FragDB
Secure Localized Storage Based on Super-Distributed RFID-Tag Infrastructures

Marc Langheinrich
Institute for Pervasive Computing, ETH Zurich, Switzerland
Location-based Access Control
FragDB: A Location-Based Access Control System
Location-Based Access Control in the Real World
Marc’s Not In My Office
Coffe Break

Kaffepause @ Informahlhubs
März

Cafeteria
A Classroom

No ID Check Here

See What’s Marc Teaching Today
Examples of „Hands-Free“ Access Control

- Information Not „Secret“
  - But wouldn’t want it broadcasted either
- Location-Based Access
  - If you’re in the vicinity, feel free to look
- No Management – „Hands-Free“
  - No users, passwords, certificates, policies
FragDB: A Hands-Free Access Control System
Like Virtual Post-Its

Your Data

A Place

A Visitor

May 11, 2007

PALMS 2007 Workshop
Basic FragDB Principle: Fingerprinting
Principle: Fingerprinting Place & Time

You

A Visitor

UPDATE

UPDATE
Principle: Fingerprinting Place & Time

- Places Change – Fingerprints Should, Too
  - Otherwise: one visit gives continued access
  - Old fingerprints „fade away“
Fingerprint Requirements

- **Fluid Boundaries**
  - Tolerate „close enough“ positions

- **Time Variance**
  - Fingerprints change over time

- **Time Continuity**
  - Old fingerprints fade-away slowly

- **Secure Storage**
  - Access to central server yields no information
Technology Enabler: RFID (Hitachi mu-Chips)
μ-Chip 2005 (Hitachi)

- **RFID Chip**
  - Size: 0.4 x 0.4 mm
  - Carrier frequency: 2.45 GHz
  - Operating distance: 0-25 cm
  - Memory capacity: 128bit ROM
  - Operating temperature: -27 to +75ºC
  - Anti-collision: no
  - Response time: 20 ms
  - Optional external antenna
Super-Distributed RFID Tag Infrastructures

Bohn, Mattern: Super-Distributed RFID Tag Infrastructures. EUSAI 2004, Eindhoven, NL

- Passive RFID tags deployed in vast quantities and in a highly redundant fashion over large areas or surfaces
FragDB: Basic Principles
FragDB: Fragmented Database Storage

- Each Tag-ID Represents Single Storage Cell
  - Data is fragmented and stored „in“ tags
  - Central storage (encrypted with hashed ID)

- 1. Fluid Boundaries: Forward Error Correction
  - Data is redundantly stored across several cells

- 2. Time Variance: Ids Change Over Time
  - Probabilistic after $n$ readouts (currently simulated)
4. Secure Storage

- **Cell Data is Encrypted With Key == Hashed Tag ID**
  - No need for key management

- **Storage Cell Location NOT tag ID, but Hashed Key**
  - Otherwise: trivial DB-scan attack possible
  - But: simple to compute cell location from tag ID
3. Time Continuity

- Tags „remember“ their old IDs
  - Old tags gradually lose fidelity (i.e., bits)
What Can You **Do** With This?
Classroom Cam

Pass Through Here to Get Lecture Video
Example: Fingerprinting Road Infrastructures

Continually Fingerprint Road

Store Warning on Previous Segment

Store Warning for Approaching Cars
Prototype Implementation
<table>
<thead>
<tr>
<th>Name</th>
<th>Algorithm</th>
<th>Status</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID.java</td>
<td>FEC 2:1</td>
<td></td>
<td>Mon Jul 10 16:00:1...</td>
</tr>
<tr>
<td>test.mp3</td>
<td>FEC 2:1</td>
<td></td>
<td>Mon Jul 10 16:00:1...</td>
</tr>
<tr>
<td>SimpleVirtualSurface.java</td>
<td>Simple Split</td>
<td></td>
<td>Mon Jul 10 16:00:1...</td>
</tr>
<tr>
<td>IDSnapShot.java</td>
<td>Redundant Split</td>
<td></td>
<td>Mon Jul 10 16:00:1...</td>
</tr>
<tr>
<td>VirtualReaderWithRD.java</td>
<td>Redundant Split</td>
<td></td>
<td>Mon Jul 10 16:00:1...</td>
</tr>
<tr>
<td>Virtual2DSurface.java</td>
<td>Simple Split</td>
<td></td>
<td>Mon Jul 10 16:00:1...</td>
</tr>
<tr>
<td>VirtualSurface.java</td>
<td>Simple Split</td>
<td></td>
<td>Mon Jul 10 16:00:1...</td>
</tr>
<tr>
<td>VirtualReader.java</td>
<td>FEC 2:1</td>
<td></td>
<td>Mon Jul 10 16:00:1...</td>
</tr>
</tbody>
</table>

**File 4**

<table>
<thead>
<tr>
<th>ID</th>
<th>Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>8AF62</td>
<td>File942, File4</td>
</tr>
<tr>
<td>F2539</td>
<td>B35F*</td>
</tr>
<tr>
<td>B35F*</td>
<td>File4, File952</td>
</tr>
<tr>
<td>0439*</td>
<td>1231*</td>
</tr>
<tr>
<td>04DA*</td>
<td>B3EC*</td>
</tr>
<tr>
<td>43B21</td>
<td>E321*</td>
</tr>
<tr>
<td>54017</td>
<td>File944, File12</td>
</tr>
<tr>
<td>8DC12</td>
<td>File944</td>
</tr>
<tr>
<td>03BCA</td>
<td>BC3**</td>
</tr>
<tr>
<td>948AA</td>
<td>DE2**</td>
</tr>
<tr>
<td>7843A</td>
<td>E321*</td>
</tr>
<tr>
<td>43B21</td>
<td>File91, File12</td>
</tr>
<tr>
<td>File4</td>
<td>File4, File42, ...</td>
</tr>
</tbody>
</table>

**File 91**

<table>
<thead>
<tr>
<th>ID</th>
<th>Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>74A**</td>
<td>File91</td>
</tr>
<tr>
<td>9DB**</td>
<td>File91</td>
</tr>
<tr>
<td>89***</td>
<td>File44265</td>
</tr>
<tr>
<td>4E***</td>
<td>File32</td>
</tr>
<tr>
<td>File4</td>
<td>File4</td>
</tr>
<tr>
<td>File942</td>
<td>File4</td>
</tr>
<tr>
<td>File442</td>
<td>File942</td>
</tr>
<tr>
<td>File942</td>
<td>File942</td>
</tr>
<tr>
<td>File12</td>
<td>File91, File74</td>
</tr>
<tr>
<td>File44</td>
<td>File4, File74</td>
</tr>
<tr>
<td>File12</td>
<td>File14, File44</td>
</tr>
<tr>
<td>File44</td>
<td>File856</td>
</tr>
<tr>
<td>File14, File74</td>
<td>9E4**</td>
</tr>
<tr>
<td>File4856</td>
<td>4E***</td>
</tr>
</tbody>
</table>

Current ID: 8AF62, F2539
Summary
FragDB – „Hands-Free“ Access Control

- Mimics real-world location-based access control
  - Useful for many types of semi-public data, e.g., out of office notices, lecture materials, road conditions, ...
- Principle: Embedded RFID's & Fragmented Storage
  - Fluid Boundaries
  - Time Variance
  - Time Continuity
  - Secure Storage
- Built Simulator and Prototype (mu-Chips)
More in the Tech Report
find it at: people.inf.ethz.ch/langhein/

- Effects of „ID-fading“
  - time- vs. usage-based updates
- Strategies for data searches
  - How to reassemble a file
Service Announcement
Ubicomp Privacy Workshop 2007

Organized By
John Canny (UC Berkeley)
Marc Langheinrich (ETH Zurich)
Sarah Spiekermann (Humboldt University Berlin)

Technologies, Users, Policy

- Keynotes & Contributions by Leading Privacy Experts
  Lorrie Cranor, Jason Hong, John Krumm, Serge Guthwirth, Paul de Hert, ...

- Selected Papers Published in „Personal & Ubiquitous Comp.“

- Submission Deadline: June 1, 2007

www.vs.inf.ethz.ch/events/uc7privacy/