# Security aspects in mobile health technologies
# Usable polices for Access Control Systems

COINS Oct/2014

Leonardo Horn Iwaya (PhD Student)

leonardo.iwaya@kau.se

Agenda

- Previous MSc research
  - Security in "mobile health" systems
  - Security framework for data collection

- PhD research topic
  - Formal definitions for usable (and comparable) access control rule sets (e.g ., for configuring firewalls and IDSs)

Security aspects in mobile health (mHealth) systems

Project Scope

Ericsson Research
(Brazil & Sweden)

Heart Institute
(InCor)

Laboratory of
Computer Networks
and Architecture

- Period: May 2011 - July 2013

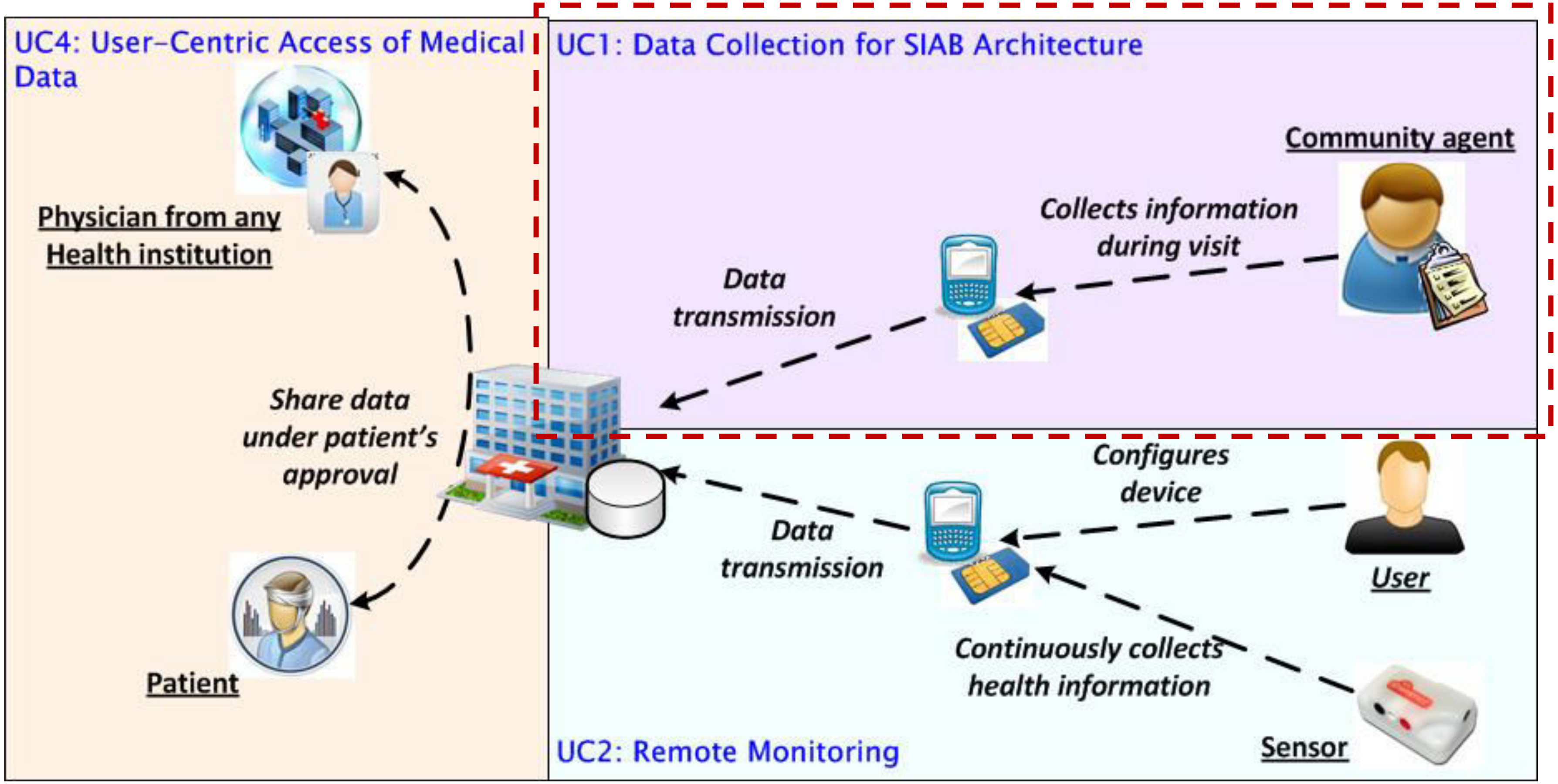
- Investigate the “**(mobile) health ecosystem**” around the patient

- Create a **patient-centered solution** able to **receive** and **provide** health information **from** and **to** the “health ecosystem”
    - Enforce **security** and data **privacy**
    - **Motivate patients** to take a larger **responsibility** for their **own health**

- Develop a **proof of concept(s)** system (prototype)

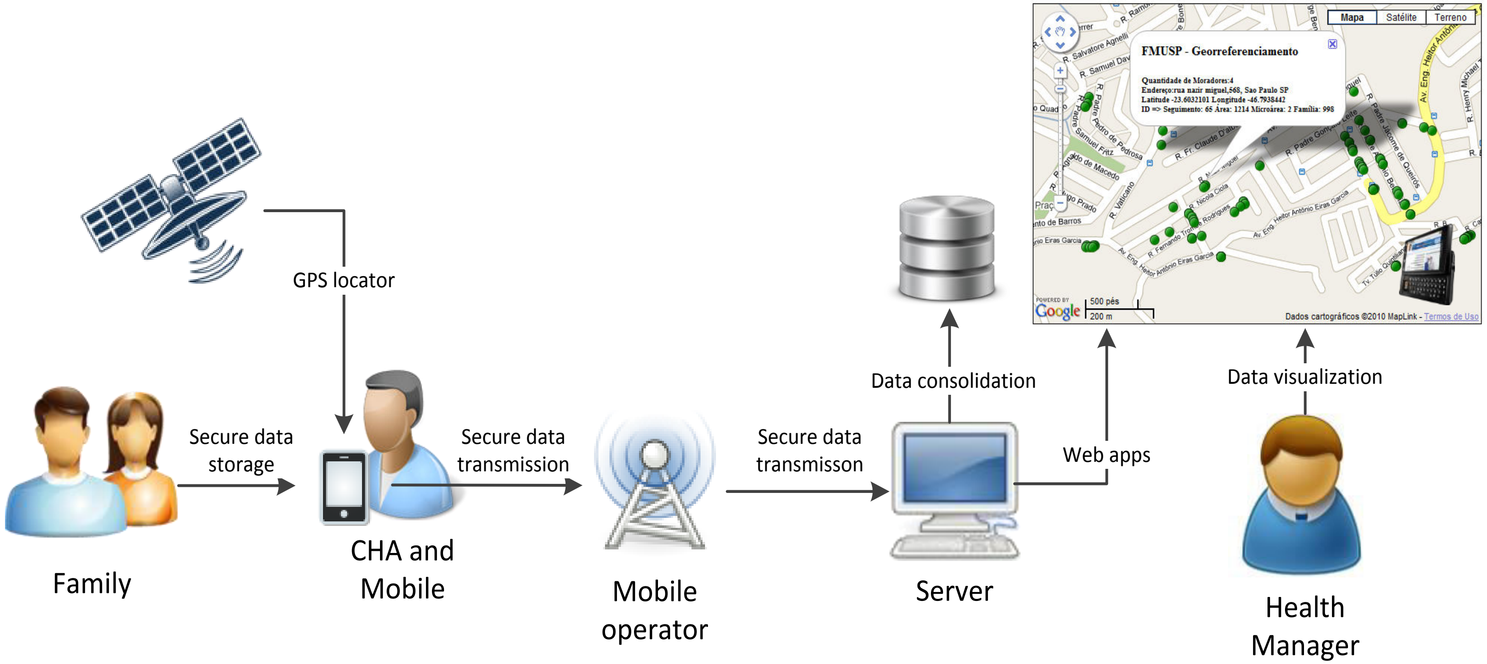
L.H. Iwaya, M.A.L. Gomes, M.A. Simplício, T.C.M.B. Carvalho, C.K. Dominicini, R.R.M. Sakuragui, M.S. Rebelo, M.A. Gutierrez, M. Näslund, P. Håkansson.
Mobile health in emerging countries: A survey of research initiatives in Brazil, International Journal of Medical Informatics, 82, 5, May 2013.

Use cases for mHealth in Brazil


UC4: User-Centric Access of Medical Data
Physician from any Health institution
Share data under patient's approval
Patient
UC1: Data Collection for SIAB Architecture
Community agent
Collects information during visit
Data transmission
Configures device
Data transmission
User
Continuously collects health information
Sensor
UC2: Remote Monitoring

Presentation Focus

Data Collection Scenario in Brazil



FMUSP - Georreferenciamento

Quantidade de Moradores:4
Endereço:rua nazir miguel,568, Sao Paulo SP
Latitude -23.6032101 Longitude -46.7938442
ID => Seguimento: 65 Área: 1214 Microárea: 2 Família: 998

Data collection scenario

1. **Tolerance to delays** and lack of connectivity (e.g., when using 3G networks);
2. Protection against **device theft** or **loss** of devices;
3. **Secure data exchange** between mobile device and server;
4. **Lightweight** and **low cost** solution;
5. **Device sharing** among health care workers;
6. Security features should not impair the application **usability**.

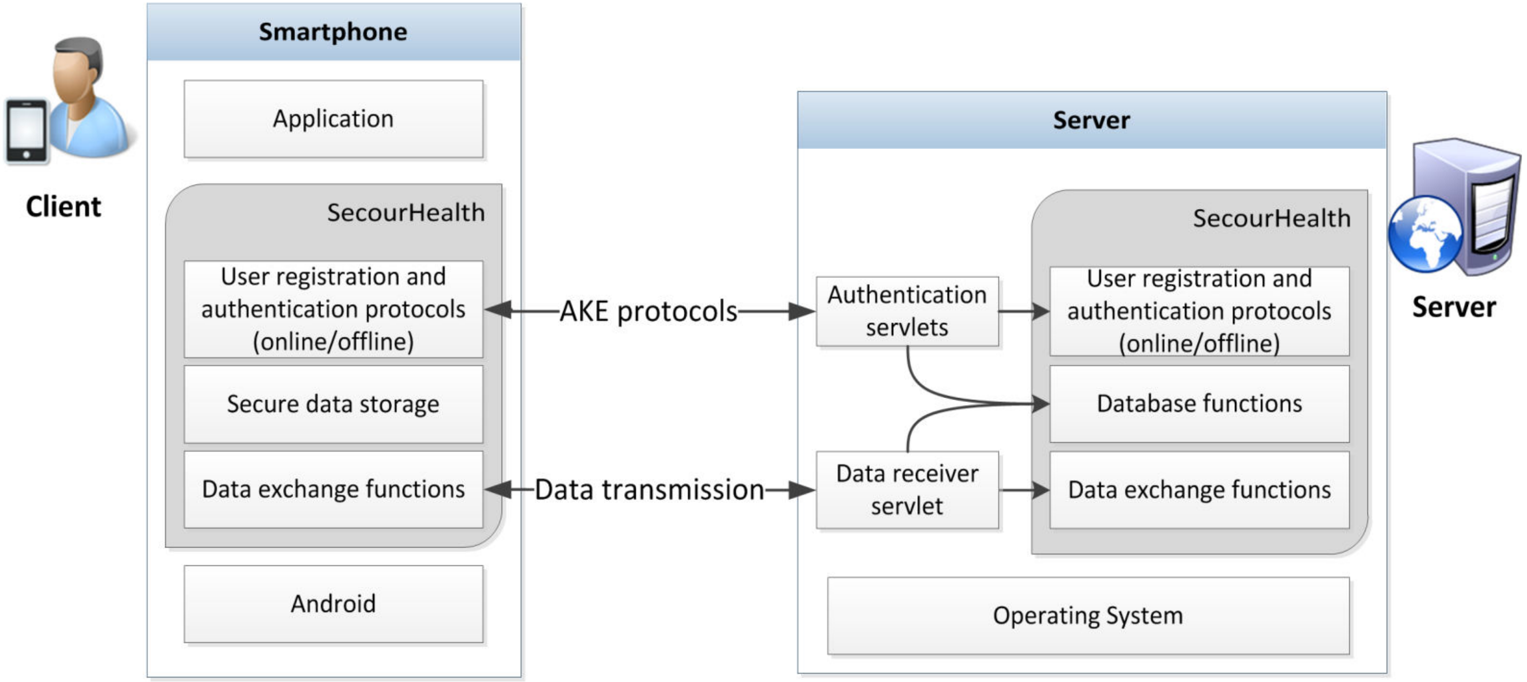
M. A. Simplicio Jr., L. H. Iwaya, T. C. M. B. Carvalho, M. Näslund. **SecourHealth: a delay-tolerant security framework for mobile health data collection**.
IEEE Journal of Biomedical and Health Informatics, April 2014 (*article in press*).

SecourHealth

- ❑ The French word "*secours*", means **to help** or a **relief**.

The framework covers:

- ❑ User registration ("first login")
- ❑ Offline authentication
- ❑ Secure data storage
  - ❑ **No** *forward secrecy* (K_{nofs})
  - ❑ **Weak** *forward secrecy* (K_{wfs})
  - ❑ **Strong** *forward secrecy* (K_{sfs})
- ❑ Data exchange with the server
- ❑ Device Authentication
  - ❑ (optional feature based on GAA/GBA)



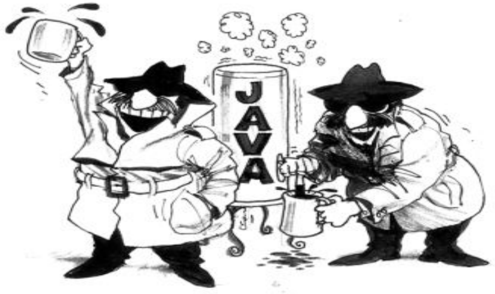
Architecture building blocks

M. A. Simplicio Jr., L. H. Iwaya, T. C. M. B. Carvalho, M. Näslund. **SecourHealth: a delay-tolerant security framework for mobile health data collection**. IEEE Journal of Biomedical and Health Informatics, April 2014 (*article in press*).

SecourHealth Implementation

- GeoHealth Study Case
  - The **SecourHealth** framework was **integrated** within GeoHealth, to be used for data collection in the Family Health Strategy government program.
  - Healthcare workers use an **Android** smartphone to collect data
  - The data plans for **3G** have nominal **speed** of 300Kbps

- Motorola Milestone 2
  - 1GHz, 8Gb memory flash, 512 Mb RAM, 3G connectivity



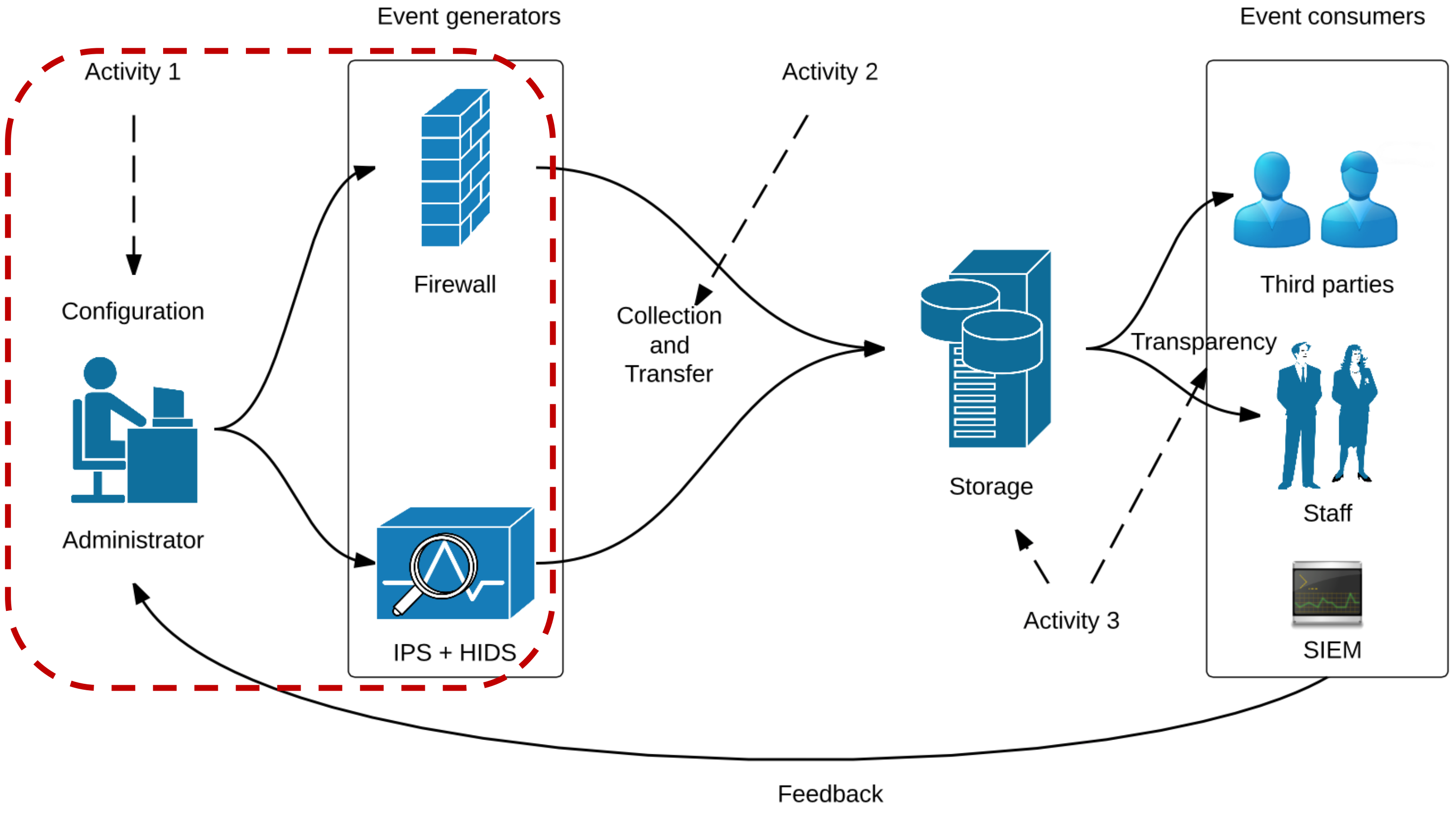
- Developed with Android Software Development Kit (SDK)
  - Cryptographic libraries **Javax.Crypto** and **Bouncy Castle**.

M. A. Simplicio Jr., L. H. Iwaya, T. C. M. B. Carvalho, M. Näslund. **SecourHealth: a delay-tolerant security framework for mobile health data collection**. IEEE Journal of Biomedical and Health Informatics, April 2014 (*article in press*).

Usable polices for Access Control Systems

Problem overview

- Security control configuration



M. Beckerle and L. A. Martucci. **Formal definitions for usable access control rule sets from goals to metrics**.
In Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13), 2013.

Preliminary research strategy

1. Literature **review** of **usable** access control rule sets and respective **formal** models

2. Analyzing how **security experts** evaluate configuration files
   - What are the most **relevant configuration files characteristics** regarding their security and usability?

3. The **formalization** of a basic **configuration file** model
   - How to define formal (extensible) models to accommodate different applications (e.g., firewall and IDS)?

4. **Metrics** can then be defined to **compare/evaluate** configuration files
   - Identify strengths and weaknesses among candidate files.

5. Design a **support** system that allows **security experts** and system administrators in **managing** configuration files of event generators

Questions, discussions and feedback

- *Muito Obrigado!*

(Thank you very much!)