Distributed Enforcement of Unlinkability Policies: Looking Beyond the Chinese Wall

Apu Kapadia, Prasad Naldurg,
Roy H. Campbell

Dartmouth College (ISTS)

Microsoft Research, India

University of Illinois at Urbana-Champaign

Policy 2007

Lack of audit-log privacy

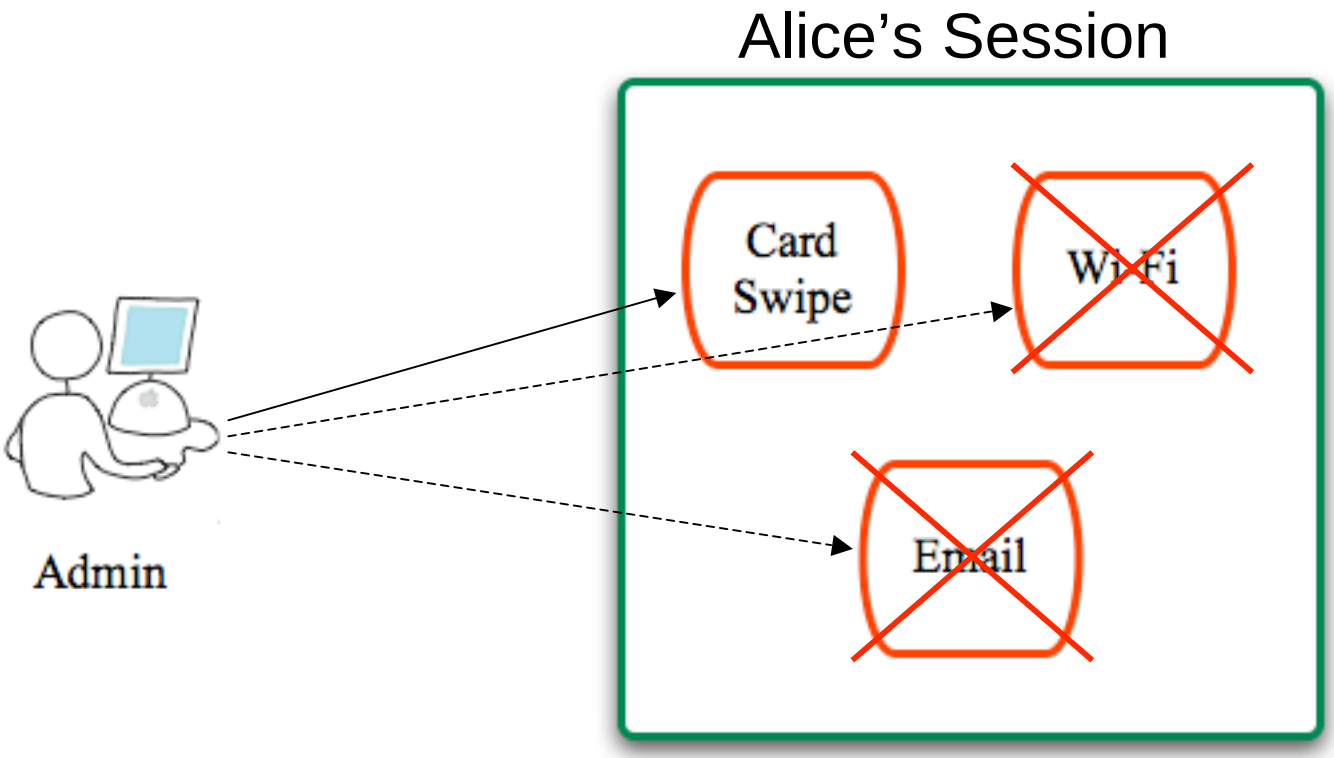
- Enterprise-level access to services
  - Doors, printers, Wi-Fi, vending, …
  - Accesses logged at several severs
- Security of audit logs
  - Access by authorized administrators
- *Privacy of audit logs*
  - Who is allowed to link records?
  - Wi-Fi logs + Email logs = exposed location

Unlinkability: “Two or more accesses cannot be tied to the same user”

- Cryptographic approaches
  - Mathematical unlinkability
  - Not always feasible (legal requirements)

- Unlinkability through access control
  - Prevent users from accessing records that can be linked

Chinese Wall is not scalable

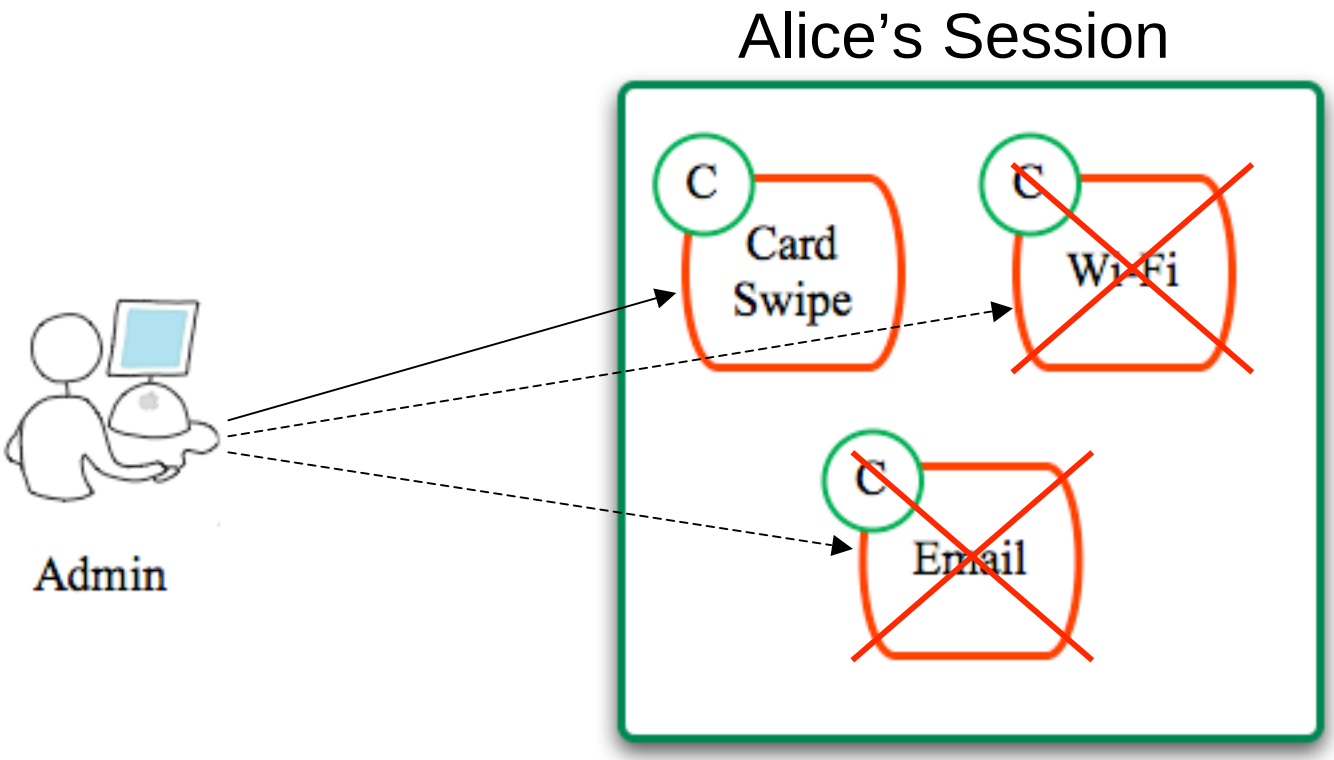


Need to maintain access history

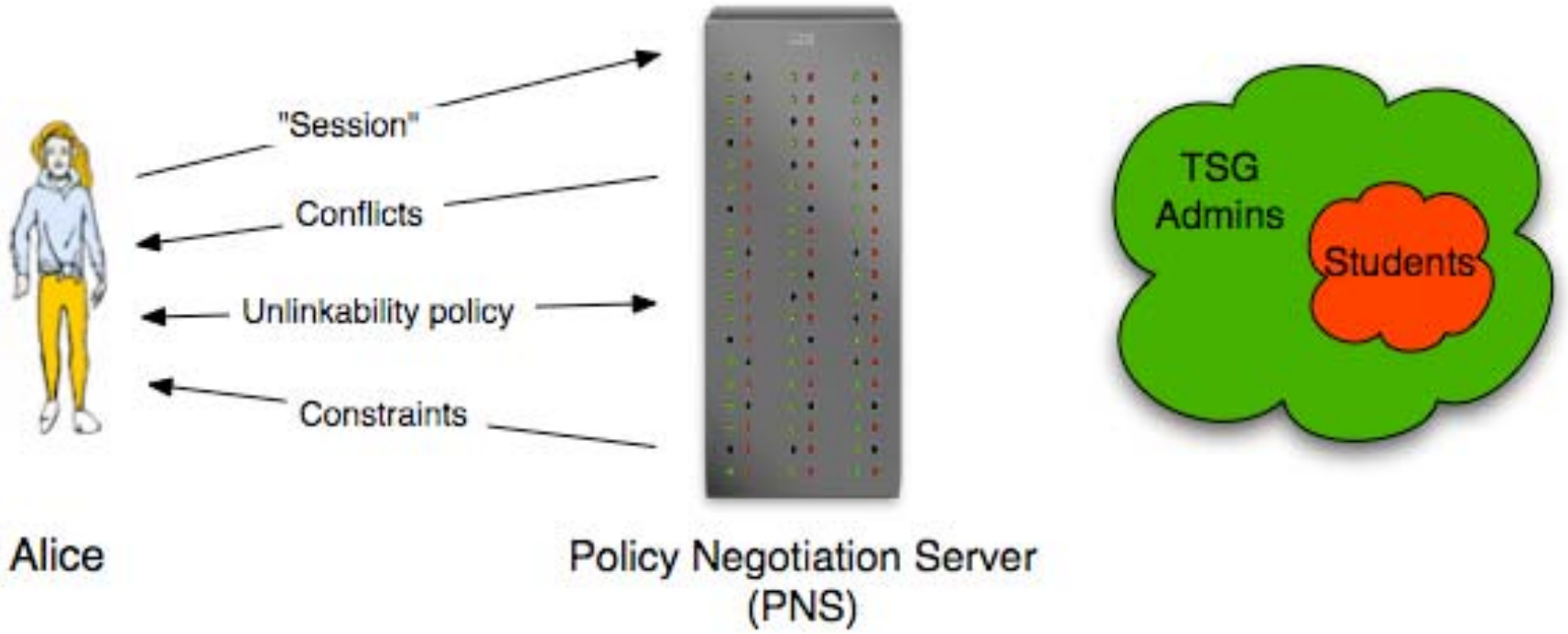
Modified semantics for decentralized enforcement

- Unlinkability semantics
  - Prevent access to two or more audit flows
  - *But* don't guarantee access to audit flows of administrator's choosing

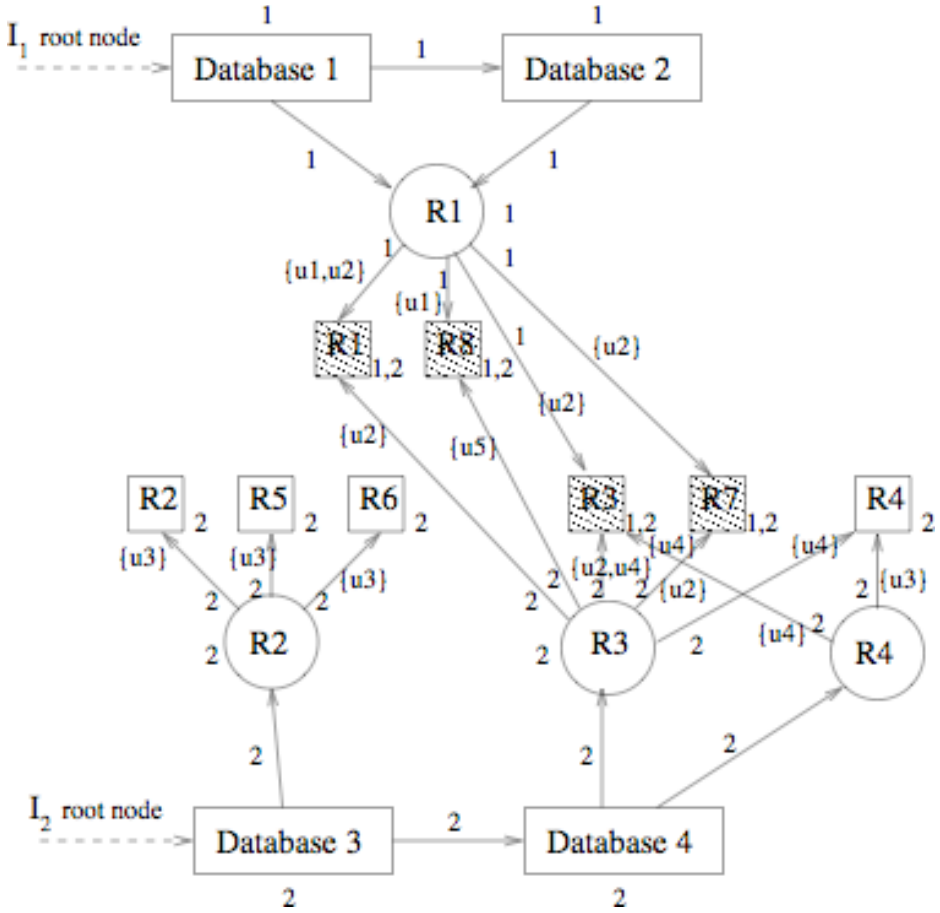
Attached constraints are easy to enforce locally



Users negotiate unlinkability policies with the PNS



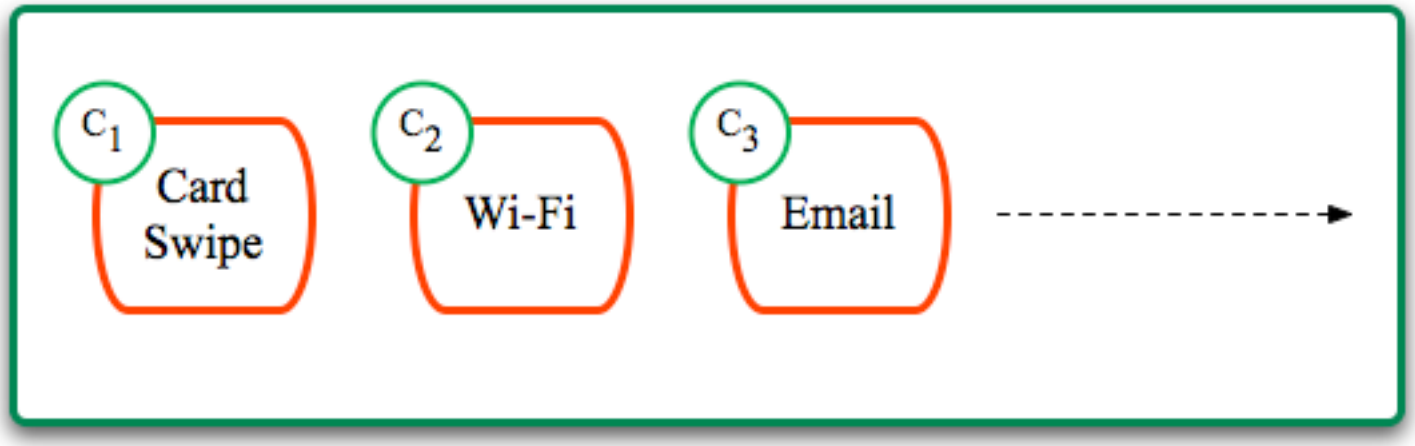
Computing linkability threats



Correctness of policy constraints

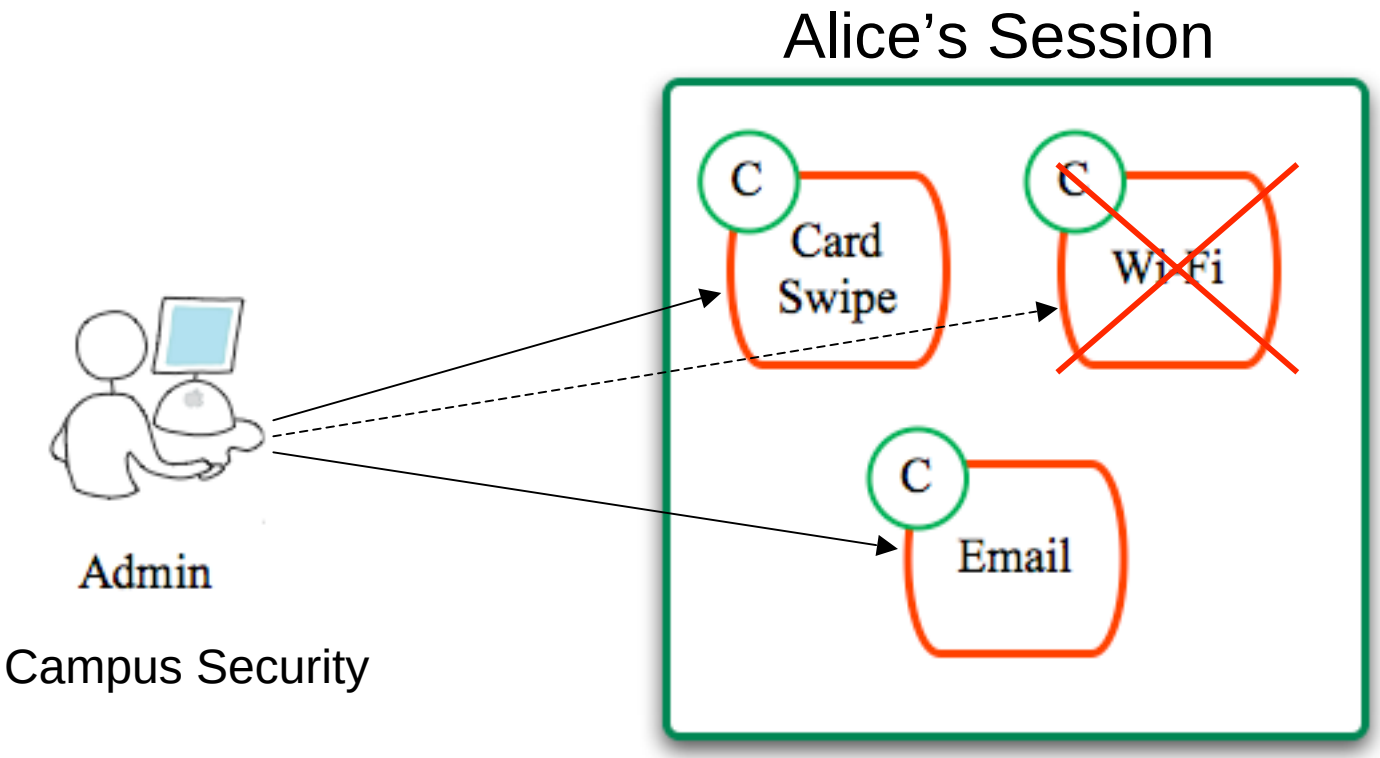
- Secure
  - Prevents linking of records
- Precise
  - Users who cannot link records are allowed access

Open-ended sessions are permitted

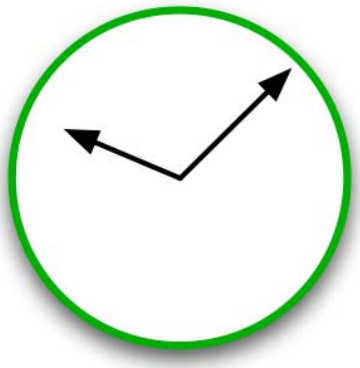


Secure and Precise

Evolving protection state can make deployed policies stale

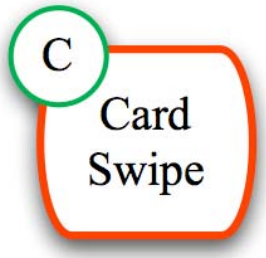


Use *versioning* to cope with evolving permissions



Logical clock

User
version number



Policy
version number

Security and Precision

- Security and precision guaranteed
  - If user's version number $\leq$ policy version number
- Loss in precision
  - For users with larger version numbers
  - But security is maintained

Future Directions

- More precision
  - Better policy analysis?
- Better versioning scheme
  - More version numbers?
- Experimental evaluation
  - Degradation of precision
  - Overhead of evaluating constraints
- Usability
  - Interaction with Policy Negotiation Server

Conclusions

- Unlinkability through access control
  - Policies attached to audit records
- Efficient decentralized enforcement
  - Modified Chinese Wall semantics
- Copes with evolving protection state
  - Versioning scheme to maintain security and precision