Privacy in the Smartphone Age

Di Ma

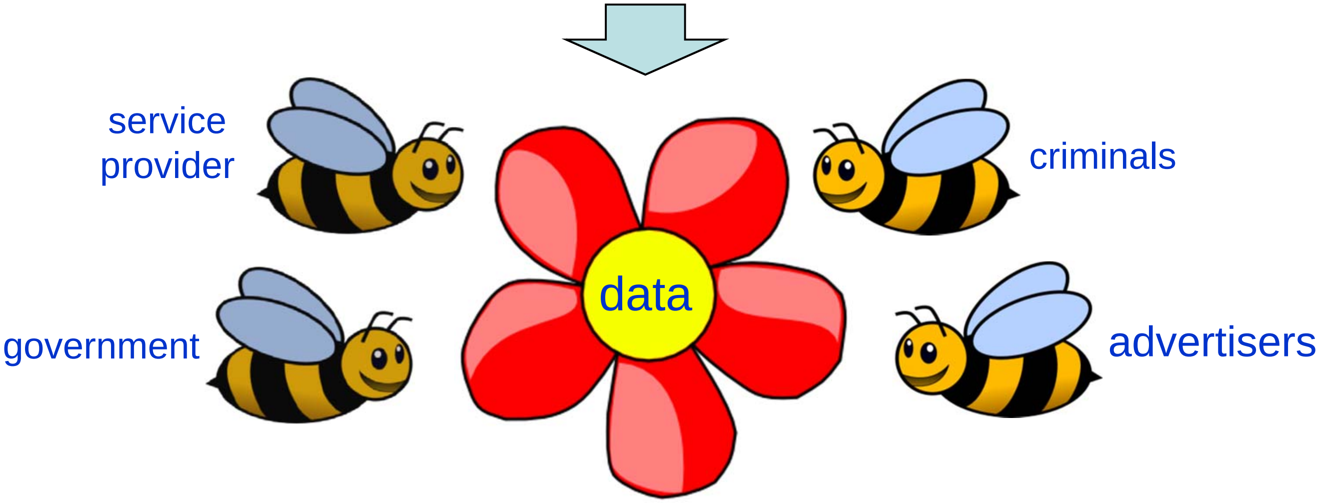
NSF US/Mid-East Workshop on Trustworthiness in Emerging Distributed Systems and Networks

June 4-6, 2012
Istanbul, Turkey

The issue

“Privacy in the smartphone age”

- **Is important because smartphones are**
  - undoubtedly becoming ubiquitous
    - 4 time faster than mobile phone market (IDC report)
  - more than just a phone or a desktop computer
  - increasingly with new functionalities
    - i.e., NFC-enabled smartphone as payment tokens (Google Wallet)
  - ...



service provider

criminals

data

government

advertisers

The issue

“Privacy in the smartphone age”

- **Will become even more important**
  - When we shift to a mobile, cloud-based computing world
    - Increased risk of private data falling prey to snooping by
      - the government, private hackers, or the cloud service provider itself
    - Still cloudy on whether server-side data is protected by law, e.g., the Fourth Amendment
  - When users are continuously supplied with unlimited amounts of free apps
    - Apps gather sensitive phone/user information
    - Apps may contain malware
      - Reputable apps can be repackaged and injected with malicious links

The current practice

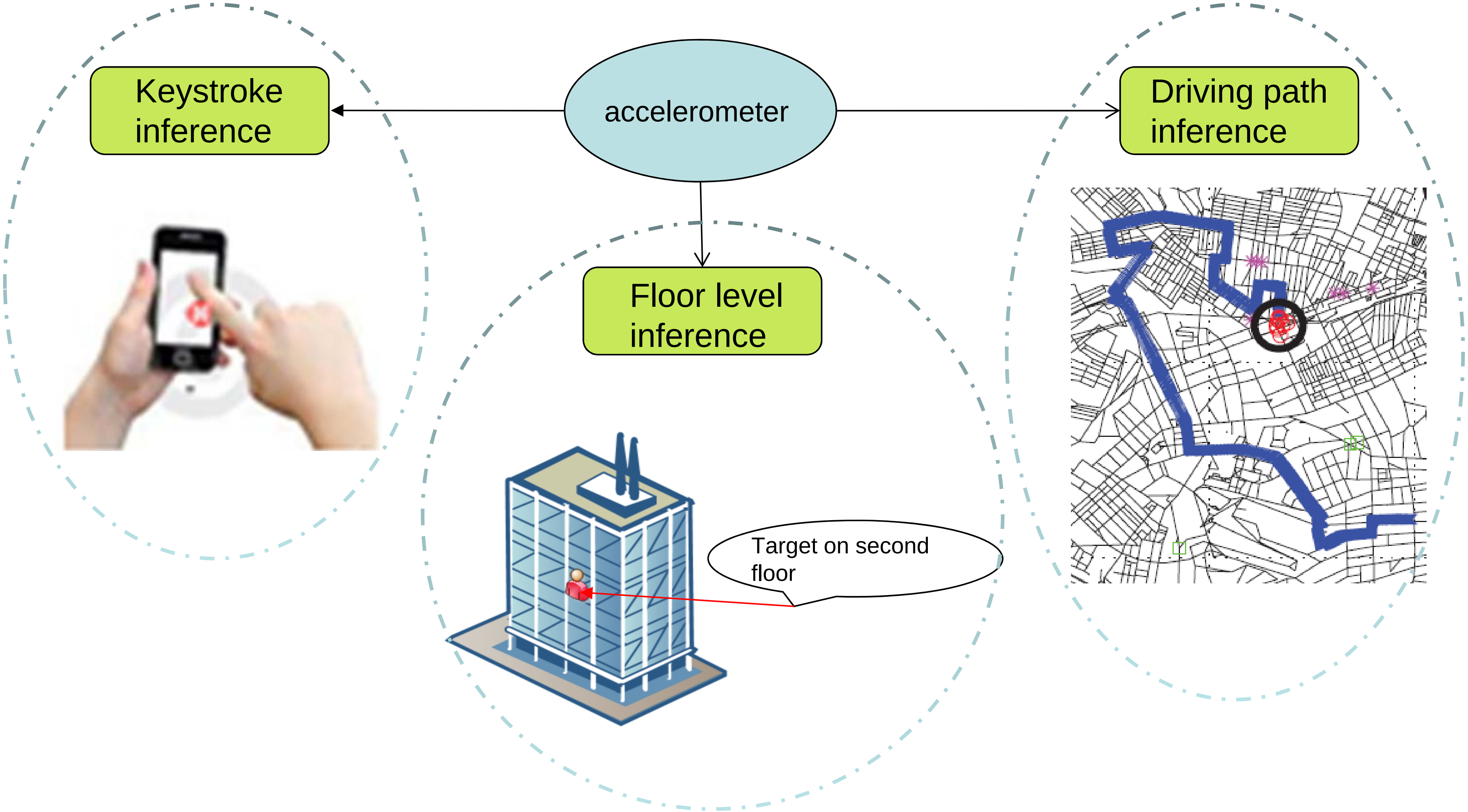
- Major manufactures employ **application permissions** to prevent sensitive data from unauthorized access
  - Sensitive: GPS, camera, microphone, SMS, ...

- However,
  - It relies upon user diligence and awareness
  - Permissions are granted **all-at-once and only at installation time**
    - Subsequent permission check is transparent to users
  - Permission check can be circumvented through permission attacks

- Even sensitive data can be protected, is it enough? how about non-sensitive data?
  - Non-sensitive: accelerometer, proximity sensor, light sensor, ...

New privacy attacks

non-sensitive data can reveal **sensitive** information!!!



accelerometer

Keystroke inference

Floor level inference

Driving path inference

Target on second floor

The challenges

- **Understand the implications of various data and their fusion on privacy**
  - Non-sensitive data can reveal sensitive information
  - Non-sensitive data, collected over **a sufficiently long time**, can reveal sensitive information
  - Multiple non-sensitive data can reveal sensitive information

- **Communicate the result to users in a comprehensible way**
  - To assist them to have **controlled release** of personal information
    - Privacy is culture-dependent, individual-dependent, time-dependent, situation-dependent ...

- **Develop automatic and adaptive defenses**
  - to satisfy the requirement for controlled release of personal information