Motivation & Use Case

Despite the increasing adoption of cloud services, users remain concerned about protecting sensitive data in the cloud. Once data has been given away, there do not exist reliable means to exercise control over its further usage. It remains uncertain whether, how, and by whom released sensitive data may be accessed, stored and used.

Use Case: Insurance company
- In-house computing cluster for data analysis
- Usage of cloud services for email, web, collaboration
- Data usage control solutions on all computing devices
  - Goal: Eliminate data misuse and data leakage

Problem & Expected Contribution

How can we enforce usage control requirements if data flows between systems, services, and applications that are distributed logically, physically and organizationally?

Expected Contribution
- Conceptual and technical framework for enforcing data usage control requirements in distributed systems
- Enhanced data security and privacy in cloud environments

Cross-System Data Flow Tracking

1. How can data flow across systems be tracked and data usage policies be propagated accordingly?
   - Private client asks for health insurance offers
   - Later, the client refuses any offers
   - Regulations demand data deletion at all systems

Achieved Results [1,2,3]
- Generic model for cross-system data flow tracking
  - TCP/IP instantiation
  - Architecture, implementation and evaluation
- Cross-system data flow tracking
- Policy propagation
- Based on system call interposition

Remaining Objectives
Reduce overapproximations using protocol semantics
- Combine system call interposition with
- Qualitative analysis of network messages

Distributed Policy Decisions

2. How can usage control decisions be taken if data and policies are distributed across systems?
   - Corporate client asks for insurance offers via email
   - Agents may have worked on competitor’s data
   - No processing of request by such agents

Goal
- Methodology for distributed policy decisions
- Conceptual framework and implementation

Anticipated Solution
- Decentral: local decisions wherever possible
- Hierarchical: decision components where needed

Guarantees

4. Which guarantees for usage control enforcement can be provided under which preconditions?
   - Deliberate data release to cloud provider
   - Enforcement of usage policies at these providers
   - Technical measures providing appropriate guarantees

Adaptivity

3. How can usage control requirements be enforced if data processing systems keep changing?
   - Annual recalculation of insurance premiums
   - Temporary utilization of external processing power
   - No data misuse or leakage through these resources

Goal:
- Reliable enforcement if systems keep changing
- Fallback solutions for legacy systems

Anticipated Solution
- Transparent enforcement mechanisms
- Integration at low layer systems

References

Contact
Florian Kelbert
Technische Universität München
Garching b. München, Germany
keilbert@nics.tum.edu
http://www2.cs.tum.edu/keilbert