Privacy Issues and Techniques for Monitoring Applications

Vibhor Rastogi
RFID Security Group
Privacy in Monitoring Applications

- Monitoring apps collect personal information
  - Support useful application
  - Results in privacy issues

- RFID Ecosystem: RFID monitoring system
  - Monitors location information about users & their objects
  - Information is stored in a trusted central server
  - Users query the central server
RFID Ecosystem

Bob & Alice are friends
Charlie & Alice have a scheduled meeting
Suppose a user asks a query
- Is the answer public or private?
- It depends on multiple factors [Belloti et. al.]
- Context information of the *Querier* and the *Subject*

Rule-based access control
- Rules control the release of personal information
- Need to incorporate all the above factors
Access Control: Challenges

- Rules need to incorporate context information
  - Many rules need to be defined
  - Rules difficult to understand and manage
- Context information might have to be inferred
- Context information may be uncertain
Managability of Rules

- Our Solution
  - We identify a list of interesting scenarios and applications
  - Rules are defined to support the scenarios
  - A constrained space of predefined rules
  - Users have an option to enable/disable them

- Example: Ownership scenario & Ownership rule
The ownership scenario

Bob: Where is my book
System: Alice carries book

If B carries A’s object then release B carries object to A
Context is crucial

- Thus, the right context needs to be inferred
- Done using PEEX
Context is uncertain

- Access control Rules
  - If context then release secret to user

- Context is uncertain
  - For example: 20% chance that 'Alice Carries Book'
  - Let Pr(context) = $p_c$ & Pr(secret) = $p_s$

- Access control semantics
  - If $p_c = 1$ reveal $p_s$
  - If $p_c = 0$ hide $p_s$
  - If $(0 < p_c < 1)$ then what?
Our approach: Perturbation method

- Reveal partial information in uncertain context
- Perturb $p'_s = p_s + \text{noise}(p_c)$
- Compromise soundness
  - Answers returned may be wrong
  - Justifiable as system is itself uncertain!
  - Degree of confidence in answer also returned
Noise function

-0.5 <= noise(pc) <= 0.5

\[
Pr[\hat{n}(p_c) = x] = \begin{cases} 
  k, & 0 \leq |x| \leq r \\
  \frac{1}{k}, & r < |x| \leq \frac{1}{2}
\end{cases}
\]
Conclusion

- Designing simple & intuitive rules important
- We design ACP for the RFID Ecosystem
  - Infer high level context
  - Inferred context uncertain
- Implementation of ACP
  - Use perturbation methods for uncertain context