Towards Privacy in the RFID Ecosystem

Evan Welbourne, Travis Kriplean

**rfid privacy threats**

**System Security**
- Outside attacker gains access to DB
- Inside attacker with RFID hardware

**Malicious Peers**
- Other users query to track me
- My data could be mined
- Peers collude to learn even more

**Institutional Surveillance**
- System owner tracks users
- Other institutions can gain access
- User is unaware of what is being stored and for how long

**research questions**

- How much can be inferred from the data?
- Can we achieve provable privacy?
- How to balance privacy and utility?
- What are the users’ privacy concerns?

**privacy vs. utility**

- No data collected
- Open database
- Privacy vs. Utility
- System Security
- Malicious Peers
- Institutional Surveillance

**data perturbation**

- Perturb returned data (sanitization interface)
- Add noise to database
- Sub-linear queries for a provable privacy guarantee?

**data anonymization**

- Use k-anonymization in spatio-temporal responses
  - “There are 10 people in the ubicomp lab”
  - “Evan is in the building” vs. “in his office”
  - “Evan was here today” vs. “here right now”

**access control**

- Explicit access controls on data sharing between users
- Fine-grained access control (tuple level) for authorization views

**initial model: ecosystem provides perfect memory**

- Each user carries a “person ID” tag
- Ecosystem acts as personal recorder
- Records RFID events the user could have seen in person
- Each user is presented only with this view of the DB
- Fine-grained access control provides this DB view

**future work**

- Add a set of administrator-defined system-wide database queries
- Study explicit user privacy controls
- Investigate provable database privacy techniques
- Can an economic model for “pricing” queries based on privacy be created?
- Study privacy models in-situ with real applications and users