Physical Access Control

Information Disclosure in a Community-Oriented RFID Deployment

Travis Kriplean
Computer Science & Engineering
University of Washington
The RFID Ecosystem

- RFID allows tracking of tagged objects
- Tags and readers/antennas
- Readers communicate with a central database
The RFID Ecosystem

- RFID allows tracking of tagged objects
- tags and readers/antennas
- readers communicate with a central database

RFID tags

RFID antenna

Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu
The RFID Ecosystem

- RFID allows tracking of tagged objects
  - tags and readers/antennas
  - readers communicate with a central database

RFID tags

RFID antenna

Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu
The RFID Ecosystem

- a building-wide RFID infrastructure
  - 300 RFID reader antennas
  - people carry personal tags
  - hundreds of tagged objects
- long-term research test bed

Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu
The RFID Ecosystem

• create information-rich environments that empower people

• allows applications such as an object or friend finder, personal reminders, and event notification

• complex social space

• useful applications require information to be disseminated

• information is actionable will likely impact social dynamics

Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu
A pervasive dilemma...privacy vs. utility
A pervasive dilemma...privacy vs. utility

divulge no information
perfect privacy, no utility
A pervasive dilemma...privacy vs. utility

divulge no information
perfect privacy, no utility

all phenomena recorded, indexed, and shared
no privacy, full utility
A pervasive dilemma...privacy vs. utility

divulge no information
perfect privacy, no utility

all phenomena recorded, indexed, and shared
no privacy, full utility
A pervasive dilemma...privacy vs. utility

- Divulge no information
  - Perfect privacy, no utility

All phenomena recorded, indexed, and shared

- No privacy, full utility

How can privacy assurances be architected into the system while still providing useful applications?
Prison building at Presidio Modelo, Isla De la Juventud, Cuba

image from Wikipedia
“The state of conscious and **permanent visibility** [assures] the automatic functioning of power...”

Michel Foucault, *Discipline and Punish*

Prison building at Presidio Modelo, Isla De la Juventud, Cuba

image from Wikipedia
Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu
What information should be disclosed to whom as a default?
Surely there’s a safer, yet useful default...
Physical Access Control (PAC)

- every user has access to a **personal store of data**
  - stores events that occurred when and where they were **physically present**
  - augments users’ memory of places, objects, and people **encountered**
- provides **symmetric visibility**
- **principle**: start from human sensory capacity and extend from there
Conceptual Demo

Time: 0

Building floor plan
Conceptual Demo

Time: 1

Building floor plan
Conceptual Demo

Time: 2

Building floor plan
How does PAC *not* model everyday experience?
How does PAC *not* model everyday experience?

- 360° vision

screen capture from “The Big Lebowski”
How does PAC *not* model everyday experience?

- 360° vision

- perfect observations entering a room full of people

screen capture from “The Big Lebowski”

from doe.gov
How does PAC *not* model everyday experience?

- 360° vision
- perfect observations entering a room full of people
- memory does not decay
How does PAC *not* model everyday experience?

- 360° vision
- perfect observations entering a room full of people
- memory does not decay
- loss of *plausible* deniability
Applications of data collected through PAC

- Personal Diary applications
- Object Finder
- Personal History Analyzer
Applications of data collected through PAC

- Personal Diary applications
- Object Finder
- Personal History Analyzer

PAC is a default. We can make situationally-appropriate extensions as necessary.
Modes of information disclosure

Malicious
Personal information is compromised by unauthorized parties
Addressed by secure systems engineering

Institutional
Organizations collect, use, and share personal and behavioral data
Addressed by contracts, federal law, corporate practice...
Modes of information disclosure

Malicious
Personal information is compromised by unauthorized parties
Addressed by secure systems engineering

Institutional
Organizations collect, use, and share personal and behavioral data
Addressed by contracts, federal law, corporate practice...

Mediated
Peers and superiors access information through some authorized interface
Mediated by access control policies
Implementation of PAC in the RFID Ecosystem
RFID Ecosystem architecture

tag read event (TRE): \{tag identifier; antenna identifier; timestamp \}
RFID Ecosystem architecture

tag read event (TRE): \{\text{tag identifier; antenna identifier; timestamp}\}
Mutual visibility

determine whether the entities described in two tag reads were mutually visible (share an unobstructed line of sight)

\{Alice A; Antenna 1; 08:02:45 \}

\{Bob B; Antenna 2; 08:02:50 \}
Mutual visibility

determine whether the entities described in two tag reads were **mutually visible** (share an unobstructed line of sight)

{Alice \(A\); Antenna \(1\); 08:02:45 }  
Mutually visible?  
{Bob \(B\); Antenna \(2\); 08:02:50 }
Mutual visibility (continued)

\{\text{Alice} \ A; \ \text{Antenna} \ 1; \ 08:02:45 \} \\
Mutually visible? \\
\{\text{Bob} \ B; \ \text{Antenna} \ 2; \ 08:02:50 \}
Mutual visibility (continued)

- need to use antenna location as tag location

Mutually visible?

{Alice \( \text{A} \); Antenna \( \text{1} \); 08:02:45 } 

Mutually visible?

{Bob \( \text{B} \); Antenna \( \text{2} \); 08:02:50 }
Mutual visibility (continued)

- need to use antenna location as tag location
- two tags read events are said to be mutually visible if they satisfy two constraints:
  1) **temporal constraint:** occur within a time window $\Delta$ of each other
  2) **spatial constraint:**
     A) are read by the same antenna or
     B) the involved antennas are considered mutually visible

Mutually visible?

{Alice A; Antenna 1; 08:02:45 }
{Bob B; Antenna 2; 08:02:50 }
Deployment challenges
Deployment challenges

- antenna placement

\{A; A1; 08:02:45 \}
\{B; A2; 08:02:45 \}
Deployment challenges

- antenna placement

- distinguishing tagged objects from tagged people

{A; A1; 08:02:45}
{B; A2; 08:02:45}
Deployment challenges

- antenna placement
- distinguishing tagged objects from tagged people
- “misplaced” user tags
Conclusion

• start from a safe principle of symmetric visibility

• define Physical Access Control

• instantiation within an RFID deployment
Collaborators:

Evan Welbourne       Magda Balazinska
Nodira Khoussainova  Gaetano Borriello
Vibhor Rastogi       Yoshi Kohno
                     Dan Suciu

Physical Access Control for Captured RFID Data

Vol. 6, No. 4
October–December 2007

IEEE Pervasive Computing
www.computer.org/pervasive