Privacy and security in older adults independent living assistance platform

10th FRUCT conference, 10.11.2011, Tampere

Dr. Pekka Jäppinen
Lappeenranta University of Technology

Open your mind. LUT.
Lappeenranta University of Technology

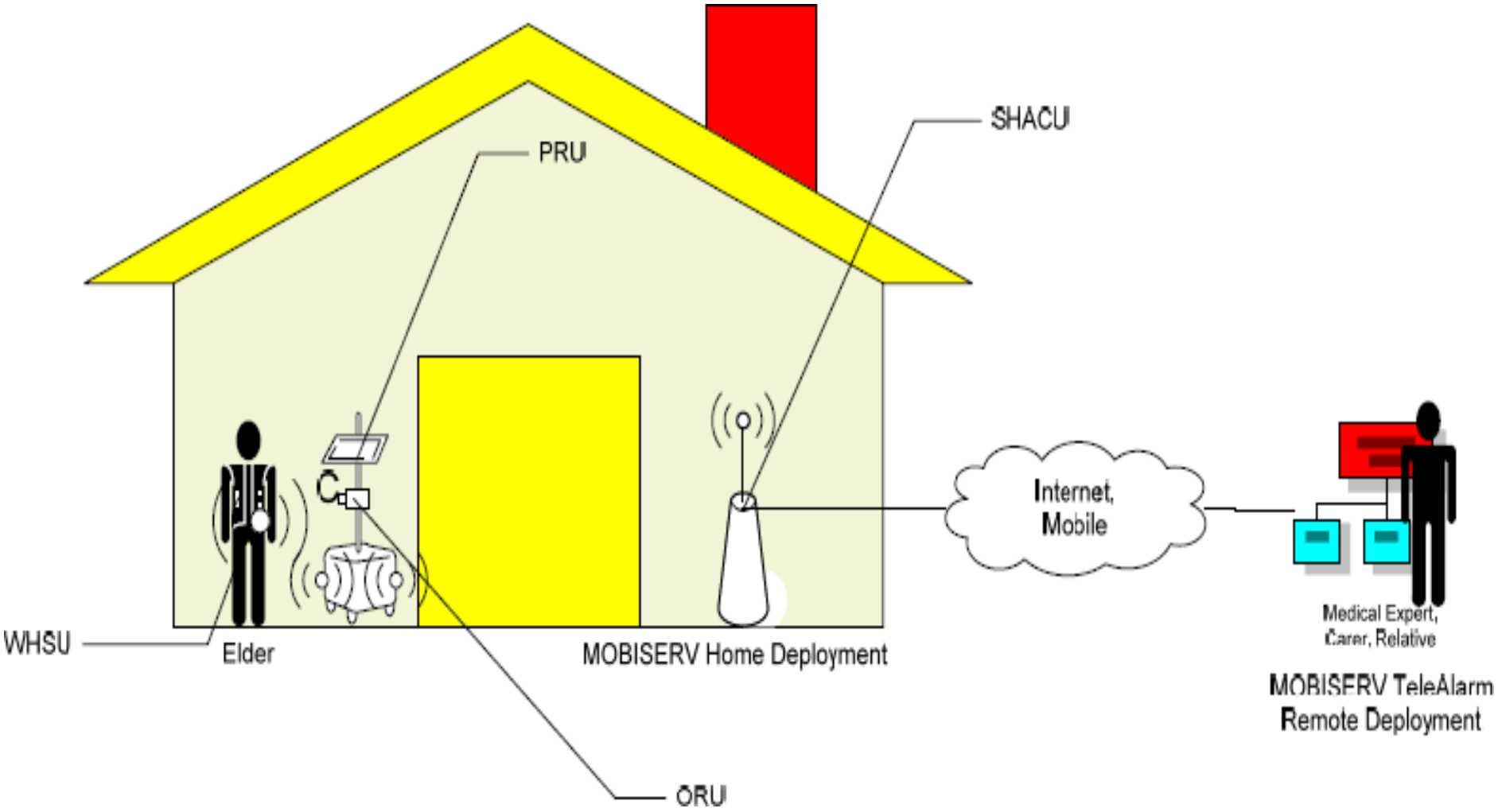
Open your mind. LUT.
Lappeenranta University of Technology

Structure of presentation

- Overview of Mobiserv
- Importance of security and privacy
- Security goals
- Information evaluation
- Vulnerable points
- Information flow analysis

Open your mind. LUT.
Lappeenranta University of Technology

Mobiserv



Pekka Jäppinen
Lappeenranta University of Technology

Open your mind. LUT.
Lappeenranta University of Technology

Mandatory Functionalities

1. F02 Reminder and encouragement to drink
2. F01 Reminder and encouragement to eat
3. F19 Reporting and communicating to health professionals
4. F17 A tele-medicine/self-check platform
5. F18 Games for Social and Cognitive Stimulation
6. F11 Voice/Video/SMS via Robot communication with friends and relatives
7. F14 A mobile screen connected to the front door
8. F06 Response to call for help from the user
9. F08 Encouragement for exercising

Open your mind. LUT.
Lappeenranta University of Technology

Importance of security

- Mobiserv applications use information about user that may be sensitive
  - e.g. health status, medication etc.
  - Loss of privacy affects acceptability of solution
- Many features rely on accurate information
  - Corrupted data may cause unexpected behaviour on the system
- Denial of Service
  - Reduces the trust and acceptability of system

Open your mind. LUT.
Lappeenranta University of Technology

Information Security Goals

- Confidentiality
  - Only those who have right to access the data may do so.
- Integrity
  - The data has not been changed
    - during transmission
    - in storage
- Availability
  - Those who have right to access the data may access it
    - Easily
    - Quickly

Open your mind. LUT.
Lappeenranta University of Technology

Analysis for data

- Evaluation of the data handled and stored in the system from security goals perspective
- What happens if
  - Data is eavesdropped
  - Data is manipulated
  - Data is unavailable
  - Data is lost
- How important it is to prevent those happening
  - Security is not black and white.
  - Focus on relevant problems

Open your mind. LUT.
Lappeenranta University of Technology

Example

- Video feed to detect eating activity
  - Integrity loss may cause false positive or false negative on detection.
    - Problem is not very severe
    - Minimal benefits for outsider to do such attack
  - Availability loss to video feed will cause the loss of functionality
    - Minor nuisance
  - Loss of confidentiality can cause loss of privacy
    - Enables possibility for monitoring of older person
    - Severe problem for acceptability

Potential vulnerable points

- Storage points
  - Where the data is held
  - Analysis can be done in different detail levels
    - Laptop, Robot, Monitor ...
    - Calendar, Log ...
    - Hard drives, Memories ...
- Handling points
  - Where the data is read and written (created and deleted)
    - Laptop, smart garment … Screens, keyboards, cameras...
- Transmission point
  - Where the data is transferred between
    - Physical objects: Smart garment → robot
    - Components:

Open your mind. LUT.
Lappeenranta University of Technology

Storage points

- Internal points
  - Points within the system
    - Datalogger, robot, shacu
  - Security is in developers hand
- External points
  - Points outside the system
    - google calendar, relative, caretaker
  - Security cannot be affected by the system developers.
  - What information and to who will be given
    - Depends who we trust

Open your mind. LUT.
Lappeenranta University of Technology

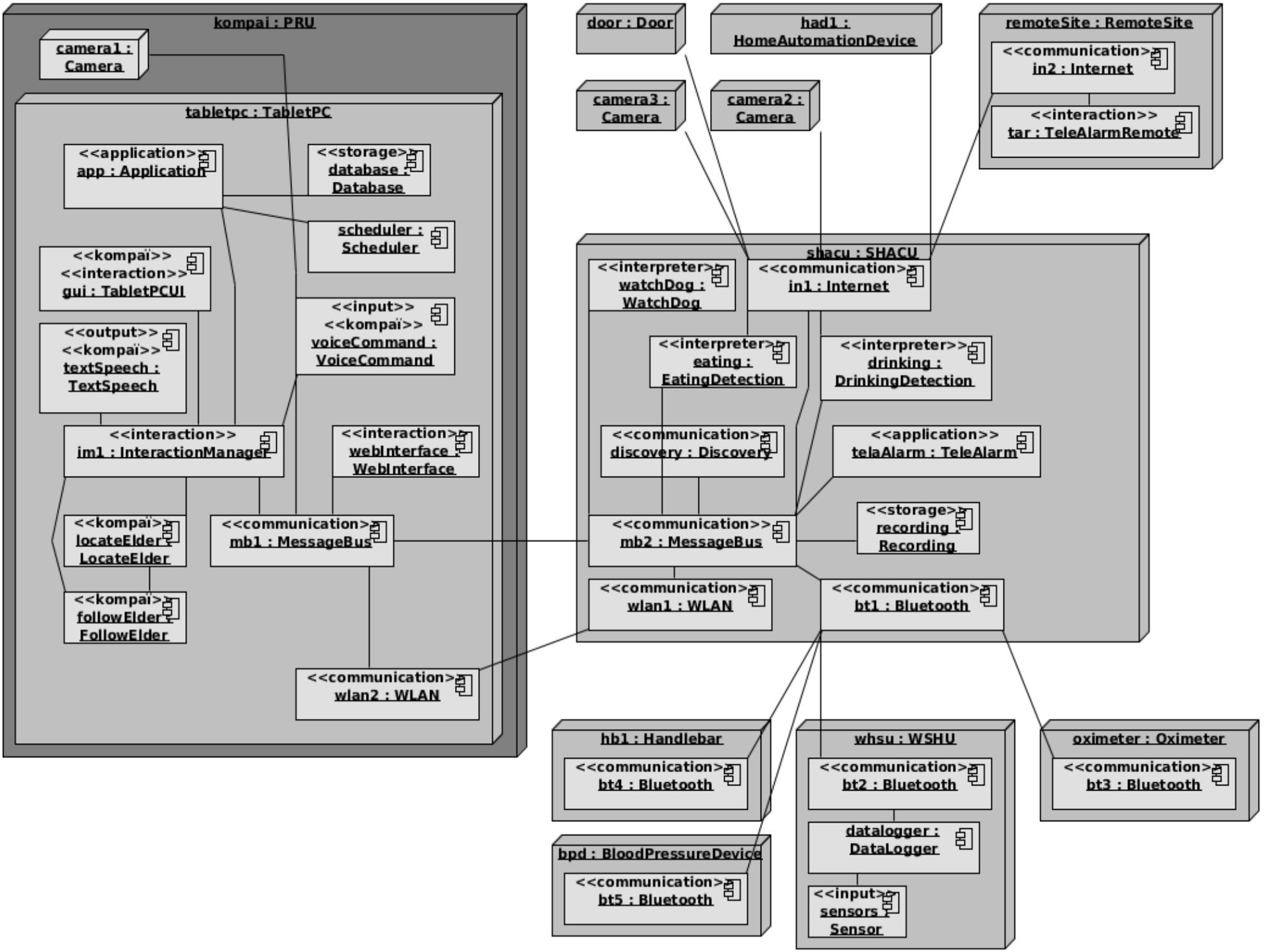
Data input and output

- Where the information comes from
  - Write (create/delete) operation
  - Sensors, Robot UI (touchscreen, microphone), cameras, Internet
  - Integrity and availability of system can be compromised from here
- Where the information goes to
  - Read operation
  - ScreenMonitor, speaker (relative, doctor, elder)
  - May affect on confidentiality

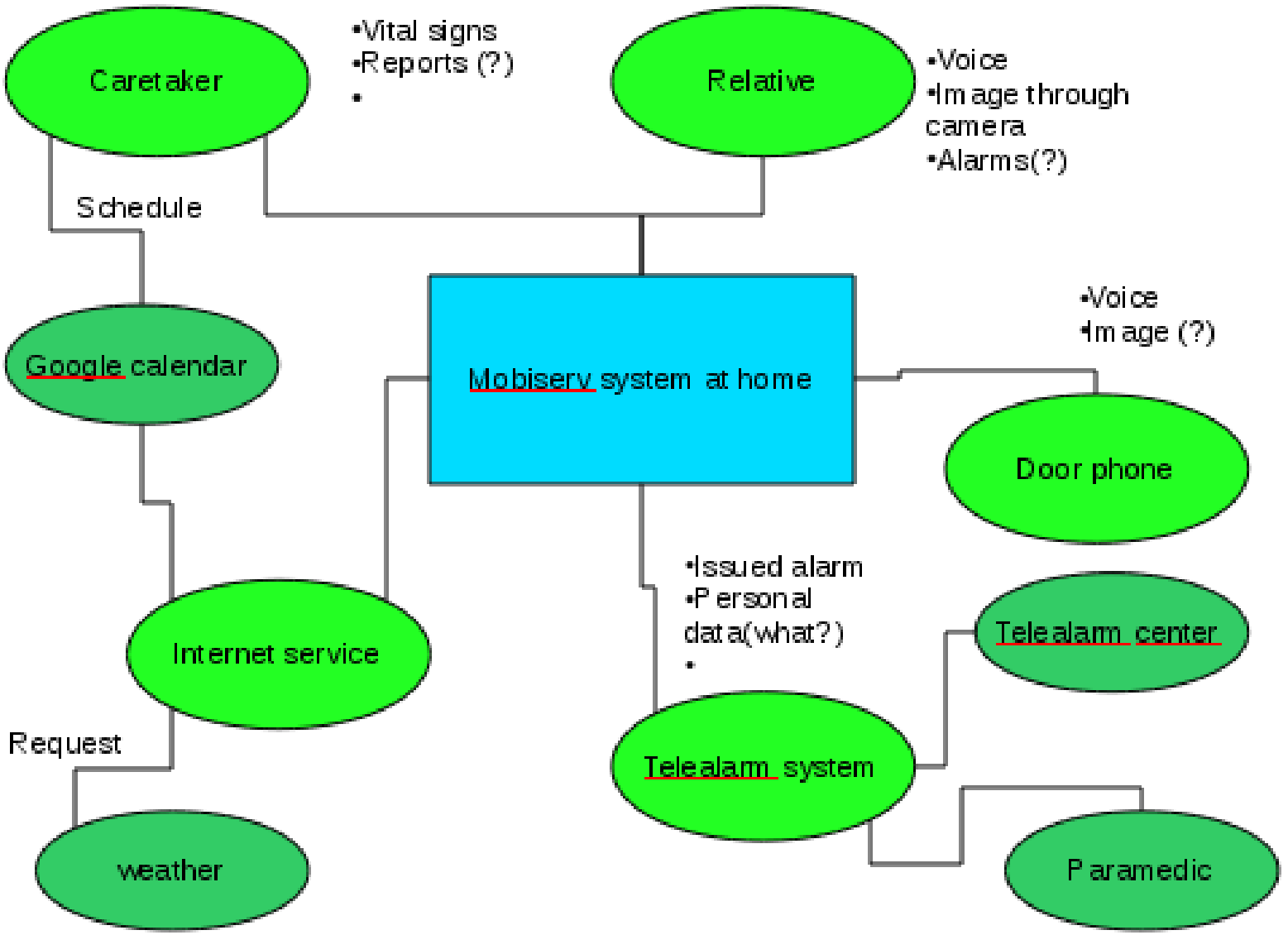
Open your mind. LUT.
Lappeenranta University of Technology

Data transmission

- Within System
  - Smart garment - data logger - robot - SHACU
  - Security measures can be defined in system specification
- System-outside
  - Connections to Internet services
  - Interoperability challenges
- Communication between components outside the system.
  - e.g. caretaker- google calendar
  - No control
  - Explicit Trust to service provider


kompai : PRU
camera1 : Camera
tabletpc : TabletPC
<<application>>
app : Application
<<storage>>
database : Database
scheduler : Scheduler
<<kompai>>
<<interaction>>
gui : TabletPCUI
<<input>>
<<kompai>>
voiceCommand : VoiceCommand
<<output>>
<<kompai>>
textSpeech : TextSpeech
<<interaction>>
im1 : InteractionManager
<<interaction>>
webInterface : WebInterface
<<kompai>>
locateElder : LocateElder
<<communication>>
mb1 : MessageBus
<<kompai>>
followElder : FollowElder
<<communication>>
wlan2 : WLAN
door : Door
had1 : HomeAutomationDevice
remoteSite : RemoteSite
<<communication>>
in2 : Internet
<<interaction>>
tar : TeleAlarmRemote
camera3 : Camera
camera2 : Camera
shacu : SHACU
<<interpreter>>
watchDog : WatchDog
<<communication>>
in1 : Internet
<<interpreter>>
eating : EatingDetection
<<interpreter>>
drinking : DrinkingDetection
<<communication>>
discovery : Discovery
<<application>>
telaAlarm : TeleAlarm
<<communication>>
mb2 : MessageBus
<<storage>>
recording : Recording
<<communication>>
wlan1 : WLAN
<<communication>>
bt1 : Bluetooth
hb1 : Handlebar
<<communication>>
bt4 : Bluetooth
whsu : WSHU
<<communication>>
bt2 : Bluetooth
datalogger : DataLogger
<<input>>
sensors : Sensor
oximeter : Oximeter
<<communication>>
bt3 : Bluetooth
bpd : BloodPressureDevice
<<communication>>
bt5 : Bluetooth

Combining data and system



Open your mind. LUT.
Lappeenranta University of Technology

Data analysis example

- Door ring
  - Door ring signal is activated by the press of door bell. It activates a ringing sound effect in the house.
- Source: Door bell outside of house
- Source Access: Not access control
- Transmitted between: door bell->shacu->robot
- Stored at: Buffers on Shacu and robot
- Storage length: only for duration of handling the signal
- output: ring tone at Robot or Shacu speaker

- Disclosure of data: Not meaningful. However lack of response can be interpreted as empty house. Insignificant threat
- Denial of service: Older adult will not know someone is at door. Insignificant threat
- Corrupted data: No ringing. Insignificant threat
- Fabricated data: May be used to cause repeated door bell ringing. Insignificant threat. Hard to execute, no real use.

Open your mind. LUT.
Lappeenranta University of Technology

Privacy

- Privacy is not only about encrypting personal data
  - Before storing personal data, consider if it is really necessary
  - Differentiate Identity from the data when possible
- Camera recording people eating and drinking is intrusive
  - Store and handle only essential information
  - Only hand movements and mouth location stored and analysed
    - Person cannot be identified from image (nor what if anything he/she is wearing)

Open your mind. LUT.
Lappeenranta University of Technology

Conclusions

- Securing your system is important for its acceptability, especially when handling personal information.
- Privacy can be best protected by carefully considering what is actually needed
  - Identifying data is not always necessary.
- Security is always a compromise.
  - Know what are the main vulnerable points
  - Focus your resources on the important points
    - Man power, processing power, batteries...
-