Context Mobile Electronic Personality

W. Oyomno, P. Jäppinen, E. Kerttula

05.11.2009

LAPPEENRANTA
UNIVERSITY OF TECHNOLOGY

Outline

1. Background

2. Motivational concerns

3. Vulnerabilities & mitigation

4. Conclusion

Background

- Context information - Enriching information about an entities prevailing situation e.g. location, activity, role, company

- Personal information - set of all data associated with a specific individual - meaning only in how it associates/differentiates

- Personal trusted devices – evolution of mobile device to offers strong authentication of the user for number of services

- Privacy - claim to determine when, how, and to what extent information about them is communicated to others

Motivational concerns

- Multiple sensors in mobile terminals
- Proliferation of mobile computing
- Ease to compose / disseminate services
  - 3 Service spheres
  - Societal transformation – post9/11
  - Information age participation – trade personal information
- Merging service spheres & new business models

Motivational concerns ...

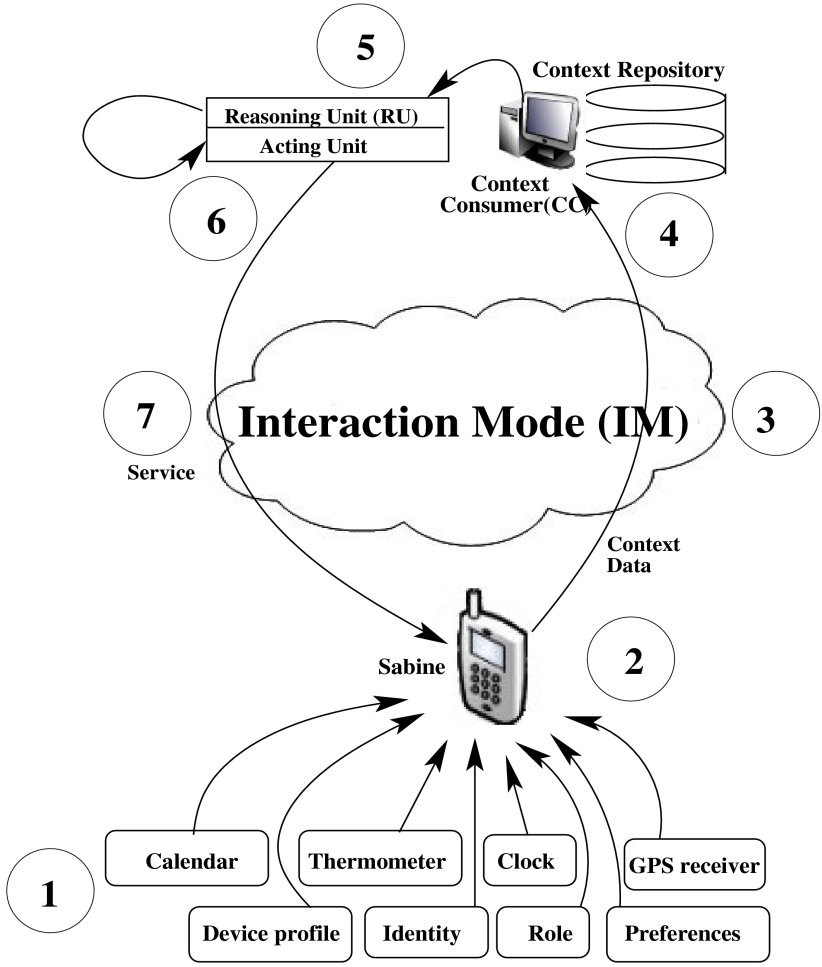
- Scattering of PI
- Diminished control over PI collection/use - re-purpose
- Trade-off, harmless, lone-information pieces
- Compounding *context* + *PI* + *service character*
  - Exposes “the deep truth”
- Privacy leaks in using context-aware services
  - Surveillance, identity thefts, falsification ...

Vulnerabilities & mitigation

- Acquisition & representation leaks - *in-train, with-mike, where*
- Interaction leaks – *Eavesdroppers, header mining - not-home*
- Caching & retention vulnerabilities – *how, duration*
- Usage & disposal leaks - *3rd party processing*
- PI chain of custody & context life cycle

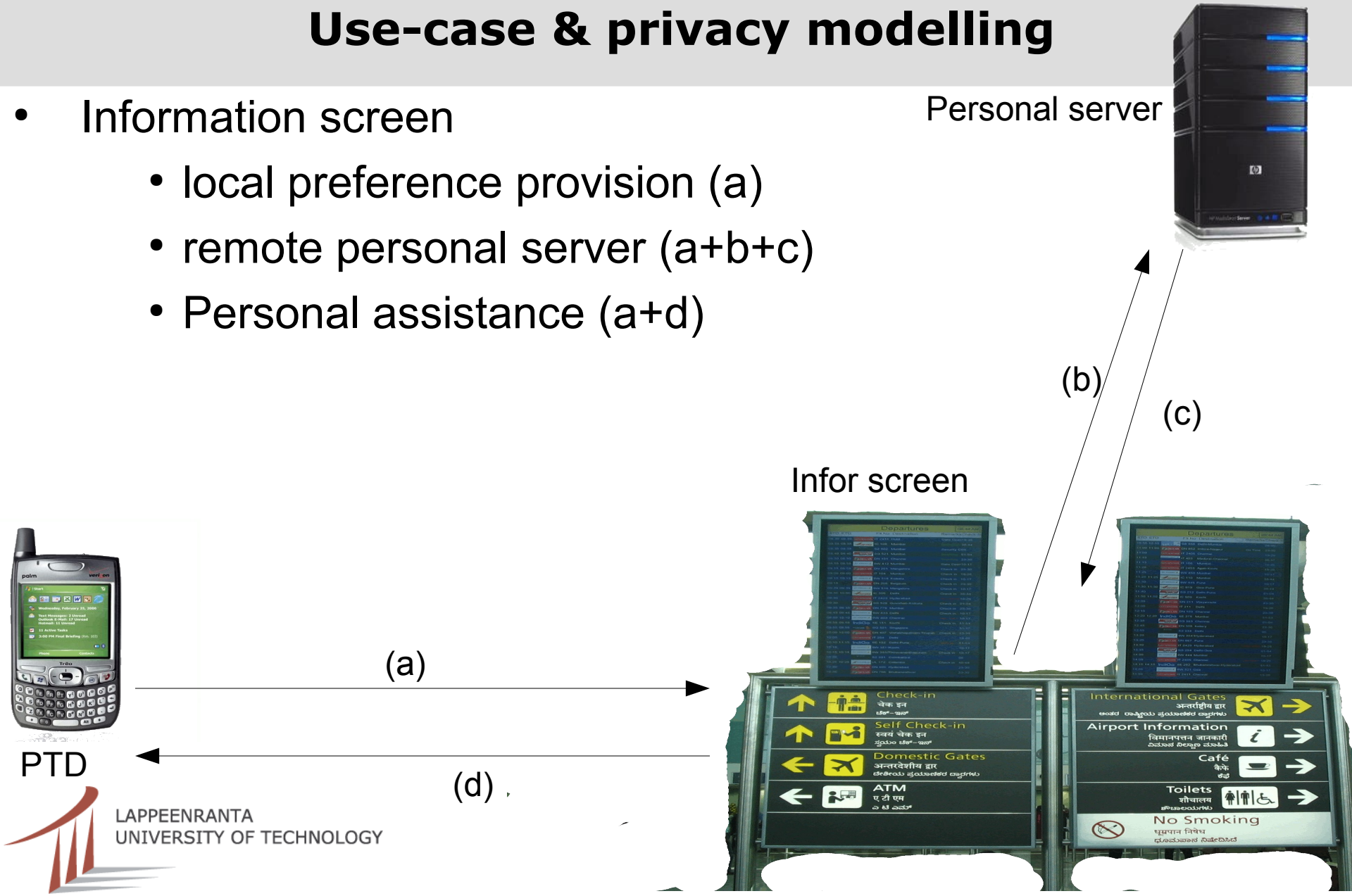
Vulnerabilities & mitigation ...

- Key privacy questions
  - Private info piece & with whom are they associated
  - Withheld from whom
  - Benefits & in whose interest?



Use-case & privacy modelling

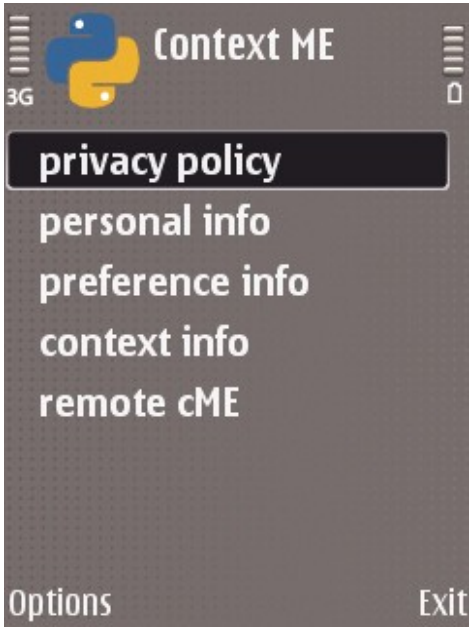
- Information screen
  - local preference provision (a)
  - remote personal server (a+b+c)
  - Personal assistance (a+d)



LAPPEENRANTA
UNIVERSITY OF TECHNOLOGY

Privacy modelling

Privacy policies




```
<policy:detail="privacy policy">
    <policy:policy_head="introduction">
        <policy:policy_use="information"/>
        <policy:policy_owner="resto-loco"/>
        <policy:policy_validity="indefinate"/>
    </policy:policy_head>
    <policy:policy_part="rule 1">
        <policy:info_request>
            <policy:value="name"/>
            <policy:value="address"/>
            <policy:value="meal"/>
        </policy:info_request>
        <policy:value="info_purpose">
            <policy:value="restaurant"/>
        </policy:info_purpose>
        <policy:info_retention="string">
            <policy:value="6 hours"/>
        </policy:info_retention>
        <policy:info_benefit="string">
            <policy:value="preferred meal"/>
        </policy:info_benefit>
        <policy:disclose_sphere="string">
            <policy:value="community"/>
        </policy:disclose_sphere>
    </policy:policy_part>
</policy:detail>
```

Privacy modelling ...

Personal server

- Single access tickets
- S/KEY mechanism

ME - Personal Server

Remote Control - ME

[Identities] [Personal Information] [Contacts] [Preferrences] [Exit]

wagner's Preferences, favourites & likes

Preset prefs

	Information	Purpose	Domain	Retain	Disclose
News	weather	content filt	individual	8 hrs	community
Sport	ice-hockey	tailor	community	4 hrs	personal
Music	jazz	adapt	corporate	16 hrs	governmer
Meals	italian	emergency	social net	32 hrs	individual
Movie-Tv	bb	follow up	contact	128 hr	community
Shopping	shopping centre	prioritise	government	8 hrs	governmer

Language: French

update preference

LAPPEENRAN
UNIVERSITY (

Conclusion

- Overview of context-awareness & PI in services
- How & why it is reason to be concern
- Expressed the complexity with mitigation
  - Privacy paradox, UI
- Privacy preserving implementations
- Contributions/critics/discussions/suggestions

References

- Ben Wood, Carolina Milanesi, Ann Liang, Hugues De La Vergne, Tuong Huy Nguyen, and Nahoko Mitsuyama. Forecast: Mobile terminals, worldwide, 2000-2009. Technical report, Gatner Research, 2005.
- Adam Greenfield. *Everyware, The dawning age of ubiquitous computing*, volume 1.New Riders, 1 edition, 2006.
- Mark Weiser. The computer for the 21st century. In *Scientific American Journal*, pages 94 – 104, New York, NY, USA, 1991. ACM.
- Pekka Jäppinen. *Mobile Electronic Personality*. PhD thesis, Lappeenranta University Of Technology, 2004.
- Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Advances in Elliptic Curve Cryptography*, volume 1. Cambridge University Press., 2 edition, 2005
- A. Lugmayr, T. Saarinen, and J.-P. Tournut. The digital aura - ambient mobile computer systems. *Parallel, Distributed, and Network-Based Processing, 2006. PDP 2006. 14th Euromicro International Conference on*, 1(1):7 pp.–, 2006.