p7q15
AH

Q2 Additional Topics 2003 (relates to lectures 9-11 by F Stajano)

(a) Discuss the location privacy problem for the Active Badge system:

(i) Define location privacy.

(ii) Define a sensible security policy for the system with respect to location privacy.

(iii) What elements of the system does a user need to trust?

(iv) What if one does not want to be tracked? [6]

(b) In the Active Badge system, the badge emits its identifier and the building infrastructure picks it up. To protect location privacy, some have suggested to reverse this architecture: the room would transmit its identifier and the badge would pick it up. Discuss advantages and disadvantages of this arrangement. [2]

(c) You are required to design the security architecture for a location-based system. You are the cellular phone operator, so you know the location of users; application providers selling their location-based services to users must go through you. Of course you know the position of all active phones at all times, but you want to reassure your users that application providers can't track them. State your security policy and describe your implementation that enforces it. [6]

(d) Describe at least two attacks against the system you designed in the previous question. [6]

(a)

(i) Location privacy is the ability to prevent others from learning one's present or past location.

(ii) Reciprocity. All sightings available to all badge users and nobody else, except that each user can divulge her own sightings to anyone. When A sets a watch on B, B is notified. Instantaneous only: sightings are not stored.

(iii) All the infrastructure (sensors, middleware, applications) must be trusted since it could log or divulge location data. Since all users receive all sightings, any malicious insider could also log or divulge; so each user also needs to trust all other users.

(iv) One may avoid being tracked by not using the device, but this implies giving up any benefits it provides. An advantage of the badge for users not wanting to be tracked is plausible deniability: if the badge is left face up in an office, the system can't distinguish it from that of someone who just is in that office.

(b)

Advantage: nobody knows your location information unless you tell them.

Disadvantage: not as useful as it sounds, since to get services from applications you must still divulge your location information to them. Some applications (e.g. xab) only work if you feed them a continuous stream of location updates, at which point it does not matter if the architecture is straight or reversed.

(c)

Policy: Users are anonymized. Applications receive their location but not their identity. Applications can't infer user identity from the data they receive. Even if they collude.

Implementation: Each phone is mapped to a unique pseudonym. Applications only see pseudonyms, never phone numbers or user identities. At regular intervals, every phone gets a new pseudonym. Middleware (controlled by cellular operator) feeds location updates (timestamp + location + pseudonym) to applications and routes application replies to the correct phones.

(d)

Applications may try to link old and new pseudonyms by modelling likely user movement: intuitively, someone on the Cambridge-London train will still be on the Cambridge-London train after a change of pseudonyms, and this may be visible from the location information. Operationally, the attacker will calculate the probabilities of the various mappings between old and new pseudonyms, given the observed facts.

Stateful applications may try to identify users based on their state. This state can't be stored at the application, or the attack would be trivial (the new pseudonym accesses the state for the old, so it reveals the mapping). So the state must be retransmitted by each new pseudonym. Then the application will look for old and new pseudonyms that have the same state.