Architecture review

Architectures for Large-Scale, Networked Systems

Individual user using globally available service

Single administration domain

Federated administration domains

Independent, external services - to be integrated

Detached, ad-hoc, anonymous groups;
anonymous principals, issues of trust and risk

Federated administration domains: Examples

- national healthcare services:
  many hospitals, clinics, primary care practices
- national police services:
  many county police forces
- global company:
  branches in London, Tokyo, New York, Berlin, Paris...
- transport
  County Councils responsible for cities, some roads
- active city:
  fire, police, ambulance, healthcare services.
  mobile workers
  sensor networks e.g. for traffic/pollution monitoring

Federated domains - characteristics

- names: administered per domain (users, roles, services, data-types, messages, sensors, ...)
- authentication: users administered within a domain
- communication: needed *within* and *between* domains
- security: per-domain firewall protection
- policies: specified per domain e.g. for communication, access control *intra and inter-domain*, plus some external policies to satisfy government, legal, and institutional requirements
- high trust and accountability within a domain,

  known trust between domains

Independent, External Services - Examples

- commercial web-based services
  e.g. online banking, airline booking etc.

- national services used by police and others
  e.g. DVLA, court-case workflow

- national health services
  e.g. national Electronic Health Record (EHR) service

- e-science (grid) databases and generic services
  e.g. astronomical, transport, medical *databases*
  for *computation* or *storage*

- e-science may support “virtual organisations” – collaborating groups across several domains

Independent, external services - characteristics

- naming and authentication
  may be of individuals via trusted third parties (TTPs)
  and/or via home domain of client

- access control policies
  related to client roles in domains and/or individuals
  support for “*virtual organisations*” spanning domains

- need for: accounting, charging, audit
  these may be done by trusted third parties
  a basis for mutual trust (service done, client paid)
- trust
  based on evidence of behaviour
  clients exchange experiences, services monitor and record
  assume full connectivity, e.g. TTPs can authenticate/identify

Examples of detached ad hoc groups and the need for trust

- Commuters regularly play cards on the train
- Auctions – build up trust of an ID through small honoured purchases, then default on a big one
- E-purse purchases – trust in system
- Recommendations: e.g. in a tourist scenario - restaurants, places to visit. Recommendations of people and their skills.
- Wireless routing via peers:

  routing of messages P2P rather than by dedicated brokers – reliability, confidentiality, altruism
- Trust has a context – skills may not transfer

  e.g. drivers of cars, trains, planes ...

Detached, ad-hoc, anonymous groups

- e.g. connected by wireless
- can’t assume trusted third-parties (CAs) accessible
- can’t assume knowledge of names and roles, identity likely to be by key/pseudonym
- new identities can be generated (by detected villains)

- parties need to decide whether to interact
- each has a trust policy and a trust engine
- each computes whether to proceed – policy is based on:

- accumulated trust information
 (from recommendations and evidence from monitoring)
- risk (resource-cost) and likelihood of possible outcomes

Promising Approaches for Large-Scale Systems

- Roles for scalability
- Parametrised roles for expressiveness, scalability, simplicity
- RBAC for services, service-managed objects, including the communication service
- Policy specification and change management
- Policy-driven system management

- Asynchronous, loosely-coupled communication
  publish/subscribe for scalability
  event-driven paradigm for ubiquitous computing
- Database integration – how best to achieve it?

And don’t forget:

- Mobile users
- Sensor network integration