Protecting Privacy in Sensor-Enriched Internet Services

Presenter:
Yan Ke, CMU

In collaboration with:
Phillip B. Gibbons, Brad Karp, Rahul Sukthankar, Intel
Srinivasan Seshan, Suman Nath, CMU

March 28, 2003  CMU Aladdin Data Privacy Workshop

Parking Space Finder Service

Irisnet: The Big Picture

User
Sensing Agent
Sensing Agent
Irisnet: The Big Picture

Privacy Goal:
To prevent someone from using Irisnet to automatically collect private information.

Organizing Agents (OA)
- Distributed XML Database
- Distributed Query Processing (XPath)
- Caching to improve performance
- Redundancy to reduce failures

Example Webcam Services
- Parking Space Finder
  - Find me the cheapest available parking spot within 2 blocks of CMU
- Waiting time monitors
  - Which restaurants have the shortest long lines?
- Historical camera views
  - I left my umbrella somewhere today. Show all views of me from today.
- Silent witness
  - Who hit my parked car?
- Triggered event monitor
  - Notify me when the 61C bus is coming down the street

Intelligent Sensing Agents (SA)
- PC-class machines, running Linux
- Filter sensor data to protect privacy
- Shared by different services.
- Execute senselets (code) uploaded by OAs
- Collect data from attached sensor(s)
- Send gathered data back to OAs
Current SA Implementation

- Privacy Filters
  - Hide Face
  - Low resolution
  - Edges only
  - Color histogram
- Sensor Buffer
- Senselets
- OA’s

Can be dynamically loaded and updated

Flow Control

- Rate matching of privacy filter to fastest senselet.
- Coalesce requests from senselets, preferring already used frames.

System Issues – Example Problem

- CPU is fully loaded.
- Filter produces frames faster than any of the senselets can consume them.
- Default Linux process scheduler produces suboptimal scheduling of filter and senselets.

Demo
Future Work

• Privacy checks at other places of infrastructure

- Authentication
- Access Control
- Low data rate output
- Check conformance to XML Schema
- Multiple filter types
- Senselets with different levels of privacy certification

Ability to recover hidden information for post mortem analysis.

Conclusions

• Protecting privacy without degrading performance and utility in real sensor deployments is a challenging problem.

• We built initial privacy protection mechanisms into Irisnet.

• Ability to download arbitrary privacy filters, leveraging the latest image processing algorithms.

• Open to suggestions to other potential problems and solutions…