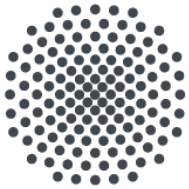
Exploratory Study of STPA-Priv to elicit Privacy Risks in eHealth

Kai Mindermann,
Frederik Riedel, Asim Abdulkhaleq, Christoph Stach, and Stefan Wagner



University of Stuttgart
Germany

Baden-Württemberg Stiftung
WIR STIFTEN ZUKUNFT

Agenda

- Problem Statement
- Description of Explored eHealth Scenario
- Overview of System Theoretic Process Analysis (STPA)
- Exploration of STPA-Priv
- Related Work
- Conclusion

Problem Statement

- STPA-Priv looks like a viable approach for elicitation of privacy risks
- Almost no literature and documentation available (for –Priv)
- How must/can privacy be analyzed based on control structure model compared to safety and security?
- => Apply to a real world scenario and explore STPA-Priv

Describtion of Explored eHealth Scenario

Serious eHealth game

- Goal: Replace need for handwritten diabetes diary for children suffering from diabetis
- Additional requirement: What are healthy places in the town?
- Using smart device for children
  - Glucose measurment
  - Notifying patient to inject insulin
  - Tracking position (GPS)
  - Tracking arm movements (food intake/exercising)

eHealth Scenario

Involved parties

Medical Devices:

- Health data, e.g.,
  - Blood sugar
  - Blood pressure

Smart Devices:

- Sensor data, e.g.,
  - Location
  - Activity
- Private data, e.g.,
  - Contacts
  - Appointments

Patients (Children):

- Health data

⇒ **Understand their condition**

- Activity recognition

⇒ **Ease treatment-related tasks**

Parents:

- Health condition

⇒ **Check wellbeing**

- Location information

⇒ **Act in case of an emergency**

Physicians:

- Need exact health data

⇒ **Complete health record**

- Pre-analyzed data

⇒ **Reduce effort**

Insurance Companies:

- Health data summary

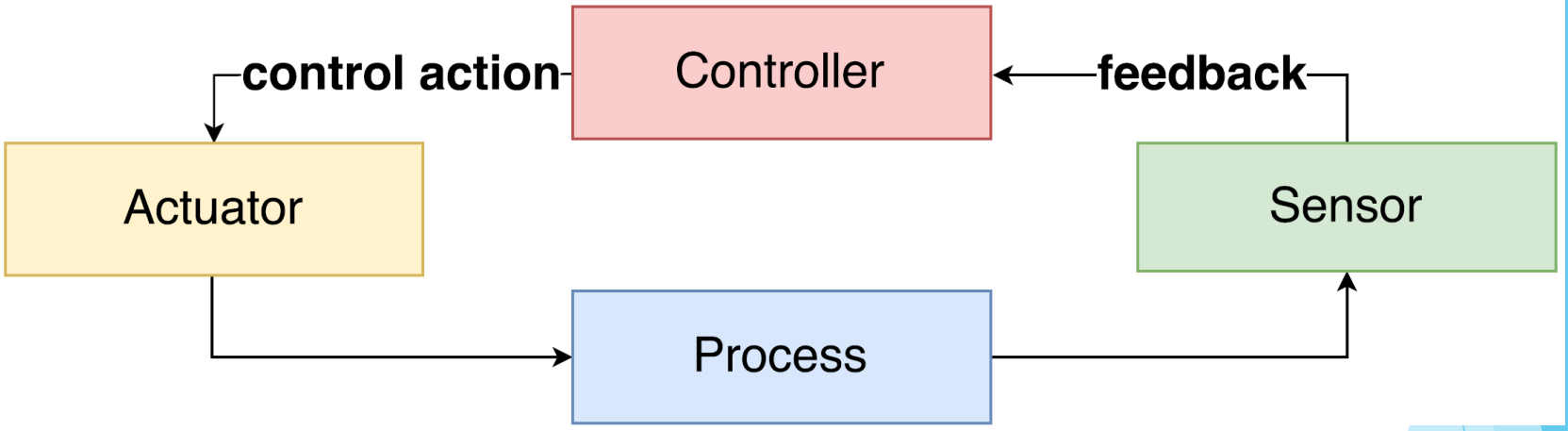
⇒ **Reward a healthy lifestyle**

System Theoretic Process Analysis (STPA)

System Theoretic Process Analysis (STPA)

- Originally for safety analysis
- Top-Down approach
- Treats accidents as a **control problem**, not a failure problem
- **Defined steps** that should be repeated iteratively while finding **new insights in later steps** to maintain full coverage
- Can work both on existing system and parallel to creating a new system

Control Structure / Feedback loop



STPA-Priv vs. STPA

STPA-Priv	STPA-Sec	STPA (Safety)
Define **Adverse Consequences**	Define Losses	Define Accidents
Define Vulnerabilities		Define Hazards
Specify **Privacy Constraints**	Specify Security Constraints	Specify Safety Constraints
Create Control Structure Model / Derive Control actoins		
Define **Privacy-compromising Control Actions**	Define Unsecure Control Actions	Define Unsafe Control Actions

Exploraration of STPA-Priv

Define Adverse Consequences

- User is not aware of active analytics program and is therefore suspect to surveillance.
- Insurance company has access to detailed blood-sugar values.
- Insurance company has access to detailed location data.
- Other players can track location of player.
- Parents can track location of children.
- …

Define vulnerable system states

- Privacy policy has not been presented to user.
- Detailed location data is sent to insurance company as part of the general therapy data.
- High scores include location information.
- …

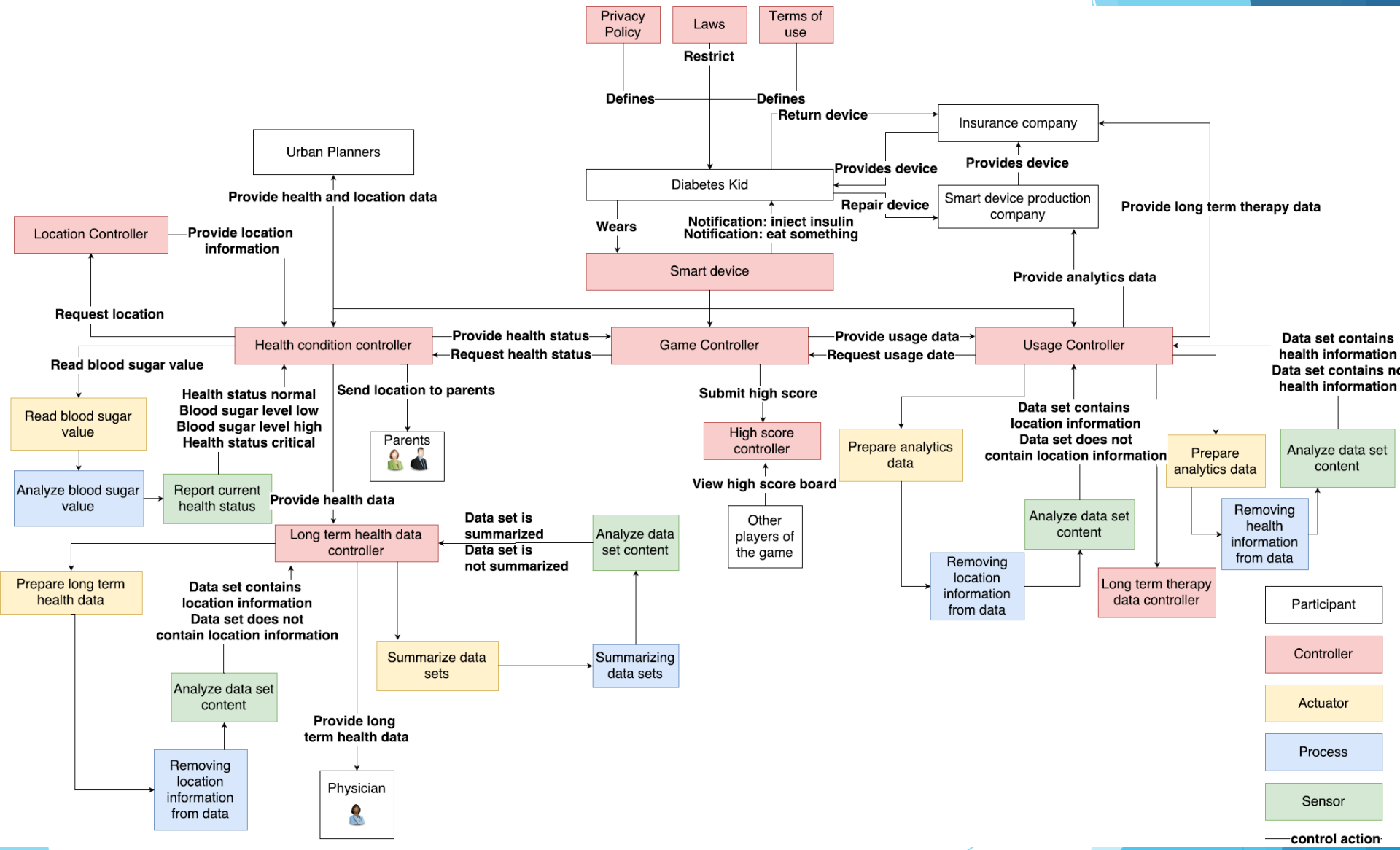
Specify privacy constraints

- **Negation** of vulnerable system state descriptions

Creating the control structure model

- Start with a very high level view with just one process
  - Assume the system is one black box
- Apply STPA
- Increase the details of the black box, revealing different needed controllers and interactions
- Apply STPA

- It should always be possible to improve the actual control structure. At least STPA can give reasonable suggestions for possible improvements.


Privacy Policy
Laws
Terms of use
Restrict
Defines
Defines
Return device
Insurance company
Urban Planners
Provides device
Provides device
Provide health and location data
Diabetes Kid
Smart device production company
Repair device
Provide long term therapy data
Location Controller
Provide location information
Wears
Notification: iniect insulin
Notification: eat something
Smart device
Provide analytics data
Request location
Health condition controller
Provide health status
Request health status
Game Controller
Provide usage data
Request usage date
Usage Controller
Data set contains health information
Data set contains no health information
Read blood sugar value
Health status normal
Blood sugar level low
Blood sugar level high
Health status critical
Send location to parents
Submit high score
Read blood sugar value
Parents
High score controller
Prepare analytics data
Data set contains location information
Data set does not contain location information
Prepare analytics data
Analyze data set content
Analyze blood sugar value
Report current health status
Provide health data
View high score board
Other players of the game
Analyze data set content
Removing health information from data
Data set is summarized
Data set is not summarized
Long term health data controller
Analyze data set content
Removing location information from data
Long term therapy data controller
Prepare long term health data
Data set contains location information
Data set does not contain location information
Summarize data sets
Summarizing data sets
Participant
Controller
Actuator
Process
Sensor
control action
Analyze data set content
Provide long term health data
Removing location information from data
Physician

Define privacy-compromising control actions

- Check for each control action if it could violate the privacy constraints

- „Reset device“ (at manufacturing company)
- Not providing causes vulnerable system state.

- „Send location to parents“
- Providing causes vulnerable system state.

Derive Causal Factors

- Derivation of Causal Factors
- Each causal scenario gives an explanation how the privacy-compromising control action could be enabled.
- Providing high score when score includes location information.
  - High score data filtered incorrectly.
- Not deleting data from device when sending it back to insurance company causes hazard.
  - User does not delete information from device when he decides to send it back to the insurance.

Tool Support for STPA with XSTAMPP

- https://github.com/asimabdulkhaleq/XSTAMPP

Related Work

Related Work

- **LIN(D)DUN** Threat Tree/Catalog and Analysis Process
- Based on Data flow diagram
- Categories: linkability, identifiability, non-repudiation, detectability, information disclosure, unwareness, and noncompliance

- it "[. . .] mainly focuses on the privacy of the data subject (i.e. the person the data are about). Rather than focusing on internal processes and flows[. . .]"
  K. Wuyts and W. Joosen, "LINDDUN privacy threat modeling: a tutorial," Department of Computer Science, KU Leuven, Tech. Rep., 2015.
- So STPA-Priv should uncover risks in between and with human interaction

Conclusion

Conclusion

- Privacy risk analysis with System Theoretic Process Analysis applied to a real world eHealth scenario
- STPA-Priv can be a straighforward process, but a lot of things are still unclear

- My take is, that this scenario or other scenarios miss a lot of components (controllers/actions) that can make sure, data is only sent/received/worked with in specific circumstances (constraints)
- It is crucial to define and know exactly what data is collected

Conclusion

- What is privacy for X?
  - It is different for each individual and each stakeholder
  - Not sharing anything will terminate the service
  - Sharing everything may expose everything
  - What is in the middle?
- Appropriate Categories for *Providing* privacy-compromising control actions?
  - Not providing / Providing
  - Too Early / Too late
  - Wrong timing / Wrong order

Thanks for your attention!

CC0, Evan-Amos