PlugDB : a Personal & Tamper Resistant Data Management Engine

SMIS team, Inria Paris – Rocquencourt
Objectives of the SMIS team

Ultimate goal
- A decentralized and privacy-by-design paradigm for personal data management
- Operational platforms to validate the concept
- Measure success factors with a multi-disciplinary approach and field experiments

Our research contributions
- Access and Usage control models (e.g., right to be forgiven, minimum exposure [7])
- Embedded structures & algorithms to enforce them (e.g., RDBMS/RBAC [1], search/TBAC [2,3])
- Global queries and big data analysis (e.g., anonymous datasets, SQL aggregates [4])
- Privacy-by-Design architectures (e.g., personal cloud [5], smart homes [6])
- Prototype: PlugDB (open source, open hardware)

Collaborations
- Academics: Digital Society Institute (multi-disciplinary), Citylab@Inria
- Institutional: French General Councils, Paris Health Agency
- Startups: CozyCloud, Ye$Profiles

Objective in the “Smart City & Mobility Innovations”
- A privacy preserving platform for social sensing and quantified-self appliances
Vision & research challenges

Current Web model
- **Delegation** => a privacy issue
- **Centralization** => a security issue
- **Compartmentalization** => issue of completeness

Personal Web model: give back data to users
- **Support**
  - Companies: avoid “de-intermediation”
  - Institutions: empower users (health, energy)
- **Completeness** => new usages
- **Privacy** is under control
  - Expose results, not micro-data
  - Privacy preserving global treatments
Our proposal: PlugDB

How to give back the data to users?
- On personal computers?
  - Self-administration, security
- On a cloud service?
  - May worsen the privacy problem

Our approach: PlugDB, a tamper resistant data management engine...

...which:
- stores, indexes, structures, queries, recovers data
- authenticates, evaluates access & usage control
- is self-administered and interfaces with smartphones, tablets, PC, etc.

...and provides strong privacy and security guarantees:
- secure hardware: tamper resistant, open hardware
- secure software: isolated, small footprint (potential formal proofs), open source
Competitive advantage wrt competitors

Privacy rules enforcement

• Access and Usage control models
  - Access control: RDBMS/RBAC [1], search/TBAC [2,3]
  - Usage control: right to be forgiven, minimum exposure [7]

• Anonymous global queries and big data analysis
  - Generate anonymous datasets
  - Produce global SQL aggregates without revealing individual micro-data [4]

• Privacy-by-Design architectures
  - Personal cloud [5]
  - Smart homes [6]

Patented processes (due to HW/SW combination)

• E.g., medical diagnosis (healthcare & cancer follow-up)

Community checks

• open source database software
• open hardware platform
Other application domains

Home energy cloud – Energy trail management (demo)
Healthcare – medical and social personal folder (experimented in France)
Personal Cloud – Secure home cloud (with CozyCloud)
Vendor Relationship Management (VRM) – Secure data renting (with Ye$Profile)
Educational platform for P-b-D apps – Univ. of Versailles, ENS-IIE, INSA...
Inquiries / MOOCS – Keep your interaction data under your control

References

Thank you

Nicolas Anciaux
Inria SMIS team
Nicolas.Anciaux@inria.fr
http://www-smis.inria.fr/~anciaux/