

Security Challenges of Location-Aware Mobile Business



Emin Islam Tatlı, Dirk Stegemann, Stefan Lucks
Theoretical Computer Science, University of Mannheim
Mobile Commerce and Services (WMCS'05), July 2005

Outline

- The Mobile Business Research Group
- Context- and Location-awareness
- Application Logic Framework
- Security Challenges
- Further Research&Focus

Mobile Business Research Group

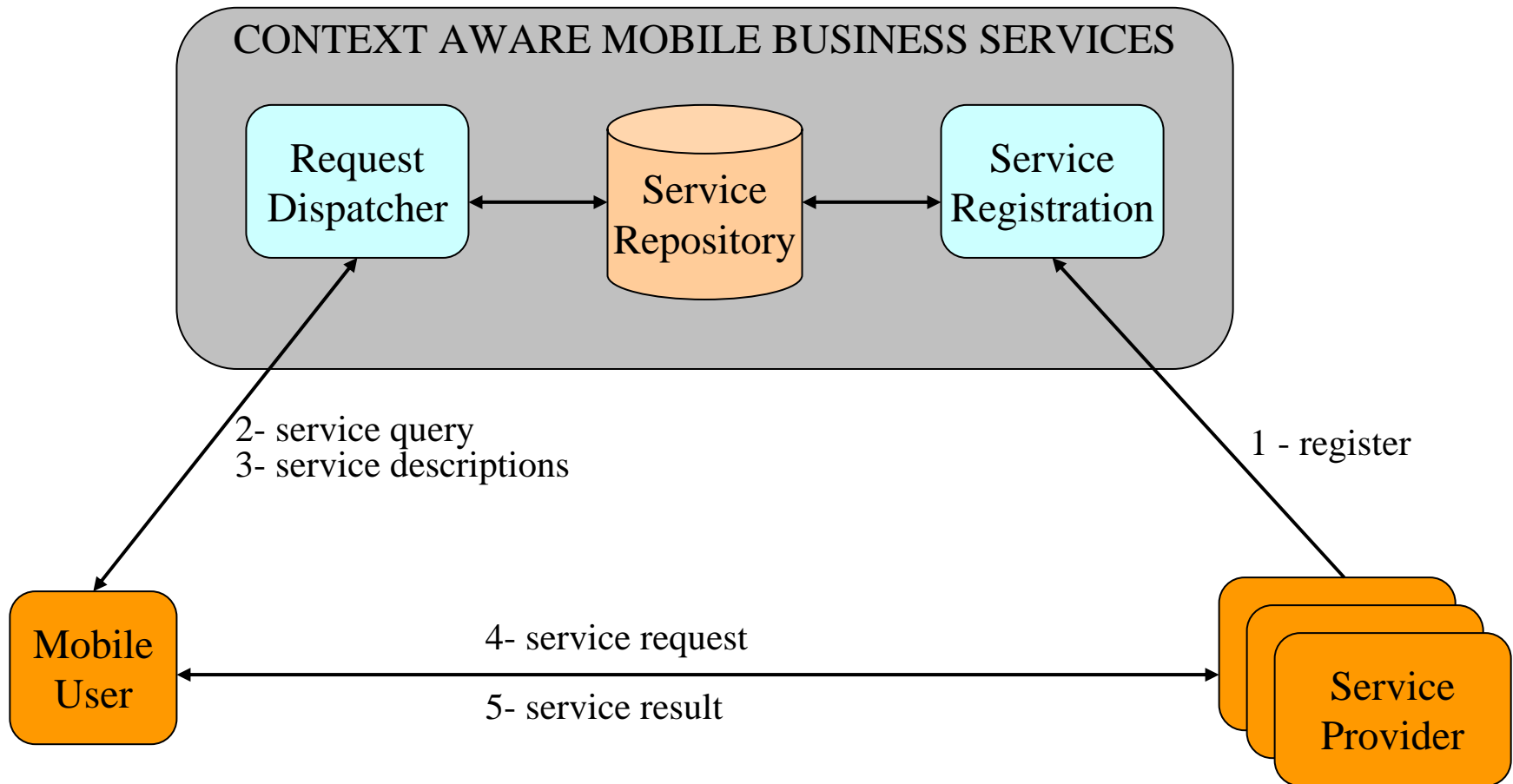
Generic platform for context-aware and especially location-aware mobile business applications

- Joint project of 7 research groups at the University of Mannheim
- Cooperation with
 - SAP AG, Walldorf
 - CAS Software AG, YellowMap AG, Karlsruhe
- Web: <http://www.m-business.uni-mannheim.de/>

Context-aware Applications

- **Context** = any information that can be used to characterize the situation of an entity (e.g. *location*, time, identity, level of mobility)
- A **Context-aware application** considers context when providing its service
- Examples
 - Find a pizza delivery service that can deliver my favourite pizza for less than 8 EUR within 15 minutes to my current location
 - Locating moving objects (e.g. fleet management)
 - Locating kids
 - Indoor navigation in fairs
 - Location-based chat/games
 - Panic alarms

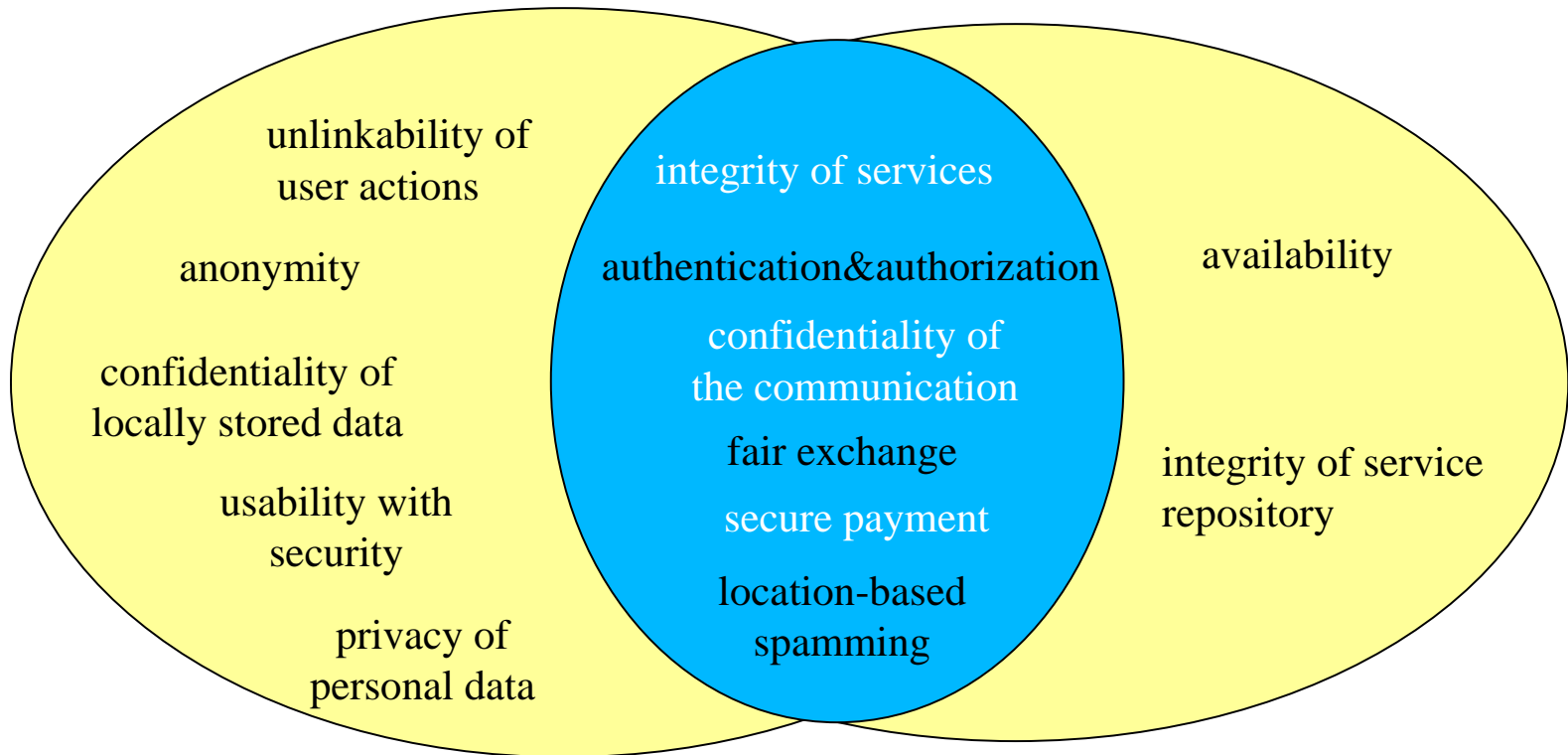
Application Logic



Security Challenges

Mobile Users

**Broker &
Service Providers**



Anonymity

- Mobile users require to hide their real identities
- Anonymity ensures that a user may use a resource or service without disclosing the user's identity
- Service providers require a unique representation of users
- **Solution:** Pseudonymity
 - Enables *content anonymity*, but not *communication anonymity*

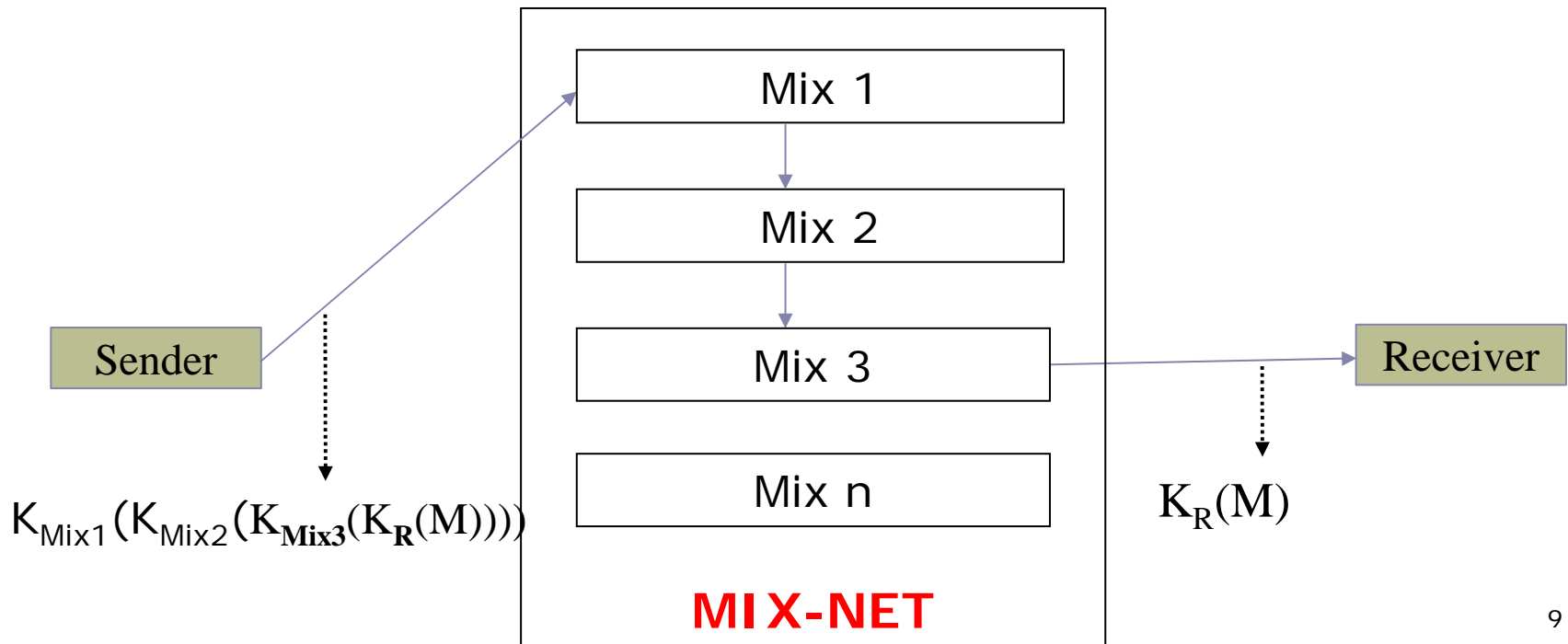
Unlinkability of User Actions

- unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system
- Main existing solutions for unlinkability:
 - Proxies
 - Mix-net
 - Peer-to-peer networks

Mix-Net

□ Mix:

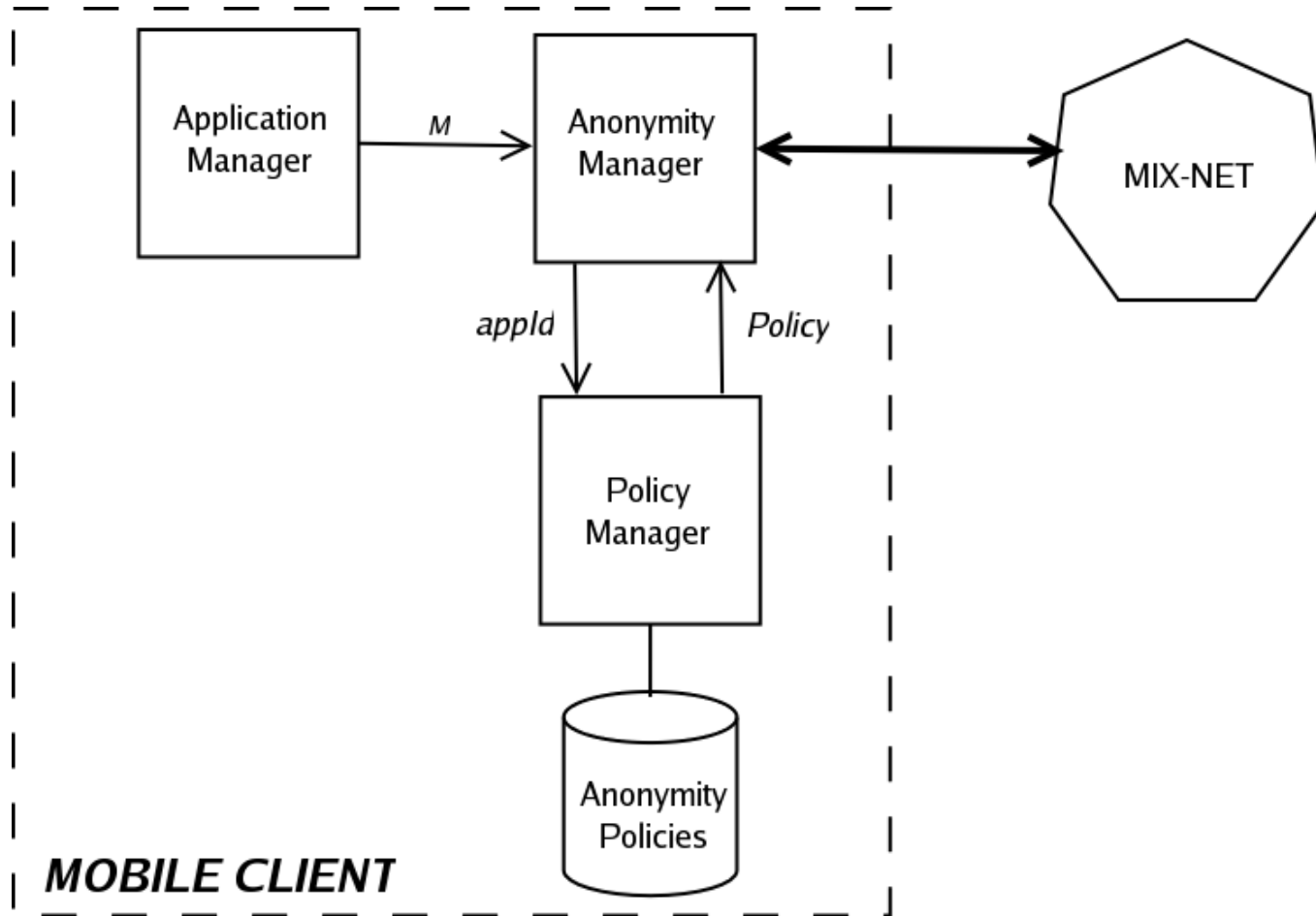
- Computer between sender and receiver
- Decrypts messages and forwards to other mix/receiver



Dynamic Anonymity

- Different applications require different anonymity levels
 - finding the nearest shop vs. mobile dating
- Different users require different anonymity levels
 - Celebrity v.s. a normal person
- Performance problems of Mix-net

The Framework



Privacy of Personal Data

- Service providers request different kinds of personal data (even only for profiling of users)
- Personal data is private, especially location
- Privacy is the ability and/or right to protect your personal secrets
- **Solution**
 - Identity Manager

Identity Manager

- Enables full control of personal data
- Presents an interface for
 - creating different virtual IDs
 - binding a subset of personal data to each ID
- During communication with a service provider, the user chooses a suitable ID for this particular type of communication
- Before any personal data is sent to a service provider, the user is asked to allow this transmission

Identity Manager (cont.)



Confidentiality of Locally Stored Data

- Thefts are very common in the mobile world
- User's local data (e.g. profiles, passwords, private keys, etc.) should be protected from unauthorized disclosure
- **Solution**
 - Two-factor authentication
 - Password-based encryption

Usability vs. Security

- Trade-off usability and security: users prefer usability
 - weak, easily-guessable passwords
- Different sensitivity of users for security
 - digital certificates
- Enhance usability and security according to personal needs
- **Solution**
 - Dynamically configurable security policy management system

Usability vs. Security (cont.)

- Components of a dynamically configurable security policy management system
 - Password Manager
 - Single-Sign-On
 - Security Level Manager
 - Identity Manager

Future Research and Focus

- Design an open security architecture which can easily be integrated within the m-business application framework
 - Evaluation of user acceptance criteria
 - Policy-based components for enabling dynamic security configurations

- Verification and implementation of security protocols

- Secure mobile payment transactions
 - Evaluation of existing payment protocols from the perspective of user acceptance

Security Challenges of Location-Aware Mobile Business



Emin Islam Tatlı, Dirk Stegemann, Stefan Lucks
Theoretical Computer Science, University of Mannheim
Mobile Commerce and Services (WMCS'05), July 2005