Highly automated smart rooms provide services to improve productivity, energy-efficiency, and health in a variety of situations.

Smart room data can disclose personal information such as preferences, habits, presence, a history of locations & activities, medical information, and relationships.

Privacy Problems

Smart room systems can yield many potential benefits
But they also pose a great threat to privacy
No good smart room privacy solution has been found yet
Needs more research & more suitable privacy definition

Privacy Goals and Definitions

- Many different definitions of privacy exist
- No comprehensive and universal definition available
- Each for different (implied) privacy goals and scenarios
- Try to minimize or consolidate assumed trust
- Trade-off between strong privacy guarantees and utility

Differential Privacy

- Adherence to access control policy satisfies this definition of privacy
- Dangers from unintended leaks and flaws in policy
- Trojan application uses data for alternate purposes
- Grants access to a less trustworthy party to enable a desired service

\[ \Pr[|\kappa(D_1) - \kappa(D_2)| \leq \varepsilon] \leq e^{\varepsilon} \] for all data sets \( D_1 \) and \( D_2 \) differing on at most one element, and \( S \subseteq \text{Range}(\kappa) \).
- Composes well (with auxiliary information)
- Masks the effect of individuals by adding Laplace noise to query results
- Prevents personalization, limits smart room applications
- Fixed privacy budget limits queries & useful life of system
- Solution: separate privacy budget for each time period
- Interactions between participants make DP for participants difficult
- Like DP problem for (social) networking graphs
- DP for each data set entry is possible, but not the same

Due to interactions, one participant may dramatically affect the result of smart room data queries (such as for the number of contacts at a networking event).

Summary and Conclusions

- Access Control
- \( k \)-Anonymity