SDSI: Privacy and Security

Dan Boneh
Privacy

How sensor data is processed today:

aggregator sees all data in the clear

data mining results

Philips Hue
Privacy: the SDSI vision

Results are obtained by a private distributed computation:
Example 1: road repair

Car app: when car activates ABS system it records location and time

NHTSA: find road segments where > 100 cars activated their ABS system last week

• Computation should NOT reveal WHO
Example 2: prediction models

Fridge: sends encrypted contents to the cloud

Model deduction on encrypted data:
- Fridges who have items A, B, C also have item D

⇒ Fridge can alert owner when it is out of item D

Privacy: cloud does not learn who has what in their fridge
Abstract Problem

Private distributed computation among millions of data sources