Fraunhofer FOKUS
Institute for Open Communication Systems

Competence Center
Electronic Safety for the Public and Industries ESPRI
Privacy-Aware and Distributed System Design for Personalised Alerting

Hans G. Ziegler and Michael Klafft

Fraunhofer Institute for Open Communication Systems
Agenda

• Opti-Alert
• Privacy dimensions
• Personal data / sensitive personal data
• Broadcast-based alerting
• System design
• Subscription-based alerting: client-/server-centric design
• System security
Opți-Alert

• EU research project
• Funded under the 7th Framework Programme (Grant Agreement No. 261699)
• Goal: Raising the efficiency of alerting systems through personalized, culturally sensitive multi-channel communication
• Interdisciplinary project involving partners from six different countries: Austria, France, Germany, Italy, the Netherlands, Sweden
Privacy Dimensions

Privacy of personal information

Privacy of personal behaviour

Privacy of personal communications

Privacy of the person
Personal Data
Directive 95/46/EC

• Any information that relates to an identified or identifiable natural person

• Legitimate processing of personal data can be ensured if
  • the data subject has given his consent (Art. 7a) or
  • if the task is carried out in public interest or in exercise of official authority (Art. 7e).
Sensitive Personal Data
Directive 95/46/EC

• It is prohibited to process personal data that reveals
  • racial or ethnic origin,
  • political opinions,
  • religious or philosophical beliefs,
  • information about health or sex life (Art. 8 no. 1).
Broadcast-Based Alerting

- No user registration takes place
- One message for all recipients or group of recipients
- Radio, TV, RDS
- Personalisation might be realisable, however
  - full data must be sent to the users
  - filtering on the user’s device required
System Design
Subscription-Based Alerting
Server-Centric System Design

- Users have to register
- Alert messages are adapted based on user profile data
- User profiles are comprised of
  - registration data
  - socio-cultural factors
Subscription-Based Alerting
Server-Centric System Design
Subscription-Based Alerting
Server-Centric System Design

• Socio-cultural information to target
  • Senior citizens (age)
  • Immigrants/Tourists (language, home country)
  • People with children (school address etc.)
  • Disabled people (disability type)
• Other data: Phone number (SMS), email-address, device-id (smartphone)
Subscription-Based Alerting
Server-Centric System Design

• Region-specific information
  • Specific social behaviours or stereotypes
  • Level of disaster experience
  • Disaster likelihood / frequency
  • Trust in authorities
Client-Centric System Design
Client-Centric System Design

- Minimisation of central storage of sensitive data
- No personal data stored on server (except communication data)
Client-Centric System Design

Communication flow:

• 1. Server sends generic message to client (Push-Notification)
• 2. User opens alert application
• 3. Client requests personalised message
• 4. Server responds
Pro and Contra: 
Server

• Pro:
  • only 1 interaction between server and client required
  • in case of SMS no internet connection required

• Contra:
  • central storage of personal data,
  • no smart phone features
Pro and Contra: Client

• **Pro:**
  - client-side storage of personal data,
  - smart phone features can be leveraged (e.g. maps, navigation, current position)

• **Contra:**
  - multiple interactions required,
  - higher network traffic,
  - multiple potential points of failure
System Security

- Known Partners Pattern: Server and client certificate
- Multi-Part Identity: Client authentication plus separate user authentication
- Trusted Platform Module (Intel)
System Security

- Trusted Platform Module
  - Properties: Fixed platform properties (e.g. Hardware)
  - Measurements: Integrity of entities that can change (e.g. OS, programs etc.)
  - Isolation using virtualisation via guest partitions:
Thank you for your attention!