Cloud Computing + Mobility

Research Challenges in Privacy & Security

Stefan Saroiu
Microsoft Research Redmond

Observations

- Cloud computing is here to stay
  - Huge interest from companies due to business model

- Users move more of their data to the cloud
  - Office Online, Google Docs, GMail, Facebook, etc…

- Cell-phones are becoming sensing devices

- Data gathered by cell-phone is highly sensitive
  - Could be gathered continously
  - Location and activity information

Challenge #1: Securing Data

- Who has access to the data in the cloud?
  - Complicated by the many roles present
    - System admins., H/W ops., coders/testers
  - Accidental data leaks do occur!

- Worst-case threat model: physical attacks
  - TPMs designed for secure boot
  - TPMs not designed for cloud computing threat model

- Who is notified when data is subpoena-ed?

Challenge #2: Handling Confidential Data

- Can't encrypt my GMail e-mail!

- Can cloud functionality be offered for highly confidential data?
  - Users are not willing to give up control of such data

- Possible examples of confidential data:
  - Location trace information
  - Medical records
  - Results of genetic testing

Challenge #3: Malicious Users

- Mobile devices are becoming contextual sensors:
  - Location, noise, weather, ambiance

- Malicious users can misuse their mobile sensors:
  - Collaborative sensing: data pollution
  - Cheat to gain more functionality

- Can't solve with infrastructure monitoring
  - Danger: it could be turned into a big-brother scenario

Challenge #4: Securing Computation

- What if computation in the cloud becomes insecure
  - e.g., Wrong location information

- Is audit sufficient to handle secure computation
  - Are more active solutions (e.g., BFTs) necessary?

- Should cloud providers' policies be regulated?