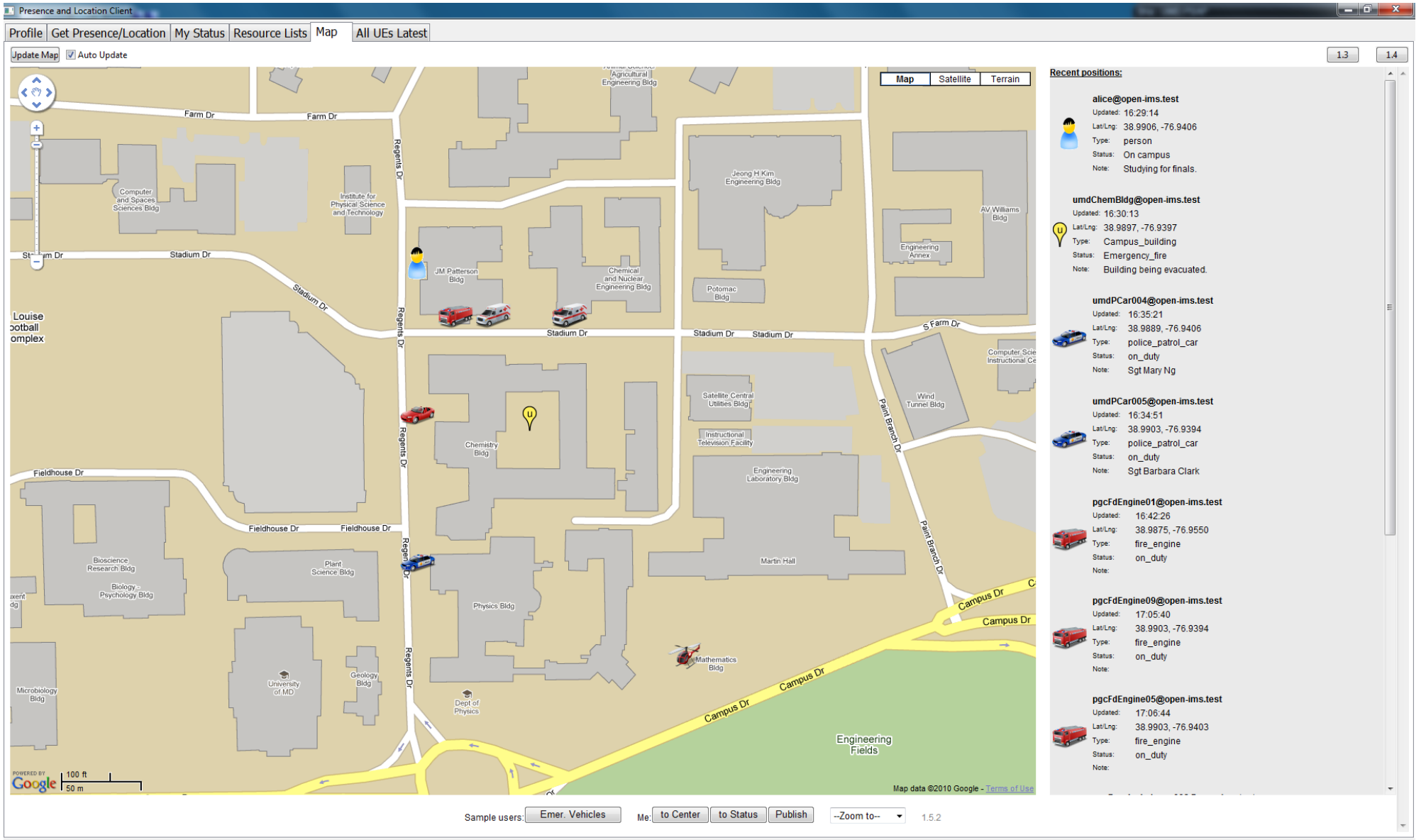
Introduction – Location-Based Services

- The spread of smart-phones with GPS capabilities creates potential for providing location-based services
- IMS-based network infrastructure would enable seamless scaling, roaming and interoperability
- Location-based services
  - Provide greatly improved situational awareness to first-responders in a disaster
    - Search for mobile resources
      - Which fire trucks are available within 15 miles of the disaster? What is their status?
      - Where is the nearest trauma helicopter? Status?
      - Is the Fire Chief stuck in traffic? Where?
  - Road, highway, stadium, traffic monitoring
  - Privacy and permissions
    - The target should have full control of who can know her location
      - My boss may only know where I am only between 9:00 am and 5:00 pm
      - I am known to a (car) traffic monitor, but my identity is anonymous
  - Performance issues
    - How frequently to publish one's location?
    - How frequently to update the location for each subscription
    - Do you overwhelm the wireless network / IMS Core / App servers with messsages?

E-911 / Location-Based Services / IMS Prototype



Emergency Services Workshop – Response Scenario



Telcordia.

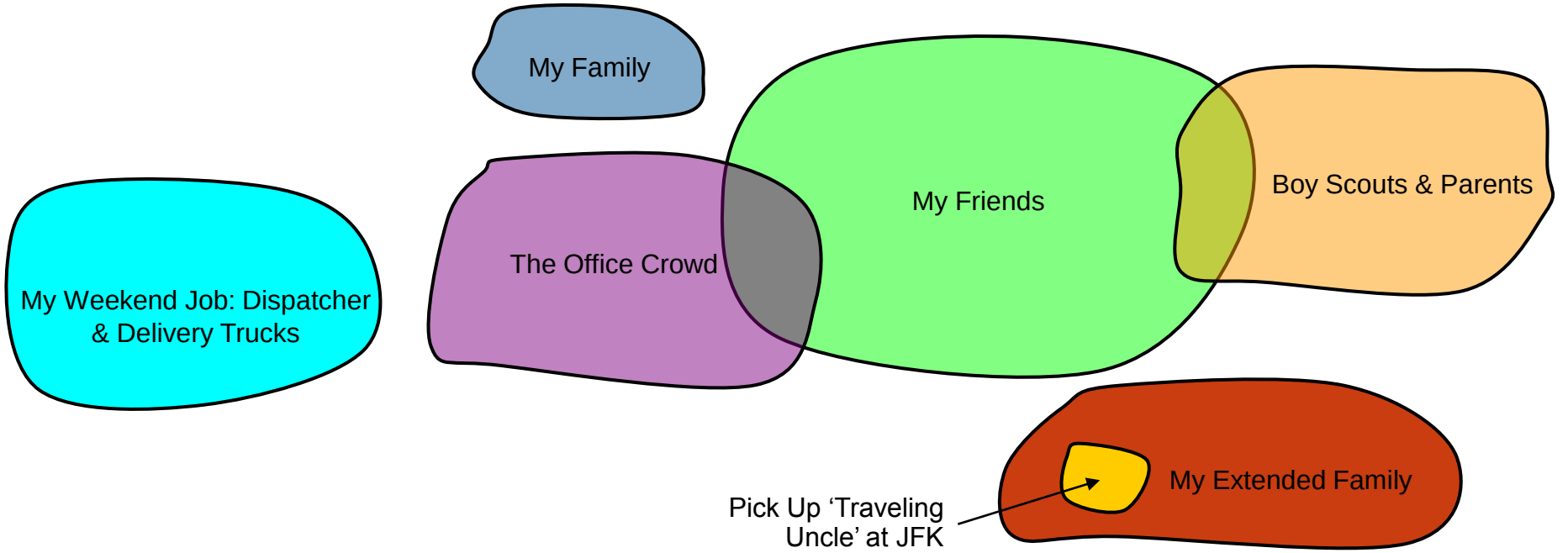
The Situation Handle

- Problem:
  - A hazmat specialist from another county needs to be “brought in” to the developing E-911 situation. How does the dispatcher do this?
- Solution 1 – Write an application for E-911. All first-responders are in the application
  - Cons:
    - Special application
    - Large list of first responders needs to be handled in an application-specific way
    - E-911 app instance for NYPD knows nothing about E-911 app instance for Prince George County Police
- Solution 2 – Have a generic web-based SA capability.To bring in a new person dispatcher provides this person with permission to view each entity in the situation.
  - Cons:
    - Hazmat specialist from another county is racing towards the fire in his car. Dispatcher keys in permission for this person to view each entity in the situation
    - Too long, too tedious
      - The ‘situation’ could move far more quickly!
- Solution 3 – Have a dynamically-formable construct called a “situation”.
  - The situation has a handle.
  - To “invite” the hazmat specialist into the situation, the dispatcher securely communicates the situation handle.
  - The situation becomes instantly visible to the hazmat specialist
  - The hazmat specialist becomes visible to the situation.

A Generic, Web-Based Situational Awareness (SA) Service

- Current Trends
  - Situational Awareness is critical to the military on the battlefield
  - The deployment of smartphones makes SA possible for everybody
- Google Latitude lets you see your friends' locations
  - But Google Latitude is 'flat'
    - There is only one situation – you and your friends
- Facebook is not just flat – it is deadly
  - Who is listening is a mystery to the user
  - Service may wither because of this security concern – not authentically about friends
- The typical SA application is in the form of a dedicated system
  - The military has single-situation SA applications, such as Boeing's 'Datamaster Lite' and Harris's C2CE-CNR.
  - The mother of all SA applications – air traffic control
- But the internet could potentially provide a web-based SA service to numerous enterprises simultaneously
  - Each user could belong to multiple 'situations' simultaneously
  - A user could switch from situation to situation, instantly invoking a rich communications context, enhanced by location
  - Security structures could prevent 'bleeding' of data between situations. Also, protect privacy

A Generic, Web-Based Situational Awareness (SA) Service



- A web-based SA service to numerous enterprises simultaneously
  - Each user could belong to multiple 'situations' simultaneously
  - A user could switch from situation to situation, instantly invoking a rich communications context, enhanced by location
  - Security structures could prevent 'bleeding' of data between situations.
    - Also, protect individual privacy
  - 'Office Crowd' really shouldn't find out about 'My Weekend Job'
  - 'Traveling Uncle' is a short-term situation.

Situation Examples

- The family
  - This is a 24-hour situation
  - Helpful to know where the members are
  - Talk or text to one individually
  - Conference as a family
- The week-end trek
  - Lasts for the duration of the trek
  - Members can't find the trail-head, get lost in the woods – location, talk, conference
- Scout troop
  - Famous for giving fuzzy directions to trail-head
- The trucking company
  - Know where each truck is, who is caught in a traffic jam,
  - ...which drivers are available,
  - ...where, and how they can get to somewhere else
- The office group
  - Group can see me from 9 to 5 only.
  - ...Should NEVER find out about my trucking night job
- Corporate sales-force, scattered across the world
- Freight company
  - Ships, packages, containers
- The election campaign
  - There may be multiple levels of situation here
  - The volunteers, the organizers, the insiders
  - Timed visibility to multiple situations may also be useful
- School re-union in a strange city
- The Traveling Uncle – being picked up at the airport
  - Situation consists of as little as two people
  - Lasts an hour – then is deleted

SA Service – Service Definition

- The service allows casual internet users to spontaneously create ‘situations’ in which they collaborate
- A person with a smartphone may be invited into a ‘situation’
- ...Can view and find on a map other participants in the situation
- ...Can belong simultaneously to multiple situations
  - Can switch on her device from situation to situation
- ...Can participate on the situation’s voice or text conference
- ...Can control her visibility within the situation
- ...May contain a minimum of two participants
  - No upper limit – may expand to tens of thousands
- At all times:
  - The User is clearly aware of the membership of the situation which may be monitoring her
  - The User can control her visibility to the situation:
    - None
    - Anonymized
    - Fully visible
  - The User can set her visibility to change on a schedule

SA Service – Service Definition – 2

- A User Equipment (UE) is a device capable of:
  - Participating in the service
  - Publishing its location
  - Optionally, engaging in voice conversation
  - Optionally, engaging in text interactions
  - Optionally, able to send attachments (video, pictures)
- A UE has a unique published identity
- A Person is vaguely understood to be associated with one or more UEs
- It is also possible for an animal or inanimate object, e.g. a package to be associated with a UE
- A 'situation' is a context in which two or more UEs can collaborate, over the internet
- A UE can create a new situation
  - The situation must have a name
  - The UE becomes a 'super-UE' of the situation
- There may be multiple super-UEs and/or UEs in a given situation
- A UE may be invited into a situation by a super-UE already in the situation
  - There is no other way for a UE to be included in a situation.
  - The UE → situation operation requires two conditions:
    - Consent by the UE
    - Consent by the situation (represented by a super-UE)
  - A UE may 'call' a situation, requesting entry. Likewise, a situation may call a UE, requesting inclusion of the UE.
  - A 'call' by one of these two parties => consent for the operation

SA Service – Service Definition – 3

- Modes of communication:
  - Iconic communication – A UE on the map is centered and 'glows' with a standard message
    - E.g 'Join voice conference', 'Check bulletin board', 'I'm calling you (voice)', 'You got a text message', etc.
  - Text communication
    - Bulletin board – whole situation
    - Private message
  - Voice communication
    - Situation-wide conference call
      - Always ongoing – you join or leave
      - One call / situation
    - Point-to-point private call
  - Video
    - Situation-wide video conference
  - Sharing files / attachments
    - Data, pictures, voice, video

SA Service – Security Aspects

- Entry into a situation is by invitation (by a super-UE) only
- Super-UE has administration and security privileges – UE does not
- The creator of a new situation is automatically its super-UE
- A super-UE can confer super-UE status on another UE
- A super-UE may kick somebody off a situation
- Conversely, you can leave a situation
  - Cannot be forced to belong (see Golden Rule)
- A user has the ability to change her visibility to a given situation, now, or on a schedule
- Periodically, the service force-reminds each UE about who is watching
- Golden Rule (wish):
  - No one can ever see me without my explicit consent

SA Service – Security Problems

- The user has to trust at least one Location Server
  - Or can location be shared, like music-copying – without a server?
- If the service spans multiple operators, can the user limit trust to just one operator?
  - Is there an architecture, whereby user location / data can be shared with one operator only – and not shared with “roaming” operators?
- Is the UE / super-UE concept good enough?
  - Was it good enough in UNIX?
- What are possible security disasters, when you have numerous instances of SA service supported by the same net infrastructure?
- Security requirements
  - A lot of work has been done to support a few well-known security requirements
    - Allow only authorized access to an application or network (authorization)
    - Prevent Mary from evesdropping on a private conversation between Bob and Alice (encryption)
    - Prevent virus’s, worms or malicious software from harming the network
  - But SA and location-based services may impose new security requirements
    - Allow only authorized access to a non-permanent, dynamically-created entity (the situation)
    - Force others to respect my location visibility requests
    - Encrypt location and location-changes when sent across a third-party network
- Is the Golden Rule destined to be broken?

Questions / Comments ??