Towards Privacy in the RFID Ecosystem

Travis Kriplean, Vibhor Rastogi, Evan Welbourne and the RFID Ecosystem Team

RFID Privacy Threats

Malicious Attackers

- Outsider gains access to data
- Insider compromises RFID hardware

"Curious" Users

- Peer or superior obtains private data
- Peers collude to learn even more

Institutional Surveillance

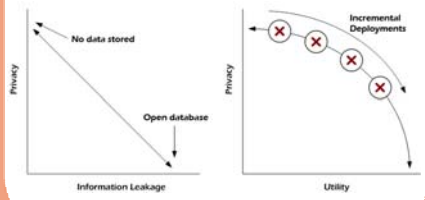
- System owner tracks users
- Unauthorized or unclear policies:
  - Onward transfer
  - Retention

Research Questions

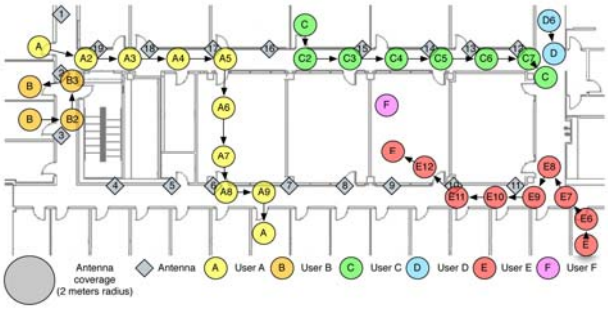
- How can privacy be built-in?
- Can we leverage data privacy techniques?
- How can attacks be detected, prevented, and deterred?
- How to provide privacy when data is probabilistic?
- How can users understand, control, and manage privacy?

Privacy vs. Utility

- Balance is crucial
- Utility to support applications
- Principled info disclosure:
  - What, when, where, how, and to whom to disclose?



Default Policy: Physical Access Control



Six people moving over the course of 15 time steps. Each user's location is annotated with the timestamp at which they move to the space. No timestamp indicates that they remain in that space.

Colocation	Start	End	Detected
A, C	2	5	X
D, C	7	15	X
D, E	7	9	-
C, E	7	9	-
A, E	9	9	X
F, E	12	15	-

PAC in a nutshell:

- Each user carries an ID tag
- Users access only RFID events they *could have seen in person*

- Combine virtues of network-based and wearable computing models
- Implement with authorization views:
  - Fine-grained access control
  - Defined by rules which may depend on context stored in helper tables
  - May leverage database techniques for handling probabilistic data
  - Extensions can be implemented with additional views

Extensions to PAC

- Add a set of administrator-defined system-wide database queries
- Explicit, user-defined permissions to grant access to captured data
- Define rules based on detected context events (i.e. "coffee-break")
- Incorporate data privacy techniques
- Can an economic model for "pricing" queries based on privacy be created?
- Access control rules which model social norms

User Studies

- Study users' perception of PAC
- Study user-level privacy controls
- How to present perturbed data to applications and users?