Mobile Systems Availability Integrity and Confidentiality MoSAIC

M.O.Killijian, D.Powell, M.Banâtre, P.Couderc, Y.Roudier

LAAS-CNRS - IRISA- Eurécom

Context

- 3 year project, 3 partners: LAAS, Eurécom, IRISA
  - Officially started September 2004
  - Funded by French Ministry of Research
- Spontaneous Information Systems (SIS)
  - Wireless enabled PDAs
  - Mobile AdHoc Networks (MANETs)
  - Peer-to-peer model of interactions
- New means to enforce
  - Availability
  - Confidentiality
  - Integrity
  - Privacy

} Dependability and Security

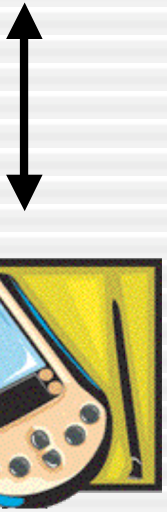
Context

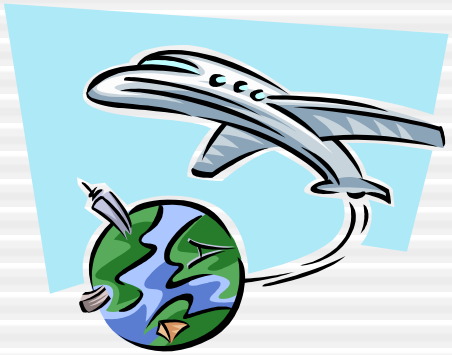
- Many research works targeting the network level
  - Routing
  - Medium Access Control
- We focus on the middleware level
  - Higher level notions/mechanisms
    - Right place for dependability mechanisms
  - Access to the application context
    - App. dependent recovery (partition/disconnection)

→ Collaborative Backup of Critical Data

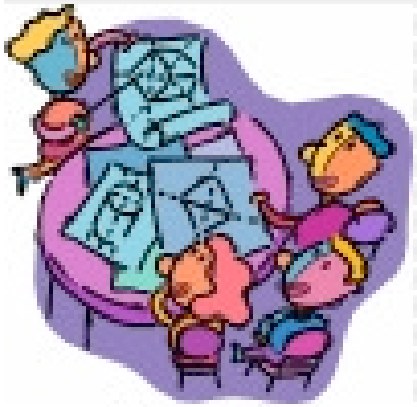
Scenario

Alice is going to a symposium





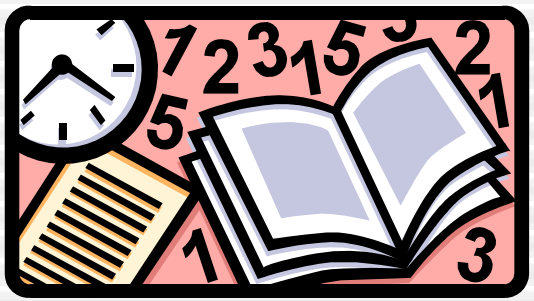
Scenario



Alice meets new people and colleagues

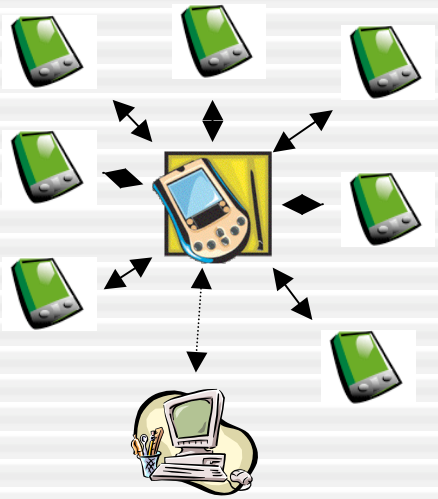
Scenario

Alice produces data and breaks her PDA



Scenario

But she gets a new PDA and is able to restore her data



Challenges for Dependability

- Intermittent access to infrastructure
- No prior organization
- Ephemeral interactions
- User transparency
- Private sensitive data
- Limited energy, computation and storage

Goals

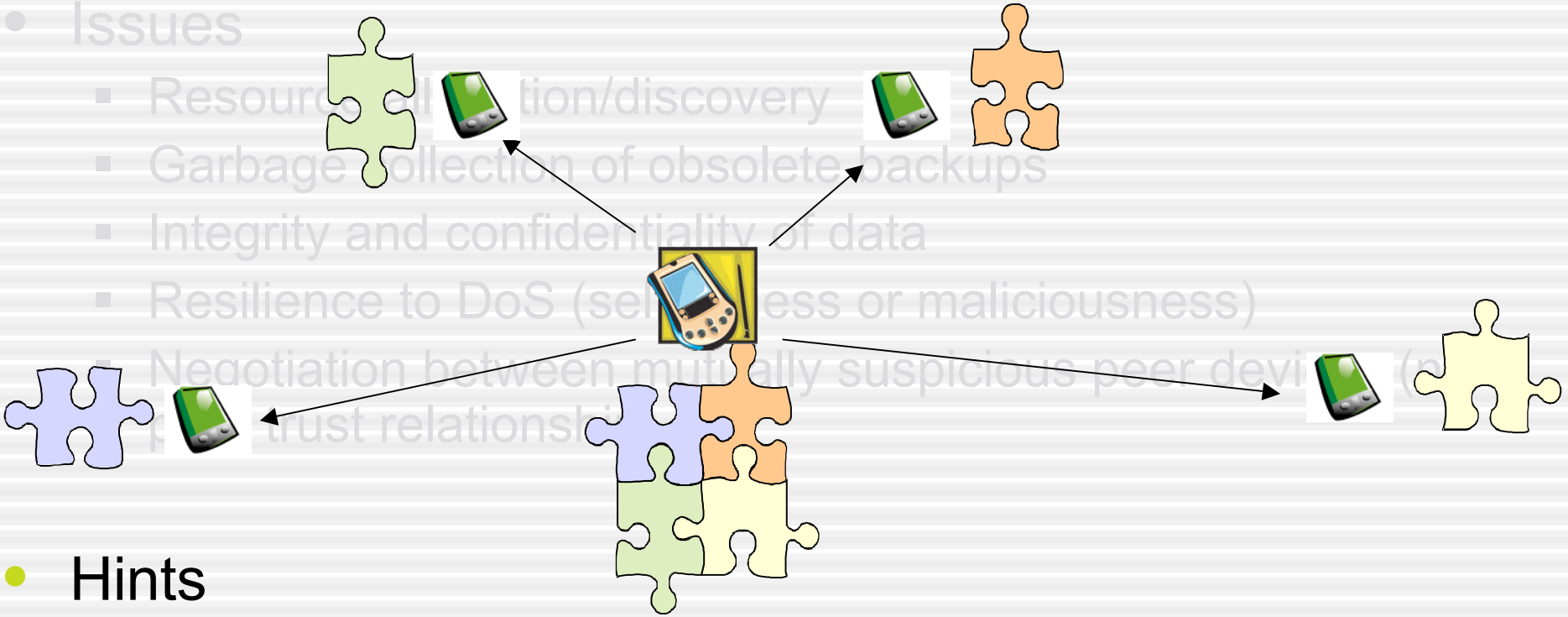
- Design and develop
  - new mechanisms for the tolerance of
    - accidental faults
    - malicious faults
  - without usual strong assumptions
    - synchronous communication
    - global clocks
    - infrastructure
- New middleware for dependable mobile systems

Collaborative critical data backup

- Issues
  - Resource allocation/discovery
  - Garbage collection of obsolete backups
  - Integrity and confidentiality of data
  - Resilience to DoS (selfishness or maliciousness)
  - Negotiation between mutually suspicious peer devices (no prior trust relationship)
- Hints
  - Fragmentation-Redundancy-Dissemination
  - Peer-to-peer
  - Mobility for dissemination

Collaborative critical data backup

- Issues
  - Resource allocation/discovery
  - Garbage collection of obsolete backups
  - Integrity and confidentiality of data
  - Resilience to DoS (selfishness or maliciousness)
  - Negotiation between mutually suspicious peer devices (no trust relationship)



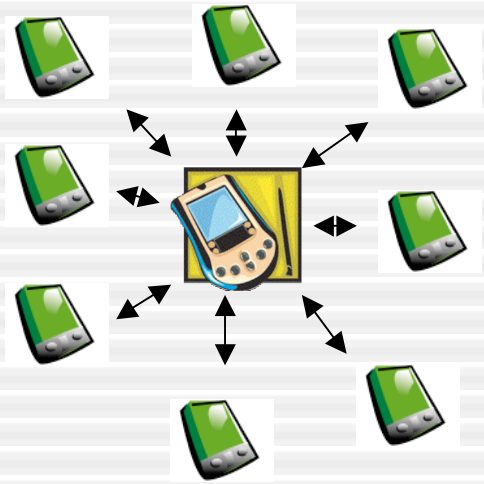
- Hints
  - Fragmentation-Redundancy-Dissemination
  - Peer-to-peer
  - Mobility for dissemination

Trust management for collaborative services

- Issues
  - No prior trust relationship
  - Protect from and identify malicious devices
  - Accountability, privacy, integrity,confidentiality
- Hints
  - Self-carried reputation
  - Currency-based incentives
  - Hybrids

Collaborative Backup for Ubiquitous Computing

- Transparent distributed backup of critical data for mobile systems over wireless communications
  - Inspired by peer-to-peer techniques
  - Fragmentation-Redundancy-Dissemination based
- No-prior trust relationship
  - Automated resource discovery and negotiation
  - E-cash and reputation schemes
- Privacy
  - Tamper-proof hardware/trust core
  - Identity management (authentication, multiple IDs, etc.)



Mobile Systems Availability Integrity and Confidentiality MoSAIC

http://www.laas.fr/mosaic